BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 1, Number 371 (2018), 94 – 101

UDC 342.003.347/1

N. V. Kushzhanov, U. Zh. Aliyev

Turan-Astana University, Astana, Kazakhstan.
E-mail: kushzhan@bk.ru aliyevu@mail.ru

DIGITAL SPACE: CHANGES IN SOCIETY AND SECURITY AWARENESS

Abstract. Digital transformation of world permits all areas in our life from economy to policy, society and culture. The recent scandal with community service center and data protection showed how much sensitive we are in front of cyber-attacks and vulnerable when it comes to our personal security. The security awareness is necessary skill in present life, it's important for our job, social interactions and etc. EAUE stepped in new stage of interaction its formation of Digital Space, where no borders or limitation of information and resources. Cybersecurity as a national strategy and plan needs to deliver not only better security in government and business services, but a fundamental shift in the safety of the electronic environment in which they operate. Over the last 20 years, the IT community has failed to deliver a data utility that has the level of trust common in other utilities. What can the IT community do to turn around the current obstacles to developing an effective digital society? The purpose of this research paper is to discuss the security challenges that are associated with the digital age. The topic of cyber security is one that should be talked about more often in today's society. This paper points out the importance of cyber security awareness and protection. It touches on the major ideas of why our community and corporations are currently in a predicament. Lastly, the paper ends with proposed solutions on what can be done to address cyber security challenges in digital life.

Keywords: security; mobile devices; security awareness; cyber threats, digitalization, digital space.

Introduction. Mobile devices (i.e., cellphones, laptops, tablets) have become an indispensable part of our everyday life, since they fulfill the increasing users' desire for Internet connectivity and access to information, social and private networks at any time and place. Owing to the proliferation of "smart" devices and the escalating dependency on them with respect to the execution of everyday tasks, they have evolved from a communication medium to a multifunctional equipment. The reduced cost, in combination with the increasing computational and storage capacity of mobile devices, allow them to accommodate critical functionalities with significant security and safety related impact such as e-banking, control systems and Internet of things architectures. Such devices do not simply store information related to their owners, but also receive data on people and infrastructure related in some way to them. As a result, they can retrieve, store and modify extensive quantities of diverse and potentially sensitive information.

Furthermore, the users are accustomed to the notion of continuous connectivity, even across networks with potentially unknown configurations. Such transmissions are likely to be vulnerable to unauthorized access and, consequently, they constitute a security risk. In many cases, these risks materialize as direct criminal attacks, such as privacy intrusions or unauthorized disruptions of communication. Moreover, they can expose the users to more complex types of malicious activity, such as identity theft, blackmailing, active data collection, or defamation. In light of the increasing risks due to the aforementioned use of mobile devices, it is important that users are aware of the risks they are exposed to and, more importantly, that they are informed about how to protect themselves.

The exponential spread and scale-up of digital technologies and services has profound global implications, creating opportunities for sustainable development and inclusive growth, but at the same time new threats and challenges. Digitalization has an important role to play in a wide range of areas including gender, good governance, transparency and accountability, the fight against corruption, job

creation and private sector development, access to micro-finance, improving access to public services - notably energy, protecting the environment and addressing climate change, providing humanitarian aid, promoting education, health or agriculture. As such, digital solutions can help combat poverty, contribute to better targeting and the linking of humanitarian and development activities, and help to manage migration and address shortcomings in a number of EU partner countries where identification and civil registries, digital entrepreneurship and Small and Medium Enterprises (SME's), e-Services, e-Government, mobile financing or blockchain secured transactions can reduce inequalities and increase prosperity. Digitalization acts as an accelerator and enabler of many, perhaps all of the SDGs. The 2030 Agenda for Sustainable Development sets specific targets in this respect.

Security awareness is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially *informational*, assets of that organization. Many organizations require formal security awareness training for all workers when they join the organization and periodically thereafter, usually annually.

The ability to evolve a digital society and to gain the many promised benefits depends in large part on a widespread confidence in the fabric of cyberspace. The denial-of-service attacks against Paypal and Amazon.com (2010), CNN (2008), Twitter (2009), the Australian Parliament (2010) and US oil firms (2011) may or may not have been successful in damaging the target, and indeed may have been used for publicity by Internet security companies, but they have increased public concern over security in cyberspace. The more serious intrusion attacks against Sony Corp. (in which credit card details of thousands of gamers were released) and RSA (in which highly sensitive information relating to its secure two-factor authentication device was compromised) demonstrate that the Internet is increasingly a very dangerous place to operate.

