II

SECTION

Strengthening International Security: Role of Parliaments

SECTION II

Strengthening International Security: Role of Parliaments

In today's world, the complex of problems of international and national security continue to aggravate, and the scale of new challenges and threats is increasing.

The most serious fundamental global threats include a systematic disdain among a group of countries for foundational norms of international law, a tendency toward unilateral approaches, the use of methods of force or sanction pressure on sovereign states, interference in their internal affairs.

Systemic risks to international security at the current stage include the escalation of tension and the growth of conflict potential, the intensification of confrontation in various regions of the world, the conventionalization of reliance on the power factor, the spread of block approaches and zero-sum games instead of sustainable collective decisions based on compromise and mutual respect for the interests of others.

As the President of Russia V.V. Putin said, "in the last 25 years, the threshold of using force has significantly decreased." "The anti-war immunity, which was acquired after the two world wars and existed at a psychological, subconscious level, has begun to weaken."

International terrorism, drug trafficking, proliferation of nuclear weapons, as well as threats to international information security remain serious global threats which directly affect the security of most countries and entire regions.

At a new stage in the technological development of armaments and military equipment in the face of growing international tension, the current state of the arms control system, as well as the non-proliferation of weapons of mass destruction (WMD) and their means of delivery take on particular relevancy.

In this context, the role of parliaments is growing, not only as key developers of legislation on security regulations and drivers of its international harmonization, but also as authoritative guides for affirming collective principles in world affairs and unifying the agenda for countering traditional and new challenges and threats, de-escalating tensions in international relations, reducing the potential for confrontation and conflict, broad cooperation between countries and their international and regional security and stability, including on the East-West and North-South lines, eliminating emerging threats to peace, settling disagreements on the basis of an equitable, mutually respectful dialogue, while scrupulously observing the fundamental norms of international law in the interests of the security and well-being of peoples; approving principles of responsible behavior in the global information space; refusing unilateral attempts to resolve international disputes with the use of force or sanctions pressure.

1. International Terrorism as a Global Threat

The concept of ***"international terrorism"*** (IT) doesn't have a single generally accepted interpretation. At the same time, a considerable number of UN documents, normative acts and recommendations on various aspects of fighting against terrorism have been developed.

International terrorism has unique characteristics which distinguish it from other types of terrorist activity. IT includes terrorist acts carried out on the territory of two or more states or affecting the interests of two or more states, as well as the coordinated activities of terrorist organizations (TOs) in several countries.

1.1. Modern Terrorism: Key Features

IT expansion is closely connected to the spread of religious and ideological extremism in the countries of the Near and Middle East, which intensified after the fall of secular authoritarian regimes ("Arab socialism" in Egypt, Syria, Iraq).

In many Muslim countries, radical Islamism[1] is a response to globalization processes, ***growing interference in the internal and regional processes of countries in the Near and Middle East by the US and other Western countries and the unsettled internal social and political problems in these countries.***

The growth of international terrorist activity is accompanied by an aggravation of competition for political and economic leadership and control over the world financial system and natural resources (including oil production) between key world powers in a time of globalization and a transition to a new economic order.

In some cases receiving external support, international terrorist groups use it to implement their own strategies and expand their influence.

Relying on external financial and logistical support and new information and communication technologies (social networks, encrypted instant messengers, Internet banking, cryptocurrencies) has allowed international terrorism to ***scale from a predominantly regional phenomenon (local terrorist groups) to a global threat*** (international network structures). At the same time, however, local terrorist groups (like Hamas) largely retain their role and influence in their regions, but no longer determine the face of modern terrorism.

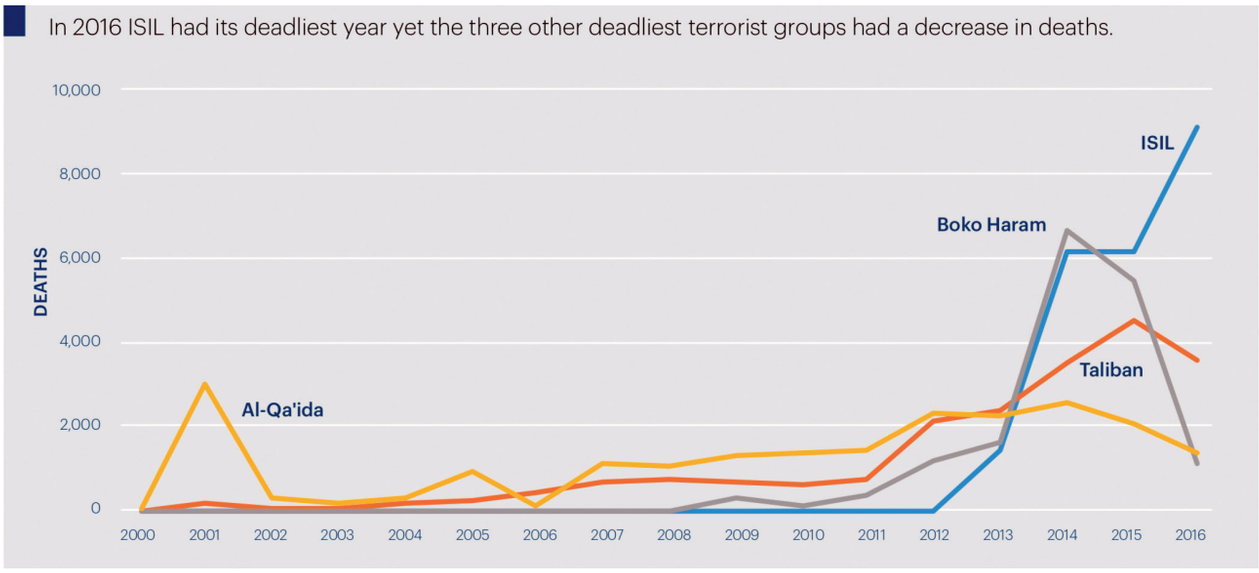
The phenomena of Al-Qaeda and the Islamic State as terrorist structures of a new type are connected with modern network and media technologies, which they use both for propaganda and recruiting supporters and for finding new sources of funding.

The globalization of terrorist networks has led to their close integration with international criminal money trafficking. It has resulted in the creation of international "transnational criminal corporations" with their own illegal economic activity. Terrorists play the role of a power wing in them[2]. The use of new organizational forms and network technologies has led to a

[1] Radical Islamism is a religious and political opposition to existing political regimes in Muslim countries, and it advocates a complete reorganization of society and the state in accordance with the norms of the Sharia. It is the main core of the ideology of Islamist TOs.

Figure 1

The number of victims of terrorist groups, 2000–2016



Source: *Global Terrorism Index / Institute for Economics and Peace, 2018, p. 72 (http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf)*

significant increase in the terrorist activity of these structures and a proportional increase in economic losses from their activities (Figures 1 and 2).

Estimates of the numbers of key terrorist groups of the world, including Islamic State and Al-Qaeda, are shown in Table 1.

The main regions of systematic activity of terrorists have remained essentially unchanged over the last few years. The key ones are:

1) ***Syria and Iraq***, where there are the Islamic State, Hezbollah, and Jaish al-Fatah, which was joined by the Jabhat al-Nusra group in 2015;

2) ***Afghanistan and Pakistan***, where the Taliban has great influence and where the Islamic State is trying to consolidate;

3) ***Nigeria*** (Boko Haram in coordination with the Islamic State); 4) ***Yemen*** (Al-Qaeda in the Arabian Peninsula);

5) ***the territory of the former uniform Somalia*** (Al-Shabaab and other groups);

6) ***the countries of West Africa*** (active are Boko Haram, the groups of the former Al-Qaeda in the Maghreb and Ansar Ad-Din);

7) ***the Maghreb states and Egypt*** (Muslim Brotherhood, the pressure from ***terrorist networks*** based in neighboring regions is also increasing).

For shelter bases and regrouping zones, terrorists use developing countries in crisis, burdened by ethnic and religious conflicts, where central governments are weakened, and the capabilities of special services and security agencies are limited.

International terrorist groups carry out targeted penetration into developed countries in order to recruit supporters and fighters and search for new sources of funding (mainly donations). By the forces of locally formed terrorist cells, they also manage to carry out resonant and brutal acts of terrorism against civilians (in Madrid in 2004 — 192 victims, London in 2005 — 52 victims, Paris in 2015 — 130 victims, at the Brussels airport and metro in 2016 — 33 victims, explosions in the metro of St. Petersburg in 2017 — 15 victims and others).

