INFORMATION SECURITY THREATS IN THE DIGITALIZATION OF GOVERNANCE AND THEIR IMPACT ON ELEMENTS OF THE DEFENSE SECTOR

Andras TOTH
| ORCID 0000-0001-6098-3262|
toth.hir.andras@uni-nke.hu
Ludovika University of Public Service, Faculty of Military Sciences and Officer Training,
Signal Department,
Budapest, Hungary

Abstract

Digital government has several identified vulnerabilities and threats that affect its smooth functioning. Several of these are not new, but it is clear that unknown attack vectors are emerging as digitalization becomes more widespread. These include, for example, cloud vulnerabilities, which currently play a prominent role in very few of the typical attacks on the government sector in recent times. He used databases such as Elsevier Scopus, ProQuest, Science Direct, and Web of Science to ensure that the author obtained the best answers to the research questions he investigated. A comparative analysis of the academic literature and relevant peer-reviewed reports was conducted following a literature review to identify the most common security problems, threats, and typical attack vectors affecting information and communication systems that serve as critical information infrastructure for digital states and elements of the defense sector. Accordingly, the author identified the potential threats that are most prevalent for both the state and each sector. The results obtained are not specific to an actual nation, as very few countries have fully digitized their operations.

Keywords: Digital government, Information and communication systems, Information security, Security threats, Defense sector

Introduction

Digital technologies are becoming more widely used and are impacting our lives and work. Citizens, businesses, public administrations, and governments need access to these technologies to take full advantage of these capabilities. To achieve this, significant capacity building is needed to ensure that all users, regardless of their level of education, have access to current technologies and services. To develop effective digital governance, individuals and businesses must be receptive to digitalization, which requires a reliable and efficient infrastructure and IT environment. Public administrations must support well-prepared and motivated civil servants while providing user-friendly services to citizens and businesses. In addition, it is essential for

individuals and businesses to continuously adapt and develop their digital skills to keep pace with the rapidly evolving technological landscape. Digital literacy can be achieved through training programs and educational initiatives that promote digital literacy and empower users to take full advantage of the technologies available. In addition, the collaboration between the public and private sectors is essential to create a seamless digital experience for all stakeholders, foster innovation, and stimulate economic growth. By working together, governments and businesses can identify and address different industries and communities' specific needs and challenges. Such collaboration can lead to tailored solutions such as industry-specific training programs or digital infrastructure investments that support the overall digital transformation of society. In addition, promoting a culture of lifelong learning and providing accessible resources can ensure that individuals have the opportunity to continuously update their skills and remain competitive in the digital age.

This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-22-5-NKE-88 New National Excellence Program of the Ministry of Innovation and Technology.

1. The basics of digital governance and digital government

To ensure that digital governance and the other elements of the digital government meet all needs, a framework that sets out the basic guidelines for building a digital government that meets all needs should be developed. The European Commission's study on digital government transformation provides a framework for Member States to develop their digital governance systems. The OECD (Organisation for Economic Co-operation and Development) report "Towards a data-driven public sector" highlights the need for a major shift in the way governments use digital technology and data, in particular in the transition from "e-government" to "digital government". The e-government strategy focuses on digitizing analog processes to increase efficiency. In contrast, digital government practices focus on meeting individual user needs through the e-design and redesigning of services and processes. This shift towards digital government is driven by the recognition that more than simply digitizing existing processes is needed to harness the potential of technology and data. It requires a more user-centric approach that considers citizens' diverse needs and expectations in the digital age. This includes design services and processes that are intuitive, accessible, and personalized, ultimately leading to improved outcomes and better citizen satisfaction (OECD, 2019).

