

**Confidential**

---

---

## RUSSIA

The circulation of this report is strictly limited to members of the *Dialogue Club International* and of the *Centre russe d'études politiques*.

This issue is for your personal use only.

Published in Russian and in English  
by *Dialogue Company Ltd.*

Issue № 9 (237), vol.15 2016

---

November 23, 2016

Russia Confidential editors report from Moscow:

NEW AGENDA FOR THE 21<sup>ST</sup> CENTURY:  
NEW TECHNOLOGIES AND GLOBAL SECURITY CHALLENGES

*(A review of the international conference "Emerging Technologies and Global Security: An Agenda for the 21st Century")*

ANNOTATION

*On September 29, 2016 Moscow hosted the international conference "Emerging Technologies and Global Security: An Agenda for the 21st Century". The event was organized by PIR Center and the Diplomatic Academy of the Russian Foreign Ministry. It was attended by more than 130 Russian and foreign experts who represent different professional communities, but are ready and willing to work together on utilizing the opportunities opened up by new technologies while at the same time minimizing the global security risks they pose.*

*The conference focused on the development of new measures that could allow us to minimize the risks of new technologies without stifling their potential to do good. Specific areas under discussion included security of space exploration, nuclear nonproliferation and nuclear security in a new technological reality, political and legal aspects of the use of lethal autonomous weapons systems, and modern cybersecurity threats to critical infrastructure.*

*In this issue of Russia Confidential we offer highlights from these debates, and summarize the key ideas and proposals voiced at the conference.*

In his opening remarks at the conference, **PIR Center Director Albert Zulkharneev** focused on the impact of new technologies on global security. On the one hand, new tech opens up huge opportunities for resolving various problems facing our planet by facilitating access to energy, information, and knowledge. But on the other, it can also be used for destructive purposes, thereby compounding the existing challenges and giving rise to many new ones – such as the development of new types of weapons that fall outside the scope of any international regulatory frameworks. This calls for an in-depth discussion and new proposals on how to reduce the risks posed by new technologies without stifling their potential to do good.

PIR Center Director Albert Zulkharneev believes that this goal – as well as the goal of normalizing international dialogue amid the ongoing crisis in Russian-Western relations – can be facilitated by a greater involvement of the new generation of innovating entrepreneurs who want international cooperation to be as free as possible of political risks. This is why, Mr. Zulkharneev stressed, the organizers of the conference invited representatives of Russian high-tech companies such as Kaspersky Lab, Info Watch, the Skolkovo Foundation, and others.

**Jarmo Sareva, Director of the United Nations Institute for Disarmament Research (UNIDIR)**, highlighted the global security implications of the arrival of autonomous systems, new space-, cyber-, and biotechnologies, 3D printing, and directed-energy weapons. He focused in particular on the following challenges:

- ✓ *Non-state actors can now gain access to relatively cheap systems that have a great military utility;*
- ✓ *The complexity of identifying the perpetrators of attacks that utilize new technologies undermines the existing deterrence system;*
- ✓ *International law has yet to adapt to the emergence of some new technologies; there is no adequate regulation, which jeopardizes the normal functioning of the international system.*

Amb. Sareva argued that to respond to these challenges, we need to develop a whole set of new legal, political, and technological measures. In particular, more emphasis should be placed on convening groups of governmental experts to draw up international legal mechanisms of regulating new technologies, bring up to speed our ability to identify the perpetrators of cyberattacks, increase transparency, build trust, and minimize the risks of devastating attacks that utilize new technologies by making the security systems more resilient.

**Amb. Lassina Zerbo, Executive Secretary of the Comprehensive Nuclear Test Ban Treaty Organization (CTBTO) Preparatory Commission**, spoke of the effective verification system his organization has put in place. The system is based on the latest technological solutions, and can quickly provide CTBTO member states with vital information they require for their decision-making.

Amb. Zerbo argued that the CTBTO verification mechanism could become a model for monitoring systems in other areas – but first, that mechanism must be seen to be working effectively, which will only become possible after the CTBT entry into force.

Amb. Zerbo also said the Preparatory Commission would support efforts aimed at making its data and technologies available for civilian and scientific use, such as building tsunami early warning systems and nuclear incident monitoring mechanisms.

## SECURITY OF SPACE EXPLORATION

Participants exchanged opinions on key challenges facing peaceful space exploration, as well as opportunities for international cooperation in that area.

