

**Tarasova Krystyna**

Ph.D., lecturer

Odessa national economic university

Odessa

## GLOBAL CYBER RISKS AND ALTERNATIVE VARIANTS OF FUTURE

Our world today is in the midst of the greatest information revolution in the history of humanity. Hereby, more than 40 % of the world's population has access to the internet web, with more and more users coming online each day. Even among the poorest 20 % of people, nearly 7 persons out of 10 have a mobile phone. [1, p. 2].

During the last decade, the number of internet users has grown more than by 3 times – from 1 billion in 2005 to an estimated 3.2 billion at the end of 2015. Presently typical day in the life of internet users consists of 207 billion of sent e-mails, 4.2 billion of Google searches, 2.3 GB of web traffic, 152 million of Skype calls and 36 million of Amazon purchases [1, p. 6]. It means that businesses, people, and even governments are now more connected than ever before. The information revolution has brought and immediate private benefits such as easier access to the information, better convenience, free digital products, and new different forms of leisure.

For example, in Kenya after the introduction of the digital pay system M-Pesa, the sending remittances decreased by 90%. The online platform of e-commerce Alibaba accelerates efficiency of the economy of China through the reduction of coordination costs.

But have new technologies generated faster economic growth and are the countries reaping sizable digital dividends? Arises and another question – will the information technologies continue to bring economies to innovation and prosperity? In so far, developing technologies bring not only new possibilities but also – new risks.

IT-risks or cyber risks appear in many forms, all of which can represent major threats to doing business. Enterprises increasingly face new exposures, including third-party damage, business interruption and different regulatory consequences. These risks are among the most dangerous risks to the doing business are that are detrimental to the global economy to the tune of 445 billion dollars a year [2, p. 10]. More than that, all of the current IT-trends foretell an even darker future with more cyber incidents. According to the model built by Denver's Pardee Centre of International Futures and Atlantic Council, the associated cyber-security costs will outweigh the benefits from the worldwide internet connection in 2019. Moreover, according to these project models, annual security costs in high-income countries have begun to outweigh economic benefits from global e-connection. For all developing economies the inversion of benefits and costs is expected to occur within next three-five years [3, p. 2].

But, there is a positive side. Whereas the cyber costs tend to be experienced as 'one-time deals', cyber benefits tend to deliver positive effects after they originally left for many years to come.

Based on those facts, scientists also made a prediction as touched to the four possible variants of future, symbolically named Cyber Shangri-La, Independent Internet, Leviathan Internet and Clockwork Orange Internet [3, p. 5]. The substance of those possibilities is expressed in table 1.

Table 1

**Alternative worlds: scenarios of international development**

Variant of future	Characteristics	Impact on the economy
Cyber Shangri-La	Newly created technologies create benefits faster than costs are accumulated. The cyber defense mechanisms are easier and cheaper, their improvement becomes faster than offences arise.	ICT becomes the main driver of innovation process; it benefits among the world as nearly all firms have access to similar technologies. Global cooperation on cyber security is relatively high.
Independent Internet	ICT companies continue to develop new e-defenses but cyber-terrorists still thrive.	ICT is an important driver of innovation but there is a risk of rising income inequality between countries in the future. As for now, the ICT globalization is high.
Leviathan Internet	Cyber-security decreases all over the world. Most of the nations have predominantly open internet borders and from time to time suffer from cyber-attacks. Some countries, like China and Russia, choke off their national borders so that all the information and attacks have difficulty penetrating.	There is little trust between friendly countries. Some nations close off their national e-borders which lead to the ICT inequality. The impact on the economic development is fairly modest with stably growing GDP. But this growth is far lower than it could have been with open borders.
Clockwork Orange Internet	Cyber offence mechanism is unstoppable. ICT usage is very limited and is reserved only for those people who are rich enough to pay for proper security measures.	The international cooperation is limited due to the lack of trust between countries. The cost of the digital economy is rising much faster than dividends of them. Most heavily by cyber-crimes are affected higher-income countries and so-called 'middle economies'.

It's hard to say which variant of future is more likely to come. But more and more scientists make gloomy predictions. The threat of cyber risk will continue to rise, and it's up to the governments to choose their policy to make one of these predictions to come true.

**References**

- 1.Global Economic Prospects. June 2016. Divergences and Risks [Electronic resource]. – 2016. – № 26. – Available at: <http://pubdocs.worldbank.org/en/842861463605615468/Global-Economic-Prospects-June-2016-Divergences-and-risks.pdf> (date of appeal: 14.10.16). – Title screen.
- 2.Allianz Risk Barometer Top Business Risks 2016 [Electronic resource]. – 2016. – № 5 – Available at: [http://www.btsau.net.ua/sites/default/files/news/pdf/prikladi\\_oformlen\\_literatur.pdf](http://www.btsau.net.ua/sites/default/files/news/pdf/prikladi_oformlen_literatur.pdf) (date of appeal: (14.10.16). – Title screen.
- 3.Risk Nexus. Overcome by cyber risks? Economic benefits and costs of alternate cyber futures [Electronic resource]. – 2015. – Available at: <http://publications.atlanticcouncil.org/cyber risks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf> (date of appeal: 14.10.16). – Title screen.

