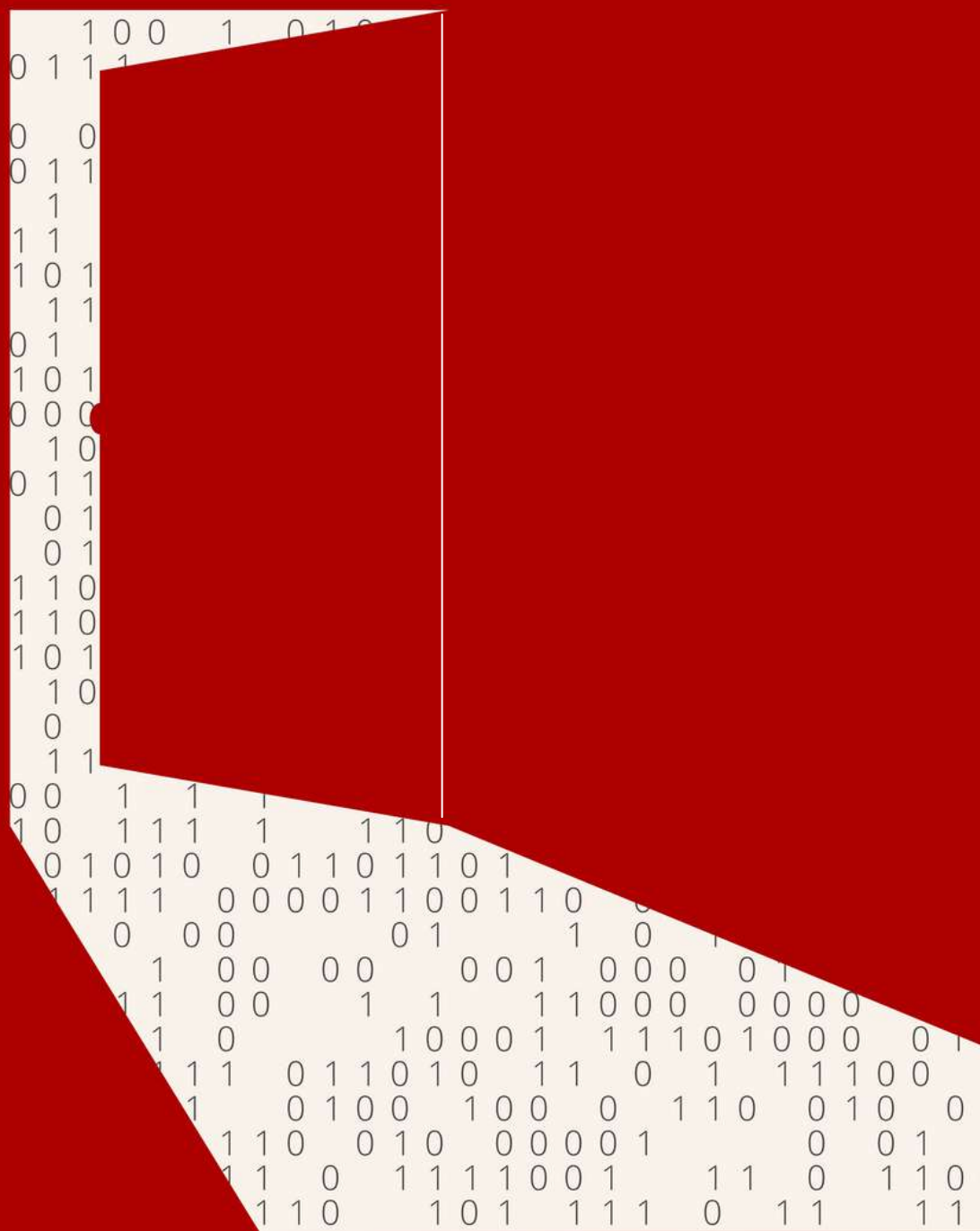


EXTRACT FROM THE  
***ASTANA CLUB***  
TOP 10 RISKS FOR  
***EURASIA 2021***



# RISK 8

## GLOBAL CYBER CRISIS



Source: Shutterstock  
Author: Serg001

## GLOBAL CYBER CRISIS

**8**  
**RISK**

The COVID-19 pandemic has given an unprecedented impetus to the global digitalization process. During the periods of total lockdown, digital space made it possible to preserve the functionality of the global economy, but at the same time, it significantly increased its dependence on processes in the virtual sphere.