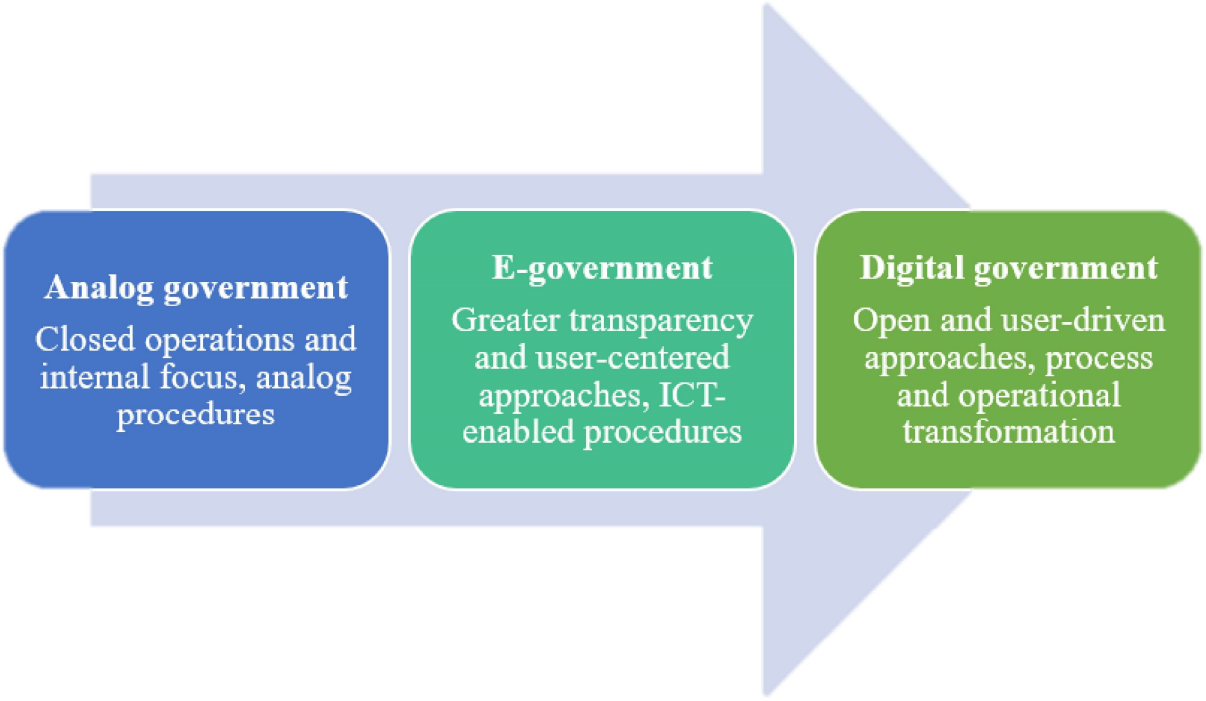

Fig.1. Transformation from analogue to digital government. Source: Recommendation of the Council on Digital Government Strategies OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406

Transforming organizational behavior and creating a digital culture shaped by design is key to achieving digital transformation and more efficient and effective digital government. Organizations can streamline their operations and improve the overall user experience by adopting digital governance practices. A shift towards user-centered design will enable personalized and accessible services that meet the diverse needs of citizens. In addition, adopting a digital culture fosters innovation and collaboration, paving the way for continuous improvement in the delivery of efficient and effective digital government solutions. Digital government practices also enable organizations to collect and analyze vast data, leading to data-driven decision-making and better policy outcomes. This data-driven approach allows governments to identify trends, patterns, and areas for improvement, ultimately leading to more informed and evidence-based decision-making processes. Adopting digital government practices can revolutionize how governments interact with citizens and deliver public services, creating a more efficient and inclusive society. By leveraging digital technologies, governments can streamline administrative processes and reduce bureaucratic inefficiencies. This saves time and resources and enhances transparency and accountability in governance. Additionally, digital government practices can

empower citizens by giving them easy access to information, services, and opportunities, fostering a more participatory and engaged society (Magyar & Bús, 2022).

