ICC International Cybersecurity Congress | SBERBANK

ICC 2019

International Cybersecurity Congress

icc.moscow

ICC International Cybersecurity Congress | SBERBANK

Making
the digital world
a safer place

Dmitry Medvedev

Prime Minister
of the Russian Federation

The International Cybersecurity Congress for the second consecutive year has been gathering representatives of government agencies, international organisations, businesses, as well as security experts from around the world. A few years ago, we began to prepare for the onset of the digital era oblivious to the fact that we were already living it. The digital expansion has brought about changes to government services, educational faculties and medical capabilities. Russia has one of the highest rates of Internet proliferation, mobile communications and the development of electronic services, and the cost of web access is one of the lowest in the world. The growth of the Russian Internet sector is up to 15% per year.

However, digitalisation, rapid growth of technologies, innovative achievements are known to come with risks and threats. According to analysts, the total damage to the global economy due to cyberattacks in 2019 could increase to $2.5 trillion. Government efforts alone are not enough to tackle the problem of cyberthreats — everyone, including businesses must be involved in this process. Today's open dialogue shows that together we can truly move forward in the fight against cybercrime and cyberthreats. I am confident that this event will prove to be another step towards a secure digital future for us all.

Herman Gref

CEO, Chairman of the Executive Board,
Sberbank

In the era of global digital transformation, security of all the elements of modern systems becomes an issue of utmost importance. Ensuring their protection requires not only powerful internal competence but also effective international cooperation. In the frame of such collaboration, being open and ready to share information on potential threats and successful cyberattacks helps to arrive at the right conclusions and to act preventively. Therefore, the core idea of the Congress is not to reinvent self-protection but to broaden the global coalition against cybercriminals.

Stanislav Kuznetsov

Deputy Chairman of the Executive Board,
Sberbank

More than 2,500 delegates from 65 countries attended the second International Cybersecurity Congress. We are looking at two exciting days ahead of us (more than 60 sessions, seminars, and reports), during which everyone will have a unique opportunity to share experiences, exchange views, establish business relations and cooperation. I do hope to instill trust, cooperation and tightening of communication as the heart and essence of this forum.

Contents

Key observations

Building international collaboration

Cyberspace is borderless; therefore, effective security is impossible without international, cross-sector cooperation and trust-based collaboration in which public and private partnerships play an especially significant role.

Exchanging threat intelligence

The attacks are becoming more sophisticated and complex to be recognised. Cybercriminals can go on for months inside a company's IT-infrastructure without being noticed. Such attacks cause tremendous damage, especially, to critical infrastructure. It is necessary to upgrade outdated systems, introduce new security methods and actively exchange information on cyberthreats with other organisations.

Improving overall cyberliteracy

The state should protect the rights of its citizens across cyberspace and increase their overall cyberliteracy. The success of many attacks is directly linked to users being unprepared.

Defining the legal ecosystem

In order to increase resistance to cyberthreats it is necessary to elaborate domestic and international rules and standards on cybersecurity.

Overcoming the labour drought

There is a serious shortage of specialists in the sector. Building up the manpower capacity is one of the paramount challenges of the coming years.

Addressing top management

The issue of providing cybersecurity is expanding beyond the sole responsibility of technical specialists. Strategic decisions on cybersecurity must be taken at the executive level of companies and entities as an integral part of risk management and corporate governance.

Implementing 'security by design'

Development of technologies is following an obsolete path: security elements are still regarded as an addition to the system rather than its integral part. For global IT proliferation and development of the digital economy, it is necessary to shift to the 'security by design' model, wherein security measures are introduced at the stage of development.

Forecast and prevention

Preventive measures and the possibility to foresee threats is the next evolutionary stage when approaching cybersecurity. Companies and states should follow the trends of the cybersecurity sector and opt for prevention of attacks in order to effectively secure digital assets.

2,729
participants

65
countries

637
companies

36
partners

66
business program events

102
speakers

Panel discussions

Opening plenary session

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

The future of Russia and the whole world is tied to the digital economy and the processes of global digital transformation.

This new economy is experiencing a serious shortage of cybersecurity experts and the international community understands the need to fill this gap.

Telecommunications is a global industry which directly influences the development of the Internet; therefore, businesses and governments ought to unite efforts in providing security in this sector.

The growth and sophistication of cyberthreats are linked to the latest technological developments making cybersecurity one of the key strategic factors in ensuring a state's well-being.

The main challenges for global cybersecurity:

- *manpower capacity building,*
- *development of related technologies and cooperation,*
- *exchange of data on threats,*
- *critical infrastructure security,*
- *elaboration of international standards and rules.*

98%

*Internet proliferation level that Russia is expected to reach by 2024**

~3 million

*cybersecurity specialists are in demand by the world community today***

* Konstantin Noskov.
** Hans-Wilhelm Dünn.

Panel session

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 the 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

Cybersecurity is a serious challenge and a significant problem, the solution of which foresees development of public-private partnership. It is not only the governments that should cooperate, but law enforcement agencies of various countries as well. For example, international courts need help to elaborate clear, open standards of evidence assessment and to combat adulteration of electronic evidence.

Heads of multinational technological corporations call on the states and international regulators for more active participation in global cyberspace management. There is an urgent necessity to tailor international rules and standards, and to create a single regulatory body.

Over the past several years, criminals have been attacking not only companies and private individuals, but also socially significant facilities. Preventive measures and experience-based opportunities are needed, to foresee threats and create strong mechanisms of informational exchange.

Fighting 'internet offshores' requires mutual efforts: criminals have to understand that they cannot avoid responsibility by changing the domain as they are still breaking international laws by committing cybercrime.

62%

*of countries have no cybersecurity strategy in place**

5x

*growth in attacks on state and private assets observed in Spain in 2014–2018**

* Alberto Hernández Moreno.

Panel session

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 security of the financial sector is on top of the agenda. 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 mitigate 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

Traditional strategies in providing cybersecurity fail to protect against targeted attacks. The players in the financial sector need to develop new methods of protection and collaborate with other institutions — both private and state.

One of the key trends in cybersecurity is to focus on forecasting threats and predicting attacks.

Client protection is an issue of utmost importance for financial organizations. It is solved by means of increasing the level of staff's cyber competence, constant exchange of data and experience, use of neural networks, directing more resources to cybersecurity.