As is known, addiction breeds vulnerability. During the pandemic, the massive digital transition led to a parallel increase in cyber threats. This dangerous trend is superimposed on the problem of the absence of any generally accepted rules of conduct between states in global cyberspace.

As a result, in 2021 the world may for the first time face a global cyber crisis.

### THE BEGINNING OF A CYBER PANDEMIC?

The incident with the Sunburst virus hacker attack, which became known in mid-December 2020, showed the potential scale of modern cybersecurity threats.

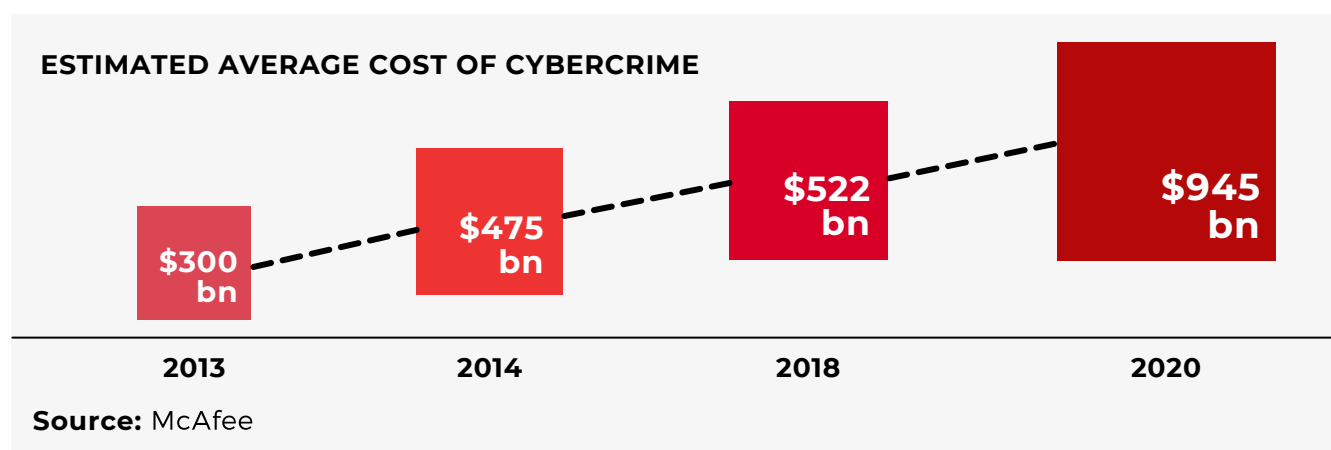
As a result of the hacker attack, which has already been referred to as "the largest in the history of the United States," more than 40 key government

agencies in America were affected, including the Department of Commerce and Energy, the US Department of State, and a number of important research centers.

The hackers did not act directly by attacking US government facilities, but through the so-called "supply chain" of software provided by SolarWinds. As a result of the hacker attack, about 18,000 of the company's customers were affected, 80% of which are located in the United States.

In general, the active transition to the online sphere during the pandemic has spurred an unprecedented increase in cyber incidents around the world. For example, in April 2020, the US FBI reported a 400% increase in cyberattacks compared to the pre-pandemic period and the increase in the number of cyberattacks in the United States already, amounted to 800% in May. Similarly alarming statistics were provided by Interpol, which identified more than 200,000 incidents in 80 countries in May 2020.

In recent years, there has been a steady upward trend in financial damage from cyberattacks on a global scale. The pandemic has exacerbated this trend significantly. Thus, according to the report "The Hidden Costs of Cybercrime"



by the Center for Strategic and International Studies (USA, CSIS), global losses from cybercrimes this year may well reach about \$ 1 trillion. The growth in comparison with 2018 is 50%.

Against this backdrop, governments and businesses around the world are forced to devote increasing resources to combat threats in the digital space. According to the consulting company Gartner, Inc., by 2022 the global information security market will have reached a record \$ 170.4 billion.

### **TECHNOLOGICAL DRIVERS OF CYBER THREATS**

Technological advances, especially in the field of new digital technologies, will seriously exacerbate the situation with cyber threats in 2021. In general, the following main group of technologies can be distinguished which will scale risks in cyberspace in the near future.