According to the European Commission's study on digital government transformation, digital governments are using technological advances to simplify transactions for end users, including citizens, businesses, and governments. These governments make better decisions and contribute to more efficient service delivery models by analyzing data and analytics. This leads to improved efficiency, effectiveness, transparency, openness, long-term cost savings, better governance, and a better quality of life for citizens. Digital governance, on the other hand, is the governance of a nation, state, or organization that uses information and communication systems to disseminate information and integrate different models and processes into government systems and services. Digital governance can guarantee the quality of government services, improve collaboration between organizations, empower individuals through access to information, and enable effective government management. By leveraging technology and data, digital governance can increase transparency and accountability in decision-making processes. It enables real-time monitoring and evaluation of government initiatives, ensuring efficient and effective allocation of resources. In addition, digital governance enables governments to be more responsive to the needs and demands of their citizens, thus contributing to a more inclusive and participatory democracy. Digital government can also streamline bureaucratic processes and reduce the administrative burden for citizens and government officials, leading to greater efficiency and cost savings, ultimately benefiting the whole economy. Digital government can also facilitate cooperation and information sharing between different government departments, helping to achieve a more coherent and coordinated approach to problem-solving.

A comparison of digital government and digital governance broken down into its essential elements is shown in Table 1.

Table 1. The basics of digital governance and digital government

	E-government	Digital government
Meaning	The use of information and communication technology to support the activities and operations of government and to increase the knowledge of the public and provide digital services.	Improving the dissemination and depth of knowledge to the public and the quality of services through the use of information and communication networks.
What is it?	System	Functionality
Communication protocol	One-way communication protocol	Two-way communication protocol

2. Information security threats and vulnerabilities

Information security is key for governments, as public data and information are often sensitive and vital to the functioning of the state and the protection of people's interests. Digital governments use various tools to store, retrieve, and process data, which can have different vulnerabilities and security holes, increasing information security concerns. In order to keep information secure, states need to undertake activities such as continuously upgrading and protecting their systems and databases and developing, implementing, and monitoring information security policies and procedures. In addition, digital states must conduct regular risk and vulnerability assessments to identify potential weaknesses in their systems. This proactive approach will allow them to address vulnerabilities immediately and reduce the risk of cyber-attacks or data breaches. In addition, developing robust incident management plans and training employees on cybersecurity best practices are essential to maintaining a secure digital government. These incident response plans should outline the steps to be taken during a cyber attack or data breach, including communication protocols and strategies to minimize damage (Bederna et al., 2021). Regular training can help employees stay up-to-date on the latest cybersecurity threats and prevention techniques, enabling them to protect the digital government's systems and data actively (Váczi et al., 2021). By implementing these measures, digital governments can significantly improve their cybersecurity posture and defend against potential threats.

In digital governance, the triple bottom line of CIA (confidentiality, integrity, availability) is essential. Confidentiality is the property that prevents the information from being disclosed or accessed by unauthorized organizations or persons and protects data from unauthorized access. Activities against confidentiality include theft of assets, password theft, and sensitive information posted on websites without access restrictions due to configuration errors. Maintaining confidentiality is key in various sectors, such as healthcare, finance, and government, where sensitive information, such as personal records, financial data, or classified documents, needs to be protected. Breaches of confidentiality can have serious consequences, such as identity theft, financial loss, or threats to national security. Organizations need to implement robust security measures and educate employees on the importance of confidentiality to prevent potential breaches. Organizations can use encryption technologies, access controls, and secure networks to protect sensitive information from unauthorized access. In addition, regular security audits and employee training programs can help ensure consistent adherence to confidentiality protocols and the identification and prompt management of potential vulnerabilities. Integrity refers to ensuring and maintaining the truthfulness and accuracy of data throughout its lifetime. The fundamental purpose of integrity is to protect all data from being altered, modified, or updated