Table 1. The Numbers of Major Terrorist Groups

Organization		Estimate of the number of active fighters in 2016–2017 (in thousands of people)
The Islamic State	in Syria and Iraq	12–15
	In Libya	up to 6
Al-Qaeda	in the Arabian Peninsula	up to 4
	in the Maghreb	several thousand people
The Taliban	in Afghanistan	up to 60
	in Pakistan	several thousand people
Jabhat al-Nusra		up to 10
Al-Shabaab		up to 5
Boko Haram		7–10

Sources: *Country Reports on Terrorism / U.S. Department of State, 2017; Giustozzi A. Afghanistan: Taliban's organization and structure / Landinfo, 2017.*

1.2. Sources and Amounts of Terrorist Financing

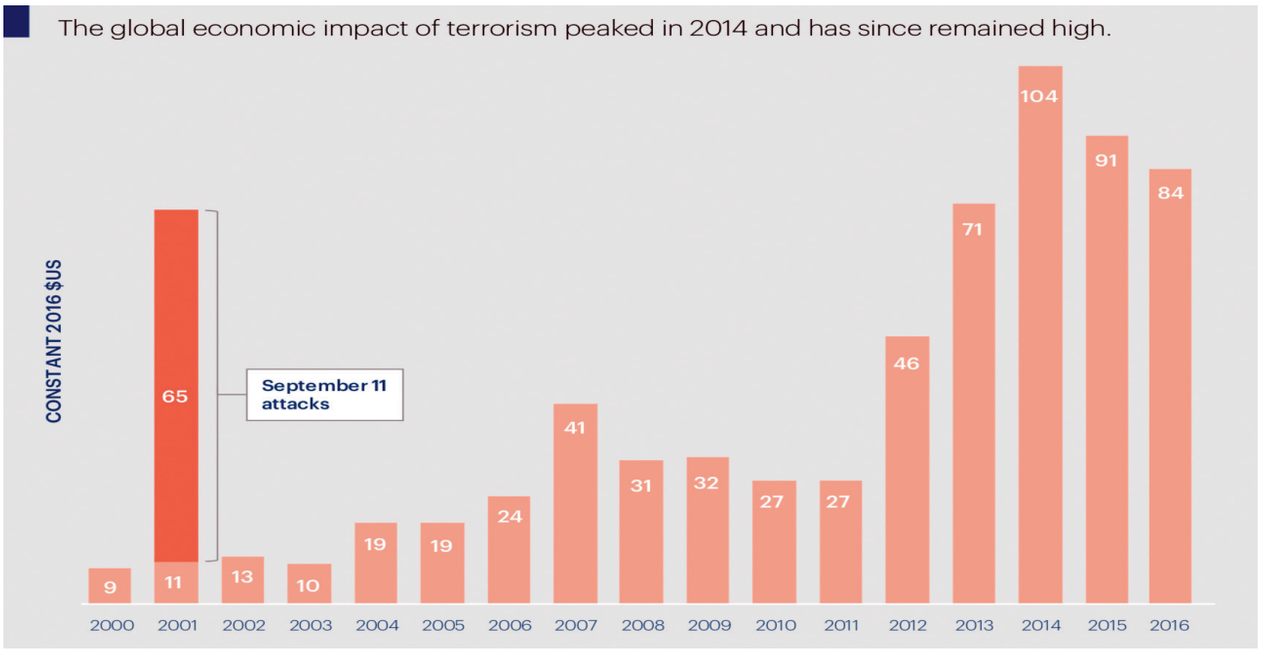
Almost all groups get a significant part of their income from ***donations and/or direct requisitions. The most organizationally developed quasi-state terrorist groups actively monetize the resources of the*** controlled territories (Table 2).

The main source of income for the Islamic State in 2014–2016 was the sale of oil and its processed products from the

[2] Hesterman J. Transnational Crime and the Criminal-Terrorist Nexus: Synergies and Corporate Trends. Maxwell, AB: AirUniversity, 2004. P. 62–65.

Figure 2

The economic consequences of terrorism, 2000–2016, in USD bn.



Source: *Global Terrorism Index / Institute for Economics and Peace, 2018, p. 80 (http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf)*

eastern Syria deposits that they controlled at that time. The most important financing channel for the Taliban is Afghan heroin trafficking. For a number of Latin American groups, it is cocaine drug trafficking.

Terrorists *widely use unregulated financial instruments*, primarily *cryptocurrencies*[3]. The financial base of terrorists is growing due to globalization and diversification of the network of donations and increasing reliability of payment systems.

Table 2. The Estimate of the Annual Income of Some Major Terrorist Groups in 2016

Organization	Annual revenue, in USD mn
The Islamic State	2000
The Taliban	400
Al-Qaeda (all branches)	250
Boko Haram	25

Source: *Global Terrorism Index 2017 / Institute for Economic and Peace, 2017.*

1.3. Catastrophic Terrorism

To date, *precedents of "catastrophic terrorism" with the use of weapons of mass destruction* and, in particular, the use of nuclear weapons have not been recorded in the world. However, the implementation of such scenarios is not a fantasy.

Experts consider the *following scenarios* for the implementation of acts of catastrophic terrorism as probable:

1) *blowing up (possibly with capturing) a civil nuclear infrastructure facility, a* nuclear power plant*;*

2) *polluting the* environment *with radioactive materials*;

3) *terrorists getting* components *of chemical or bacteriological weapons*;

4) *creating a "garage bomb":* building a nuclear explosive device from individual components in a large metropolitan area;

5) *stealing a nuclear warhead* and using it for a terrorist attack.

It turned out that the terrorists liquidated in Belgium in March 2016 were preparing to attack a nuclear power plant. There are hundreds of active civilian nuclear reactors in the world[4], which creates a high potential danger of such terrorist acts, the destructive power of which can be critical for both states and entire regions of the world.

The key preventive measures for such dangerous attacks are:

1) *focused attention from and monitoring by competent* international organizations*;*

2) *elaboration of national legislation* and regulations;

3) *detailed elaboration of providing physical protection* in *various threat scenarios;*

4) *high responsibility at the national and local levels for ensuring the physical protection of nuclear facilities*;

5) *concerned countries developing comprehensive cooperation on improving the physical protection of nuclear facilities*, including the improvement of legislation, the exchange of best technological practices, the exchange of intelligence services, mutual assistance.

[3] Ward A. Bitcoin and the Dark Web: The New Terrorist Threat? // RAND Corporation, Jan 2018 (https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html).

[4] At present, there are 150 nuclear power units in European countries, 37 in Russia, 99 in the USA, and 137 in Asia. See: WorldNuclearGenerationandCapacity / NuclearEnergyInstitute, 2017. (https://www.nei.org/resources/statistics/world-nuclear-generation-and-capacity).

1.4. The Role of the UN in Fighting International Terrorism

The UN has consistently adopted framework decisions on the intensification and coordination of efforts to combat terrorism at the international level. They have mainly focused on developing interstate relations (bilateral and multilateral) and creating effective search and prosecution regimes, as well as fighting against the financing of terrorist activities.

The modern corpus of decisions goes back to the following basic documents:

- The Declaration on Measures to Eliminate International Terrorism (1994), supplemented by the resolution of the 51st session of the UN General Assembly (1997);
- International Convention for the Suppression of the Financing of Terrorism (1999);
- The UN Global Counter-Terrorism Strategy (2006), which approved common approaches to combating terrorism and eliminating the conditions conducive to its emergence.

A rather complex problem of the international level is the mismatch of the lists of organizations that are recognized as terrorist organizations in different countries of the world. This is due to various factors, from technical bureaucratic difficulties in collective identification and taking into account formed, merging, splitting and disappearing groups, to political causes.

The UN plays a key role in *harmonizing lists of terrorist organizations*. Since 2017, *a Counter-Terrorism Department has been operating in the UN system*. This structure has the potential and authority to develop joint solutions for combating terrorism, including harmonizing lists of TOs and implementing special programs. Nevertheless, it is not yet possible to develop universal criteria for recognizing an organization as terrorist on the UN platform.

The current practical goal is to *improve the single international system for tracing* and prosecuting terrorists. This requires coherence in the legislation of national states in the field of combating the financing of terrorism, as well as consistency in regulating cross-border migration flows. Solving these problems requires systematic interstate contacts at the parliamentary level with the aim of sharing best practices and developing common approaches.