#### **5G TECHNOLOGY**

The next generation of 5G networks will not only allow faster transmission of huge amounts of digital data, but will also increase the risk of losing this data in cyber attacks. Experts identify the following risks associated with the expansion of 5G networks:

- Moving away from a centralized hardware-based system towards a more fragmented software-based network that is relatively easy to invade.
- Significant expansion of the coverage of potential users of high-speed Internet due to the technological capabilities of networks. A particular risk is posed by the Internet of Things (IoT), which involves the interaction of machines with each other without human intervention.

- Finally, expanding network bandwidth will also create additional opportunities for potential attacks.

#### **ARTIFICIAL INTELLIGENCE (AI)**

The expansion of the use of automated control systems in various fields, including in the military, carries significant security risks. AI technologies can be used by hackers to "autonomously hack" systems.

AI computational algorithms that operate autonomously and with minimal human intervention make it nearly impossible to identify the hackers who initiate an attack. AI will also significantly increase the speed and scale of hacker attacks, thanks to the ability to automatically process a huge amount of data.

#### **QUANTUM COMPUTERS**

Quantum computers, which are significantly superior in computing power to traditional ones, in the opinion of many experts, can become a factor that radically changes the rules of the game.

Quantum computing technologies make it possible to process colossal amounts of data in the shortest possible time, which significantly increases the risks in cyberspace. So, in the future, quantum computers can be used in cryptography for guaranteed breaking of even the most encrypted data.

Despite the fact that today developments in this area are of an experimental nature, experts do not rule out a significant breakthrough in technology within the next 3-5 years.





**Steve Durbin,**  
managing Director of  
the Information  
Security Forum

*The first nation state to develop technologies such as AI, 5G, robotics and quantum computing will gain unparalleled economic, social and military advantage over rivals. It almost goes without saying that, organizations involved in the development of these technologies will become highly enticing targets for nation state-backed espionage.*

### KEY RISK AREAS

In 2021, the following sectors will become the most challenging in terms of cyber security.

#### GOVERNMENT SECTOR

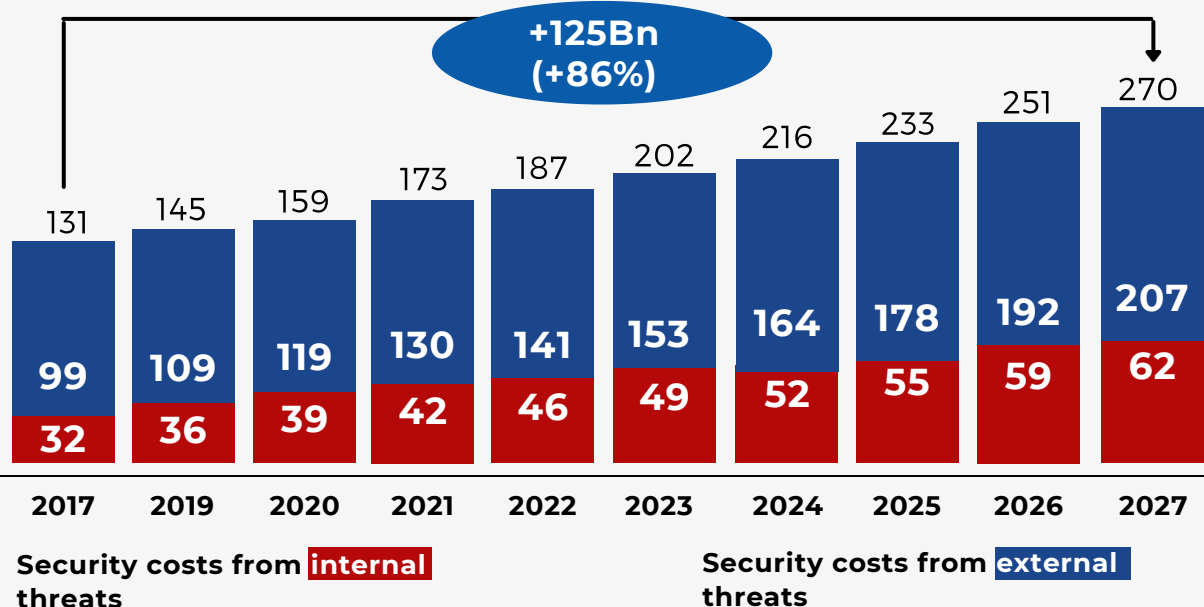
One of the main objects of hacker attacks could be information systems of state institutions, which contain huge amounts of strategic information.