without detection or unauthorized access. Unauthorized access is the most common activity compromising data integrity by allowing an attacker to view, edit, or download sensitive data without authorization. Data integrity is essential to maintain the reliability and trustworthiness of the information. It involves implementing security measures such as encryption, access control, and regular backups to prevent unauthorized changes or breaches. By prioritizing data integrity, digital governments can protect against potential risks and maintain the confidentiality and accuracy of their data. In addition, data integrity ensures that data remains consistent and accurate throughout its lifecycle, preventing unauthorized modification or manipulation. This is particularly important in sectors such as healthcare and finance, where data accuracy is critical to making informed decisions and protecting the privacy of individuals. By implementing robust data integrity measures, digital governments can build trust with their citizens and stakeholders and, in doing so, help foster a secure and trustworthy digital environment. For any information system, availability is essential to achieve successful operational and management goals. This means that computer systems, communication access paths, and security measures must function properly. Maintaining availability can help prevent denial of service attacks and ensure public data security. Digital governments, in particular, rely heavily on availability to provide essential services to citizens. With adequate availability, citizens can access government websites or conduct online transactions, leading to frustration and possible disruption of governance. In addition, maintaining availability is key to ensuring transparency and accountability in government operations, as it enables real-time access to information and data for citizens and government officials. Availability is also essential for promoting inclusion and equal access to government services. It ensures that people with disabilities or living in remote areas can benefit from online platforms and digital services offered by the government. Maintaining a high level of accessibility also helps to build trust between the government and citizens, as it demonstrates a commitment to the continued provision of efficient and accessible services (CSA Singapore, 2023a).

Table 2 illustrates some possible attack vectors that could affect aspects of the CIA triad system.

Table 2. Information security threats and vulnerabilities in digital governments

Security objective	Attack vectors
Confidentiality	Eavesdropping Key loggers Traffic analysis Encryption cracking Malicious insiders Man-in-the-middle attacks Phishing Spying

	Dumpster diving
Integrity	Modification Spoofing Manipulation Replay attack Reject Interruption
Availability	Denial of service Ransomware Application layer attacks Physical attacks

Eavesdropping attacks allow unauthorized access to data, programs, or environments, often resulting in a breach of confidentiality. Interception attacks, which use various technologies to make devices and systems temporarily or permanently unusable or inaccessible, can cause significant disruption to the functioning of the digital state, especially when launched against critical information infrastructure systems. Interruptive attacks usually affect availability but can compromise integrity. The most common availability attack is the Denial of Service attack, which can be launched against various servers, websites, government, corporate systems, and networks. Modification attacks, which attempt to gain control over devices, are often classified as attacks against integrity. However, they can also function as availability attacks. A spoofing attack occurs when an attacker creates data, processes, communications, or other activities within a system that affect the availability or operation of the system. Data forgery attacks primarily compromise data integrity but can also compromise availability. Forgers can create fake emails, which can be used to distribute malicious software such as worms, viruses, adware, etc. In the case of an availability attack, if the attacker generates sufficient amounts of malicious traffic, they may make the services that handle the traffic unavailable to legitimate system users. There are many different sources of threats to digital states, which are a direct consequence of the vulnerabilities and vulnerabilities discussed earlier. Common threats include Advanced Persistent Threats (APT) attacks, supply chain attacks, and zero-day attacks. APT attacks (Ináncsi, 2021) are often carried out by highly skilled and well-funded attackers, often using custom malware and social engineering techniques to gain initial access to the network and then move laterally across the network to obtain sensitive data (Bányász et al., 2019). The biggest threat to the digital government is the zero-day attack, which occurs when hackers exploit

the flaw before developers can address it. The most common information security threats and vulnerabilities in digital governments are shown in Figure 2.