2. Fighting the Drug Threat

The growth of drug trafficking is a critical threat to humanity

The situation with drugs in the world continues to deteriorate. Despite international efforts, the global production of narcotic drugs, and hence their consumption, continues to grow. The production and marketing chains as well as the transportation and financial networks of drug trafficking are getting more and more clever.

The cross-border nature of the main drug flows is contributing to an increase in the number of drug addicts worldwide, especially among young people. According to the UN, **more than 190,000 people die from the consequences of drug use in the world annually. In other words, this means that humanity loses about 28 million years of healthy life every year**.

The drug trade is one of the most profitable and large-scale types of transnational crime with a **volume of annual turnover**, according to various estimates, **from USD 400–650 bn** (see Table 3). A significant part of the world's illicit drug trafficking is accounted for by cocaine and opiates, with Colombia and Afghanistan respectively being the key suppliers to the world markets.

Drug trafficking is systematically linked to other types of transnational crime. The superprofits generated thereby comprise a vast financial base for international terrorism and radical currents**, support corruption**, provoke **financial fraud of money laundering and** are converted **into working capital for illicit arms trade** and **cyberspace crimes, human trafficking and the organization of illegal migration**.

Drugs and Organized Crime

Source: UNODC, adapted from Europol, *SOCTA 2017*.

The combination of new challenges and threats combined is giving rise to a global criminal anti-system, with drug trafficking as one of its pillars.

Table 3. The estimate of the annual turnover of the global black market of narcotic drugs, USD bn

Drug	Lower bound sales volume	Upper bound sales volume
Marijuana	183	287
Cocaine	94	143
Opiates	75	132
Amphetamines and new synthetic drugs	74	90

Source: *May C. Transnational Crime and the Developing World. Washington, DC: Global Financial Integrity, 2017. P. 4.*

To reduce the volume of drugs that enter the world market, it would require the **involvement of all the countries and associations where** certain **segments of drug trafficking chains are based** — from the production of drugs to their final marketing.

In order for strategies for combating drug trafficking to be effective, they should be comprehensive and inclusive as well as ensure the coordinated application of three anti-drug activities:

- cutting off production;
- counteracting transit (removing drugs from circulation at the transportation stage, including via border control);
- reducing and preventing demand in the countries of sale.

Three UN basic anti-drug conventions serve as the basis for the international regime for controlling the spread of drugs:

- the Single Convention on Narcotic Drugs (1961),
- the Convention on Psychotropic Substances (1971),
- the Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988).

The efforts of the Russian Federation to combat the international drug threat focus primarily on countering drug trafficking from Afghanistan. Russia stands for tightening measures to counteract Afghan drug trafficking as well as greater coherence and coordination thereby; this would mean, namely, activating operations to intercept drugs and eliminate drug laboratories by joint efforts of the Afghan authorities and the US-led NATO "Resolute Support" Mission. ***However, Russian proposals to integrate and intensify efforts in the fight against the Afghanistan drug threat, including joint activities with NATO and CSTO countries, are not supported*** by the US and the North Atlantic Alliance, despite separate episodes of bilateral cooperation.

At the same time, during the period of the mission of the International Security Assistance Force (2001–2014), when the country was de facto under **the military control of the US-led international contingent**, **not only did the production of heroin not decrease there, but it increased 40-fold and reached 95% of the total world amount**.

The country, controlled by international forces, has become a world "opium monopoly." **The countries of the European Union annually receive 711 tons of opium from there, and Russia receives 549 tons**.

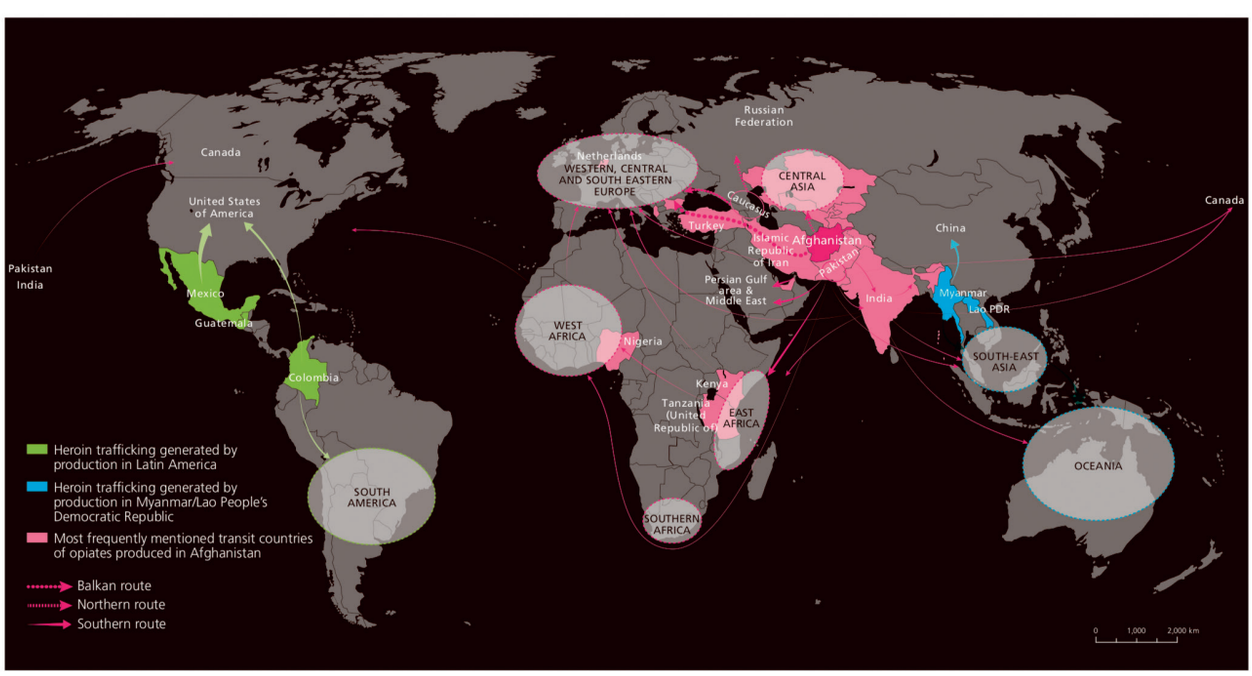
The absence of real achievements in eradicating Afghanistan drug trafficking has a profoundly detrimental effect, undermining the credibility of global governance institutions and the people's trust in the efforts of the international community.

Intensive consistent work to counteract the Afghan drug threat is conducted under the Collective Security Treaty Organization (CSTO) and the Shanghai Cooperation Organization (SCO).

The SCO has been creating a security belt for blocking Afghan drug transit since 2002. The CSTO[5] serves as the Coordinating Council of Heads of Competent Authorities to Counter Illicit Drug Trafficking.

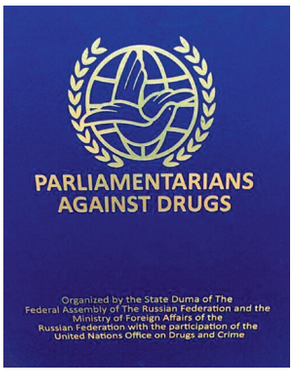
[5] CSTO member states: Russia, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan.

Main opiate trafficking flows, 2011-2015



Sources: UNODC elaboration, based on responses to annual report questionnaire and individual drug seizure database.

Notes: The trafficking flows are determined on the basis of country of origin/departure, transit and destination of seized drugs as reported by Member States in the annual report questionnaire and individual drug seizure database: as such, they are to be considered as broadly indicative of existing trafficking routes while several secondary flows may not be reflected. Flow arrows represent the direction of trafficking: origins of the arrows indicate either the area of manufacture or the one of last provenance, end points of arrows indicate either the area of consumption or the one of next destination of trafficking. The boundaries shown on this map do not imply official endorsement or acceptance by the United Nations. Dashed lines represent undetermined boundaries. The dotted line represents approximately the Line of Control in Jammu and Kashmir agreed upon by India and Pakistan. The final status of Jammu and Kashmir has not yet been agreed upon by the parties. The final boundary between the Sudan and South Sudan has not yet been determined. A dispute exists between the Governments of Argentina and the United Kingdom of Great Britain and Northern Ireland concerning sovereignty over the Falkland Islands (Malvinas).



