WORLD TRADE CENTER

Moscow, Krasnopresnenskaya emb. 12, Entrance № 4

20 June 2019, Thursday

09:00–17:00	Participants' registration
10:00–11:30	Opening plenary session
Hall Amphitheater	***The road to cyber resilience – a walk together?***
	The global network is a world which is already inhabited by more than 4 billion people. We go there to form our digital identity, store and transfer huge amounts of data every day and generally do things that we could previously do only in the real world. For the new generation, the cyberworld is becoming the main space for interaction — it is faster, full of information and opens up endless opportunities for development. However, that world is fragile — the strategies for protecting the real world have evolved over thousands of years, and here we are just beginning to shape them for the virtual sphere. And we do not have these millennia at our disposal. So, how do we protect the new digital world from digital threats? Is this a task for each state separately or a common challenge for the whole world? Which approach to choose?
	Moderator:
	Misha Glenny, Journalist, investigative reporter, expert on cybercrime
	Speakers:
	Konstantin Noskov, Minister of Digital Development, Communications and Mass Media of the Russian Federation
	Hans-Wilhelm Dünn, President, Cyber-Security Council (Germany)
	Jürgen Storbeck, Director (1999-2004), Europol
	Vladislav Onishchenko, Head of the Analytical Center for the Government of the Russian Federation
	Ömer Fatih Sayan, Deputy Minister of Transport and Infrastructure of the Republic of Turkey
11:30–12:00	Coffee break
12:00–13:00	Panel session
Press Hall	***Cybersecurity strategies: public services***
	Cybercrime is one of the most pertinent international threats of our century. This problem cannot be solved at the national level — geographically scattered groups may stretch across continents and fall under the jurisdiction of a number of states at once. Different levels of technological development, maturity of the legal framework in this sphere and geopolitical turbulence complicate cooperation and the process of resisting cybergangs. Can we make a difference? Or will cybercriminals always be one step ahead?
	Moderator:
	Andrey Bezrukov, President, Technological Sovereignty Exports Association
	Speakers:
	Craig Jones, Cybercrime Director, INTERPOL
	Alberto Hernández Moreno, CEO, Spanish National Cybersecurity Institute
	Leonid Levin, Chairman of the State Duma Committee on Information Policy, Information Technologies and Communications of Russian Federation
	Mikhail Galperin, Representative of the Russian Federation at the European Court of Human Rights, Deputy Minister of Justice of the Russian Federation
	Julian Voje, Deputy Head of Policy and Analysis, Munich Security Conference Foundation
12:00–13:00	Panel session
Hall Amphitheater	***Cybersecurity strategies: financial industry***

Banks, payment systems, credit agencies, monetary funds constitute a circulatory system of the economics providing vital services for the global community. Malfunction of just one link within the chain will lead to failure of the whole system therefore the crucial issue for is the security of the financial sector. Taking into account global digitalisation, the issue of cybersecurity takes stage and increased attention of cybercriminals considerably increases the risks of possible losses. What is the correct way to build security strategy in financial institutions? How is it possible to both secure the sector and decrease clients' possible risks? Can we foresee future threats and start building protection right now?

Moderator:

Stanislav Kuznetsov, Deputy Chairman of the Executive Board, Sberbank

Speakers:

Sunil Seshadri, Senior Vice President, Chief Information Security Officer, Visa

Georgy Luntovsky, President, Association of Banks of Russia

Mikhail Alekseev, Chairman of the Management Board, UniCredit Bank

Danijela Zizic, Chief Security Officer & Data Protection Officer, Eurobank

12:00–13:00	Panel session
Hall 2	*Cybersecurity strategies: critical infrastructure*

Today cyberattacks have the potential to cause more serious damage than physical events be they natural or man-made. Therefore, the cybersecurity of critical infrastructure comes to the forefront — a successful attack on the services of the critical infrastructure may undermine the economic stability of the country and greatly affect the standard of living of ordinary people. How to protect oneself against such situations? What exactly should states and companies be focused on doing? And what positive contribution can international cooperation bring in this area?