In the face of a common threat, it is necessary to unite the efforts for banking organizations, specifically, to help and support smaller banks, and to develop information exchange between all players.

Collaboration is now the key word in providing cybersecurity.

70%

*of all cybercrime is committed in the financial sector**

4 billion

*cyberattacks have been recorded in Russia over the past year**

$2 trillion

potential damage from cyberattacks in the financial sector

Only 7%

*of all IT expenses are related to cybersecurity**

* Mikhail Alekseev.

Panel session

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 prevent 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 of Information Technology, Saudi Aramco

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

Igor Lyapunov
Vice President for Information Security, Rostelecom

Lothar Renner
Managing Director Cybersecurity EMEAR, Cisco

Igor Milashevskiy
CEO, GLONASS

Providing security for critical infrastructure at the very least means having an attack-resistant infrastructure control system, building a trusted execution environment within this control system inaccessible to external forces, as well as regular monitoring of the entire perimeter.

Critical infrastructure security has two main characteristics:

- *The attack objective is to gain access to the management and control systems of various processes in a company (including technological ones). In this case the attack is developing quite slowly, the criminals thoroughly conceal their actions at every stage. The only way of revealing such breaches is to constantly monitor the information systems and identify anomalies and deviations.*
- *Objects in need of security may vary: management systems of communication network, production, energy, etc. The key feature of each system is reliability, but all of them have different architectures, and this complicates the establishment and observance of security requirements.*

Cyberspace is borderless; therefore, effective security here is impossible without effective collaboration during which partners will jointly process data, look for threats, and patch vulnerabilities. All this needs to be taken into account when elaborating strategies on upgrading critical infrastructure production cycles and creating new solutions.

90%

*of international companies are ready to cooperate with vendors in sharing their data on cyberthreats**

14%

*of all cyberattacks specifically target critical infrastructure***

* Lothar Renner.
** Igor Lyapunov.

Panel session

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

Alexandr Khanin
CEO, VisionLabs

Gyorgy Racz
Director, Security Systems, IBM Europe

Success in fighting cybercriminals mainly depends on the possibility to quickly identify an attack. To do this we need technologies, including those utilising artificial intelligence, that will help to quickly spot and respond to a breach.

A user is the weakest link in the chain of providing cybersecurity to the company and its clients. In 2019 over 80% of attacks on bank clients have been performed with the use of social engineering. If previously, criminals targeted mainly senior citizens, in 2019 the focus shifted to 25-30-year-olds.

3 months

*on average to identify a cyberattack**

23%

*of all attacks in 2018 targeted private individuals***

The educational system is not keeping up with the development of technologies and should, therefore, interact with the business sector, as it is the corporations that accumulate cutting-edge knowledge and experience.

The following trends can clearly be seen in the field of cybersecurity technologies:

- *increase in the number of business challenges that can be solved with the help of AI (e.g. computer vision);*
- *erasing borders between the online and the offline worlds (e.g. digital ID);*
- *focus on 'frictionless' technologies — maximum services with minimum resources.*

* Dhanya Thakkar.
** Sergey Plugotarenko.

Panel session

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. These technologies are constantly evolving, providing better speeds and new opportunities for us to enjoy, and for cybercriminals to take advantage of. Are we able to protect the users without slowing down the technological evolution?

Moderator

Boris Glazkov
Vice President for Strategic Initiatives, Rostelecom

Speakers

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

Yogesh Malik
Chief Technology Officer, VEON

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

Modernisation of telecommunications is the development of digitalisation, introduction of big data processing, including the use of AI. All this brings changes to the model of threats. Previously criminals targeted the network itself, then it was users' personal data, now it is digital assets that are under threat.

Telecom providers are working simultaneously now with 2G, 3G, 4G and 5G networks, which makes it impossible to elaborate unified requirements for their security and considerably complicates the task of protecting each network type.

Users' cyberliteracy is still at a quite low level, so providers regularly send notifications on infected devices and fraudulent links, block dangerous resources.

500 million

*fraudulent clickbaits blocked annually by telecom operators**

50%

*of users follow recommendations of telecom providers to install antivirus programs**

5G

is a standard of mobile communication intended for widespread use not only by people but smart devices also

* Valery Shorzhin.

Panel session

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

The P2P service (money transfer from card to card), with all its obvious advantages, has a number of bottlenecks:

- *in case of an erroneous transfer, the money can be debited back from the receiving party at any time;*
- *the payer's bank does not know the beneficiary, so it is difficult to verify the legitimacy of the receiving party.*

Technical means of protecting information is the main way to preserve data in its integrity. But in the case of instant payments services there are nuances associated with the need to maintain business continuity. Hence, implementing protection resources for technology, which is critical in terms of time, is a very difficult task altogether.

The most important challenging factor in the implementation of P2P services is the unification of rules. This issue can be resolved by creating regulatory documentation, which would establish common market approaches to the use of information security tools and antifraud operations.

30 systems

of P2P payments are currently in use, 20 more are standing by for launch

Panel session

AI technologies in cybersecurity

Moderator

Alexander Vedyakhin
First Deputy Chairman of the Executive Board, Sberbank

Speakers

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

Igor Lyapunov
Vice President for 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

People can no longer cope with the growing volumes of cyberthreats — artificial intelligence (AI) may help.

Application of AI in cybersecurity covers tasks related to analyzing the behavior of users or systems and identifying deviations from a given pattern. For example, AI is used in fraud monitoring systems that allow you to detect and block fraudulent transactions based on data from such analysis.

The AI can easily be weaponized for attack in the hands of a threat actor. Striking a balance between the desire to delegate authority to AI and the fear of increasing system vulnerability is one of the key cybersecurity challenges.

The potential of AI in cybersecurity is yet to be uncovered: relevant patterns of attacks are necessary for effective machine learning, but today only a few of them are suited for this purpose.

14-second

*intervals between cyberattacks**

6%

*monthly growth of social engineering attacks in 2019**

$1.5 trillion

*losses to the global economy from cyberattacks in 2018**

* Alexander Vedyakhin.

Briefing

Cyber Polygon — summarizing the results

The briefing was 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

Cyber Polygon — online training for international business cooperation in the fight against digital threats. The aim of the training is to define new and revise the old ways of detecting cyber incidents, responding and mitigating attacks, as well as improving technical and organisational forms of cooperation.

