Center for Cyber Security and
International Relations Studies

Dr. Pavel Karasev
Senior researcher
Institute of information security issues
at Moscow State University

Primakov National Research Institute
of World Economy and International Relations
Russian Academy of Sciences

Abstract

In the following article we review how ICTs have been at the foundation of a consistent paradigm shift in the social, cultural, economic and military-political fields that has occurred over the past 30 years. This shift manifested itself through the processes of mass development of the information space, the emergence of specialized ICTs as means to promote national interests, the rise of the sixth technological order, industry 4.0 and the Internet of Things. The paradigm shift in each of these areas has led, on the one hand, to new opportunities for growth, social, cultural, political and economic development, and on the other, to the emergence of new threats. At that, the application of new ICT technologies has not always been followed by a development of adequate solutions to counter these threats. Application of scientific approach followed by creation of a system of international information security could provide an answer to the most pressing issues of cybersecurity.

ICTs as a driving force behind the Global paradigm shift: Social, Cultural, Political and Economic trends.

Introduction

If we take into consideration the latest statistics, somewhere between 2016-2017 we have reached a significant milestone – more than half of the world's population, and presently this amounts to 3 billion 900 million people, have become the users of the global Internet.[1] Constantly growing is the number of enterprises and their employees that are playing a part in the implementation of Digital economy concepts. According to "Europe's Digital Progress Report 2017", over a decade employment of ICT specialists in the EU grew by 2.2million to

[1] "World Internet Users and 2018 Population Stats" available at: https://www.internetworldstats.com/stats.htm

reach 7.7 million in 2015.[2] National governments are increasingly using ICTs in their daily activities, transforming the traditional government frameworks (for example, taxation, regulation and licensing, etc.), creating and implementing e-government projects. The consequence of this surge in the use of ICTs in all spheres of human activity is the furthering of dangerous dependence on uninterrupted and reliable operation of information and communication systems. We can see new game-changing threats which use inherent vulnerabilities of ICTs and also, in some way, the vulnerabilities of human mind.

Analysis

At the current stage of the evolution of mankind, active dissemination and use of ICTs has transformed information into a strategic resource for development and has led to the emergence of a new type of society and economy. In most general view, the distinctive features of the information society are: propagation of information technologies through all spheres of life, the increasing role of information, knowledge and information technologies in the life of society. A necessary factor for this is the creation of a global information space that is designed to ensure effective information interaction between individuals, providing them with access to the world's information resources, meeting their needs for information products and services.[3]

The formation and development of a digital society in itself is a shift in the socio-cultural paradigm. Our perception of information, the culture of communication, the circle of interests and acquaintances have changed. It has been noted that with the advent of an information age digital storage overtook analog storage and by today in relative terms analog is virtually unseen.[4] To date the servers of Facebook have brought together more than 2 billion people.[5] Our "friendlist" may contain a person whom we have never seen in real life, but only in the same interest group. But who or what is hidden behind the profile in the social network, which has

---

[2] Europe's Digital Progress Report available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=45188

[3] See: Hayashi Y. Information society in Japan – the vision and challenges / Edited by Economic Council Research Committee. – Osaka.: Diamond Inc., 1969. – 289 p.
Machlup F. The Production and Distribution of Knowledge in the United States. – Princeton.: Princeton University Press, 1973. – 436 p.
Bell D. The Coming of Post-Industrial Society: A Venture in Social Forecasting. – NY.: Basic Books, 1976. – 616 p.
Masuda Y. The Information Society as Postindustrial Society. – New Jersey: Transaction Publishers, 1980. – 178 p.
Castells M. The Informational City: Information Technology, Economic Restructuring, and the Urban Regional Process. – Oxford: Blackwell Publishers Inc. 1999. – 390 p.

[4] The World's Technological Capacity to Store, Communicate, and Compute Information available at: http://www.martinhilbert.net/WorldInfoCapacity.html/

[5] Two Billion People Coming Together on Facebook available at: https://newsroom.fb.com/news/2017/06/two-billion-people-coming-together-on-facebook/

become a reflection of identity, a kind of "passport" in the information space? Indeed, ICTs provide people with ample opportunities to communicate, exchange opinions and information. However, human mental capabilities are becoming increasingly insufficient to critically comprehend the surrounding information in its entirety. Hence the threat of malicious information influence, which pursues various goals of criminal, terrorist or political nature.

Another area where we can see a paradigm shift is the international policy of the States. ICTs contributed to the transformation of ICT-environment into a new sphere of confrontation as it has already been recognized a new domain of military operations, both at national level and at the level of organizations.[6] An increasing number of States are developing ICT tools for military and political purposes – according to some sources[7], there are already more than 60 countries in the "cyber club", and even more are on the verge of entering it. Constantly on the rise is the threat of public order destabilization through the spread of destructive by means of ICTs. The proliferation of cyber weapons is to the moment a virtually uncontrolled process, which is developing outside the existing system of international security. The emergence of a multipolar world, which in itself is also a paradigm shift, reinforces this process, since States, quasi-state associations and non-state actors see the possibility of compensating their lack of power with ICT capabilities. For many years Russia has been promoting draft treaties[8] that would have limited or prohibited the development and use of cyber weapons – in other words, advocated the prevention of conflicts, and not for their legalization and regulation. Indeed, in conditions where even the problem of attribution of cyberattacks is not solved, the perpetrator can be "appointed" for political reasons – and he can experience not only sanctions, but also force. The adoption of Norms, rules and principles for the responsible behaviour of States[9] suggested by the Group of governmental experts of the United Nations is an important step in the right direction. Now, the next step should be the development of specific recommendations by the scientific community and experts on exactly how these norms, principles and rules are applied in the ICT environment.