*Experts agree that one of the key challenges facing peaceful space exploration programs is the risk of the placement of conventional weapons in space, and the lack of any legal mechanisms to prevent such a development.*

Experts also highlighted such problems as the lack of any binding commitments on cleaning up space junk, or enforcement mechanisms that could be brought to bear in cases of illegal use of space orbits. There is no legal framework to regulate the future space mining industry. Western countries are unwilling to place any limitations or restrictions on their space policies. We also have to contend with blurred lines of responsibility as far as space activities are concerned, and with attempts at recognizing private-sector entities as equal participants in space exploration, potentially giving them equal status with states and international organizations.

Several participants spoke of the extremely low level of mutual trust on space exploration security issues between the two leading space-faring nations, Russia and the United States. Russia suspects the United States of trying to keep the door open for placing conventional weapons in outer space at some point in the future. Meanwhile, Washington rejects Russian proposals on any legally binding documents to regulate space security, arguing that any such arrangements would be impossible to verify, and that they would only distract from the real issues. Participants in this discussion at the conference agreed that there was a very low likelihood of binding commitments regarding the non-placement of conventional weapons in space being agreed any time soon.

**Vladimir Yermakov, deputy head of the Nonproliferation and Arms Control Department at the Russian Foreign Ministry,** had this to say on the matter:

*"Russia's position on the need to prevent the placement of any types of weapons in outer space, and to avoid an arms race in outer space, is dictated by one basic notion: if any nation places its weapons systems in space, it will thereby gain a major strategic advantage - and not just in space. Such a step would trigger a chain reaction because other nations would immediately seek ways of minimizing the military threat coming from space."*

Mr. Yermakov said that the now-defunct ABM Treaty included clauses that amounted to a ban on anti-satellite weapons because they prohibited any space-based components of ABM systems. Washington's unilateral pullout from that treaty in 2002 left Russia with no other choice but to step up its own efforts on preventing a space arms race. As part of these efforts, in 2004 Russia proposed an initiative inviting all states to follow its own example and commit themselves to not be the first party to place weapons in space. Also, in 2008 Russian and Chinese delegations at the Conference on Disarmament in Geneva proposed a draft treaty on preventing the placement of weapons in space and banning the use of force or threat of force against space objects.

Mr. Yermakov said that the no-first-placement of weapons in space initiative was a political commitment, and as such, it was an interim and temporary measure. He argued that the initiative would outlive its usefulness once the proposed treaty on banning the placement of weapons in space has been negotiated and entered into force. In the meantime, however, the initiative remains the only practical measure that has been implemented in pursuit of the UN GA resolution "Prevention of an arms race in outer space".

**Vasily Gudnov, head of the international organizations team at the Roskosmos State Corporation's international cooperation department,** said that there was still much work to be done on international legal mechanisms regulating space activities. In particular, we have yet to develop an internationally recognized definition of such terms as "a space object", "space security", or "space debris". Developing standard definitions would facilitate progress in other areas.

**Theresa Hitchens, senior fellow at the Center for International and Security Studies, University of Maryland,** spoke of the role of the International Telecommunications Union (ITU), which assigns geostationary orbits. Developing a mechanism of enforcement of ITU decisions in cases when any particular operator's use of the orbit is deemed illegal would benefit all space-faring nations. Dr. Hitchens also highlighted the growing role of international standards (including the ISO standards and guidelines of the Inter-Agency Space Debris Coordination Committee) in regulating various aspects of space activities, and the need for further development and codification of such standards.

#### NUCLEAR NONPROLIFERATION AND NUCLEAR SECURITY IN A NEW TECHNOLOGICAL AND POLITICAL ENVIRONMENT

The launch of nuclear energy programs in the nuclear newcomer countries necessitates more stringent standards of **nuclear safety and nuclear security.**

**Dr. Mely Caballero-Anthony, chair of the UN Secretary General's Advisory Board for Disarmament Matters and head of the Center for Non-Traditional Security Studies at Nanyang Technological University, Singapore,** said that North Korea's nuclear program and the Fukushima nuclear accident had raised interest in nuclear security and safety issues in Southeast Asia. This has resulted in the establishment of the ASEAN Network of Regulatory Bodies on Atomic Energy (ASEANTOM), which brings together the ASEAN nations' nuclear energy regulators and facilitates cooperation on nuclear safety issues with the IAEA and the EU.