Moderator:

Evgeny Kovnir, CEO, ANO Digital Economy

Speakers:

Yousef Al-Ulyan, Vice President for Information Technology, Saudi Aramco

Andrey Ivashko, Director, National Computer Incident Coordination Center (Russia)

Igor Lyapunov, Vice President, Information Security, Rostelecom

Lothar Renner, Managing Director Cybersecurity EMEAR, Cisco

Igor Milashevskiy, CEO, GLONASS

12:00–13:00	Panel session
Hall 3	*Cybersecurity strategies: disruptive technologies*

Technological progress facilitates the advancement of cybercrime. Each day fraudsters find new vulnerabilities, sharpen their hacking and social engineering skills as well as develop malware that could penetrate even the most secure systems. All this creates critical conditions for many organisations and stimulates the industry to create new methods of protection. Will we be able to catch up with the criminals and provide cybersecurity on a global level?

Moderator:

Sergey Plugotarenko, Director, The Russian Association for Electronic Communications

Speakers:

Dhanya Thakkar, Vice President AMEA, Trend Micro

Dmitry Samartsev, CEO, BI.ZONE

Loo Chu Kiong, Deputy Director, Centre of Innovation, University of Malaya

Gyorgy Racz, Director, Security Systems, IBM Europe

Alexandr Khanin, CEO, VisionLabs

12:00–13:00	Panel session
Hall 1	***Cybersecurity strategies: telecommunications***

The telecommunication industry lies at the heart of Internet development. Providing communications to the population of our planet, telecom operators made it possible to instantly contact people on the other side of the world, opened up the endless expanse of the World Wide Web, where you can find almost any data in a matter of minutes. The constant development of this sphere makes it possible to carry out these actions at ever-increasing rates, opening up even more opportunities for us to enjoy, and cybercriminals alike. Are we able to protect the users without slowing down the technological evolution?

Moderator:

Boris Glazkov, Vice President for Strategic Initiatives, Rostelecom

Speakers:

Jacqueline Kernot, Partner in Cybersecurity, Ernst & Young

Allan Salim Cabanlong, Assistant Secretary Cybersecurity & Enabling Technology, Department of Information and Communications Technology of the Republic of Philippines

Yogesh Malik, Chief Technology Officer, VEON

Valery Shorzhin, Member of the Management Board, Vice President for Digital Business Solutions, MTS

13:00–14:30	Networking and free time
13:15–14:15	Closed round table
	Investment attractiveness of federal subject of Russia in regard to IT and cybersecurity
14:30–16:00	Closed round table
	Cybercrime investigations. Cooperation of law enforcement and business. International collaboration
14:30–18:00	Topical sessions
Hall 3	***Legal environment***

The section will cover the legal aspects of cybersecurity as well as the issues of international cooperation for legislative push-back against cybercrime.

14:30–15:00	Topical session
Hall 3	***Attributing cyberattacks***

Attribution of attacks is a fundamental structure in cybersecurity and state safety depends on the stability of this structure. Since 2013 a number of governments and companies have made significant advances in attributing computer network intrusions, setting precedents that had certain legal consequences, for example in the insurance industry. New norms and practices are emerging, and Thomas Rid will reflect on recent trends in cyberattack attribution.

Speaker:

Thomas Rid, Professor, School of Advanced International Studies, Johns Hopkins University

15:15–15:45	Topical session	
Hall 3	***Legislating a borderless, ungoverned virtual world – is it possible?***	

'Where is the international law of Cyber?' Significant States have proposed internationally binding treaties, other States are moving forward with regional conventions and various public-private partnerships have emerged. However, the level of engagement in international law-making for Cyber appears low. It seems we have not gained the traction needed globally to counter the very real and very present danger of cyber conflict.

Time is running out to agree an internationally binding treaty for Cyber. If we don't work together it won't happen.

Speaker:

Greg Rudd, CEO, CREST Australia & New Zealand

16:00–16:30	Topical session	
Hall 3	***Can malicious actors be held accountable for illegal acts in cyberspace?***	

Let us assume that states agree to a set of rules for the use of cyber weapons — for example, not attacking critical infrastructure during peacetime. What happens when a state violates one of those rules — is it possible to define who is responsible in this case? Enforcement techniques in use or under consideration include diplomatic pleas and threats, economic sanctions, indictments, public shaming, joint investigations, recalling diplomats, as well as military and information countermeasures. Such techniques are proving ineffective and potentially destabilizing. Mr. McConnell will outline a proposed enforcement regime to improve security and stability in cyberspace.