Cyber Polygon involved several common types of attacks being simulated on the training infrastructures of the participating organisations, and the audience were able to follow the progress of their progress via a live online stream.

Cyber Polygon enacted scenarios of massive DDoS attacks, web injections and phishing. Initially, participants were fending off attacks singlehandedly, and then with the help of the data exchange platform. After connecting to it, the work efficiency increased 7-fold.

Such trainings demonstrate the effectiveness of international public-private cooperation, assist in building competent processes for this interaction, as well as involve a growing number of specialists in the process.

12 million

*live stream spectators**

24 countries

*around the world tuned into the Cyber Polygon live stream**

234

companies followed the event

Participants

Blue Team

Red Team

7 times

*increase in security efficiency with the use of information exchange platform***

* Stanislav Kuznetsov.
** Dmitry Samartsev.

Main plenary session

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 technological 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

Dmitry Medvedev

Prime Minister of the Russian Federation

The problem of cybercrime is among the top five global risks in the World Economic Forum rating. The international expert community often puts it even higher than terrorism and environmental problems. All the advantages of digitalization will be leveled out unless we take effective measures to combat cybercrime.

The development of global security standards is an absolute necessity. The first steps have already been taken. At the end of last year, the UN General Assembly adopted a resolution proposed by the Russian Federation on curbing the use of information and communication technologies for criminal purposes and creating a working group on international cybersecurity. We are ready to cooperate, ready to share our knowledge, accumulated experience, and stand up for an equal, fair world order in the digital sphere.

4 billion

*people use the Internet**

5 billion

*people utilise mobile phones**

* Herman Gref.

Cybersecurity should be an integral part of risk management and corporate governance. Given the scale of the threat, this issue will inevitably go beyond the responsibility of exclusively technical specialists — it is important to take strategic decisions at the level of corporate management.

10 million

*samples of malware appear on the web each month**

65%

of respondents in early 2019 say they were subject to cyberattacks (compared to 40% two years prior)

The digital era opens up immense opportunities, but it also comes with global threats.
It is crucial that everyone be aware of this, from heads of states and companies to ordinary citizens.

In order to provide reliable protection against cyberthreats, besides the introduction of technical measures it is necessary to:

- *create trusted cross-border networks,*
- *improve the digital hygiene of the population,*
- *conduct a total depoliticisation of the digital agenda.*

* Herman Gref.

Topical sessions

Legal environment

The section covered the legal aspects of cybersecurity as well as the issues of international cooperation for legislative pushback against cybercrime.

Thomas Rid

Professor, School of Advanced International Studies,
Johns Hopkins University

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 reflected on recent trends in cyberattack attribution.

Attribution of cyberattacks is comprised of two aspects — a technical problem and that of evidence. A solution for this would require continuous cooperation with various entities and a scrupulous investigation of the case.

The most complex attacks are directed at critical infrastructures. Attributing these attacks is made possible with certain knowledge and skills that only a small number of specialists have. However, thanks to their efforts, it is now possible to recognise criminal actions and identify data leakage.

The quality of attribution depends on the amount of time and resources spent on revealing an incident as well as on how well the perpetrators of the attack are hiding. The context of a cyberattack, too, plays an important role: sometimes it is possible to correlate the attack with a certain external event that may assist incident investigation.

Greg Rudd
CEO, CREST Australia & New Zealand

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 a number of 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 on an international legally binding treaty for Cyber. If we don't work together, it won't happen.

In order to fight cybercrime, we need global state institutions and independent organisations that will apply and enforce international legislation on cybersecurity, set standards for attack attribution and define the punishment for criminals.

37.5%

of all online traffic was subject to cyberattacks in 2018

Globally there are:

> 5 billion
mobile users

> 4 billion
Internet users

> 3 billion
social network users

The current situation with the legislation is complicated due to the fact that not all countries consider hacking a crime. Differences in culture, mentality and strategic priorities make elaboration of international norms even more painstaking. However, initiation of such laws will become the next serious step towards gaining victory over cybercrime.

Bruce W. McConnell
Executive Vice President, EastWest Institute

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 outlined a proposed enforcement regime to improve security and stability in cyberspace.

Organisations like Global Commission on the Stability of Cyberspace (GCSC) are put in place to control standards of conduct in the digital sphere and the use of cyber tools. The mission of GCSC is to support decisions that may benefit security and stability in cyberspace.

By increasing the cost of cyberattacks, companies make them unfeasible for criminals. This can be achieved the following way:

- *scan clients' devices and require to improve their security;*
- *send notifications to the hostings utilised by the criminals;*
- *distribute evidence of cyberattack attribution;*
- *block any traffic coming from the attackers.*

Such procedures within organisations could, however, lead to the increased cost of their services and risks to reputation. Cooperation with states in these issues will help to minimise the scale of negative consequences.

GCSC

Global Commission on the Stability of Cyberspace is an international organisation to control the behavior in cyberspace

Among the countries of GCSC are Russia, the USA, the UK, Brazil, China, Estonia, France, Germany, India, Israel, Japan, Malaysia, the Netherlands, Nigeria, Singapore, South Africa

Rafael Maman

Partner in Cybersecurity and Digital Strategies, PwC Israel

Ensuring cybersecurity of critical infrastructure

Rafael Maman made 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.

In order to provide security to critical infrastructure, it is necessary to build a complex cybersecurity strategy at the state level, define national centres for cybersecurity (e.g., CERT), as well as elaborate methods and tools to manage the proposed measures. Allotting more attention to technological tools at the operational level is absolutely essential. This includes monitoring IT infrastructure of organisations, introducing recognition technologies in industrial IoT networks, creating special laboratories.

One of the foremost conditions of successful infrastructure protection is grounded legislation. A study carried out in Israel analysed the cyberspace standards of other countries, unifying them and creating a set of regulatory norms based on their findings. This process took a long time and was not an easy endeavour, but the results were indeed successful.