Meanwhile, **Ali Asghar Soltanieh,** advisor to the head of the Atomic Energy Organization of Iran, also expressed interest in closer international cooperation on nuclear safety. According to Dr. Soltanieh, prevention of incidents with "dangerous technologies" (chemical, biological, and nuclear) requires the following steps by the international community:

- 1) Begin negotiations at the UN to draft the convention on the prohibition of nuclear weapons;**
- 2) Step up efforts to achieve universal membership of the CWC and the BWC;**
- 3) Discuss the need for conducting international inspections and verification procedures in nuclear-weapon states regardless of whether they are members of the NPT;**
- 4) Develop effective cybersecurity strategies;**
- 5) Depoliticize the issue of safety and security of nuclear facilities in order to strengthen international cooperation and facilitate the exchange of knowledge and technologies in this area.**

**Gennadiy Klochko, head of the export control laboratory at the Rosatom nuclear energy corporation,** said that the nuclear export control regime was facing such challenges as 1) the rise of additive manufacturing technologies (3D printing), which enable local production of some controlled parts and components and obviate the need for their import, and 2) laser technology of uranium enrichment, which does not require large amounts of natural uranium to operate and offers a very high isotope separation ratio.

**Vladimir Orlov, head of the Center for Global Problems and International Organizations at the Russian MFA's Diplomatic Academy and PIR Center adviser,** discussed the potential threats posed by cyberattacks against critical infrastructure facilities, as well as the danger of a new arms race breaking out, with the leading military powers developing long-range conventional weapons systems, including those based on hypersonic technologies.

Dr. Orlov said the following measures could help to prevent such a scenario:

- 1) The United States and NATO should resume negotiations with Russia on missile defense in Europe and new transparency measures;*
- 2) Washington should speed up the pullout of its nuclear weapons from Europe to facilitate the establishment of a nuclear weapons-free zone in Central and Eastern Europe;*
- 3) An international conference should be convened on the subject of preventing a hypersonic arms race; the event should be attended by all the leading actors in this field;*
- 4) All the nations that possess nuclear weapons should release information about their nuclear arsenals at the Conference on Disarmament;*
- 5) All efforts must be made to achieve the remaining CTBT ratifications.*

#### LETHAL AUTONOMOUS SYSTEMS - IMAGINARY AND REAL THREATS - POLITICAL AND LEGAL ISSUES

The conference was the first international event held in Russia to discuss the various international security issues and humanitarian aspects related to the development and use of lethal autonomous weapons systems.

**Andrey Grebenshchikov, first secretary of the multilateral disarmament unit at the Russian MFA's Nonproliferation and Disarmament Department,** said that the Russian Foreign Ministry had been monitoring the development of lethal autonomous weapons systems (LAWS) since the topic was first raised at the Human Rights Council, and that it continued such monitoring after the LAWS topic was transferred to the Inhumane Weapons Convention talks, where it has been discussed unofficially over the past three years.

Grebenshchikov also clarified Russia's position on LAWS, and the reasons why Moscow is cautious about the idea of a preventive ban on such weapons. Those reasons are as follows:

- 1) So far, the issue remains theoretical as no working lethal autonomous systems have been built as yet, and many delegations have a fairly vague idea of what such systems might look like.*
- 2) It is difficult to differentiate clearly between civilian and military autonomous systems.*
- 3) There are doubts as to whether the existing international legal mechanisms are truly inadequate for regulating the LAWS issue.*

Grebenshchikov also noted that

*"All the problems facing the LAWS issue stem from the need to agree a working definition of such systems. Russia would not want negotiations on this matter (if and when they take place) to leave this important point out in the hope that it will somehow be resolved at a later point. Also, there are many subsequent LAWS issues that hinge on the precise definition; these include the definitions of autonomy, critical functions, meaningful human control, predictability, etc."*

This is why at the latest informal meeting of LAWS experts the Russian delegation distanced itself from the informal recommendation to the IWC Review Conference calling for the establishment of a governmental experts group on LAWS. The Russian delegation formulated its position as a dissenting opinion, arguing that the discussion should remain informal for the time being. This position is based on the notion that every aspect of this complex issue should be analyzed before making an informed decision in accordance with the IWC principle of balance between humanitarian aspects and the interests of military security.

**Mary Wareham, coordinator of the Campaign to Stop Killer Robots,** defined LAWS as future weapons systems that, once activated and using their sensors and artificial intelligence, will be able to designate and engage targets autonomously, without meaningful human involvement in target designation and strike authorization for each individual attack.

Wareham argued that LAWS should always remain under meaningful human control, and called for a preventive blanket ban on the development, manufacture, and use of fully autonomous weapons systems. She noted that even though most countries say they have "no plans" for developing LAWS, in practice they have to pursue such R&D to keep up with the latest technologies. She highlighted the fact that some Pentagon officials are promoting the idea of a "third deterrence strategy" that is based on an ever-growing autonomy of weapons systems, including the emergence of fully autonomous weapons.