Legislative support of comprehensive work to counter the spread of narcotics is the priority of national parliaments and the most important area of interparliamentary cooperation.

At the initiative of the State Duma, **the "Parliamentarians Against Drugs" international conference** was held in Moscow in December 2017. It brought together representatives of more than 40 states, heads of legislative and executive authorities, the UN Office on Drugs and Crime and leading specialized non-profit organizations.

The practical issues of interaction of parliamentarians from different countries in the fight against the drug threat were specifically considered in the context of the authority of the legislative power.

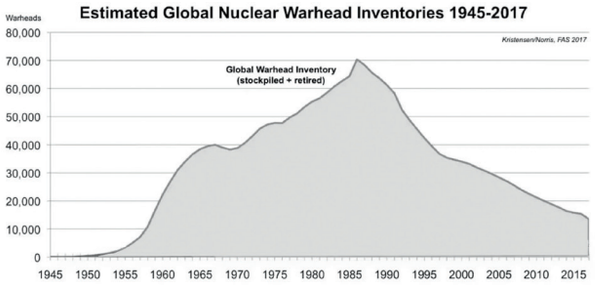
The main conclusions of the discussions during the conference are as follows:

- **the need for rapid improvement of legal regulation and mutual harmonization of national legislations through exchanging best practices**;
- **cooperation of parliaments in creating conditions for intensification of partnership through national anti-drug and law enforcement agencies**;
- **activating legislative and political work against drug propaganda for tightening of liability, creating a sustainable rejection of drug use and the drug-promoting subculture in society**;
- **the focus of the world parliamentary movement on countering the drug threat as one of the key security issues, making the anti-drug subject one of the priorities of international parliamentary cooperation in various bilateral and multilateral formats, ensuring systematic work in this direction**;
- **building an inclusive system of interaction between the legislative and executive branches, the scientific and expert community, civil society structures, global governance institutions and multilateral intergovernmental associations in order to make the world drug-free**.

3. Nuclear Non-proliferation and Arms Control

The cornerstone of the international security system is the nuclear non-proliferation regime and nuclear disarmament. Nuclear disarmament implies a reduction, or complete elimination, of nuclear weapons (NW). The concept of non-proliferation is based on the prevention of horizontal proliferation of nuclear weapons between countries, as well as the prevention of vertical distribution, i.e. nuclear powers stockpiling nuclear weapons.

Figure 3. The world's nuclear arsenal in terms of number of warheads, 1945–2017.



Source: *Status of World Nuclear Forces / Federation of American Scientists, March 2018 (https://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/)*

Thanks to a number of measures on arms control and disarmament, the stockpiles of nuclear weapons (NW) were reduced after the end of the Cold War. In total, the world's nuclear arsenal decreased from 70,300 units at the peak of the Cold War (1986), to 14,200 units as of 2018 (Figure 3).

3.1. Erosion of the Regime of Non-proliferation of Nuclear Weapons

The most important tool aimed at limiting the circle of countries possessing nuclear weapons is the **Treaty on the Non-proliferation of Nuclear Weapons** (NPT) of 1967. Its participants are 191 countries, and among the nuclear powers are Russia, the United States, Great Britain, France and China.

The basis of the NPT is the balance of three components: nuclear non-proliferation, disarmament and respect for the right to use nuclear energy for peaceful purposes. The treaty excludes the transfer of NWs, as well as materials and technologies for their production to non-nuclear states. International guarantees to exclude the transfer of peaceful use of atomic energy into military channels are introduced. Article VI has a special place in the Treaty, directly binding the participants to further nuclear disarmament.

A Review Conference is held every 5 years to review the functioning of the NPT and to agree on a list of recommendations for strengthening the Treaty. The conferences of 2000 and 2010 ended with the adoption of action plans for nuclear disarmament, but the implementation of many agreed measures failed.

The 2015 Review Conference ended without result; the adoption of the final document was blocked by the delegations of the United States, Britain and Canada, which further weakened the foundations of the NPT.

Despite a number of mechanisms that underpinned the **NPT** and the non-proliferation regime, it **failed to prevent the emergence of unrecognized nuclear states**. Israel, India and Pakistan, which are not signatories to the NPT, are continuing to develop their own nuclear programs, as is North Korea, which withdrew from the NPT in 2003 and then carried out six nuclear tests from 2006 to 2017.

Recently, there has been a serious **weakening of the system of non-proliferation of nuclear weapons**. Power politics of individual nuclear powers (for exam-

ple, the military intervention of the US in the conflicts of 1990–2010 in Yugoslavia, Iraq, and Libya) strengthens the intent of "threshold" non-nuclear states to creating their own nuclear weapons, as well as means of their delivery. A number of countries are beginning to view nuclear weapons as a weighty guarantee against aggressive actions and interventions by other powers in the face of the growing dysfunction of international security institutions.

The crises surrounding the nuclear missile programs of North Korea and Iran are connected, among other things, to a sense of their lacking security. At the same time, regional security systems are not organized properly and cannot guarantee the prevention of unpunished interference in internal affairs.

The risk of a regional nuclear war persists. In May 2018, US President D. Trump announced US withdrawal from the Joint Comprehensive Plan of Action for the Iranian Nuclear Program[6], which in practice was an important element of the non-proliferation system. This destabilizing step can push Iran to create nuclear weapons and activate missile programs.

The situation is burdened by the **crisis that has emerged in the regimes of arms control.** By blocking the ratification of the Comprehensive Nuclear Test Ban Treaty (CTBT) and disrupting the implementation of the agreement with Russia on the disposal of surplus weapons-grade plutonium, **the United States is weakening the system of non-proliferation and nuclear disarmament**.

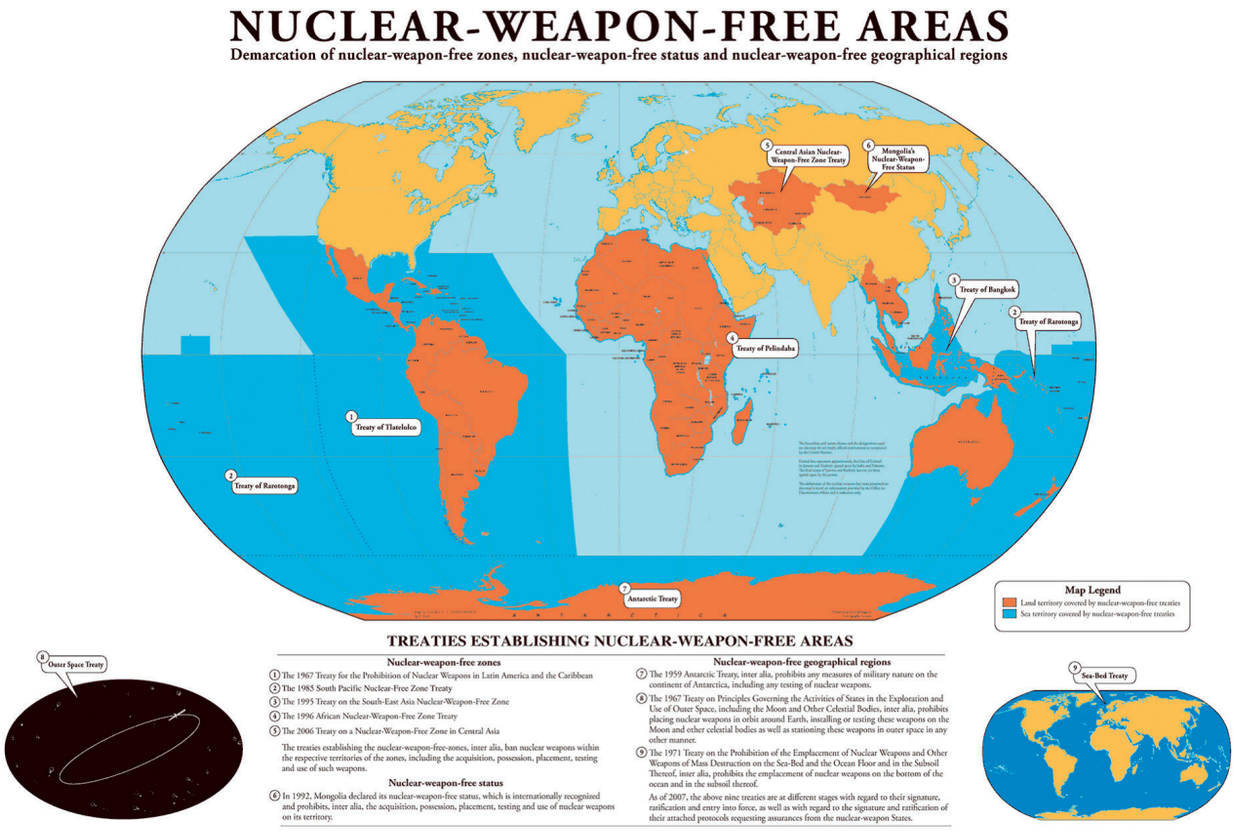
The dissatisfaction of countries that are not members of the "nuclear club" was expressed in developing the Treaty on the Prohibition of Nuclear Weapons, which was supported by the 122 countries at the UN General Assembly in July 2017. The document prohibits developing, testing, storing, acquiring, transporting and using nuclear weapons. If the Treaty enters into force, it will not be carried out by the nuclear powers. Therefore, it can become another "apple of discord" in the system of non-proliferation of nuclear weapons.