Speaker:

Bruce W. McConnell, Executive Vice President, EastWest Institute

16:45–17:15	Topical session	
Hall 3	***Ensuring cybersecurity of critical infrastructure***	

Rafael Maman will make an analysis of the history of cyberwars, the latest developments in the field of ensuring cybersecurity of critical infrastructure of national importance, as well as the main problems that we encounter on the way to ensuring an adequate level of cybersecurity of critical infrastructure, what we call the "known unknowns" of operating technology security.

Speaker:

Rafael Maman, Partner in Cybersecurity and Digital Strategies, PwC Israel

14:30–18:00	Topical sessions	
Press Hall	***Capacity building***	

The section will focus on issues of increasing the competence of specialists and global capacity building in cybersecurity, as well as ways of developing international cooperation in this area in order to increase the level of countering cybercrime.

14:30–15:00	Topical session	
Press Hall	***Cybersecurity education in the nuclear and energy sector***	

Guido Gluschke will give an overview on educational cybersecurity activities in the nuclear power and energy fields, international trainings and other forms of professional development in these spheres. The speaker will also address faculty engagement within the energy sector.

Speaker:

Guido Gluschke, Director, Institute for Security and Safety, Brandenburg University of Applied Sciences

15:15–15:45	Topical session	
Press Hall	***Building a global cyber ecosystem: the role of the academia***	

Most experts agree that in order to establish a thriving cybersecurity ecosystem, well-coordinated interaction between the following components is essential: Corporate, Military and

Academia, as well as support of start-ups and presence of investors. Yuval Elovici will give a detailed analysis of the contribution of the academia to such ecosystems, using real-world examples and case-studies.

Speaker:

Yuval Elovici, Director of the Telekom Innovation Laboratories, Associate Professor at the Ben-Gurion University of the Negev

16:00–16:30	Topical session
Press Hall	***Islands of freedom: how universities become growth points of cybersecurity capacity***

Cybersecurity places increased demands on technical knowledge and depth of development of various fields of applied mathematics and IT technologies, and at the same time, this area is criminalized, which makes it difficult for beginners to acquire many practical skills. The experience of the faculty of the CMC of Lomonosov Moscow State University and the Faculty of Computer Science of the National Research University Higher School of Economics, shows how the combination of academic freedom, science, education and business allows us to vertically and horizontally scale human resources in this area.

Speaker:

Denis Gamayunov, Head of Cybersecurity, Research Lab at Information Security Chair, Department of Information Security, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University

16:45–18:00	Panel session
Press Hall	***P2P transfers – where is security?***

Moderator:

Artem Kalashnikov, Head, FinCERT

Speakers:

Viktoriya Nikitina, Head of Information Security Statutory Regulation Department, Bank of Russia

Artem Sudarenko, Deputy Head, FinCERT

Anna Goldstein, Head of Software Solutions Center, National Payment Card System

Dmitriy Gadar, Vice President – Director of Information Security Department, Tinkoff Bank

14:30–18:00	Topical sessions
Hall 2	***Threat intelligence***

The section will touch on acute digital threats and key global challenges of cybersecurity, as well as recommendations for increasing the overall resilience to cybercrime.

14:30–15:00	Topical session
Hall 2	***Customer is not always right***

Evgeny Voloshin will talk about the evolution of cyberattacks, the shifting focus from complex technological scenarios to socio-technical ones, as well as a qualitative change in the approach to social engineering.

Speaker:

Evgeny Voloshin, Chief Expert Services Officer, BI.ZONE

15:15–15:45	Topical session
Hall 2	***Evolution of targeted attacks on the financial sector***

Based on the attacks of Lazarus cybergang.