**Song Xinping, professor at the Xi'an Political Academy in China,** opined that the use of lethal autonomous systems could violate the basic principles of international law. He spoke in favor of developing clear LAWS-related definitions, including the grading of such systems depending on their degree of autonomy, lethal power, and the role in which they will be used. He said the LAWS issue should be discussed and dealt with at the UN so that any future agreement in this area could gain broad acceptance and a universally binding nature.

**Albert Yefimov, head of the Robotics Center at the Skolkovo Foundation,** used practical examples to explain that proper artificial intelligence will not be developed any time soon, and that killer robots remain a very distant prospect. The existing AI systems have a very limited capability, and any autonomous systems are easily incapacitated by modern electronic warfare instruments. Yefimov concluded that a human being will always be at the heart of decision-making, and that the problem of critical functions being delegated to machines is contrived.

**Thomas Grant, research fellow at the Lauterpacht Centre for International Law at the University of Cambridge,** used past examples from international law on science and technology to analyze the potential LAWS legislation issue. He said that whereas the

signatories of the 1868 St Petersburg Declaration merely reserved the right to consider the issues raised by new technologies in the future, Article 36 of Additional Protocol I to the 1949 Geneva Convention states that members have a duty to do so.

Dr. Grant gave an example of an ambiguous interpretation of international law being resolved in court. The example centered on a dispute between Australia and Japan over the definition of "killing whales for scientific research". An international court ruled that "issuing a license [for killing whales] cannot merely depend on national definitions". Dr. Grant concluded that modern international law has begun to treat the issue of science as a subject that cannot be defined by any individual nation.

**Gilles Giacca, legal advisor to the International Committee of the Red Cross**, said the ICRC had already drawn up working definitions of LAWS. ICRC experts believe that LAWS already exist in various shapes and forms, and that there is no guarantee of the military being able to retain the required degree of control over the autonomous systems they develop.

*Almost all the participants commented on the major legal hurdles that will have to be overcome on the way towards putting in place international LAWS regulation. One of the key problems is the absence of shared terminology required for a substantive discussion.*

On the whole, the debate showed that international nongovernmental organizations have a lot of motivation, international support, and persuasive arguments in favor of adopting a separate protocol on LAWS as part of the IWC - and if that endeavor fails, the entire LAWS debate can be taken to another venue.

In this context, **senior PIR Center researcher Vadim Kozyulin** believes that Russia may benefit from taking a more energetic stance on the issue; its delegation at the IWC panel could propose measures to restrict the use of autonomous systems in those areas where the Russian defense industry is lagging behind the Western leaders. These areas include massive use of LAWS as part of the Military Swarming and Centaur Warfighting strategies, as well as the use of Big Data for military purposes, whereby human operators are gradually being sidelined from the situation assessment and decision-making cycle.

#### CYBERSECURITY THREATS TO CRITICAL INFRASTRUCTURE

Participants in the conference made an emphasis on the new challenges that have emerged in connection with the rise of the industrial Internet of Things. They spoke of the need for coordination of efforts by governments and the industry itself to develop and implement new security standards. Representatives of the leading Russian cybersecurity companies (Kaspersky Lab, InfoWatch) also highlighted the importance of the private sector and the governments realizing the need for a transition from merely countering traditional information security challenges and threats to comprehensive cyber-physical security solutions, especially those designed to protect critical facilities. Participants spoke of the importance of international cooperation for neutralizing the information security risks facing critical facilities - especially cooperation aimed at developing cybersecurity services, rapid response centers, and databases on incidents at industrial facilities.

Speaking of peaceful nuclear energy facilities, participants discussed the need for international cooperation in exchanging best practices, experience, and technological

expertise on protecting such facilities from information security challenges. They highlighted several specific problems facing the peaceful nuclear energy industry and requiring concerted efforts, primarily at the IAEA. **PIR Center consultant Oleg Demidov** emphasized the following challenges:

- 1) *Complexity of the IT infrastructure of nuclear energy facilities;*
- 2) *The remaining gap between the approaches to nuclear security and information security;*
- 3) *The growing threat of targeted cyberattacks against nuclear energy facilities.*

Participants in the conference argued that the neutralization of these threats might soon require not only technical measures or decisions by the national regulators, but also efforts at various international venues to reach new agreements on preventing and limiting cyberattacks against critical facilities, including the nuclear energy infrastructure. **Vadim Podolny, a cybersecurity consultant**, emphasized the importance of the growing involvement of Russian industry experts in the ongoing development of new IAEA technical guidelines on cybersecurity measures at nuclear power plants and other nuclear facilities.

