American Journal Of Social Sciences And Humanity Research

VOLUME Vol.05 Issue05 2025
PAGE NO. 310-315
DOI 10.37547/ajsshr/Volume05Issue05-61

The Impact of Digital Technologies On Public Administration In The International Information Society

Nurullayeva Durdona

Master degree student 1- course, Tashkent state university of oriental studies, Uzbekistan

Received: 14 March 2025; **Accepted:** 26 April 2025; **Published:** 30 May 2025

Abstract: This article discusses the current problems of cybercrime and online extortion on the Internet. In particular, such cases, which occur frequently in the global information society, are not only criminal, but also cause material, moral and spiritual problems. The government, which plays a key role in the functional economic and social development of society, is also experiencing significant economic losses due to such crimes. At the same time, cyber attacks are causing significant damage not only to the public sector, but also to the education, healthcare, and banking systems. The article examines cybercrimes committed in various sectors and provides conclusions on their prevention.

Keywords: - Digital transformation, OECD, Artificial intelligence, ChatGPT, digital government, cyberattacks,education sector, healthcare system, cryptocurrency, Cyber transformation.

Introduction:

The public sector plays a key role in the functioning and development of society, providing citizens with access to essential services such as health, education, security and social protection, as well as performing regulatory functions, infrastructure development and business support. In today's world, government agencies are also responsible for managing vast amounts of data, including citizens' personal information, financial records, and strategic information important to national security. To adapt to the digital era and take advantage of its benefits to maximize operational efficiency, the public sector in many countries is undergoing digital transformation. In 2022, nearly all OECD countries (29 out of 30) reported that they were developing and implementing national digital government strategies. In Europe, according to the strategic program for the digital decade, by 2030 the goal is to make all basic government services available online and give access to a digital identity card to all citizens. In Russia, by 2030, it is planned that 100% of executive branch employees will use government communication services in their work, all government services will be provided with the ability to obtain results online, and 90% of mandatory reporting documents will be collected and stored electronically . The public sector requires to be digital by design to fully adapt and take advantage of the digital age for better serving people, improving policy making and maximise government performance (OECD, 2020a). Becoming digital by design requires: 1) setting a strategic vision and clear mandate for digital government; 2) securing solid organizational leadership to steer digital government policies and actions; and 3) establishing effective co-ordination and collaboration within and outside the public sector for government-wide digital transformation in a coherent and inclusive manner. More notably countries have made considerable progress in establishing formal co-ordination bodies or mechanisms responsible for steering digital government policies and initiatives in the public sector, such as Korea’s e-Government Promotion Committee or Luxembourg’s Inter-ministerial Council for Digitisation. In 2019, 18 out of 26 countries (69%) had such a body or mechanism in place, rising to 29 out of 30 (97%) in 2022. his means that seven countries have since established one. Implementation and use of AI in the public sector also vary across countries. Twenty-three of the 30 countries surveyed (77%) reported using AI in at least one of three evaluated categories: public sector internal processes, public services design and delivery, and policy making. Looking specifically at each category, 22 out of 30 countries (73%) used AI to improve internal public sector processes. For instance, Finland’s Aurora AI recommends public services to end

users based on their attributes. In contrast, only a small number of countries (11 out of 30, or 37%) have applied AI to improve policy making, such as Estonia's semi-automatic remote sensing information system for geo-referencing forest resources and improving environmental decision-making capabilities. Only ten countries (33%) are using AI across all three categories while seven (23%) have not developed AI projects in any of the three categories .

The higher the level of digital development, the more the state depends on technology. The rapid pace of technological progress is not always accompanied by a corresponding pace of strengthening cybersecurity. Cyber threats such as cyber espionage, hacktivism, and cyberattacks for extortion or disruption pose a serious threat to the public sector. Attackers, whether lone actors, organized crime groups or hacktivists, seek to gain access to sensitive information, disrupt government systems and extract economic, political or strategic benefits from it. The study presents the landscape of current cyber threats to the public sector, based on data on successful cyberattacks from 2022 to the first half of 2024. During the research of the shadow market, we analyzed 213 sources, including telegram channels and forums on the dark web with a total number of users of more than 38 million and a total number of messages of more than 155 million. The sample included the largest sites in different languages with a diverse thematic focus. To analyze the access market, advertisements published in 2023–2024 were considered. The most popular targets for attackers over the entire period under review were computers, servers and network equipment: 80% of successful attacks were directed at them. Government agencies employ large numbers of personnel who are also susceptible to attack by attackers: in almost half of the incidents (47%), attackers used human factors weaknesses and social engineering methods. Moreover, people are increasingly becoming targets of attacks: the number of incidents increased from 43% in the first half of 2023 to 49% in the second half of the year and to 57% in the first half of 2024 . Web resources were targeted by attackers in 36% of successful attacks. In a tense geopolitical environment, the threat of attacks from hacktivists has increased significantly. Their favorite methods are massive DdoS attacks and website defacements, which we will consider in more detail below.