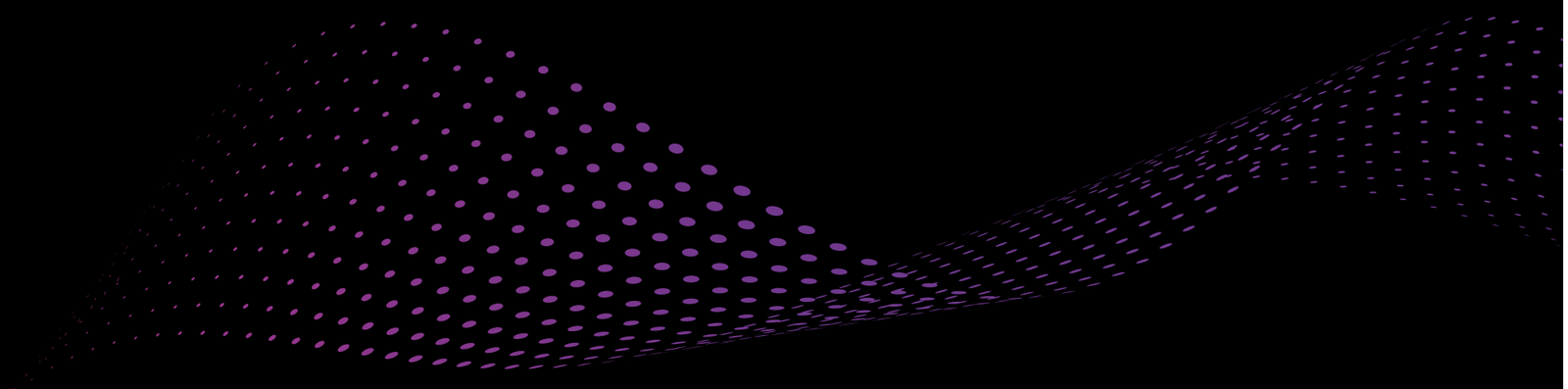
Israel is spearheading the creation of laboratories for testing and control of industrial systems, which gives all entities, from operators of critical infrastructure to research officers, state authorities and technology providers, the opportunity to carry out testing before system commissioning.

1982

the year of the first ever recorded cyberattack on critical infrastructure — according to expert opinion

Capacity building

The section focused 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 to better address cybercrime.



Guido Gluschke

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

Cybersecurity education in the nuclear and energy sector

Guido Gluschke gave 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 also addressed faculty engagement within the energy sector.

One of the most essential issues in cybersecurity is protection of nuclear power facilities from digital threats. IAEA started a course on cybersecurity in Brandenburg University of Applied Sciences in 2012 to train specialists in this field.

The students learn both nuclear and computer security management and international law. This is a distance learning course as IAEA aims to enrol people from as many countries as possible.

Practical exercises are an important component of cybersecurity curriculums. Normally these are large-scale events and it may take a whole year to prepare for them. NATO was among the first organisations to hold a cyber exercise of this kind.

When discussing cybersecurity issues at the international level one has to consider and overcome national and cultural differences. Supranational regulators are required to introduce a definitive glossary on cybersecurity and to resolve issues linked with the lack of or an altogether different interpretation of certain notions across various languages.

Yuval Elovici

Director of the Telekom Innovation Laboratories,
Associate Professor at the Department of Information
Systems Engineering, Ben-Gurion University of the Negev

Building a global cyber ecosystem: the role of the academia

Most experts agree that in order to establish a thriving cybersecurity ecosystem, a well-coordinated interaction between the following components is essential: corporate, military and academia, as well as support of startups and presence of investors. Yuval Elovici gave a detailed analysis of the contribution of the academia to such ecosystems, using real-world examples and case studies.

Ben-Gurion University of the Negev pays special attention to the fusion of AI and cybersecurity, specifically the potential capabilities of AI in security technologies and in studying cybercriminal methods. So far, the researchers have been focused on three directions:

- *protection against incidents (detection of attacks and unauthorised access);*
- *performing complex operations on hacking and intrusion;*
- *modification of input data aimed to mislead the AI protecting the system.*

Israel is one of the leading countries in introducing innovations in cybersecurity. The state creates research centres where the academia is congruent with the development of innovative technologies, which are then immediately tested by Israeli police.

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

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.

Today the educational process is geared towards fast practical training. If the goal is to teach how to develop secured software, the students are practically trained to search for and patch vulnerabilities.

The necessary knowledge and skills are acquired at universities by means of learning, working and playing. Each week, the students learn something new about cybersecurity and then verify the gained knowledge in game form: over the weekends ethical hacking competitions such as Capture The Flag (CTF) take place.

The MSU Cyberschool project is due to be launched this year: talented senior high school students will be gathered in teams, taught how to play and thus be motivated for further learning.

120

students enrol for the course on computer systems security at Lomonosov Moscow State University (MSU) and Higher School of Economics University

~100%

of students begin working in the cybersecurity sphere after practical education

6 times

growth of the number of students in cybersecurity in MSU since 2010

Security is fun

the motto to inspire students to take up information security

Threat intelligence

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

ICC International Cybersecurity Congress | SBERBANK

Evgeny Voloshin
Chief Expert Services Officer, BI.ZONE

Customer is not always right

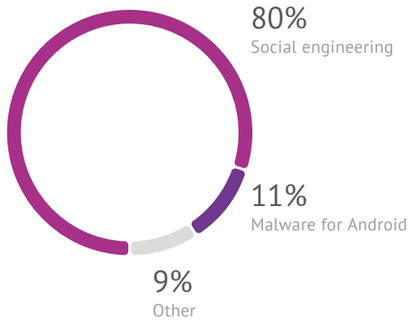
Evgeny Voloshin talked about the evolution of cyberattacks, the shifting focus from complex technological scenarios to socio-technical ones, as well as a qualitative change in the approach to social engineering.

Implementation of state and private initiatives on exchange of information on latest threats has allowed for a 10-fold decrease in financial losses incurred by banks.

In 2018 the number of thefts from ATMs decreased by 40% — today the attacks are implemented mainly via digital channels.

In 2019 the vector of cyberattacks has changed fundamentally: previously they were aimed at banks and commercial organisations, now — at private individuals. Criminals count on a variety of social engineering tactics: calls, polling, frauds in loyalty programs.

Attacks on bank clients



7,400

mobile devices in Russia are infected by malware every week

~$1.1 million

were stolen from Russian banks in 2018, and this figure is several-fold less than that of the year before

Bank management understands the importance of applying preventive measures when building up corporate cybersecurity, i.e. analysis of attack scenarios, exchange of indicators of compromise, exposure of criminals' phone numbers and card details at regional, national and sectoral levels.

78%

of Russians use banking services via mobile applications

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

Evolution of targeted attacks on the financial sector

Based on the attacks of Lazarus cybergang.