---

[6] See: p.7 of Quadrennial Defense Review 2001 available at: http://archive.defense.gov/pubs/qdr2001.pdf;
Warsaw Summit Communiqué available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

[7] J.V. De Vries, D. Yadron Cataloging the World's Cyberforces / Jennifer Valentino-DeVries, Danny Yadron // The Wall Street Journal. – 2015. – Oct. 11

[8] See: Convention on International Information Security (Concept) available at: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=en_GB

[9] See: Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174) available at: http://undocs.org/en/A/70/174

In the economic and technological sphere we can witness the fourth industrial revolution and the convergence of nano-, bio- , information and cognitive technologies (NBIC). Transition to the sixth technological order, development of the ICT-sector changes in the structure of the world economy, the global market is becoming much more dynamic and competitive, e-commerce is developing and many new enterprises are emerging. And one should not forget the rapid development of the Internet of Things. or IoT. According to Gartner, the number of such devices in 2017 was 8,4 billion[10] and it is estimated[11] that by 2020 the overall number of IoT devices will reach 50 billion – it is unknown how well their cybersecurity will be ensured. Trustlook research paper[12] shows that the level of user awareness about IoT risks is relatively low. For instance, 35% of users do not change the default password, while 54% do not use any additional security software. ICTs are at the core of such new technologies as Big data, Quantum computing, Augmented and virtual reality, and Blockchain. We are just beginning to make wide use of these innovations, but often do not take into consideration the associated risks. To ensure emergence of practical solutions in this area the State policy is not enough, there have to be initiatives of private businesses – owners of critical information infrastructure and manufacturers of connected devices.

Conclusion

Having reviewed the trends and the paradigm shifts the mankind is experiencing, the conclusion would have to be in a form of an admission of a fact that we are lagging behind the rapid development and introduction of technologies in our lives. Quoting Martin Luther King, "Our scientific power has outrun our spiritual power. We have guided missiles and misguided men". It seems what we do not have is a much more needed thing – a deep scientific understanding of the ongoing processes and analysis of their consequences. How can an individual and society defend themselves against fake news, political manipulation and the influence of terrorist and extremist ideology? How to counteract threats to strategic stability and promote equitable strategic partnership in the global information space? How to ensure sustainable growth and development of the economy without sacrificing security?

In the face of immediate and future threats development of a system of international information security appears to be one of the most elaborated answers to the posed questions.

---

[10] Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. available at: https://www.gartner.com/newsroom/id/3598917

[11] Cisco IoT Threat Defense. available at: https://www.cisco.com/c/dam/en/us/solutions/collateral/security/iot-threat-defense/at-a-glance-c45-739074.pdf

[12] IoT Security: a coming Crisis? available at: https://newblogtrustlook.files.wordpress.com/2017/09/iot-security-survey-infographic-2017.pdf

This approach provides for the creation of new, or the expansion of already existing international and national institutions designed to regulate the activities of various actors of the global information space. The duty of academia in this system is to work out and present to mankind the answers to threats not only of today, but also of the future. At the same time, effective work in this direction is impossible without the joint efforts of scientific teams of different States.

Bibliography

1. "World Internet Users and 2018 Population Stats" available at: https://www.internetworldstats.com/stats.htm
2. Bell D. The Coming of Post-Industrial Society: A Venture in Social Forecasting. – NY.: Basic Books, 1976. – 616 p.
3. Castells M. The Informational City: Information Technology, Economic Restructuring, and the Urban Regional Process. – Oxford: Blackwell Publishers Inc. 1999. – 390 p.
4. Cisco IoT Threat Defense. available at: https://www.cisco.com/c/dam/en/us/solutions/collateral/security/iot-threat-defense/at-a-glance-c45-739074.pdf
5. Europe's Digital Progress Report available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=45188
6. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. available at: https://www.gartner.com/newsroom/id/3598917
7. IoT Security: a coming Crisis? available at: https://newblogtrustlook.files.wordpress.com/2017/09/iot-security-survey-infographic-2017.pdf
8. J.V. De Vries, D. Yadron Cataloging the World's Cyberforces / Jennifer Valentino-DeVries, Danny Yadron // The Wall Street Journal. – 2015. – Oct. 11
9. Machlup F. The Production and Distribution of Knowledge in the United States. – Princeton.: Princeton University Press, 1973. – 436 p.
10. Masuda Y. The Information Society as Postindustrial Society. – New Jersey: Transaction Publishers, 1980. – 178 p.
11. See: Convention on International Information Security (Concept) available at: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=en_GB

12. See: Hayashi Y. Information society in Japan – the vision and challenges / Edited by Economic Council Research Committee. – Osaka.: Diamond Inc., 1969. – 289 p.
13. See: p.7 of Quadrennial Defense Review 2001 available at: http://archive.defense.gov/pubs/qdr2001.pdf;
14. See: Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174) available at: http://undocs.org/en/A/70/174
15. The World's Technological Capacity to Store, Communicate, and Compute Information available at: http://www.martinhilbert.net/WorldInfoCapacity.html/
16. Two Billion People Coming Together on Facebook available at: https://newsroom.fb.com/news/2017/06/two-billion-people-coming-together-on-facebook/
17. Warsaw Summit Communiqué available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

Tutti gli scritti pubblicati dal CSSII sono sotto la responsabilità esclusiva dei singoli autori