In malware attacks, the consequences are devastating and lead to serious disruptions and leaks. In April 2023, a Royal ransomware attack on the city of Dallas' computer servers caused police, court, 911, online bill payment, and public library systems to crash. As a result of the leak, the attackers gained access to 1.2 TB of confidential data of more than 26,000 people . The most common type of crime is Ransomware. It is through it that every year millions of losses are caused to the public sector, government and other sectors. Ransomware is a form of malicious software that infiltrates a computer or network and limits or restricts access to critical data by encrypting files until a ransom is paid. The first use of ransomware dates back to 1989, when floppy disks were high-tech and the price of the ransom was a mere $189. Ransomware attacks are on the rise and continue to be a disruptive force in the cybersecurity industry, affecting everything from financial institutions to higher education. Ransomware attacks targeted the education sector more than any other industry in the last year, with 79 percent of surveyed higher education institutions across the world reporting being hit . Lower education reported compromised credentials (36%) and exploited vulnerabilities (29%) as the top two root causes of ransomware attacks. Emails (malicious emails or phishing) were the starting points for nearly one-third of the attacks (30%), suggesting that the lower education sector is highly exposed to email-based threats. In higher education, exploited vulnerabilities (40%) were the most common root cause of ransomware attacks, with compromised credentials falling in second place at 37%. Together, they account for over three-quarters of ransomware attacks (77%) in higher education. Email-based attacks (malicious email or phishing) are a less common root cause but still drive almost one in five ransomware incidents (19%) . Across the full survey cohort, higher education was one of the sectors most likely to report exploited vulnerabilities as the root cause of attacks. At the same time, lower education was one of the sectors most likely to have attacks originating from compromised credentials.

The next step is the health care system which was already stretched and stressed by the pandemic, continued to be heavily targeted in 2020 with at least 560 facilities being impacted in 80 separate incidents (an attack on a health system can impact multiple facilities). The most significant incident of the year was the attack on the Universal Health Services which operates around 400 hospitals and other healthcare facilities. Other significant incidents included the attacks on Boston Children's Hospital, Crozer-Keystone Health System, University of Vermont Health Network, and Lake Region Healthcare. The impact of the attacks was alarming: ambulances were rerouted, radiation treatments for cancer patients were delayed, medical records were rendered temporarily inaccessible and, in some cases, permanently lost, while hundreds of staff were furloughed as a result of the disruptions. The University of Vermont Health Network, which furloughed 300 staff, estimated the cost of the attack

at $1.5 million per day. PHI and other sensitive data was stolen in multiple incidents and published online in at least 12 incidents. The 12 incidents all occurred in the second half of the year .