The main fraud method used by the Lazarus gang is a specifically designed trojan, a tool for data collection. Previously, the trojan only performed reconnaissance — collected data, based on which a decision was made whether or not to attack a specific computer. However, in order to carry out the attack, another program was used. In June 2017 this trojan was rewritten on PowerShell, and in July 2018 — for macOS. In May 2019 this trojan was rewritten to produce a newer version.

Over the past six months Lazarus has made considerable renewals and upgrades to its toolkit. In order to fight off such attacks it is necessary:

- *to protect not only email and web traffic but also the employees with legitimate access to social networks;*
- *to provide control of data integrity on bank computers as Lazarus often destroys critical data after a successful operation using various encryption programs;*
- *to be aware that criminals utilise opensource solutions like PowerShell Empire, MetaSploit, CobaltStrike and have rewritten all their tools (not only a certain trojan) in PowerShell.*

Timur Biyachuev
Vice President Threat Research, Kaspersky Lab

Advanced threat trends

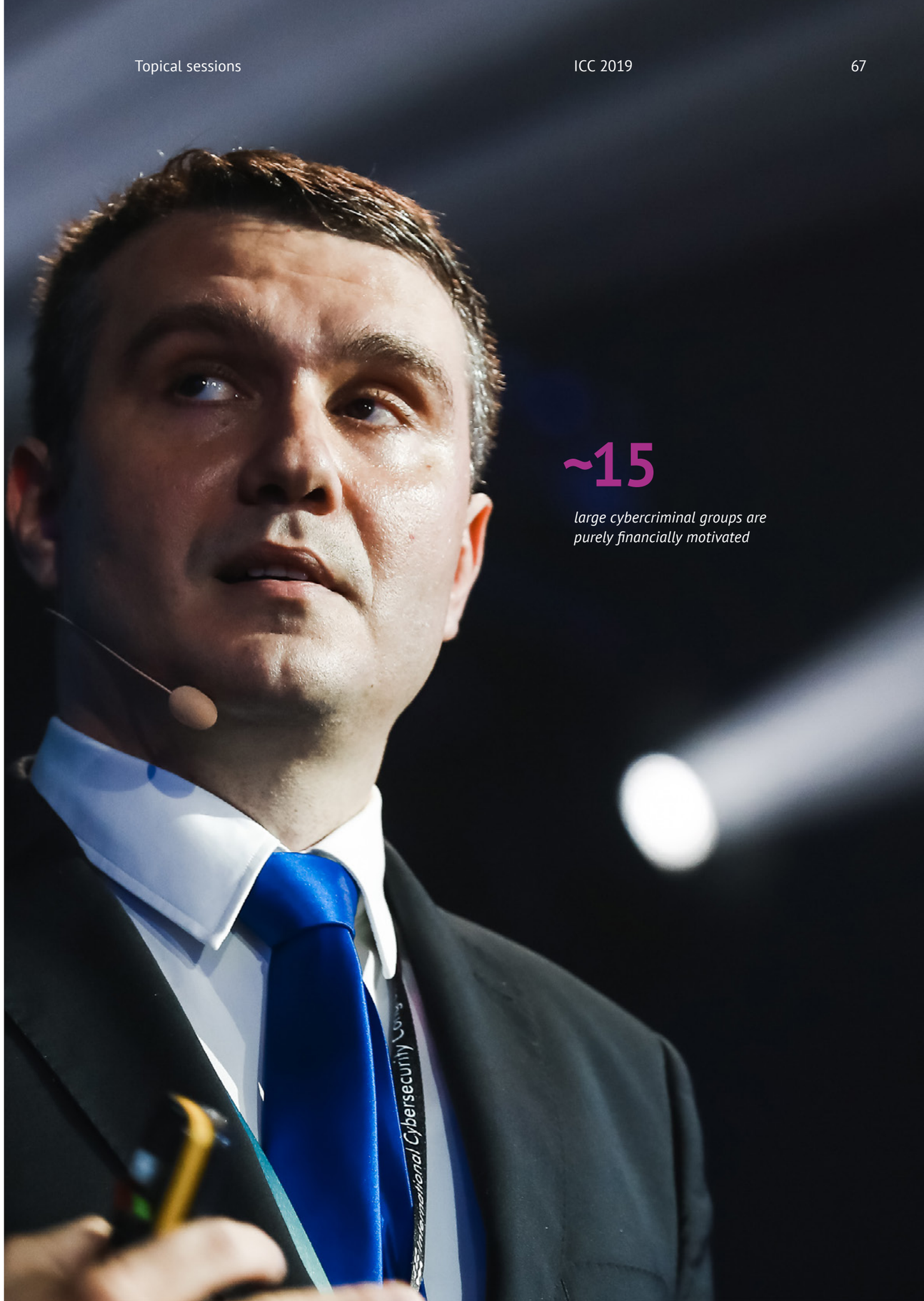
The following sectors are attacked most often:

- *financial,*
- *telecommunication,*
- *industry (mining, nuclear, aerospace),*
- *media,*
- *government,*
- *military,*
- *intelligence services.*

Among the latest trends are supply chain attacks and network equipment attacks. The former is a serious problem for large entities: they rely on regular updates of hundreds of specialised software programs that run the risk of being embedded with malware. Attacks of the latter type are equally dangerous as it is impossible to install any sort of antivirus or protection on the network equipment and the process of upgrading this software is not as easy as it is with ordinary computers.

The number of cybercriminal groups is perpetually growing, and their methods are being continuously advanced. Last year saw the arrests of several group leaders. However, instead of disbanding, the groups have splintered off into smaller ones and started exploring new opportunities and tools for mischief.

Security can be ensured by end-to-end systems with forecasting, prevention (including threat intelligence reports), detection, and quick response.



~15

large cybercriminal groups are purely financially motivated

Alexey Novikov
Director of Expert Security Center, Positive Technologies

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 18 months? 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?

Boring incidents, which arise due to basic deficiencies within the infrastructure, are very brief and employ automated open source tools. These are often ignored by businesses.

Average incidents lead to a full system compromise, the toolkits in these cases are used manually. Businesses usually turn to law enforcement for investigation.

Very interesting incidents, otherwise known as APT attacks, are always targeted, meticulously planned and, as often the case, successful. Such attack campaigns are aimed at gaining total and longest possible control over the infrastructure.

How can one tackle APT attacks and fend off criminals?