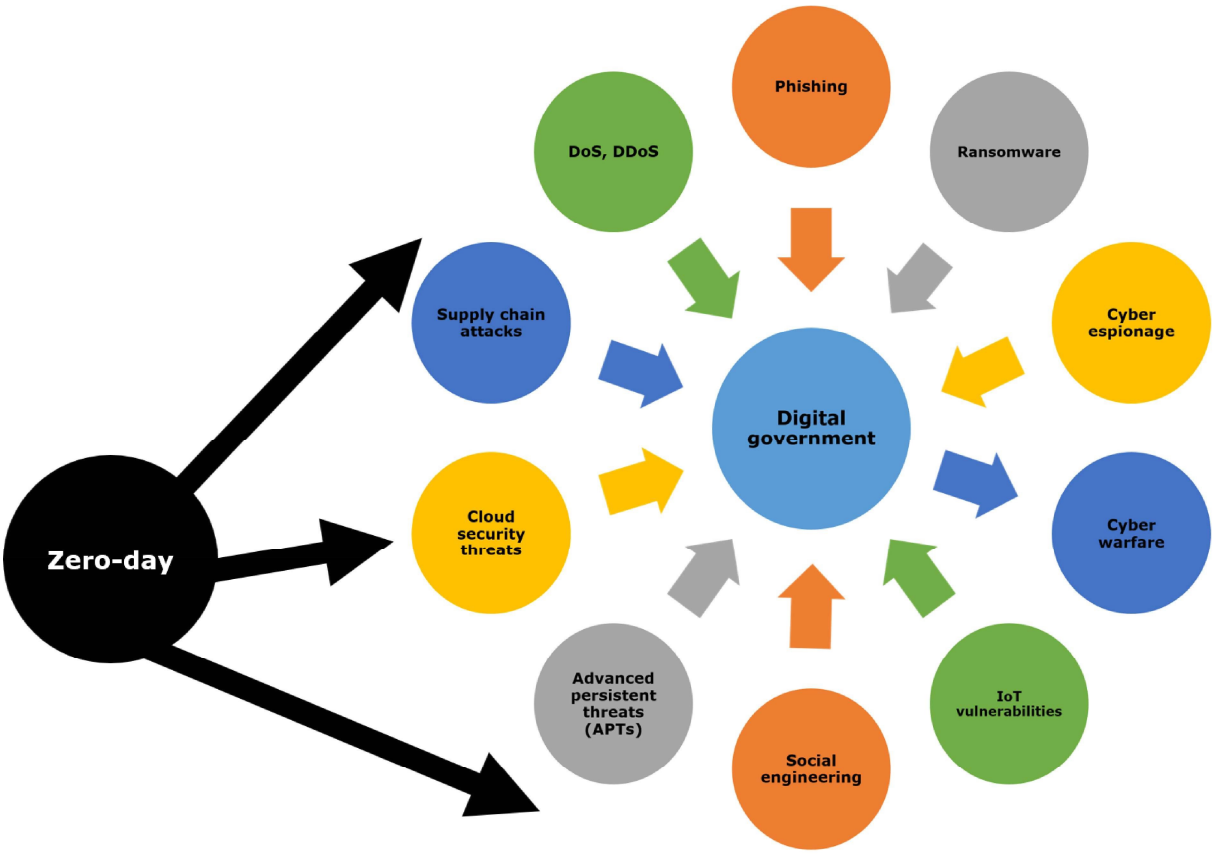

Fig.2. The most common information security threats and vulnerabilities in digital governments

3. The impact of threats on specific elements of the defense sector

Digital governments and their defense sector elements (law enforcement, military, disaster management, national security) should implement measures to maintain adequate information security, including updating systems and databases, implementing policies, and working with cybersecurity organizations. Common security challenges for digital governments include data protection, secure storage, secure transmission of sensitive data, defense against hackers, and maintaining defense systems. These challenges include protecting personal data, ensuring secure storage, and the appropriate data transfer between different systems. By working with experts and collaborating with cybersecurity organizations, governments can effectively prevent and manage cyber-attacks and ensure the safety of their citizens. Governments can also benefit from sharing information and best practices with other countries to improve their cyber security measures. This international cooperation will

allow a more comprehensive approach to addressing emerging threats and preventing cyber criminals. By fostering these partnerships, governments can create a global network of support and expertise, ultimately strengthening their cybersecurity resilience (Bányász, 2020).