Speaker:

Dmitry Volkov, Chief Technical Officer & Co-founder, Group-IB

16:00–16:30	Topical session
Hall 2	***Advanced threat trends***

Speaker:

Timur Biyachuev, Vice President Threat Research, Kaspersky Lab

16:45–17:15	Topical session
Hall 2	***An incident. How to bounce high?***

The total number of incidents is steadily increasing, as well as their complexity. However, in terms of investigating and responding to them, they are all divided to three categories: very interesting, average and boring. What incidents does the business most often give up and why? Are APT attacks boring? Who is behind such attacks and how difficult / expensive is it to organize them? How have the attacks on organisations of various sectors of the economy changed over the past year and a half? Is it possible to resist the attacks that we consider interesting? Is it worth spending time and resources on countering primitive and boring attacks? What is worth preparing now?

Speaker:

Alexey Novikov, Director of Expert Security Center, Positive Technologies

17:30–18:00	Topical session
Hall 2	***Predicating the unpredictable: a look into 2019 cyberthreat landscape***

The pace of change in the cyber world makes predictions almost impossible to make. Can we truly prepare for what's next? Probably not entirely, but there is a lot we can learn from our ongoing research of current cyberthreats.

Speaker:

Jonathan Fischbein, Head of Technical Marketing, Check Point

14:30–18:00	Topical sessions
Hall Amphitheater	***Disruptive technologies***

The session will shed light on the prospects of innovative technologies in cybersecurity, as well as the issues of strengthening collaboration to resist cyberthreats.

14:30–15:00	Topical session
Hall Amphitheater	***Future vehicular mobility transition and its impacts on cybersecurity***

Since introducing the technology for autonomous driving, cybersecurity was mostly an afterthought. But failures in this sphere can damage brands or even kill passengers, and undermine trust of the public in the future mobility concepts. The industry is slowly starting to incorporate improvements, especially since the hacks of connected vehicles by white hat hackers on public TV. The executive management of autogroups needs to learn to recognise these issues and take into account the security risks, arising on the way towards the bright future.

Speaker:

Clemens Dannheim, CEO, Objective Software

15:15–15:45	Topical session
Hall Amphitheater	***Cybersecurity in digital chaos***

Speaker:

Sergey Lebed, Chief Information Security Officer, Sberbank

16:00–16:30	Topical session
Hall Amphitheater	***Cybersecurity in the era of mobility: protect business by protecting ourselves***

In the modern world there is an obvious trend for mobility – remote job locations, constant moving, necessity to use various devices for work and to keep them constantly updated, and

that is besides the headache stemming from the employees in charge of cybersecurity. Hence, it becomes clear that it is not the person that is mobile, but rather their "digital identities", which also need to be protected somehow. All this considered makes us think about a complex approach to understanding a person's cybersafety. Standard means no longer apply here – something new is needed.

Speaker:

Anton Okoshkin, Chief Technical Officer, BI.ZONE

16:45–17:15	Topical session
Hall Amphitheater	***Machine learning on the other side of cybersecurity barricades***

Machine learning is widely used in technologies to counter various attacks. But what if the attackers also turn to these tactics? Ivan Novikov will give examples of attacks using machine learning as well as techniques for detecting new vulnerabilities based on these examples.

Speaker:

Ivan Novikov, CEO, Wallarm

17:30–18:00	Topical session
Hall Amphitheater	***The use of prognostic and statistical analysis methods for automating the processes of predictive response to new cyberattack techniques***

Predictive cyberattack scenarios, being integrated with log data streams coming from various protection tools and IT infrastructure, effectively model potential attack vectors and the attacker's behavior. This makes it possible to automate the process of responding to incidents in predictive mode.

Speaker:

Kirill Kertsenbaum, Head of Sales, Symantec Russia

14:30–18:00	Topical sessions
Hall 1	***Investments in cybersecurity***

The session will explore the issues of investing in the cybersecurity industry, as well as key points for developing innovations in this area.

14:30–15:00	Topical session
Hall 1	***Investments - risk, return & impact***

Why are we investing and advising institutional and private entities together with governments to invest in cybersecurity? What are the risks, the returns and the impact on the society, economy and other spheres of life? Is it worth investing in cybersecurity?

Speaker:

Ben Banerjee, Board Member, InnMind

15:15–15:45	Topical session
Hall 1	***Cybersecurity investment opportunities***

The global cybersecurity investment market is actively developing with Compound Annual Growth Rate (CAGR) exceeding 20%. One of the active players of this market is Skolkovo Innovation Center. Vasily Belov will speak about the main trends and investment opportunities in the industry.

