Confidential

RUSSIA

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

This issue is for your personal use only.

Published monthly in Russian and in English by *Trialogue Company Ltd.*

Issue № 5 (245), vol.16. 2017

June 26, 2017

Russia Confidential reports from Moscow:

INTERNATIONAL SECURITY TODAY: WITH RUSSIA, WITHOUT, OR AGAINST IT?

(based on materials of the VI Moscow International Security Conference organized by the Russian MoD)

(CONTINUED; SEE BEGINNING IN No 4 (244))

In this issue of Russia Confidential, we continue our review of highlights of the 4th Moscow Conference on International Security attended by leading security experts, military specialists, and decision-makers from 86 countries.

The focus of this issue is on information security - which was for the first time made a topic of a separate discussion at the Moscow Conference - and on missile defense discussed at a joint briefing given by Russian and Chinese military experts. The briefing was a good example of practical cooperation between the two countries' defense ministries.

INFORMATION SECURITY:
SPACE OF EQUAL RIGHTS OR ARENA OF STRUGGLE FOR SUPERIORITY?

Information security was for the first time made a topic of a separate discussion at the Moscow Conference, whereby a specific importance of the topic was highlighted.

The Secretary of Russian Security Council Nikolay Patrushev emphasized such problems of information security as acts of information aggression perpetrated by certain states, and their efforts to maintain their unilateral advantage in governing the global information infrastructure – which opposes the efforts of creating international system of information security under the UN auspices. Unlike NATO, which is working to provide cybersecurity only for its own members, Russia advocates equal security for all states.

The chief of the Russian General Staff and First Deputy Minister of Defense Valeriy Gerasimov spoke of NATO's decision on the possibility of invoking Article 5 of the Washington Treaty (the collective defense clause) in response to a cyberattack.

- ***Such a decision could lead to NATO members groundlessly pinning the blame for attacks on other countries without any proof, and using force against them under that pretext.***

Approaches of the Russian military were discussed in detail by the key Russian expert on information security, **Deputy Head of the Main Operations Department of the Russian General Staff Igor Dylevskiy.** He noted that information technologies are increasingly used for aggressive purposes, and could even trigger an international military conflict, which is illustrated by examples of *color revolutions* and conflicts of the last decade. The situation is compounded by the fact that many states (more than 120, according to some estimates) are currently developing information weapons — techniques, means, and methods specifically assigned for conducting information warfare, and potentially capable of inflicting huge damage.

- ***Russia realizes, Gen. Dylevskiy said, that banning the development of such weapons or verifying whether individual states - let alone terrorists – possess them is not a realistic proposal. Nevertheless, Russia believes it should be possible to elaborate mechanisms of information weapons nonproliferation and reduce the likelihood of them being used against national critical infrastructure facilities.***
- ***The West, however, prefers a different approach, in view of the Russian general. Decisions adopted by NATO in recent years make it clear that the alliance is prepared to use military force for collective defense in response to a cyberattack, and that it regards cyberspace as a new "operations theater" for collective defense.***
- ***From the Russian point of view, a destructive impact on a nation's information infrastructure can be regarded as a breach of sovereignty, tantamount to an act of aggression. However, to that end, the list of actions recognized as acts of aggression, which was adopted by the UN General Assembly in 1974, should be updated and amended. As for the possibility of nations exercising their right to self-defense and collective defense in accordance with Article 51 of the UN Charter in response to an armed attack that relies on information weapons, Russia believes (unlike NATO) that the issue has yet to be fully clarified. In the absence of international laws regulating this subject, an information attack can be recognized as an armed attack by the UN Security Council; in such an event, the party under attack will have the right to defend itself.***
- ***Speaking of the applicability of humanitarian legislation to information technologies, it is clear to Russia that some of the traditional criteria used to define combatants cannot be applied to entities that operate in information space, which is why it is necessary to develop and implement appropriate international legal methodology.***

Deputy speaker of the Russian Duma Irina Yarovaya briefly outlined the evolution of the American approach first to psychological, and now to information warfare.

