

ISC 2019 第七届互联网安全大会

当前国际信息安全的紧迫问题- 俄罗斯视角

阿纳托里·斯米尔诺夫
俄联邦国际信息安全协会理事长

小鹅助理



扫码添加小鹅助理，与数万科技圈人士
分享重量级活动PPT、干货培训课程、高端会议免费
门票



阿纳托里·斯米尔诺夫
Anatoly Smirnov

俄联邦国际信息安全协会理事长
General Director, National Association
of International Information Security, Russia





ACTUAL PROBLEMS FOR INTERNATIONAL INFORMATION SECURITY - A VIEW FROM RUSSIA

ANATOLY I. SMIRNOV

Director General of the National Association of International Information Security,

Doctor of Historical Sciences, Professor of MGIMO

of the MFA of the Russian Federation

<http://namib.online/>





互联网安全中心

**Vladimir Putin and Xi Jinping signed a
Joint Statement on Developing
Comprehensive Partnership and Strategic
Interaction Entering a New Era
and a Joint Statement on Strengthening
Global Strategic Stability in the Modern
Age (The Kremlin, Moscow June 5, 2019)**

Internet Security Conference 2019

ISC

Internet Security Conference



**Vladimir Putin and Xi Jinping signed a
Joint Statement on Developing
Comprehensive Partnership and Strategic
Interaction Entering a New Era
and a Joint Statement on Strengthening
Global Strategic Stability in the Modern
Age (The Kremlin, Moscow June 5, 2019)**





第七屆國際網路安全大會

Joint Statement on Developing Comprehensive Partnership and Strategic Interaction Entering a New Era

6. Expand contacts on issues of international information security, strengthen measures to protect the security and sustainability of the critical information infrastructure of the Parties. Strengthen exchanges in the field of legislative regulation of activities in the information space, jointly promote the principle of managing the information and telecommunication network "Internet" in accordance with international law and domestic regulatory requirements. Counteract the introduction of unreasonable restrictions on access to the market for ICT technology products under the pretext of ensuring national security, as well as unreasonable restrictions on the export of high-tech products. To ensure the peaceful and safe functioning of the Internet on the basis of equal participation of all states in this process, to promote the establishment of an orderly management of the global information space. To continue work in order to further develop within the UN the rules of responsible behavior of states in the information space and develop a universal, legally binding document on countering the use of information and communication technologies for criminal purposes.



Russian National Security Strategy, December 2015





FOREIGN POLICY CONCEPT OF THE RUSSIAN FEDERATION

Approved by V. Putin 30.11 2016



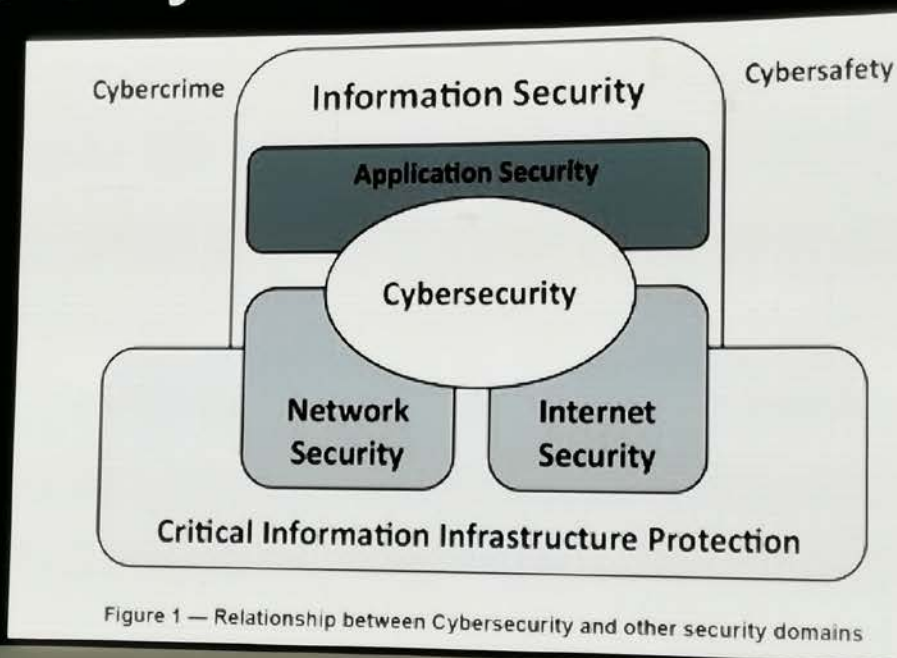
28. Russia takes necessary measures to ensure national and international cyber security, counter threats to State, economic and social security emanating from cyberspace, combat terrorism and other criminal threats involving the use of information and communication technology;

- deters their use for military-political aims that run counter to international law, including actions aimed at interfering in the domestic affairs of States or posing a threat to international peace, security and stability;
- and seeks to devise, under the UN auspices, universal rules of responsible behaviour with respect to international cyber security, including by rendering the internet governance more international in a fair manner.