- *share information on the actions of criminals and effective countermeasures;*
- *know the infrastructure of the company and its protection mechanisms inside out;*
- *perform full-scale investigation of incidents, do not focus on simply curing the symptoms;*
- *give a definitive classification to incidents;*
- *build a cybersecurity system capable of withstanding all modern challenges.*

* Advanced persistent threat.

18%
boring incidents for investigation

10%
average incidents for investigation

72%
very interesting incidents

43%
of attacks in the I quarter of 2019 have been specifically targeted

Jonathan Fischbein
Head of Technical Marketing, Check Point

Predicting 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.

When analysing cyberthreats, one usually studies motives, methods and objects of the attacks.

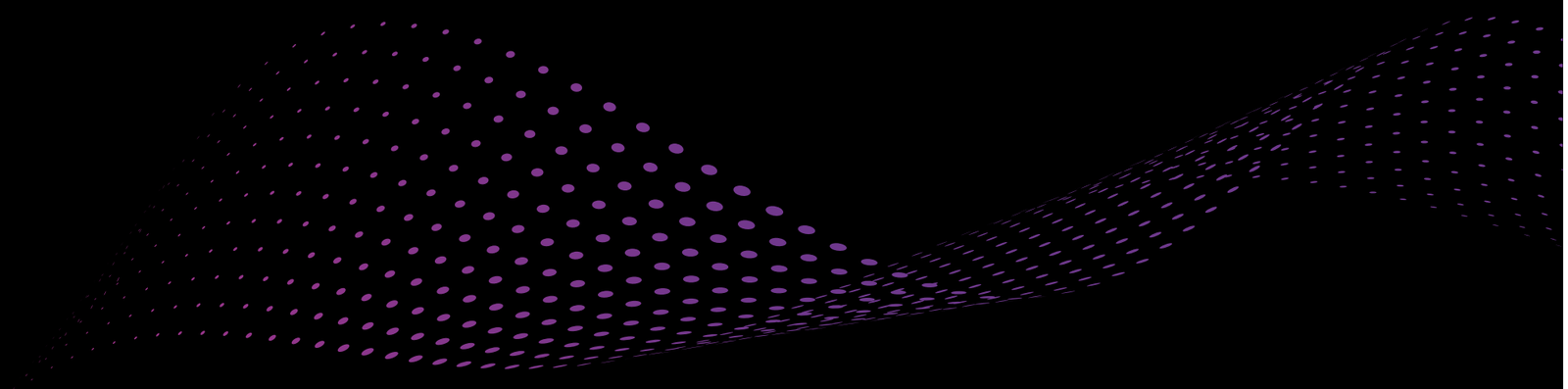
Most intrusions are aimed at stealing monetary assets, getting access to information, damaging or strengthening political and commercial influence. In 2019–2020 the main motive will still be money, but it is expected that the number of attacks seeking to gain influence will likewise be on the rise.

The main methods in use by the criminals include distribution of bank malware and ransomware as well as cryptojacking, which means utilising a device for cryptocurrency mining without its owner being aware of it. In 2019 these trends are likely to continue, and the number of criminals will skew upward.

Targets of attacks are mainly personal computers, networks, applications, mobile devices and cloud storage. For 2019 the main entry points are IoT devices; we can expect more thefts from electronic wallets; and witness the first attempts of manipulating AI systems.

Disruptive technologies

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



Clemens Dannheim
CEO, Objective Software

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. Car group executives need to learn to recognise these issues and take into account the security risks, arising on the way towards the bright future.

Production companies that used to deliver only hardware for vehicles are now becoming software developers, both for manned and unmanned vehicles.

Systems of autonomous driving shall include:

- *exact positioning,*
- *detailed environment simulation,*
- *forecasting and decision-making on the choice of trajectory,*
- *connection to cloud storage for receiving necessary information,*
- *access to banking services.*

MBUX (Mercedes-Benz User Experience)

is a platform with some AI elements, 'over-the-air' updating and self-learning, developed by Daimler company group

Unmanned vehicles will be connected to the general network that will allow the exchange of data. This situation gives rise to certain risks and, with it, the necessity to protect the communication channels between vehicles in order to ensure their cybersecurity.

Sergey Lebed
Chief Information Security Officer, Sberbank

Cybersecurity in digital chaos

There are two approaches to ensuring security: the first one is based on security system requirements, the second – on risk management.

When security solutions are introduced, unique business features or some IT infrastructure characteristics are often ignored which results in ineffective protection: the company has everything from resources to staff, however the security level remains low. To adequately address this problem, security must take into account the particular features of an organisation and leverage the synergy between security and IT technologies.

Cybersecurity maturity level cannot be higher than that of IT. Basic IT processes are fundamental for effective management systems, both of IT infrastructure and of cybersecurity.

There are essentially two ITSM processes, without which it is impossible to instill any order into IT companies. These are: asset management and change management.

In the modern world of cyberthreats, where the attacker almost always comes out a winner, an approach to cybersecurity management is all the more eagerly sought, an approach where cyber resilience takes central stage.

3 billion

cyber incidents happened in the course of 2018

2 million

cybersecurity specialists in deficit across the globe

66 days

average recovery period after an attack

8.5 thousand

RFC standards regulate compatibility and interaction on the web

Anton Okoshkin
Chief Technical Officer, BI.ZONE

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.

Digital and physical realities are almost integral. This also refers to security: all-round introduction of IoT devices and digitalisation of various processes significantly broaden the landscape of prospective risks. Telephones, laptops, accounts in social networks, mail servers and forums, our environment (office, home, airports, hotels, transport, restaurants) — the number of threats in such a complex system is near infinite.

To protect the employees it is necessary to keep them informed, increase their level of cybersecurity awareness, analyse digital footprint data and the environment related to their device activity.

The cyberrisks posed by staff are direct risks to the company, and like any other risk, they, too, need to be measured and taken into account when assessing the level of company's cybersecurity.

4 seconds

the time interval for new samples of malware to emerge

$7

the cost of hiding a malware sample from most common antiviruses in the darknet

563 million

user accounts were compromised as a result of only 3 leaks in 2018

Ivan Novikov
CEO, Wallarm

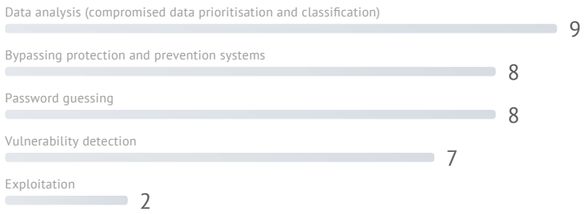
Machine learning on the other side of cybersecurity barricades

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

Machine learning technologies are one of the aspects of the AI and can be used both for ensuring cybersecurity and for hacking.