The evolution of non-proliferation regimes led to **creating zones free of nuclear weapons and other weapons of mass destruction**. Such zones were created in the 1950s and 1960s on the basis of regional agreements between countries, where participants refuse to possess nuclear weapons. At the moment, five agreements have been put into effect on WMD-free zones (Figure 4): Treaty of Tlatelolco (South and Central America, Caribbean), 1967; Treaty of Rarotonga (South

[6] President Donald J. Trump is Ending United States Participation in an Unacceptable Iran Deal (https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-ending-united-states-participation-unacceptable-iran-deal/).

Figure 4

Nuclear-Free Zones in the Modern World



Source: *United Nations Office for Disarmament Affairs (UNODA).*

Notes: *Also on the map are: Antarctica (a nuclear-free zone since 1959), the bottom of the seas and oceans (the Treaty of 1971); the non-nuclear character of outer space is specified (the 1967 Outer Space Treaty).*

Pacific), 1985; Bangkok Treaty (South-East Asia), 1995; Treaty of Pelindaba (Africa), 1996; Semipalatinsk Treaty (Central Asia), 2006.

Creation of WMD-free zones in the Middle East has been a current topic in recent years, which is connected with the proliferation of nuclear technologies in the region due to plans of the region's countries to develop nuclear energy (Iran, UAE, Egypt, Turkey, Saudi Arabia, Jordan). Creating such a zone was one of the conditions for the Arab countries to support the decision on the indefinite extension of the NPT in 1995. In 2015, the US, unwilling to deteriorate their relations with Israel, blocked the convening of an international conference on the creation of such a WMD-free zone.

Northeast Asia is a region where creating a WMD-free zone is also very important. Two countries of the region, Japan and South Korea, have developed a nuclear power industry and corresponding infrastructure. North Korea is a "de facto" nuclear state. The establishment of a WMD-free zone in the region will require the denuclearization of North Korea with the adoption of security guarantees by the countries of the region.

One of the key documents in the development of the NPT ideas was the Comprehensive Nuclear Test Ban Treaty (CTBT), which has been open for signature since 1996. The treaty makes provisions for expanding the nuclear test banning zone established in 1963, which is the atmosphere, space and underwater space, to an unconditional ban, i.e. banning nuclear weapon testing completely. To date, 166 countries have ratified the treaty. Due to the fact that several states haven't ratified it (in particular, the US and China), it has not yet entered into force.

In addition to refusing to ratify the CTBT, a serious concern is the **US plans to develop low-yield nuclear warheads** which were formally announced in the updated Nuclear Policy Review in early 2018. Such a policy casts doubt on US commitment to respect both its obligations under Article VI of the NPT and the moratorium on nuclear testing.

The draft of the Fissile Material Cut-off Treaty (FMCT) has been under discussion for more than 20 years. The treaty could become a powerful practical tool for non-proliferation policy. However, the parties cannot agree on the initial terms of the contract, in particular the issue of declaring and inspecting the initial stocks of nuclear materials. It will be particularly difficult to declare the materials contained in nuclear munitions.

In January 2006, Russian President Vladimir Putin proposed the creation of international centers for providing nuclear fuel cycle services for the controlled development of peaceful nuclear energy. Such platforms, controlled by IAEA, could contribute to the objectives of non-proliferation and at the same time guarantee the supply of nuclear materials. Since 2007, Russia and Kazakhstan have been implementing a pilot project of the International Uranium Enrichment Center in Angarsk (Russia). Since 2010, under the auspices of the IAEA, the first guarantee stock of nuclear materials has been created there.

The processes of disarmament and non-proliferation are dialectically interrelated. Progress in arms control creates incentives for advancement in the field of non-proliferation. At the present time, however, the process of reduction and limitation of arms has reached an impasse.

3.2. Arms Control Agreements

Arms control is one of the key conditions for maintaining international security.

The cornerstone agreement in the sphere of offensive nuclear weapons is the Prague START (Strategic Arms Reduction Treaty), concluded between Russia and the US in 2010**,** which established **ceilings for the strategic forces of each of the two powers** in the number of deployed carriers and the number of warheads for them at **700** and **1550** units, respectively. Today, participation in this agreement ensures the strategic parity and strategic stability between the two countries.

The anti-Russian campaign which has been unleashed in the West and the unrelenting tension in Russian-American relations (including the sanction regime against Russia) seriously hamper the dialogue on the preservation of the Treaty and on further possible reductions.

In 2002, the United States unilaterally withdrew from the 1972 **ABM Treaty** (Anti-Ballistic Missile Treaty), **which was an important element of the strategic stability system.** Having thus obtained freedom of action, in addition to developing missile defense in its national territory, Washington is deploying regional missile defense segments in the Euro-Atlantic and Asia-Pacific regions. Such intentions and the plans for creating a missile defense area in Europe in particular have caused serious concern in Russia due to the fact that these means can be directed against the strategic nuclear forces of the Russian Federation and used for striking Russian territory.

The principal position of Russia is the preservation of strategic parity, taking into account the potential of the US missile defense system, the American potential of conventional high-precision long-range weapons, as well as the prospects for joining the dialogue on START for third countries, which still remains bilateral.

The treaty on medium-range and shorter-range missiles (1987) is an indefinite agreement providing for the elimination and prohibition of the production, testing and deployment of ballistic and cruise land-based missiles with a range from 500 to 5,500 kilometers by the USSR/Russia and the US.

The treaty **has become an important element of strategic stability**, as it eliminated certain unilateral advantages of the United States associated with medium-range missiles in nuclear equipment deployed in Europe that has minimal flying time to the territory of Russia. Washington's recent criticism of the Treaty and the discussion of the possibilities of getting out of it may be connected to a possible wish on the part of the United States to return these unilateral advantages. The further fate of the Treaty is at risk.

The Russian side is concerned about the presence of American nuclear weapons in Europe. As before, there is American nuclear arsenal in Europe,

numbering **up to 200 air bombs**. Although**, after the collapse of the Soviet Union, Russia withdrew its nuclear weapons into its national territory, the United States did not follow suit**[7].

Russia and the United States consider the **lack of prospects of other nuclear states joining this process** as one of the obstacles to negotiations on further reductions of tactical nuclear weapons.

From the mid-2020s**, the US plans to begin a cycle of full renewal of its strategic nuclear forces** (the strategic nuclear triad)[8]. **The cost of this 30-year-long program will be about USD 1.2 tn. Russia is also modernizing its nuclear forces**.

In the event of problems with the conclusion of a new treaty or the prolongation of the Prague Treaty, the envisaged programs may be revised with a view to increasing the number of strategic systems and warheads, which may create **potential conditions for a new arms race**.

At present, the world's leading military powers are deploying **a significant number of** diverse **long-range strike systems, and** above all, **high-precision conventional weapons capable of hitting targets that in the past could only be destroyed using nuclear munitions**. **In the United States,** these plans are being implemented within **the concept of a non-nuclear, rapid global strike**.

Similar weapons are being created in Russia and China.

Introducing restrictions in this area is on the agenda.

Leading military powers are actively developing and partially deploying new-generation weapon systems, including high-precision cruise missiles, unmanned air, ground and underwater systems, as well as cyber weapons, which **will influence the** military balance **and strategic stability**. However, no approaches have yet been developed at the international level to limit such systems.

There is a real **threat of armament of outer space**, since international law, in accordance with the 1967 Outer Space Treaty, doesn't directly prohibit placing any weapons other than weapons of mass destruction in space.