联网安全中心

ISO/IEC 27032:2012 Information technology Guidelines for cybersecurity





第七届中国网络安全大会



联网安全中心

HYBRID WAR - THE RENAISSANCE OF CONTAINING RUSSIA





USA: ICT in the "power" scenario of containment of the Russia

- - Refusal to prevent conflicts in the ICT environment (statement by the presidents of the Russian Federation and the USA in 2013);
- - Obama's decision to set up a cyberbomb in the Kill of Russia (WP 23.6.17);
- - Wikileaks: the CIA has software for attacks under the "alien flag" (03.2017);

Internet Security Conference 2019

ISC

Internet Security Conference

2019





USA: ICT in the “power” scenario of containment of the Russia

- - Refusal to prevent conflicts in the ICT environment (statement by the presidents of the Russian Federation and the USA in 2013);
- - Obama's decision to set up a cyberbomb in the KII of Russia (WP 23.6.17);
- - Wikileaks: the CIA has software for attacks under the “alien flag” (03.2017);
- - The National Security Doctrine (Dec 2017) contains 45 times the term “Cyber”, opponents: China, Russia, Iran, North Korea;
- - The Law «On Countering America's Adversaries through Sanctions» (02.08.2017) (Russia, Iran, North Korea); (62 sanctions, incl. in the ICT)
- - CLOUD Act (03/23/2018) to obtain the FBI, the CIA, etc. PD from all devices around the world (and the Russia), vendors of which are US firms;
- - 08.16.2018 - D. Trump canceled B. Obama's decrees on the rules of cyber attacks
- - 09.2018 - DoD cybersecurity strategy - cyber war preamble
- - 09.2018 - National cyber strategy - course on cyber attack
- - 1.2019 - The Trojan Horse Strategy
- - Strengthening the role of ICT in hybrid wars, robotic scrolling for “cyber rebellion”





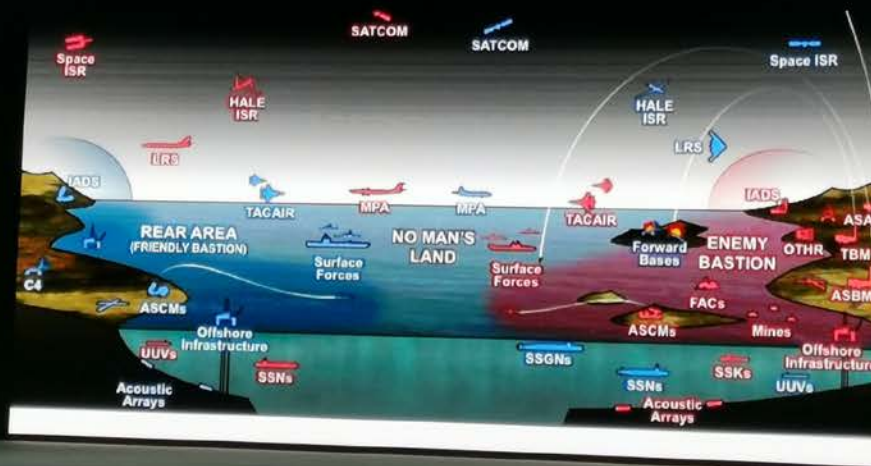
The threat of NATO's claims to global leadership using Deadly Autonomous Systems (CAC) using AI





The threat of NATO's claims to global leadership using Deadly Autonomous Systems (CAC) using AI

- UN GGE for Non-Conventional Weapons: CAC will provide
- the military with technological separation from rivals.
- "Full Spectrum Dominance" - the ability to control any situation
- and defeat the enemy in the entire range of military operations.
- Third offset strategy: autonomous AI robots will be able to ensure military dominance on the planet by replacing nuclear weapons and high-precision ammunition.