On the one hand, machine learning helps to reveal attacks, deviations, vulnerabilities as well as to analyse and prioritise risks. On the other hand, it can be used to evade protection, reveal and exploit vulnerabilities, mine passwords, prioritise and classify compromised data.

The state of machine learning for cyberattacks (rated 0–10 on feasibility):



9–10 points — production-ready tools with more proven results than other algorithms
7–8 points — practical results and tools, applicable for common use cases
5–6 points — practical results, inapplicable in common practice
3–4 points — less than 5 researches on the field of study
0–2 points — less than 2 researches on the field of study

Cognitive science

is an interdisciplinary sphere uniting philosophy, linguistics, anthropology, neurobiology, psychology and AI theory

Kirill Kertsenbaum
Head of Sales, Symantec Russia

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.

The adaptive security architecture includes 4 obligatory stages:*

- *attack prediction,*
- *prevention,*
- *detection,*
- *response.*

Some companies hedge their bets on prevention, others on detection. But only prediction allows companies to provide a high level of cybersecurity without increasing expenses on protection — this can only be achieved through optimisation of processes and analysis of available data.

In order to build a prediction system, it is necessary to change the format of data storage and processing. An approach referred to as 'data lake' is a clear-cut solution to this issue, where:

- *the main data set comes from own protection assets;*
- *mechanisms of statistical analysis process the events collected by telemetry;*
- *the system gives a statistical model of a user's median behaviour as well as quantity and criticality of deviations, and also performs regressive analysis.*

In the end, a system with a minimum of false positives would be able to identify an incident and make an independent decision with regards to it.

250

*various techniques are used by cybercriminals to prepare and carry out an attack***

70

of them (the majority) are developed to evade means of protection

14

(the smallest share) accounts to use access gaining techniques

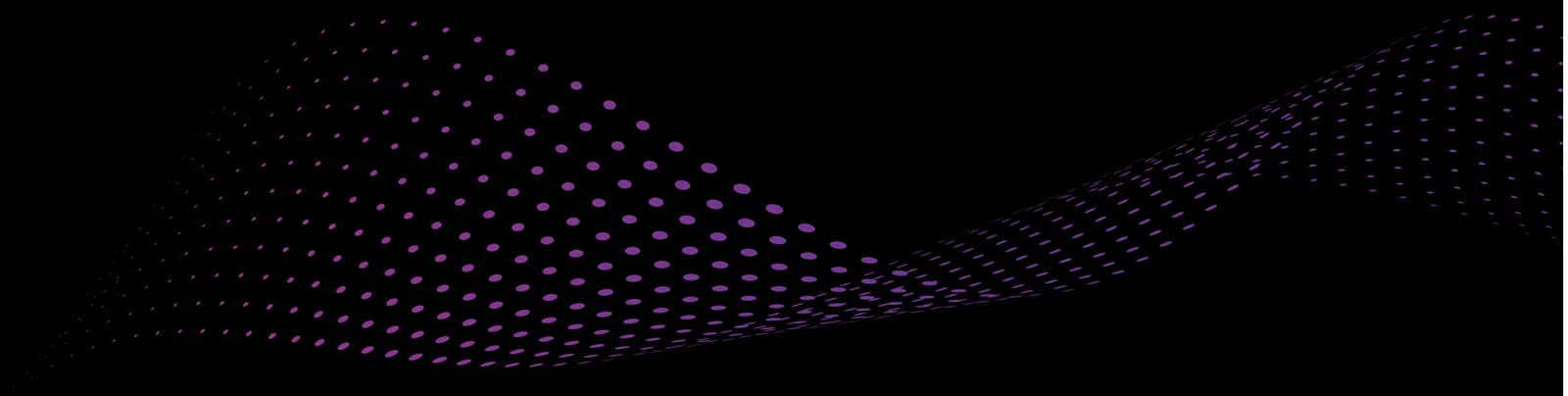
12 stages of an attack***

1. *Initial access*
2. *Execution*
3. *Persistence*
4. *Privilege escalation*
5. *Defense evasion*
6. *Credential access (account manipulation)*
7. *Data discovery*
8. *Lateral movement*
9. *Data collection*
10. *Data exfiltration*
11. *Command and control of infected infrastructure*
12. *Exposure*

* Developed by Gartner.
** Data of MITRE.
*** Classification of MITRE.

Investments in cybersecurity

The section explored the issues of investing in the cybersecurity industry, as well as key points for developing innovations in this area.



Ben Banerjee
Board Member, InnMind

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?

Cybersecurity is one of the key issues and main challenges of the digital era. Like in many other spheres, preventive measures in protection against cyberthreats turn out to be more efficient than dealing with the consequences of an attack. However, this requires considerable investments.

The most active investors in cybersecurity are tech corporations, financial companies and state entities. Notably, banks and state organisations generally have less strict limitations on the expenses for cybersecurity as they understand the scale of the danger.

Investing in cybersecurity is similar to investments in any other sphere. The only difference for investors is the way the end users perceive cyberthreats. If they do not see the risks and ignore the necessity behind a specialised product, they will refrain from spending their money on it.

35 times

market growth over the period of 13 years

$120 billion

was the size of the cybersecurity market in 2017

Vasily Belov
CEO, Skolkovo Ventures

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 spoke about the main trends and investment opportunities in the industry.

Investments in cybersecurity are one of the fastest-growing sectors of the venture market. Today it is driven by big data and AI projects.

First of all, the companies invest in security of cloud applications and IT infrastructure (industrial IoT, critical infrastructure).

Apart from big players, there are also non-strategic customers in this sphere, mostly banks. In 2018 the total volume of mergers was valued at $23 billion.

Venture transactions settled on the Russian market are also starting to draw the attention of analysts.

Was invested in cybersecurity in 2018
$6 billion

The annual growth of Russian venture market
~$ 0.4 billion

25%

average growth of investments into cybersecurity in 2018

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

Innopolis — special economic zone

Cybersecurity is one of the key areas of Innopolis staff training. The Innopolis University provides education for future cybersecurity specialists, many residents are engaged in the issues of protection addressing cyberthreats.