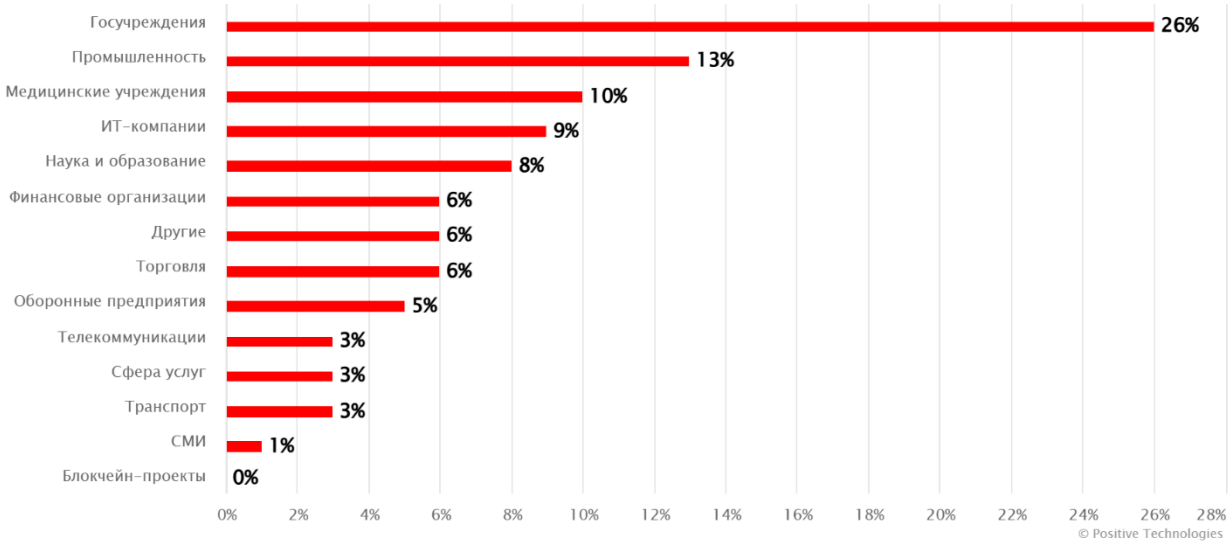
Since the start of bitcoin, the world's first cryptocurrency, transferring money and data has become increasingly efficient. Now, the size of the cryptocurrency space has grown exponentially, with innovations and a collective market capitalization of more than $1.2 trillion. But with this advancement in digital and financial technology, new threats in cybersecurity have come to the surface. Crypto payments to ransomware attackers hit $449.1 million in the first half of 2023, up $175.8 million from the same period last year . In 2022, the total cryptocurrency value received by illicit addresses was $20.6 billion — an all time high . Hackers who attacked an oil company earned over $90 million in Bitcoin. Elliptic found that there were 47 bitcoin wallets — that is, digital cryptocurrency accounts belonging to distinct entities — that paid Bitcoin ransoms to the group of hackers. The total amount of the ransoms, paid in untraceable cryptocurrencies, was more than $90 million. The group became active in October 2020 and scaled up its operations in 2021. Ransomware attacks are on the rise in the US, with Temple University data cited by the Washington Post showing a record high of almost 400 attacks in 2020. The Washington Post reported that experts are concerned about the trend as hackers target cities, hospitals, and critical infrastructure this year .

Between 2018 and December 2023, 423 individual ransomware attacks were carried out against US government organizations, potentially impacting more than 250 million people and costing an estimated $860.3 million in downtime. After three consecutive years of attacks on government organizations declining (dropping from 118 in 2019 to just 40 in 2022), 2023 saw a significant uptick. It saw 69 attacks–a 73 percent year-on-year increase. In this update, we changed the way we calculate downtime figures. Previously, we used an estimate that placed downtime per minute at $8,772 across a number of industries. That estimate came from a 2017 study and does not solely relate to government organizations. Over the last few years, we have collated a large amount of data on the true cost of ransomware attacks on the government. We now use an average cost of ransomware recovery as quoted by 69 government organizations. For example, in 2023, seven government organizations spent $10.8 million on ransomware recovery efforts. Based on the number of days lost to these recoveries, we calculated an average cost per day of $167,798 in downtime. When applying this average daily downtime cost to government organizations that haven't disclosed costs, we estimate they accumulated $181.3 million in downtime costs throughout the year .