- ***One of the defining characteristics of the American approach, according to Yarovaya, is waging information wars against their opponents during peacetime, before actual war starts. This is why, she opined, information attacks by the United States can be regarded as a prelude to further hostile actions. Analysis of the mechanism used by the Americans in various parts of the world – including the Middle East during the "Arab Spring" - suggests that the same technology was used in each case: first comes an information intervention, followed by economic and political colonization of the target country.***
- ***the United States had essentially monopolized and privatized information space. The U.S. corporation ICANN has the exclusive authority to assign domain names, thereby making the United States the only power in the world that can grant or deny other entities the permission to maintain their presence in cyberspace.***
- ***There is a stark difference in the definition of information space in U.S. and Russian doctrines. The Russian military doctrine states that information space should be a space of security and equal sovereign rights, whereas the Americans emphasize their aspiration to ensure their own information superiority.***

Natalya Kaspersky, head of the *InfoWatch* group, spoke of the recent publication by *WikiLeaks* of what appear to be internal CIA documents on the development of malicious software. These documents suggest that the CIA has a special division that disguises viruses as legitimate software developed in other countries, including Russia, China, and several Arab states. Kaspersky said that in view of these new revelations, any attempts at equating cyberattacks to conventional attacks are extremely dangerous because there's a great risk of the victim of a cyberattack delivering a retaliatory strike against a party that had nothing to do with the initial attack and was simply framed.

The Israeli expert Yaakov Kedmi argued that like other types of warfare, information warfare always pursues political ends. But unlike conventional military operations, information wars are waged before, during, and after the end of military action. Another difference is that to be successful, information warfare must be offensive rather than defensive; any attempts at waging such warfare defensively always end in defeat. The Israeli expert noted that the work of the media on or near the battlefield always has one shared characteristic: irresponsibility. That is why media outlets must be supervised, otherwise their work can be detrimental to the operation and to the security of troops in the field. All reports from the battlefield must go through military censorship, otherwise they must be considered a violation of the law. Such and more stringent measures are applied even by democratic countries.

Russian journalist Vladimir Solovyev, who is also a **member of the Russian MoD's Civic Council,** said that external threats in information space are a fact of life; they cannot be eliminated completely. This should be taken into account when addressing domestic objectives with the help of a coherent and powerful ideology supported by the state and granting Russian society immunity to external threats.

Dr. Harlan Ullman, senior adviser at the Atlantic Council (USA) emphasized the importance of U.S.-Russian cooperation on various issues pertaining to the use of cyberspace so as to better understand each other's intentions. The actual parties engaged in such cooperation could include government agencies or commercial companies representing the two countries' cyber industries – but first contacts should be established without delay. Otherwise, political differences on these issues will only worsen, which none of the parties is interested in.

Professor at the Information Security Center at China's National Defense Academy of People's Liberation Army (PLA) Wen Baihua explained that in China, the balance between security in information space and freedom of access to information is maintained with the help of the principle of cyber-sovereignty which asserts the right of each country to control cyberspace in the way it sees appropriate, without letting other states interfere. That principle was proposed by China and Russia in a 2015 report by the Group of Governmental Experts; it was also reiterated by the Chinese and Russian leaders later that year. In Wen Baihua's view, in the longer term, cooperation in cyberspace in different areas should become the main instrument of resolving various problems because it is the less costly, more sustainable, and more effective way in terms of national security interests.

BMD: VIEWS OF RUSSIA AND CHINA, AND EVOLUTION OF THE U.S. AGRGUMENTS

For the first time, the agenda of the 2017 Conference included a joint briefing given by Russian and Chinese military experts at the discussion on missile defense and its impact on regional and international security.

The Russian part of the briefing was presented by **first deputy head of the Main Operations Department of the Russian General Staff Viktor Poznikhir** who explained the reasons for Russian (as well as Chinese) concerns over the deployment of the U.S. global missile defense system, offering a detailed assessment of that system's current and future capability:

- ***The information component of that capability, underpinned by stationary radars, mobile radars, and satellites, enable the system to detect the launches of Russian intercontinental ballistic missiles, track the missiles during their entire trajectory, and provide targeting data to interceptors.***
- ***The general estimated that the system will have more than 1,000 interceptors deployed by 2022, and that at some point in the future the number of the deployed interceptors will surpass the number of warheads mounted on Russian ICBMs.***
- ***Furthermore, as a result of the ongoing improvement of U.S. missile interceptors, they will eventually be able to intercept Russian and Chinese ICBMs not only during re-entry and in mid-course, but also at the ascending segment of their trajectory.***
- ***U.S. missile defense ships and American missile defense cites in Romania and Poland are equipped with universal launchers that can be used not only for interceptors but also for Tomahawk cruise missiles, which have a range of up to 2,500 km.***

These projections were illustrated by the results of computer simulation of various scenarios for the interception of Russian and Chinese ICBMs by the U.S. missile defense system; the simulations were developed by the Russian MoD's research facilities.

Thereby, the offensive capability of the U.S. missile defense system increases the uncertainty and poses a threat to Russian and Chinese security. Also, in the event of the deployment of land-based launchers, it will represent a breach of the Intermediate-Range Nuclear Forces (INF) Treaty. However, by now Washington has rejected all Russian initiatives on resolving the missile defense problem, thereby forcing Russia to take appropriate steps to respond to the new challenge. In answer to the question of what the Americans and the Europeans could do to alleviate Russian concerns, the general said that first and foremost, Washington must demonstrate a real willingness to purse dialogue on the missile defense issue, taking into account Russian and Chinese interests.