Deploying a centralized digital communications infrastructure also reflects the challenges facing the defense sector in handling sensitive data. This infrastructure provides essential information-sharing channels between sectors, allowing attackers to target systems used by the public or defense sector from multiple network directions. Although each sector may have its separate network, the centralized communication path ensures information sharing. However, this centralized communication path increases the vulnerability of the defense sector to cyber attacks. Attackers can exploit any weakness in the infrastructure to gain unauthorized access to sensitive data and disrupt critical operations (Németh & Magyar, 2020). Therefore, ensuring robust security measures and continuous monitoring of a centralized infrastructure is essential to protect national security. In addition, the defense sector should prioritize regular security audits and updates to identify and address potential vulnerabilities in the centralized communication path. The introduction of strong encryption protocols and multi-factor authentication can further enhance the security of sensitive data and deter unauthorized access attempts. By continuously investing in cyber security measures, the defense industry can effectively reduce cyber-attack risks and maintain a strong defense against potential threats (CSA Singapore, 2023b) (Gov.uk, 2023).

Based on the analyses and studies carried out, in which the author has reviewed the relevant literature and open-source technical and professional reports, it is possible to identify the most typical threats affecting the various elements of the defense sector (ENISA, 2023). These threats include cyber-attacks targeting critical infrastructure, such as electrical networks and communication systems, which can disrupt military operations. In addition, the defense sector faces the risk of espionage and information leakage, where foreign organizations seeking strategic advantage can compromise sensitive data and technologies (Németh & Magyar, 2021). The defense sector also faces the challenge of emerging technologies, such as artificial intelligence and autonomous weapons systems, which require continuous adaptation and investment to stay ahead of potential adversaries. A growing concern within the defense sector is the insider threat, where individuals with access to classified information can pose a threat by deliberately or unintentionally leaking sensitive data or sabotaging operations (Canadian Centre for Cyber, 2023) (CISA, 2023).

Table 3 illustrates the most typical vulnerabilities and threats identified in the research for each element of the defence sector.

Table 2. The impact of threats on specific elements of the defense sector

	Police	Army	National security	Disaster management
Phishing	X	X	X	
Ransomware	X		X	X
Malicious codes	X	X		X
DoS, DDoS	X		X	
Social engineering	X	X		X
Cyber espionage		X	X	
Insider threats	X	X		
Supply chain attacks		X		
Advanced persistent threats attacks		X	X	
IoT threats		X	X	
Cyber warfare		X	X	
Data breaches				X
Network failures				X
System errors				X

4. Conclusion

Several risks and vulnerabilities have been identified in the context of digital governance, as shown in the table above. Many of these are not entirely new, but it is clear that new attack vectors are emerging with the spread of digitalization. The table includes only those attack vectors identified as particularly specific to each sector in the research and which, in theory, do not include all typical attack vectors (for example, cloud vulnerabilities currently play a prominent role in very few elements of the defense sector). Elsevier Scopus, ProQuest, Science Direct, and Web of Science are just some of the databases used to find the best solutions for the research topics examined. A review of the relevant literature identified the most common security concerns, threats, and typical attack vectors affecting information and communication systems that serve as critical information infrastructure for some elements of the digital government and defense sector. A comparative analysis of the academic literature and relevant peer-reviewed reports followed this. As a result, it was possible to identify the potential threats most frequently encountered by individual sectors and governments.

As few countries have fully digitized their activities, the conclusions are not specific to one country. The findings suggest that potential threats commonly faced by sectors, and governments include cyber-attacks, data breaches, and information manipulation. These threats pose significant risks to critical information infrastructure's integrity, confidentiality, and availability. Therefore, governments must prioritize information security measures and cooperate internationally to address these challenges. The study also highlights the importance of fostering a strong cybersecurity culture within organizations and raising awareness among individuals. This can be achieved through regular training programs, robust security protocols, and the promotion of best practice adoption, which can help governments strengthen their defenses against cyber threats and protect sensitive cross-border information.