Russia is consistently fighting against the militarization of outer space. In 2004, Russia **unilaterally announced its refusal to place weapons in outer space first.**

At the Conference on Disarmament in Geneva in 2008, Russia and China officially introduced the draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects (PPWT). However, **the US is blocking the negotiations**, as **Washington** has traditionally **not accepted the prospects of any restrictions on military space activities**.

Since 1999, Western countries have been delaying the process of ratifying the 1990 Agreement on Adaptation (1999) on the 1990 Treaty on Conventional Armed Forces in Europe under various pretexts. Meanwhile, NATO went through several waves of expansion, which increased the imbalance in the number of conventional weapons in favor of the alliance. In this situation, Russia was forced to completely suspend its participation in the Treaty in 2015.

The process of NATO expansion to the East and the Alliance's military infrastructure approaching to Russia's borders have for many years been a factor that complicates Russia's dialogue with Western countries in the area of "tough security".

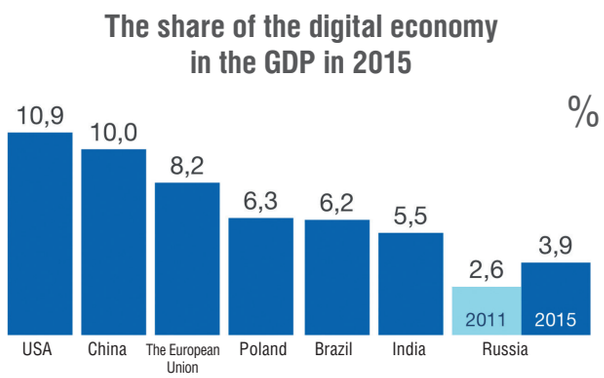
The West used the Ukrainian crisis of 2014 to strengthen and build up the force component of NATO borders and to deploy military contingents of the alliance near the western borders of Russia, which seriously aggravated the military-political situation in Europe.

4. Information and Communication Technologies (ICT) and the Development of the Digital Economy

The digital economy is shaping a new structure of the information space and new models of production relations based on digital platforms; it's covering global markets and the entire sectoral composition of the world economy. Technologies and platforms of the digital economy form the environment for its active self-reproduction and scaling.

The share of the digital economy in the GDP of the US and China is reaching 10 %, 8 % in the European Union, and about 4 % in Russia (Figure 5). At the same time, according to experts, the share of the digital economy can skyrocket in the coming years.

Figure 5



Source: *report of 2017 Digital Russia: New Reality (https://www.mckinsey.com/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Russia/Our%20Insights/Digital%20Russia/Digital-Russia-report.ashx).*

The cycle of the fourth industrial revolution (Industry 4.0), connected to the convergence and implementation of nano, bio, information, and cognitive technologies (NBIC), has already been launched in the economic and technological sphere of the developed countries of the world.

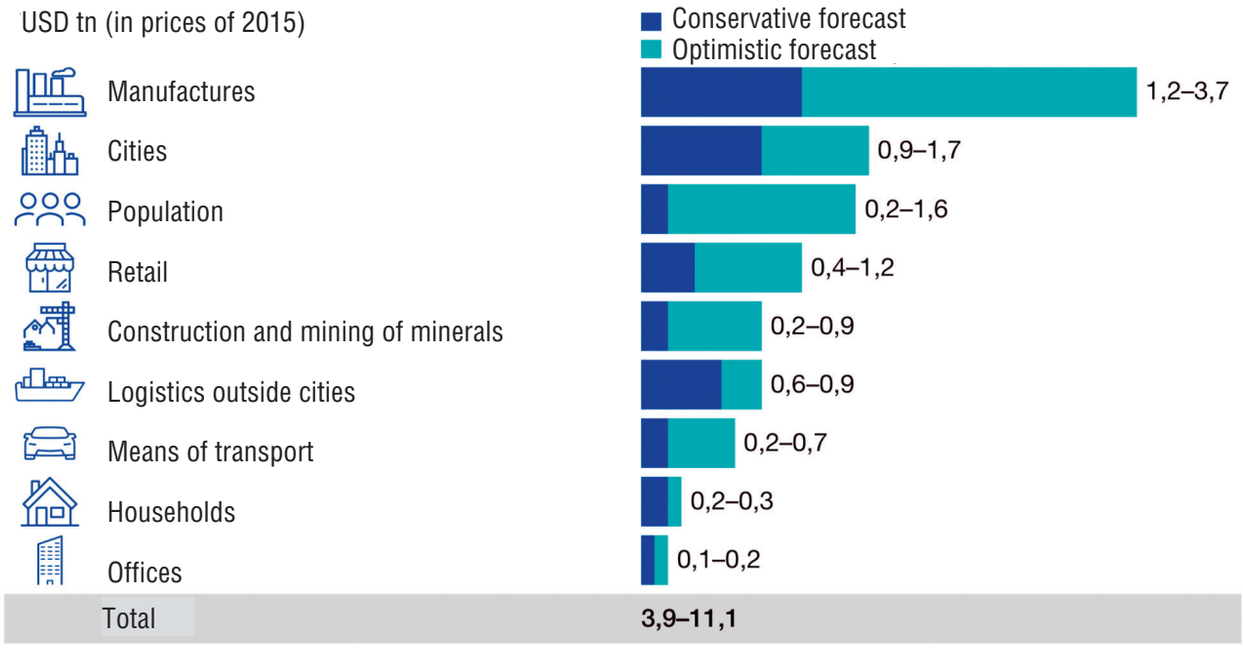
The most extensive and dynamic in this "quartet" is the group of information and telecommunication technologies (ICT), which include such new technological phenomena as Big Data processing, Internet of Things,

[7] On December 18, 2017, the Russian Foreign Ministry urged the United States to withdraw nuclear weapons from Europe. (https://topwar.ru/132210-midprizval-sshavyvesti-yadernye-vooruzheniya-izevropy.html).

[8] The strategic nuclear triad includes three components: strategic aircraft, intercontinental ballistic missiles, and nuclear submarines equipped with ballistic and cruise missiles of underwater deployment.

Figure 6

The Annual Contribution of the Internet of Things to the World Economy by 2025



Source: report of 2017 Digital Russia: New Reality (URL: https://www.mckinsey.com/~/media/McKinsey/Locations/Europe%20and%20Middle%20East/Russia/Our%20Insights/Digital%20Russia/Digital-Russia-report.ashx).

distributed registry, artificial intelligence, quantum computing, augmented and virtual reality, etc.

In 2017, the production of ICT products and services accounted for approximately 6.5 % of the world's gross product (GDP), and about 100 million people were employed in the ICT services sector.[9] According to some estimates[10], the total number of devices of the Internet of Things will be 50 billion units by 2020. The annual contribution of the Internet of Things to the world economy can be from USD 4-11 trillion by 2025 (see Figure 6).

The transition of the global economy to a new technological structure against the backdrop of a major trend towards massive development of the ICT environment and the digitization of all spheres of human activity is a key process that determines the peculiarity of the current stage of world development.

The phenomenon of changing milestones at the junction of the outgoing and emerging technological structures opens up a broad horizon of new opportunities for breakthrough economic development, but it simultaneously presents significant risks.

The distribution of bonuses based on the transition to a new technological order, which may ultimately affect the configuration of the centers of economic power in the world, will depend on how efficiently national economies take advantage of the windows of opportunities for advanced development that are available during the transition.

Everything will depend on the effectiveness of effort applied both at the national level (structural reformation of economies to adapt to the new technological order, investment programs for the development of innovative sectors, and the introduction of new technologies, as well as the creation of incentive regulations) and the international level (ensuring equal access to the use of opportunities of the new technological order).

In Russia, in accordance with the Strategy of Scientific and Technological Development, the transition to advanced digital, intelligent technologies, big data processing systems, and other new technologies is expected in the next 10-15 years. The plan for such a transition is contained in the "Digital Economy of the Russian Federation" Program.

It outlines five basic directions of efforts to develop the digital economy for the period up to 2024: legal and regulatory framework, personnel and education, the formation of research skills and technical capacities, information infrastructure, and information security.

Many states are adopting similar programs to support the digital economy; in particular, the Digital Economy Agenda has been being implemented in the United States since 2016.[11]

Most national programs for the development of the digital economy prioritize ensuring information security. In view of the cross-border and complex nature of information threats, the establishment of effective international cooperation in the field of information security depends on the progressive development of the national components of the global digital economy.