The large volume of data accumulated in government information systems and the critical importance of government functions make the public sector the most common target of cybercriminals: our data shows that over the past six years, the public sector has led the way in the percentage of successful cyberattacks. Of all successful attacks on organizations in 2023, 15% occurred in the public sector. In the first half of 2024, the trend continues, and this figure is 14%. In a tense geopolitical climate, the threat of attacks from hacktivists has grown like never before. Their favorite methods are massive DdoS attacks and website defacements, but other methods are also growing in popularity, such as exploiting software vulnerabilities: for example, hackers successfully exploited a vulnerability in the Red Alert application . You need to be prepared for attacks: use firewalls (WAFs), monitor traffic to identify anomalies, use services to protect against DdoS attacks, and promptly fix identified vulnerabilities. In addition, some organizations are already actively adopting technologies such as AI to improve security systems. As an example Tel Aviv, June 27 (Reuters) – Israel's Shin Bet security service has incorporated artificial intelligence into its tradecraft and used the technology to foil substantial threats, its director said on Tuesday, highlighting generative AI's potential for law-enforcement. Among measures taken by the Shin Bet – the Israeli counterpart of the U.S. Federal Bureau of Investigations or Britain's MI5 – has been the creation of its own generative AI platform, akin to ChatGPT or Bard, director Ronen Bar said. "AI technology has been incorporated quite naturally into the Shin Bet's interdiction machine," Bar said in a speech to the Cyber Week conference hosted by Tel Aviv University. "Using AI, we have spotted a not-inconsequential number of threats." AI has helped streamline Shin Bet work by flagging anomalies in surveillance data and sorting through "endless" intelligence, he said, adding that the technology also had a secondary role in decision-making "like a partner at the table, a co-pilot". Acknowledging the public-domain backbone of the fast-emerging technology, Bar urged cooperation between commercial hi-tech and government agencies such as his "to ensure AI leads to evolution and not to revolution" .

Bloomberg claims that Israeli security services are recruiting companies, including spyware maker Pegasus, to help track hostages in the Gaza Strip . In the second quarter, PT Expert Security Center specialists discovered a new lightweight stealer written in Go and designed to search (by extensions) and send files from the home directory and local drives, as well as the contents of the clipboard and screenshots, to the

command server. Another example is spyware that imitates the ChatGPT client for Windows, which is distributed as a ZIP archive containing the ChatGPT For Windows Setup 1.0.0.exe file. During the installation process, the malware runs in the background and starts extracting saved credentials from your Google Chrome login credentials folder. ChatGPT has not released an official desktop client, but this fake version looks very convincing. In the fourth quarter of 2023, the share of spyware in successful attacks increased to 25% - in our opinion, this trend will continue to be relevant in 2024.



Categories of victims among organizations (proportion of successful cyber attacks)

The share of spyware among all malware used in attacks on Russian organizations was 45%, while ransomware accounted for only 27% (while worldwide, ransomware was used in 57% of successful attacks on organizations). This is due to several factors. Firstly, the level of security of Russian organizations is growing, which helps to effectively stop ransomware attacks. Secondly, the difficult geopolitical situation has provoked an increase in the number of attacks using spyware. Thus, the FSB, together with the Russian Federal Security Service, uncovered an intelligence campaign by American intelligence services carried out using Apple mobile devices using unknown malware that exploited software vulnerabilities provided by the manufacturer . One of the leading Russian cybersecurity companies was also subjected to such an attack.

Crimes related to Internet networks and mobile devices differ from other common crimes in that they can be committed remotely from anywhere in the world. They could result in damage to the friendly cooperation between the two countries or, at the very least, cause international problems. There are several problems related to cybersecurity in our country as well. The UzCert service has released data on the number of incidents aimed at cyber security infringement in the first quarter of this year. In the first quarter of 2024, during monitoring, 70 vulnerabilities and weaknesses were identified and eliminated on 19 web resources of government agencies and organizations. During this period, over 3,290,860 cyberattacks were recorded in the national segment of the Internet. For the purpose of identifying and collecting information about existing vulnerabilities and threats in cyberspace and taking measures to eliminate them, information about more than 369,660 cyber threats detected in the information infrastructures of government bodies and other organizations was transmitted to the relevant organizations through the monitoring systems of the Center. Due to non-compliance with cybersecurity requirements, incidents with attempts on cyber security have been identified on 45 sites located in the “UZ” domain zone over the last 3 months. Of these, 12 belong to government bodies and 33 to the private sector . Despite this, Uzbekistan has achieved significant growth in the global cybersecurity index and is positively assessed. Uzbekistan has improved its position in the global cybersecurity index, according to the Global Cybersecurity Index 2024 report. According to the International Telecommunication Union (ITU), Uzbekistan has made significant progress in the field of cybersecurity. The country is now included in the category of countries with an actively developing cyberspace protection system (T2 Advancing) . Since 2020, Uzbekistan’s index has increased from 71.11 to 89.2 points. Earlier, Kun.uz wrote that the President of Uzbekistan Shavkat Mirziyoyev signed a law on cybersecurity.