According to some reports, in 2020, government spending on the IT sector reached \$ 438 billion. Thus, particular attention will be paid to the security of strategically important infrastructure such as power grids and transportation systems. A survey of 700 infrastructure professionals in six countries (USA, UK, Germany, Australia, Mexico and Japan) by the Ponemon Institute found that 90% of them have suffered from at least one successful cyberattack in the past two years. For example, the US Cybersecurity and Infrastructure Security Agency (CISA) has identified 16 critical sectors, including the chemical sector, communications sector, dams, nuclear infrastructure, etc. to be at risk.

#### HEALTHCARE SECTOR

Amid the coronavirus pandemic and the growing pressure on the healthcare sector, the scale of hacker attacks in this segment has significantly increased. For example, back in April 2020, WHO representatives reported that hackers had hacked into more than 450 active

### GLOBAL SYBER SECURITY SPEND, \$ BN



Source: Gartner, Australian Bureau of Statistics

e-mail boxes of the structure in order to send false information, as well as to gain access to donations to fight the pandemic.

As the coronavirus crisis develops further, huge funds will be poured into the health sector, which will stimulate the interest of hackers. For example, the 2017 NotPetya virus attack cost the pharmaceutical giant Merck over \$1.3 billion.

#### FINANCIAL SERVICES SECTOR

Despite growing cyber risks, many financial institutions continue to show low readiness for potential hacker attacks. For example, according to Deloitte, financial institutions on average spend only 10% of their IT budget on cybersecurity measures. In early 2020, the Federal Reserve Bank of New York conducted a study on the threat potential of cyberattacks for the US payment systems.



**Tim Maurer**, director of the Cyber Policy Initiative and a senior fellow at the Carnegie Endowment for International Peace

***More must be done to better protect the financial system as the linchpin for the post-pandemic economic recovery against cyber threats. Over the past few years, the G20, the G7, the IMF, and others have launched important initiatives that can serve as a starting point for a more coherent international approach to tackle this collective problem. Yet, the current efforts remain highly fragmented and siloed across government agencies, central banks, and industry without a clear organizing principle or clear division of roles and responsibilities.***

Simulations have shown that a successful cyberattack on only one of the five largest US banks can bring to a halt up to 40% of the country's payment system.

As demand for online financial services continues in 2021, the risks of cyberattacks in the financial sector should be expected to increase globally.

#### THE GEOPOLITICAL DIMENSION OF THE CYBER CRISIS

The rapid development of cyberattack technologies is being pushed by the growing geopolitical competition between key world powers, primarily the United States and China. Against this background, the absence of uniform rules and standards in the system of global cyber governance creates many serious risks and threats.

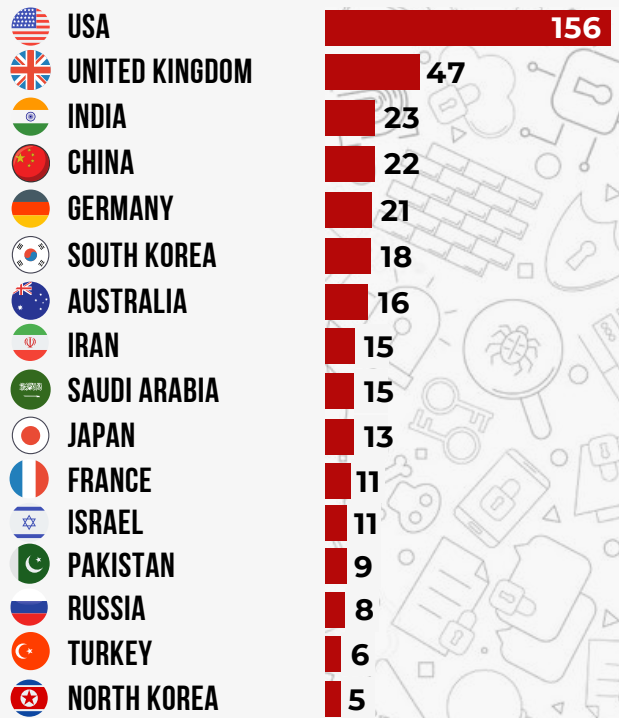
The potential scale of cyberattacks was clearly demonstrated back in 2009, when the computer system of Iran's nuclear program was infected with the Stuxnet virus, the development of which is attributed to the Israeli and US intelligence services. This was the first time a cyberattack caused physical damage to a strategic nuclear infrastructure.