The Chinese part of the briefing was given by **Cai Jun, deputy director of the Combat Operations Bureau under the Joint Staff Department of the Central Military**

Commission. The Chinese general said that America's unilateral pursuit of global missile defense capability and its determination to ignore other states' security interests and legitimate rights reflects Washington's aspiration to achieve an absolute and unilateral military superiority. That aspiration could reinforce a dangerous trend of certain nations trying to resolve international problems through the use of force, exacerbate regional tensions, and trigger a new arms race.

The general focused his attention on the situation on Korean peninsula and concluded that America's deployment of ABM elements in Asia Pacific inevitably encourages North Korea to strengthen its own nuclear and missile capability. Missile defense deployment puts in place the necessary preconditions for the U.S. and South Korea to try to resolve problems on the peninsula through the use of force. However, it has been demonstrated in recent years that the strategy of military threats does not work; that is why efforts by the U.S. and its allies to create a missile defense cordon in Asia Pacific only exacerbate the confrontation with North Korea, compound the risk of a new escalation on the Korean peninsula, and run counter to efforts by the international community to resolve problems by political means.

The Chinese representative rejected assurances by the United States and South Korea that the only purpose of the deployment of THAAD missile interceptors is to counter the North Korean missile threat.

- ***The radars used in the THAAD system have a range of over 2,000km. They can be used to track not only missile launches on the Korean peninsula, but also test launches of land and sea-based missiles in the northeast of China and in the Bohai Sea. So obviously, the real purpose of the deployment of the THAAD system is to create an additional element of America's global missile defense system in order to improve the capability of the Asia Pacific segment of that system versus China and Russia.***

The Chinese general recalled the June 2016 joint statement by the Chinese and Russian leaders on strengthening strategic stability, in which both voiced their opposition to the deployment of missile defense systems in Europe and Asia by states that are not part of those regions. He assured the audience that China and Russia would continue to take further steps in response to America's missile defense program in order to protect their own national security and strategic stability interests.

The briefings by the Russian and Chinese generals were followed by a presentation by the **head of the MoD's Central Air Force Research Institute Sergey Yagolnikov.** He argued that despite U.S. claims to the effect that its missile interceptors are no match to Russian ICBMs, calculations by Russian specialists suggest otherwise.

- ***Information about the location of the Russian missile sites, as well as data from spy satellites, make it possible to launch an interceptor much sooner after an ICBM launch than the Americans say. As a result, the interceptor will have enough time to close the distance with the ICBM at the ascending segment of its trajectory.***

Gen. Yagolnikov noted that an algorithm similar to the one he had just described was simulated during a joint Russian-NATO exercise in 2012 using a model developed by the German company IABG. Back at the time the heads of the U.S. and NATO delegations had no doubts about the feasibility of such an intercept scenario. Several U.S. scientists have reached a similar conclusion.

Director of the Center for Military-Political Analysis at Hudson Institute Dr. Richard Weitz (USA) admitted that BMD system in Europe remains an *apple of discord* between the U.S. and other countries, primarily Russia. At the same time, both Russia and

the U.S., as well as China are currently upgrading their nuclear arsenals, so cooperation on nuclear weapons reductions is difficult regardless of the differences on missile defense. Concerning the regional missile defense system in South Korea Dr. Weitz suggested that the parties could consider a number of measures to make sure that the system is used to deter only the North Korean nuclear threat – for example, by building a multinational BMD network similar to the arrangement NATO and Russia had at one point discussed for Europe. International cooperation on missile defense in the context of the Korean situation would help to strengthen security in the region; at some point in the future, its scope could also include disarmament.

The moderator of the discussion, **Lt. Gen. (rtd) Evgeny Buzhinskiy, who is the chairman of the PIR Center Executive Board,** said that in Russia's opinion, America's assurances that such a capable missile defense system is being deployed solely to intercept currently nonexistent Iranian missiles are false and don't stand up to scrutiny – especially since Iran has no plans of creating a missile with a range of more than 2,400 km, let alone an intercontinental ballistic missile.

Gen. Buzhinsky noted that previously, Washington said it needed to deploy ABM elements in Poland and the Czech Republic in order to intercept Iranian and North Korean missiles in the event of an attempted strike against targets in the U.S. But the Russian military then pointed out the distance any North Korean missile would have to travel over Russian territory in order to reach the U.S. mainland – and the North Korean argument was immediately dropped from the U.S. case for BMD in Europe.