A French company Schneider Electric is known as a manufacturer of electronic components, but in Innopolis it works on digital twins (a digital copy of a facility or a process, created for collection and repeated use of the information about it). This technology allows not only to increase efficiency of a physical facility but also to improve its cybersecurity: protection mechanisms need to be introduced at the stage of system design (secure-by-design), and the twin helps to do it most skilfully.

Japanese Soramitsu is developing its own type of blockchain protocol for systems of digital asset transfer. Distributed ledger is one of the ways to provide security-by-default (secure-by-default — a way of initial system set-up in which its security is the main priority).

Russian UNITS specialises in innovative secured data storage and innovative exchange solutions, and tests its products in the USA, Canada and Eastern Europe.

2015
year founded

80
resident companies

2,000
work places

500
vacancies from partners

2 vacancies
per specialist

Oleg Glebov
Business Development Executive, Speech Technology Centre

Biometrics in cybersecurity as an investment opportunity

By 2022, 70% of large companies 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 talked 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.

Voice control of phones and other devices, voice and face recognition in banks are the spheres where biometrics is already being applied. Such identification is easier, more convenient and more secure in some respects.

In the nearest time the 'conversation UI' feature will be implemented in IT systems, being a technology of interaction through dialog boxes between the user and the computer. It will be a dialogue between human and machine in a language comprehensible to the human user.

The biometrics market is quite new but very promising and is growing fast. It is of considerable interest for companies dealing with cybersecurity.

Three main directions where biometrics will be applied:

- *identification and authentication during access to certain systems;*
- *identification of employees (data collection, search for insiders, verification of violations by staff);*
- *new types of interfaces — voice interaction with systems, chat bots.*

Biometrics security is needed not only for businesses but for individual users, as well. Today, physical security and cybersecurity — be it video surveillance, voice monitoring, protection against malware — are detached from one another and are being implemented on different silos, but soon these types of threats will become merged.

50%

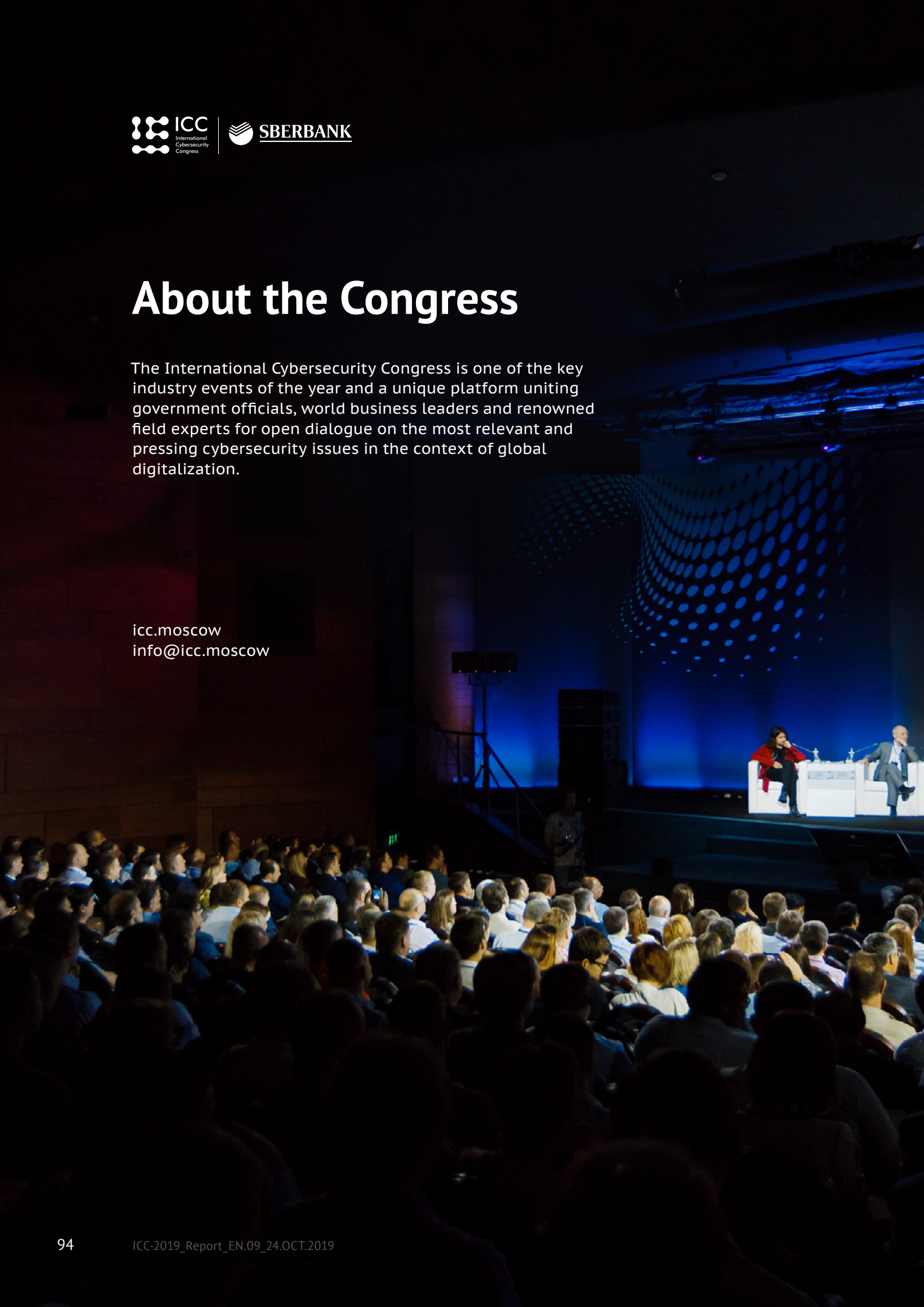
of all Internet searches by the end of 2020 will be either automatic or voiced, but not typed

30%

of all requests will come from no-screen devices, i.e. devices with voice control only

About the Congress

The International Cybersecurity Congress is one of the key industry events of the year and a unique platform uniting government officials, world business leaders and renowned field experts for open dialogue on the most relevant and pressing cybersecurity issues in the context of global digitalization.



icc.moscow
info@icc.moscow