So what has changed on the Internet? The answer, of course, is everything – business activities, information technology, the communications environment and the threat landscape. Today, vendors and attackers have become embroiled in a cyber arms race, and users are the losers. There are regular reports of government and business systems being infiltrated and data breaches in government departments. Consumers' computers, wireless modems and, increasingly, cell phones are being subverted, and even the basic fabric of cyberspace is under attack, with nations demonstrating their ability to take control of the Internet.

In the last five years, there have been a number of fundamental shifts in technology and its use that require equally fundamental shifts in attitudes towards security. Information technology has evolved from purely a means of systems automation into an essential characteristic of society: cyberspace. The kind of quality, reliability and availability that has traditionally been associated only with power and water utilities is now essential for the technology used to deliver government and business services running in cyberspace.

Technology is changing rapidly, and another fundamental shift is occurring with the emergence of cloud computing. Cloud computing enables individuals and organizations to access application services and data from anywhere via a web interface; it is essentially an application service provider model of delivery with attitude. The economies possible through use of cloud, rather than internal IT solutions, will inevitably see the majority of businesses and, increasingly, governments running in the cloud within the next five years. This substantially changes the ways in which organizations can affect and manage both their IT function and security in their systems.

Today's security standards were developed in a world in which computers were subject to fraud and other criminal activities by individuals inside and, in some cases, outside the organization. However, this has changed in the last five years with the rapid increase in organized cybercrime through the emergence of robot networks (botnets), which enable criminal activity to be conducted on an unprecedented global scale and can also be used as force multipliers to deliver massive denial-of-service attacks on targeted businesses – at a level at which nations are increasingly at risk of being cut off from the global Internet.

Unfortunately, the capability of national police forces to stop global cybercrime is developing much more slowly than the technical abilities of cybercriminals. Cybercrime is now arguably a bigger issue than illegal drugs. The adoption of the Council of Europe Convention on Cybercrime is setting the scene for a global response to cybercrime, and there are signs that police forces globally are working together. However, much more needs to be done to develop the concept of a global jurisdiction before an adequately agile response to cybercrime can be developed.

Understanding the Threat Source. Clearly, understanding the source of any threat and the likelihood of the threat being a danger to an organisation's business interests is a critical first step in building a cybersecurity strategy. Steven Bucci describes the threat actors as shown in figure.

Figure 1—Threat Actors

Threat Sources	Description
Bot network operators	Bot network operators are hackers; however, instead of breaking into systems directly, they take over multiple systems to co-ordinate attacks and distribute phishing schemes, spam and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organised crime groups are using spam, phishing and spyware/malware to commit identity theft and online fraud.
State-sponsored actors	Foreign governments and intelligence services use cybertools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programmes and capabilities.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites.
Insiders	The disgruntled organisation insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals or small groups who execute phishing schemes in an attempt to steal identities or information for monetary gain
Spammers	Individuals or organisations that distribute unsolicited email with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware or attack organisations (e.g., denial-of–service attacks)
Spyware/malware authors	Individuals or organisations that produce and distribute spyware and malware, sometimes for free and sometimes to sell to the highest bidder
Terrorists	Terrorists seek to destroy, incapacitate or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the global economy, and damage public morale and confidence.

Steven Bucci"s model of treat factors

Steven Bucci shows that while cyberthreats are changing from individual hackers through organized crime and terrorist-based attacks to national- or state-sponsored cyberattacks, the level of danger is correspondingly increasing. Thus, while individuals may cause mayhem, it has been largely unsustainable and fairly contained. Now an attack may result in widespread destruction and an ongoing undermining of state sovereignty.

There is no single solution or panacea to the issues of cybersecurity, nor should there be. Each organization should assess what its needs are, how it intends to conduct its business activities and what the risks are to that process. There is a plethora of highly capable solutions that can then be implemented and, more important, maintained.

Consumers in cyberspace, be they government, industry or society, continue to be more mobile, more demanding and less tolerant of failure. While there is an increased awareness of threats, often the increased adoption of security comes only after data breaches and system failures.

What is cyber security and why should we care? Cyber security has become a new concept in the last decade. With technology advancing every day our society is becoming more connected than we have ever been before. While these advances are making our daily lives easier they are also adding extra risks to our