1950
nuclear
weapons



1970 high-
precision
ammunition



2020
autonomous
AI robots



**NATO: Look how close Russia put its country to
our military bases!**

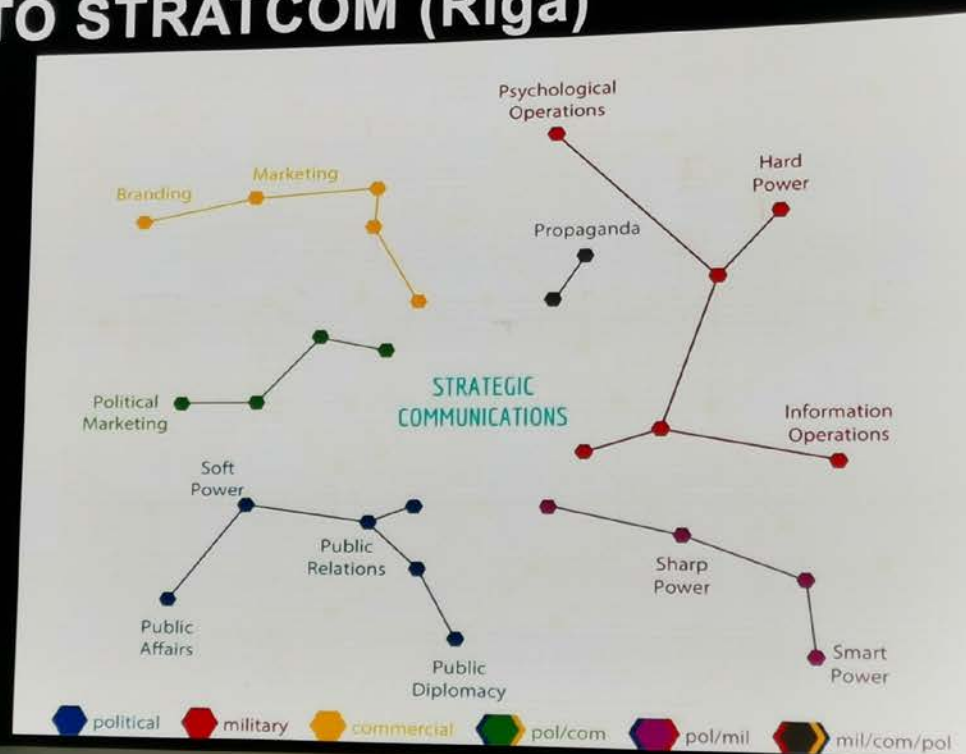
RUSSIA WANTS WAR





互联网安全中心

CoE NATO STRATCOM (Riga)





EASTERN
ECONOMIC
FORUM

4-6 SEPTEMBER
2019

VLADIVOSTOK, RUSSIA

Zone of Trust: A Safe Eurasian Cyberspace

Virtual space has become just another dimension of real space, just like the earth's surface or its atmosphere. In the coming years, many elements of Eurasia's critical infrastructure will go digital. However, digital construction can turn into a perilous venture if electrical grids, utilities, transport systems, or urban activity are in danger of being sabotaged. With trade and technological wars waged against from the outside, there is a need for digital sovereignty and technological independence: any country must be able to control and secure its own digital space and critical infrastructure. This raises the questions of shared 'rules of the game' in the digital space and of a unified effort in Eurasia to create a zone of 'digital trust.' What challenges exist on the path towards creating a zone of 'digital peace' and cooperation in the region? What do governments and businesses have to do to create a 'zone of trust'? What partnerships can be formed to achieve this goal?



National Association of International Information Security (NAIIS)

In April 2018, the NAIIS was formed. According to the Charter, the Association proactively studies the problematic issues of ensuring international information security in the interests of forming negotiating positions of state bodies.

For a year and a half, the Association took part in 32 international events, of which 11 were the organizer or co-organizer. Among the major events of 2019 are the 13th international Forum in Garmisch-Partenkirchen (Germany), a conference with the Central American Parliament in Guatemala, and the international Forum in Cuba. Members of the Presidium made over a hundred reports and published dozens of articles, issued a monograph and a unique textbook, International Information Security: Theory and Practice, in 3 volumes edited by the Special Representative of the President of Russia, member of the Association Presidium A. Krutskikh. As part of its statutory tasks, the Association is ready to interact with interested organizations of China and other states in the interest of strengthening cyber peace and security.





Thanks for attention!

ANATOLY I. SMIRNOV
Director General of the National Association of
International Information Security,
Doctor of Historical Sciences, Professor of MGIMO of
the MFA of the Russian Federation

<http://namib.online/>



小鹅助理



谢谢!

扫码添加小鹅助理，与数万科技圈人士
分享重量级活动PPT、干货培训课程、高端会议免费门票