---

[9] Report on the Information Economy for 2017 // UNCTAD [Official Website] (http://unctad.org/en/PublicationsLibrary/ier2017_overview_ru.pdf).

[10] Internet of Things: How Our Whole Life Will Change at the Next Round of Development of the World Wide Web // CISCO [Official website] (https://www.cisco.com/c/dam/global/ru_ru/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf).

[11] Commerce Department Digital Economy Agenda 2016 // National Telecommunications and Information Administration United States Department of Commerce [Official website] (https://www.ntia.doc.gov/files/ntia/publications/alan_davidson_digital_economy_agenda_deba_presensation_051616.pdf)

5. Ensuring International Information Security

Today, information and communication technologies are not only becoming the main driver of digital development, but also turning into a determining military and political factor, an integral element of the modern military potential of states (cyber potential), complementing, and sometimes replacing, conventional military means. ICTs are also widely used by terrorist and criminal structures.

Due to the interconnectedness of global information networks, no country in the world can consider itself protected from cross-border information threats and can't guarantee information security alone. This determines the active development of international cooperation in the field of information security and cyber security.

Cyber security is described as the process of ensuring the integrity, confidentiality, and accessibility of data in the global ICT environment.

Russia promotes the creation of an inclusive system *of international information security (IIS) in a broader interpretation.* The IIS system *is designed to provide a state of the global information space, where the rights in the information sphere of the individual, society, and the state, as well as elements of critical information infrastructure, are reliably protected.*

5.1. The Main Threats in Information and Cyberspace

The most acute threats to information security for modern states are related to the development of the following*:*

- ***information and cyber weapons, including cyber espionage;***
- ***cybercrime;***
- ***cyber terrorism.***

A special focus *is on the problem of cyber attacks on elements of critical infrastructure (CI),* as well as *the development of "soft power" on the basis of ICT tools, to interfere in the internal affairs of states.*

Counteracting threats in the ICT environment is complicated by its "cross-borderness," anonymity, lack of evidence, (the absence of material evidence as a legal proof), the rapid development of processes, and the difficulties in developing international legal mechanisms for preventing, identifying, investigating, and bringing those responsible to justice.

To date, the development of *cyber weapons* in the world is quite widespread. Back in the late 1990s, the US Congress announced that 120 countries were developing information weapons[12]. Over the past 5-10 years, many of the world's leading states have created cyber troops (or information security troops). In addition to the United States, the top ten countries in this area include the United Kingdom, France, Germany, Russia, China, Israel, South Korea, North Korea.

Adopted in 2015, the US *Cyber Security Strategy* is aimed not only at cyber defense, but also at conducting offensive cyber attacks[13]. The US National Security Strategy of 2017 states that "the United States will deter, protect and, when necessary, defeat the malicious entities that use cyberspace against the United States[14]".

EU / NATO countries are actively building up their cyber potential. The Center of Cyber Defense has been operating in the structure of NATO since 2008.

A serious threat in the context of the rapid development of *information and cyber weapons* is the risk of provoking full-scale interstate conflicts, primarily due to the lack of mechanisms for rapid and accurate attribution of attacks, as well as the possibility of disproportionate response to threats (in the event of serious consequences of a cyber attack, for example, a critical infrastructure failure, the injured party can use physical weapons in response, and it's usually impossible to detect the state of the threat source). Currently, there are no international regulatory and legal criteria for classifying a cyber attack as an armed attack. These risks significantly increased after the US representative announced at the Warsaw Summit of NATO in July 2016 the possibility of applying Article 5 of the Washington Treaty in response to cyber attacks on member countries of the alliance.

The threat of cybercrime causing *unacceptable damage to the economic interests of the state,* citizens, and business is becoming critical. There is a trend of a steady increase *in the total world damage from cybercrime, from USD 3 tn in 2015 to projected growth of at least USD 6 tn per year* [15] *by 2021.*

The adoption of the Convention on Cybercrime by the Council of Europe in 2001 can be considered a milestone achievement in this area[16]; it contains a proposal to implement uniform rules on criminal liability for cybercrime in the legislation of the member countries. However, the practical effectiveness of this document is limited because some countries see a violation of the principle of national sovereignty in a number of provisions of the convention (in particular, the paragraph on conducting operational and investigative measures in the information infrastructure of states without their consent, Article 32-b). At the same time, the convention is becoming obsolete due to the emergence of new technologies and varieties of cybercrime.

In 2017, Russia submitted a draft Convention "On Cooperation in the Field of Countering Information Crime" to the UN GA. The draft mainly takes into account the shortcomings of the Council of Europe convention, provides for a broad modern conceptual ap-

[12] A.V. Krutskikh War or Peace: International Aspects of Information Security / Scientific and Methodological Problems of Information Security, ed. V.P. Sherstyuk. — M., 2004.
[13] DOD Cyber Strategy 2015 (https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).
[14] National Security Strategy of the United States of America. December 2017. (https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf).
[15] Cybercrime Damages $6 Trillion by 2021 (https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/).
[16] Convention on cybercrime, Council of Europe (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

paratus and criminalization of emerging new forms of cybercrime.

A factor seriously hampering the development of international documents on cyber terrorism is the lack of an internationally recognized definition of terrorism and unified TO lists.

The UN Group of Governmental Experts (UN GGE), in order to counteract the use of ICTs for terrorist purposes, recommends "expanding the exchange of information and mutual assistance for the purpose of prosecuting terrorists and suppressing the criminal use of ICTs[17]".

A significant part of the problem is the development of the ***shadow market of malicious software.*** Criminal syndicates actively involve experts in developing tools for exploiting vulnerabilities in software[18].

The concern of most states with the ***danger of cyber attacks on critical infrastructure*** (including state authorities, electric power, oil and gas, transportation, financial systems, water supply, nuclear facilities, military and industrial complex) is connected to the fact that disabling unprotected facilities of this kind can lead to a chain reaction and a rapid onset of catastrophic consequences, which represent a full-scale threat to national security. At the same time, automated control systems for CI facilities remain potentially vulnerable to cyber attacks, even if they are not directly connected to the Internet.

Significant concerns are also caused ***by the tendency of developing effective tools of "soft power", based on new ICTs, aimed at interfering in the internal affairs of states***. For this purpose, ***cyber attacks on industrial and financial facilities, cyber espionage with the aim of discrediting unwanted political forces, as well as network technologies of directed information impact (groups in social networks / messengers) can be used to manipulate public opinion, as well as prepare and carry out mass protests***. Over the past decades, the intensity of the use of such technologies has increased both in armed conflicts (in Afghanistan, Iraq, Libya and Syria), and the "color revolutions" (Georgia, 2003, Ukraine, 2004 and 2014, Kyrgyzstan 2005, Egypt 2011, etc.).

5.2. International Cooperation in the Field of IIS and Cyber Security

Leading countries in the world are currently promoting two basic approaches to security in the ICT environment. The US and Western countries, including EU / NATO countries, are developing ***cyber security strategies*** that focus on securing information in cyberspace.

In turn, Russia, China and other BRICS, SCO and CSTO countries offer a more comprehensive and inclusive concept ***of international information security,*** which also takes into account ***the threat of a targeted information impact using ICTs for influencing social and political processes and interfering in the internal affairs of sovereign states***.

Over the past few years, the ***IIS concept has been widely supported***. The CSTO is developing a process of harmonizing the national legislation of the member states in the field of ensuring information security and countering the violations in the information sphere. Since 2009, the SCO has had an agreement on cooperation in the information space[19]. The possibility of concluding such an agreement within BRICS is also elaborated[20].

Back in 1998, at its 53rd session, the UN General Assembly (GA) adopted, at the initiative of Russia, a resolution entitled "Developments in the Field of Information and Telecommunications in the Context of International Security" (A/RES/53/70). This resolution highlighted three main areas of ICT threats (related to military, terrorist, and criminal purposes) and called for defining basic concepts and developing international principles of state behavior in the ICT field.

The UN is an effective platform for working on the issues of the security of the ICT environment. By decision of the 56th session of the UN General Assembly (2001), the GGE was established on information and telecommunications in the context of international security. In 2015, the report of the GGE ***articulated the rules, principles, and norms of responsible behavior of states in the ICT environment.*** However, ***it was not possible to reach a consensus*** on ***the application of these rules and regulations*** in 2016.