Government organizations, businesses, and any online organization must implement cyber transformation.

Cyber transformation must be carried out comprehensively for the entire state, in a coordinated manner for all state organizations. If a vulnerability is not eliminated in one state institution and this leads to consequences for citizens, then it will not be so important which state structure is to blame: the state will suffer the damage. To strengthen the protection of IT infrastructure components, it is necessary to ensure safe and effective configuration of target, key systems and penetration points. To do this, it is necessary to pay attention to operating systems and applications, web resources, domain infrastructure, virtualization environments and cloud services. Regular training of employees and managers with knowledge testing reduces the number of successful cyber attacks on the organization. Every employee of a government organization should know such aspects of cybersecurity as strong passwords, protection from phishing, software updates, information confidentiality, safe use of public wireless networks, secure channels and mobile devices. To prevent unacceptable events from occurring, it is necessary to create a threat counteraction center. This could be a global center for the automated collection of events unacceptable for the state in one place. Such a center will monitor events and promptly identify and respond to suspicious activities or other deviations from the norm that may be indicators of attacks, and take measures to counter intruders. It is necessary to identify critical government business processes and modernize them to improve quality, productivity, security, and reduce their cost. It is also extremely important to properly organize the work and communication between IT and information security departments . To determine the current state of security and understand the need for further steps, it is necessary to define metrics for effective cybersecurity and conduct regular assessments using them.

In conclusion, it is worth noting that in today's era of global development, the dynamics of the comprehensive growth of countries are taken into account. In particular, the position of countries is determined by how strong they are, especially through achievements in the economy, healthcare, education and many other areas. But we would not be wrong to say that the 21st century is the century of technology and engineering, and digital technologies are dominating other areas. Nowadays, the need to create new innovative technologies is increasing even more. Although the rapidly developing digital technologies and the emergence of the Internet have had a positive impact on people and their work, this does not mean that it is completely harmless or flawless. We know how to use the internet, but do we understand how to protect ourselves from it? Cyberattacks, which have become one of the most pressing problems of today, are precisely related to the development of technologies. To prevent such online extortion, it is necessary to strengthen cybersecurity measures and develop with the times.

REFERENCES

1. https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-v-gosudarstvennom-sektore/#id1
2. file:///D:/яндекс%20браузер/3d5c5d31-en.pdf
3. https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-v-gosudarstvennom-sektore/#id3
4. https://www.cpomagazine.com/cyber-security/city-of-dallas-suffers-a-ransomware-attack-disrupting-core-it-systems/
5. https://www.varonis.com/blog/ransomware-statistics#top
6. 6.https://assets.sophos.com/X24WTUEQ/at/j74v496cfwh4qsvgqhs4pmw/sophos-state-of-ransomware-education-2023-wp.pdf
7. https://www.emsisoft.com/en/blog/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/
8. https://www.reuters.com/technology/crypto-ransom-attacks-rise-first-half-2023-chainalysis-2023-07-12/#:~:text=Crypto%20payments%20to%20ransomware%20attackers,period%20last%20year%2C%20Chainalysis%20said
9. https://www.chainalysis.com/
10. https://www.businessinsider.com/colonial-pipeline-hack-ransom-cryptocurrency-darkside-2021-5
11. https://www.securitylab.ru/news/542573.php?ysclid=losmnomiv343763132
12. https://www.securitylab.ru/news/542573.php?ysclid=losmnomiv343763132
13. https://www.reuters.com/technology/israels-shin-bet-spy-service-uses-generative-ai-thwart-threats-2023-06-27/
14. https://www.bloomberg.com/news/articles/2023-10-26/israel-taps-blacklisted-pegasus-maker-nso-to-track-gaza-hostages-and-hamas
15. https://www.helpnetsecurity.com/2023/05/02/chatgpt-infostealer/
16. https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/#id2
17. https://kun.uz/en/news/2024/04/06/uzbekistan-reports-over-3-million-cyberattacks-for-q1-2024
18. https://kun.uz/en/news/2024/09/14/uzbekist

an-improves-its-position-in-global-cybersecurity-index
19. https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-v-gosudarstvennom-sektore/#id10