**Andrey Suvorov, head of Kaspersky Lab's critical infrastructure security division**, said that the Russian IT industry has the expertise and the technological capability to promote on the global market its own solutions in the area of standardization and comprehensive approaches to information security incident response at industrial facilities. Russian-developed solutions include the Kaspersky Industrial Cybersecurity (KICS) software, which detects and responds to traffic anomalies and to the loss of integrity of the outer perimeter of industrial networks. Suvorov also spoke of Kaspersky Lab's contribution to the development of the Industrial Internet of Things Volume G4: Security Framework, which is the only standardized approach to industrial Internet of Things security available at this time.

For full transcripts of conference speeches and presentations, please visit: <http://conference2016.pircenter.org>

Editor: Petr Artemiev, PIR Center

c) Trialogue Club International: [trialogue@pircenter.org](mailto:trialogue@pircenter.org);  
(c) Centre russe d'études politiques: [crep@pircenter.org](mailto:crep@pircenter.org)  
Moscow-Geneva, November 2016

---

**Excerpts from the Membership Terms and Conditions at the Trialogue Club International**

[...]

**3. The rights of the Club members**

3.1. Individual club members are entitled to:

3.1.3. Receive a copy of the Russia Confidential exclusive analytical newsletter by e-mail in chosen language (English or Russian). According to the Club Terms and Conditions, the transfer of the bulletin to third parties is not allowed.

[...]

3.2. Corporate Club members are entitled to:

3.2.3. Receive two copies of the Russia Confidential exclusive analytical newsletter by e-mail in chosen language (English or Russian) or in both languages simultaneously. Share the bulletin with the other representatives of the corporate member. According to the Club Terms and Conditions, the transfer of the bulletin to third parties is not allowed.

[...]

**4. The duties of the Club members**

4.1. All members of the Club must:

4.1.6. Not to share the Russia Confidential analytical newsletter, as well as the Password to the Club section of the PIR Center web-site with individuals and legal entities who are not members of the Club.

[...]

**6. Russia Confidential**

6.1. The Russia Confidential exclusive analytical newsletter is issued by the Trialogue Ltd for the Club members' private use only.

6.2. The newsletter contains exclusive analytical materials on international security, foreign and domestic policy of Russia and the CIS, prepared by the leading experts specially for Russia Confidential.

6.3. The newsletter materials are confidential and must not be quoted and transfer to the non-members for at least 30 days since the day of issue.

6.4. 30 days after the day of issue the Trialogue Ltd can remove the exclusive and confidential status of the material, after which in such cases it can be published in other editions and can be used by the Club members for quoting.

6.5. The newsletter is disseminated via e-mail between the Club members once a month in Russian or in English, depending on the choice of the Club member.

6.6. The Club member can also receive a paper copy of the newsletter in chosen language.

---

Dear members of the *Dialogue Club International*,

The 2016 Club season continues, and we are glad to **invite you to prolong your membership for 2017 or 2017-2018**, if you have not done so yet.

In 2017, the *Dialogue Club* members will continue to receive our exclusive information on the foreign policy priorities of the Russian Federation, and on current threats and challenges to global security. **Five meetings of the *Dialogue Club International*** are planned for 2017 (four in Moscow and one abroad); Club members will receive 4 issues of the Security Index quarterly journal in electronic form, **12 issues of the *Russia Confidential* exclusive analytics bulletin**, our informational and analytical newsletters.

As before, experts of the *Dialogue Club International* and of its partner organization PIR Center are open to an exchange of views on key international problems.

**Fees for *Dialogue Club* membership since 2017 are as follows:**

If paid **before 12 December 2017:**

Period	Individual membership	Corporate membership
01.01.17 – 31.12.17 (1 year)	45 000 rub.	72 000 rub.
01.01.17 – 31.12.18 (2 years)	81 000 rub.	126 000 rub.

If paid **before 31 January 2017:**

Period	Individual membership	Corporate membership
01.01.17 – 31.12.17 (1 year)	50 000 rub.	80 000 rub.
01.01.17 – 31.12.18 (2 years)	90 000 rub.	140 000 rub.

We would like to remind you that the corporate membership is based on “**1+1**” **scheme** when **two representatives** of the organization participate in the work of the Club.

On all questions concerning the *Dialogue Club International* membership, please contact us by the e-mail [secretary@dialogue-club.ru](mailto:secretary@dialogue-club.ru) or by phone: +7 (985) 764-98-96

Sincerely,

**Chairman,  
*Dialogue Club*  
International**

**Dmitry Polikanov**