The main ***conceptual difference between the Russian and American approaches*** on this issue is that, ***from the Russian point of view, conflicts in the ICT environment are unacceptable; therefore, they are not subject to regulation, but rather prevention, aversion, or suppression. The Western countries proceed from the need to regulate the military and political use of ICT,*** which, as a result, ***can legitimize the use of cyber weapons and military force in response to cyber attacks***.

The basic elements of the US position on international cooperation in the field of cyber security are defined in the International Strategy for Cyberspace which was put forward by the United States in 2011[21]. Its goal is to ***create a single platform for cooperation*** for states that adhere to a US-like position on security and the use of cyberspace. De facto, this document is not universal in nature and is focused, first of all, on cooperation with the EU and NATO countries and also with the countries participating in the Agreement on Radio Engineering Intelligence (Great Britain, Canada, Australia, New Zealand).

In 2011–2013, the United States supported some of Russia's initiatives in the field of information security.

---

[17] Report Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2015 (http://www.un.org/ru/documents/ods.asp?m=A/70/174).

[18] DOD Cyber Strategy 2015.P. 2.

[19] Agreement between the governments of the member states of the Shanghai Cooperation Organization on cooperation in the field of international information security dated June 16, 2009 (http://base.spinform.ru/show_doc.fwx?rgn=28340).

[20] BRICS can develop an agreement on information security (http://tass.ru/mezhdunarodnaya-panorama/4443112).

[21] International Strategy for Cyberspace (https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf).

In 2013, *the "Joint Statement of the Presidents of the Russian Federation and the United States of America on a New Field of Cooperation in Building Trust" was signed.*

However, the US subsequently moved on to *blocking the course of confrontation in the field of information security* and shied away from *interaction with Russia in the field of preventing incidents in the ICT environment, which is laid down in the joint statement of the presidents of Russia and the United States*[22]*. The US also rejected the agreement on the creation of a working group on cyber security which was reached during the meeting of the presidents of the two countries on the fields of G-20 in July 2017.* In a July 2000 study by the Joint Chiefs of Staff Committee of the US Armed Forces entitled "General Operational Situation of 2035," Russia and China, along with Iran and North Korea, are classified as the main opponents of the United States in cyberspace.

6. The Experience of Inter-Parliamentary Assemblies of the CIS and the CSTO in Countering Terrorism, Extremism, and Other Modern Threats and Challenges

There are active structures of inter-parliamentary interaction within the framework of the Commonwealth of Independent States (CIS) and the Collective Security Treaty Organization (CSTO), the international organizations formed by the states of the post-Soviet space.

Every six months, there are sessions of the Inter-Parliamentary Assembly (IPA) of the CIS in St. Petersburg, where about 500 delegates from the parliaments of participating countries work on model laws designed to harmonize national legislation within the integration association. Parliamentarians of nine CIS countries participate in the MPA[23], as well as Afghanistan as an observer state.

After the creation of the CSTO in 2002, the CSTO Parliamentary Assembly (CSTO PA) was formed. To date, 38 CSTO model laws have been adopted.

The CSTO PA adopted the Appeal to Parliaments of the World and International Parliamentary Organizations on Combining Efforts in Counteracting Terrorism and Other Forms of Violent Extremism at the Present Stage, which invites the establishment of contacts with the parliaments of member states and observers of the Shanghai Cooperation Organization (SCO).

Recommendations *on the approximation of the national legislation of CSTO states on combating terrorism and extremism were adopted.*

Harmonization of the legal regulation of CSTO member states in the ICT sphere is being carried out.

Recommendations on the whole range of legislative work in the field of information security were adopted and are being implemented.

In most CSTO member states, there are complexes of interrelated laws regulating the development of the information sphere — laws on the protection of electronic data, digital signatures, protection of copyright in the digital sphere, and countering extremism and terrorism in the information space.

The development of the CSTO countries' legislation *on countering terrorism and extremism* was influenced by the results of model lawmaking within the CIS.

The basis for the model legislative framework on counter-terrorism was the law "On Combating Terrorism" (in the wording of 2004). Then, the following model laws were passed: "On Counteracting Organizations and Persons whose Activities Are Aimed at Implementing Acts of Terrorism in the Territories of Other States" (2004), "On Counteracting the Financing of Terrorism" (2006), "On Countering the Legalization (Laundering) of Proceeds from Crime and Financing of Terrorism" (2008).

Recommendations on the legal regulation of the operation of open telecommunication networks to prevent their use for terrorist and other illegal purposes were approved.

The group of model laws on *industrial and transport security is closely connected with these tasks:* "On Control over the Traffic of Radioactive Materials" (2004)," On Transport Security and On Safety in Air Transport" (2007).

Recommendations on unification and harmonization of national legislations on chemical and biological security have been adopted.

A group of model laws *on combating extremism* is represented by the law "On Countering Extremism," developed in 2009.

In addition, recommendations on improving the legislation of the CIS member states in the sphere of countering extremism were adopted (2013).

Lines of model legislation *to combat illicit drug trafficking* laid the foundation for the law "On Narcotic Drugs, Psychotropic Substances, and Their Precursors" (2006).

Recommendations on the unification and harmonization of the national legislations of the CIS member states in the field of combating illicit trafficking in narcotic drugs, psychotropic substances and their precursors were adopted (2006).

Established in 2001, *the Shanghai Cooperation Organization*[24] is going through a *period of forming a parliamentary dimension* of its activities. Since 2006, the SCO has hosted the Meeting of Heads of Parliaments. This format has confirmed its relevance and is well suited for discussing the inter-parliamentary cooperation of the SCO countries in the field of security, including countering terrorism, extremism, as well as issues of international information security.

[22] The Joint Statement of the Presidents of the Russian Federation and the United States of America on the Expansion of Bilateral Cooperation. URL: http://kremlin.ru/events/president/news/18355.

[23] The representatives from Ukraine, which has begun the procedure for secession from the Commonwealth, suspended participation in IPA activities.

[24] Its members are India, Kazakhstan, China, Kyrgyzstan, Pakistan, Russia, Tajikistan, and Uzbekistan.

In 2009, the SCO adopted the Convention Against Terrorism and the Regulations on Political and Diplomatic Measures and Mechanisms for Responding to Situations Endangering Peace, Security, and Stability in the Region. Over the past few years, following the results of the SCO summits, various declarations have been adopted — Dushanbe (2014), Ufa (2015), Tashkent (2016) and Astana (2017) — to recorded the common approaches of the SCO states to countering terrorism, extremism, and IIS threats.

In the course of further development of the SCO parliamentary dimension, it is expected that the work on agreement and harmonization of legislation will be intensified, including in the field of regional security, ***combating extremism and terrorism, and the security of the ICT environment***.

The examples of efforts to harmonize national security legislation within the CIS, the CSTO, and, in the long term, the SCO, point to an objective need to intensify productive ***inter-parliamentary cooperation in countering global challenges and threats***.

The experience of inter-parliamentary assemblies of the CIS and CSTO can be widely used by parliamentary structures of other regional integration associations.

MAIN CONCLUSIONS

Joint Political Work

The international parliamentary movement has significant political potential to influence world affairs, which is possible to unlock through more active positioning as an agent of:

- reducing confrontation and conflict potential in the world;
- de-escalating tension in international relations;
- constructive, pragmatic, and productive cooperation between states and their associations in order to strengthen international and regional security and stability;
- establishing collective principles in world affairs and the uniting agenda of countering traditional and new challenges and threats;
- settling differences and eliminating emerging threats to peace through dialogue, with strict observance of fundamental norms of international law, principles of respect for the sovereignty of states, non-interference in their internal affairs;
- approving the principles of responsible behavior in the global information space and creating a security regime for the ICT environment, which helps prevent incidents in it, including interstate incidents;
- a culture of compliance with treaties and regimes for arms control and nuclear non-proliferation, as a basic factor of military and political stability;
- renouncement from unilateral attempts to resolve international disputes with the use of force or sanction pressure.

Joint Legislative and Control Work

Improvement of coordination and harmonization based on the exchange of experience and best practices of national legislations, means, and methods of parliamentary control in key areas of security:

- countering international terrorism;
- integrated fight against drug trafficking;
- ensuring a secure ICT environment, effectively managing the entire range of cyber threats — from cybercrime to cyber attacks on critical infrastructure facilities;
- providing uninterrupted operation of national systems of nuclear material safety, protection of nuclear facilities and hazardous industries.