Furthermore, cooperation between governments, private sector organizations, and international organizations is key to coordinating efforts to share information and combat cyber threats. This could include creating joint working groups and information-sharing platforms and developing common cybersecurity standards. In addition, investing in research and development of advanced technologies can help to stay ahead of evolving cyber threats and improve overall cybersecurity capabilities.

Bibliography

Bányász, P. (2020). *A közösségi média lehetőségei és kihívásai a védelmi szférában. Biztonság és honvédelem: Fenntartható biztonság és társadalmi környezet tanulmányok 2*. Budapest, Ludovika Egyetemi Kiadó pp. 587-602. 15 p.

Bányász, P.; Bóta, B.; Csaba, Z. (2019). *A social engineering jelentette veszélyek napjainkban. Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében*. Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, pp. 12-37. 25 p. DOI: https://doi.org/10.37372/mrttvpt.2019.1.1

Bederna, Zs.; Rajnai, Z.; Szadeczky, T. (2021). *Further Strategy Analysis of Cybersecurity Incidents*. Revista Academiei Fortelor Terestre / Land Forces Academy Review 26: 3 pp. 251-260. 10 p. DOI: https://doi.org/10.2478/raft-2021-0032

Canadian Centre for Cyber (2023). *National Cyber Threat Assessnent*. ISSN: 2816-9182, Ottawa, Canada, p. 40.

CISA (2023). *Cybersecurity Best Practices for Smart Cities*. Source: https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf

CSA Singapore (2023). *Advisory on the Secure Development and Provisioning of Distributed Ledger Technology*. Source: https://www.csa.gov.sg/docs/default-source/publications/2023/advisory-on-the-secure-development-and-provisioning-of-distributed-ledger-technology-(dlt)-enabled-services.pdf?sfvrsn=ab42e798_1

CSA Singapore (2023). *Secret Wars: The Digital Threat to Nations by Channel NewsAsia*. Source: https://www.csa.gov.sg/Tips-Resource/videos/secret-wars-the-digital-threat-to-nations-by-channel-newsasia

ENISA (2023). *Good practices for IoT and Smart Infrastructures Tool*. Source: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

Gov.uk (2023). *National Cyber Strategy 2022 Annual Progress Report 2022-2023*. Source: https://www.gov.uk/government/publications/national-cyber-strategy-2022-annual-progress-report-2022-2023/national-cyber-strategy-2022-annual-progress-report-2022-2023-html

Ináncsi, M. (2021). *ATP-csoportok, mint az állam biztonságát veszélyeztető tényezők*. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata 2021: 3 pp. 99-110. 12 p.

Magyar, S.; Bús, N. K (2022). *Modellek felhasználhatósága az információbiztonság területén*. Szakmai Szemle: A

Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata 2022: 4 pp. 86-95. 10 p.

Németh, A.; Magyar, S. (2020). *An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application (Part 1.)*. National Security Review: Periodical of the Military National Security Service 2020: 2 pp. 52-64. 13 p.

Németh, A.; Magyar, S. (2021). *An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application (Part 2.)*. National Security Review: Periodical of the Military National Security Service 2021: 1 pp. 218-231. 14 p.

OECD (2014). *Transformation from analogue to digital government*. Recommendation of the Council on Digital Government Strategies OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406

OECD (2019). *The Path to Becoming a Data-Driven Public Sector*. OECD Digital Government Studies, OECD Publishing, Paris, DOI: https://doi.org/10.1787/059814a7-en

Váczi, D.; Laufer, E.; Szádeczky, T. (2021). *Human risk factors to measure the potential of digital information leakage*. Biztonságtudományi Szemle 3: 3 pp. 55-65. 11 p.