Speaker:

Vasily Belov, CEO, Skolkovo Ventures

16:00–16:30	Topical session
Hall 1	***Innopolis - special economic zone***

Speaker:

Vadim Galeev, Deputy General Director for Strategic Development and Investor Relations, Innopolis

16:45–17:15	Topical session
Hall 1	***Biometrics in cybersecurity as an investment opportunity***
	By 2022, 70% of large enterprises will implement biometric authentication in their Identity and Access Management projects. How safe is this method, are there any risks of compromising biometric data and how do these risks affect investments? Will biometrics replace traditional technologies when it becomes an integral element of cybersecurity? Oleg Glebov will talk about the key areas of innovation for authentication, providing security against compromising and substitution of biometric data as well as applying sound event analysis for protection of industrial facilities.
	Speaker:
	Oleg Glebov, Business Development Executive, Speech Technology Centre
18:00–22:00	**Cocktail reception at the Bolshoi Theatre (by invitation)**

21 June 2019, Friday

09:00–15:00	Participants' registration
09:30–10:30	Panel session
Hall Amphitheater	***AI technologies in cybersecurity***
	Moderator:
	Alexander Vedyakhin, First Deputy Chairman of the Executive Board, Sberbank
	Speaker:
	Loo Chu Kiong, Deputy Director, Centre of Innovation, University of Malaya
	Igor Lyapunov, Vice President, Information Security, Rostelecom
	Sergey Garichev, Vice Rector for Research and Development, Moscow Institute of Physics and Technology
	Alexey Natekin, Founder, Open Data Science Community of Russia
	Aiden Wu, CEO, Huawei Russia
	Grigory Kabatiansky, Professor, Advisor to the Rector for Science, Skolkovo Institute of Science and Technology
	Mikhail Mamonov, Deputy Minister of Digital Development, Communications and Mass Media of the Russian Federation
10:30–11:00	Networking and free time
11:00–12:00	Briefing
Press Hall	***Cyber Polygon – summarizing the results***
	The briefing will be devoted to summing up the results of the online training Cyber Polygon, as well as discussing the prospects for joint resilience to cyberthreats.
	Moderator:
	Bruno Halopeau, Head of Cyber Resilience, Centre for Cybersecurity, World Economic Forum
	Speakers:
	Stanislav Kuznetsov, Deputy Chairman of the Executive Board, Sberbank
	Dmitry Samartsev, CEO, BI.ZONE
	Zhanbolat Nadyrov, Chairman of the Board, Transtelecom

Allan Salim Cabanlong, Assistant Secretary Cybersecurity & Enabling Technology, Department of Information and Communications Technology of the Republic of Philippines

Jacqueline Kernot, Partner in Cybersecurity, Ernst & Young

Craig Jones, Cybercrime Director, INTERPOL

Alexander Baryshnikov, Chief, Information Technology, New Development Bank

12:00–12:30	Networking and free time
12:30–14:00	Main plenary session
Congress Hall	***Secure digital world – possible future or wishful utopia?***

For centuries, scientists, writers and politicians have been fantasising about the future of the planet. When asked about what may be in store for us in the era of unprecedented technical progress, in the 19th century they spoke about submarines and flying machines, in the 20th century - about anthropomorphic robots and the colonisation of distant worlds. But we, being witnesses of this future, see something larger — a boundless world of digital opportunities, existing in parallel with the real world. This world appeared only a few decades ago and is just starting to develop and it is up to us to decide what this development will be — transparent and safe or full of digital threats.

Moderator:

Nik Gowing, BBC World News main presenter (1996-2014), Founder and Director, Thinking the Unthinkable

Speakers:

Herman Gref, CEO, Chairman of the Executive Board, Sberbank

Alois Zwinggi, Member of the Managing Board, Head of the Centre for Cybersecurity, World Economic Forum

Kairat Kelimbetov, Governor, Astana International Financial Centre

Maxim Akimov, Deputy Prime Minister of the Russian Federation

Elvira Nabiullina, Governor of the Bank of Russia

18:00–24:00	**Sberbank Night (by invitation)**