Gen. Buzhinsky also recalled the initial U.S. arguments in favor of signing the ABM Treaty in 1972. Robert McNamara, who was the U.S. defense secretary at the time, convinced the Soviet leadership that any missile defense system would not actually be defensive; its main purpose would be to defend an attacker from a retaliatory strike and minimize the damage from such retaliation. Therefore, such a system is essentially the weapon of a potential aggressor, and a factor of strategic instability.

Such an evolution of the U.S. thinking demonstrates that Washington tends to be very flexible in accepting or rejecting various arguments, depending on its own national interests at any particular moment in time.

INSTEAD OF CONCLUSION

The VI Moscow Conference on International Security was attended by more than 800 delegates from 86 countries, including 56 official military delegations, of which 22 were led by ministers of defense. There were more than 200 foreign and Russian representatives of the expert community and NGOs, as well as officials representing 7 international organizations. More than 300 journalists from 80 Russian and foreign media outlets received accreditation to cover the event.

Considerable negotiating potential of the MCIS venue is indicated by the fact that the forum gathered such seemingly irreconcilable rivals as India and Pakistan, as well as representatives of Israel, Iran and Syria at the same round table.

But one cannot fail to mention who was not present at this representative forum. Neither NATO nor the U.S. did not send their official representatives to the conference, even though it would be especially important to establish a dialogue with them in the fight against terrorism. So despite common understanding that for effectively combatting terrorism, there is a need for consolidating world efforts,

the biggest problem remains achieving the consent of the parties that take or should take part in this fight.

Western reluctance to be engaged in a serious dialogue with Russia calls into question not only the aspirations of the world community to establish a broad anti-terrorist front, but also to improve situation around many other issues of international security discussed at the VI Moscow Conference. Is it actually worth trying to build international security without Russia, let alone in hostile opposition to Russia? The conference gave a definite answer to this – no, it isn't.

Editors: Oleg Shakirov, Julia Fetisova

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

3. Club members' rights

3.1. Individual members of the Club have the right to:
3.1.3. Receive one copy of the Russia Confidential exclusive analytics bulletin by email, in their preferred language (Russian or English). Under the rules of the Club, the bulletin may not be made available to third parties. […]
3.2. Corporate members of the Club have the right to:
3.2.3. Receive two copies of the Russia Confidential exclusive analytics bulletin by email, in their preferred language (Russian or English) or in both languages, and to make the bulletin available to other representatives of the corporate club member. Under the rules of the Club, the bulletin may not be made available to third persons who are not members of the Club.[…]

4. Club members' responsibilities

4.1. All current members of the Club have the following responsibilities:
4.1.6. Not to share materials from the Russia Confidential bulletins they have received, or passwords to the Club website, with individuals and/or entities who are not members of the Club. […]

6. Russia Confidential

6.1. The Russia Confidential exclusive analytics bulletin is published by OOO Trialogue for personal use by Club members only.
6.2. The bulletin contains concise and exclusive analysis of problems pertaining to international security and Russian and CIS domestic and foreign policy issues, written specially for Russia Confidential by leading experts.
6.3. Materials published in the bulletin should be treated as confidential for at least 30 days from the date of publication. During that period they may not be quoted or made available to persons or entities who are not Club members.
6.4. After a period of at least 30 days from the date of publication, OOO Trialogue may choose to lift the exclusivity and confidentiality requirements for some of the materials published in the bulletin, in which case they may be published in other outlets and quoted by Club members.
6.5. The bulletin is sent to Club members by email on a monthly basis, in English or in Russian, depending on the individual club member's preference.
6.6. Upon request, Club members can also receive a hard copy of the bulletin in their preferred language.

Dear members of Trialogue Club International,

The 2017 Club season continues, and we kindly **invite you to extend your membership in the Club for 2017 or for the 2017-2018 period.**

In 2017 Club members will continue to receive exclusive analytics on Russian foreign policy priorities and key challenges and threats to international security. We have scheduled **5 meetings of *Trialogue* Club International** in 2017, including 4 in Moscow and 1 abroad. Club Members will receive a series of articles from the Security Index journal in electronic form, **12 issues** of the Russia Confidential analytical bulletin (in Russian or English), as well as other information and analytical bulletins.

As always, specialists of *Trialogue* Club International and its partner organization PIR Center are open for exchange of opinions on key international issues.

In **2017**, membership fees are as follows:

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

We operate a **1+1 arrangement** for **corporate members**, whereby each corporate member is entitled to have **2 representatives** participating in Club events.

For all membership issues, please email us at secretary@trialogue-club.ru or call +7 (985) 764-98-96.

Sincerely,

Chairman,
***Trialogue* Club International** **Evgeny Buzhinskiy**