Against the background of increasing geopolitical tensions, the risks of cyber aggression at the state level are significantly increasing, which could at any time transform into a full-fledged military conflict.

The key risk is that cyber warfare is a relatively new phenomenon, and there are a number of difficulties in responding adequately to it:

Firstly, it is often extremely difficult to track down the initiator of an attack and, accordingly, prove that a state is involved in cyber aggression.

**The countries which have experienced "Significant" cyber attacks the most (2006-2020)**



**"Significant" cyber attacks:** on a countries government agencies, defense and high companies equating to a loss of **more than \$1 mln**

**Source:** Global Security Mag

Secondly, the criteria for classifying cyberattacks as an armed attack have not been developed, and universal principles for investigating cyber incidents have not been formed.










Thirdly, cyberattacks are the most effective "asymmetric" option of deterrence, which does not require significant financial costs in comparison with traditional types of weapons.

Thus, the lack of basic rules of conduct in cyber warfare and the low threshold for unleashing it pose significant risks to global security.

At the same time, the cyber capabilities of states for carrying out attacks in the digital sphere are beginning to play the same significant role as traditional military power tools.

As the latest Sunburst incident showed, cybersecurity issues will play an increasingly critical role in the development of relations between Russia and the United States.

**NATIONAL CYBER POWER INDEX 2020**

Country		Overall score	Capability	Intent
USA		50,24	1	2
CHINA		41,27	2	1
UNITED KINGDOM		35,57	3	3
RUSSIA		28,38	10	4
NETHERLANDS		24,18	9	5
FRANCE		23,43	5	11
GERMANY		22,42	4	12
CANADA		21,50	11	9
JAPAN		21,03	8	14

**Source:** Harvard, Belfer Center

The Americans will certainly not leave unanswered what they consider to be a cyberattack from Russia. A retaliatory cyberattack by the Americans could lead to a spiral of confrontation that would have extremely dangerous and poorly predictable consequences.

Another area of growing cyber risks is the Middle East, where large-scale cyber operations can be directed against Iran. Moreover, it cannot be ruled out that Tehran itself initiates cyberattacks against the United States and its allies in the region.

Thus, in 2021, we may well see new cases of the use of cyberweapons on an even larger scale than before, which can provoke a full-fledged military conflict.

## SCENARIOS



### BASELINE

The world should expect a further increase in cyberattacks capable of temporarily disrupting the activities of key infrastructure facilities in health care, financial, industrial, defense and energy systems. However, the damage will be limited, which will not allow the situation to get out of control and lead to violent retaliatory actions in the physical rather than virtual dimension.

At the same time, the rise in cyber threats will stimulate appropriate coordinated responses, including broader investment in cybersecurity. However, the interstate cooperation in the field of cyber threats will continue to remain hostage to geopolitical competition, which will not allow the development of common rules and reduce the level of risks.



### NEGATIVE

The main condition for the pessimistic scenario to come true is a sharp increase in geopolitical tension between rival powers, which may lead to the start of large-scale cyberattacks at the state level.

Situations around the Iranian and North Korean nuclear programs can become potential lines of conflict. However, a more serious challenge to global stability will be a possible cyber crisis involving several major global centers of power, including the United States, China and Russia. In this case, it will be extremely difficult to predict the trajectory of the crisis development, as well as its potential consequences for the global security system.

In a full-scale cyber war between global powers, the world community may face an unprecedented crisis that can not only paralyze a significant part of the world economy, but also put the world on the brink of a real military conflict.



**Steve Durbin***Chief Executive*

Information Security Forum (ISF)

**US Tel:** +1 (347) 767 6772**UK Tel:** +44 (0)20 3289 5884 | **UK Mobile:** +44 (0)7785 953800

steve.durbin@securityforum.org

**securityforum.org****About the Information Security Forum**

Founded in 1989, the ISF is an independent, not-for-profit association of leading organizations from around the world. The organization is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organizations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions.

By working together, ISF Members avoid the major expenditure required to reach the same goals on their own.

Consultancy services are available to support the implementation of ISF Products.

For more information on ISF Membership, please visit [www.securityforum.org](http://www.securityforum.org)