Chapter 10
Information Security Challenges and Solutions in Smart Nations

Andras Toth

Abstract In the study, the author analyzed the basic conceptual environment of smart nations, the information security challenges, threats and dangers inherent in it. In the second half of the research, he seeks to answer the question of what are the most commonly used protection solutions against the threats that arise. To do these, the author has analyzed the available relevant literature and peer-reviewed reports to identify the areas most affected by potential threats, such as networks, clients and users, and the associated potential protection solutions. The analysis has produced a matrix illustrating which vulnerable areas could potentially benefit from protection solutions against typical attack vectors.

Keywords Smart nation · Digital transformation · Information security · Security challenges · Security solutions

10.1 Introduction

The outcomes presented in this article result from a longer research project funded by the Hungarian Academy of Sciences and the Ministry of Innovation and Technology. In the initial part of the research, the author examined the most common vulnerabilities and threats to the Internet of Things components and systems and the possible security solutions. He then looked at the most specific IoT solutions for critical infrastructures and critical information infrastructures and the challenges and opportunities they present. In the research process, the author found that IoT elements have a major impact on the environment around us and, for example, on critical systems used by cities and governments. He concluded that these solutions and services could have a major impact on smart cities, e-governments, and smart nations. On this basis, he started this research described in this paper, aiming to answer the following scientific questions:

A. Toth (✉)
University of Public Service, Budapest, Hungary
e-mail: toth.hir.andras@uni-nke.hu

T. A. Kovács et al. (eds.), *Security-Related Advanced Technologies in Critical Infrastructure Protection*, NATO Science for Peace and Security Series C: Environmental Security, https://doi.org/10.1007/978-94-024-2174-3_10

- What are the main information- and cybersecurity issues in digital governments?
- What are the best practices to save data and privacy in smart nations?

During the research, the author was able to study several international best practices, and participate in the Smart Nation: Strategies, Opportunities and Cybersecurity Management training under the Singapore Cooperation Program, and study e-government systems and solutions in Estonia under the Erasmus+ Cyber Aware Students for Public Administration (CASPA) program. Based on these best practices and the relevant literature and professional reports, the author has analyzed smart nations' information security challenges and solutions.

This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-21-5-NKE-149 New National Excellence Program of the Ministry of Innovation and Technology.

10.2 Methodology

To find the best answers to the research questions, the author started by identifying the relevant literature. For this purpose, he used databases such as:

- Elsevier Scopus;
- ProQuest;
- Science Direct;
- and Web of Science.

Following the literature review, the author has conducted a comparative analysis of academic literature and relevant professional reports to identify the most common security problems affecting smart nations' information and communication systems as critical information infrastructures.

10.3 Research

The first step in the research was to define the concept of a smart nation. Based on the Singapore Smart Nation concept, a smart nation means that people and businesses are empowered through increased access to data, they have greater participation in national tasks through innovative ideas and solutions, and the government uses new digital technologies to serve the needs of citizens better, thus achieving more effective government performance. These achievements provide opportunities for people to live better and more fulfilling lives, made possible by new technological improvements accessible to everybody. Moreover, in this environment, businesses can be more productive and seize the new opportunities of the digital economy. A key element of these solutions is that the nation works with international partners to achieve digital solutions and benefit people and businesses across borders.

The key to success is a complete transformation of public services based on digitalization. This will lead to a much stronger public service, where the key objective is to deliver services efficiently, support innovation, and build public trust. In addition, the data collected, and the technologies used will be harnessed to support the development of the digital economy and society alongside the digital government The digital government blueprint document identified the main parts of the digital government issued by the Singaporean government, which can be seen in Fig. 10.1. It answers the following questions:

Whom does the digital government serve?

- the citizens, the businesses, and the public officers.

What are the elements of the digital government?

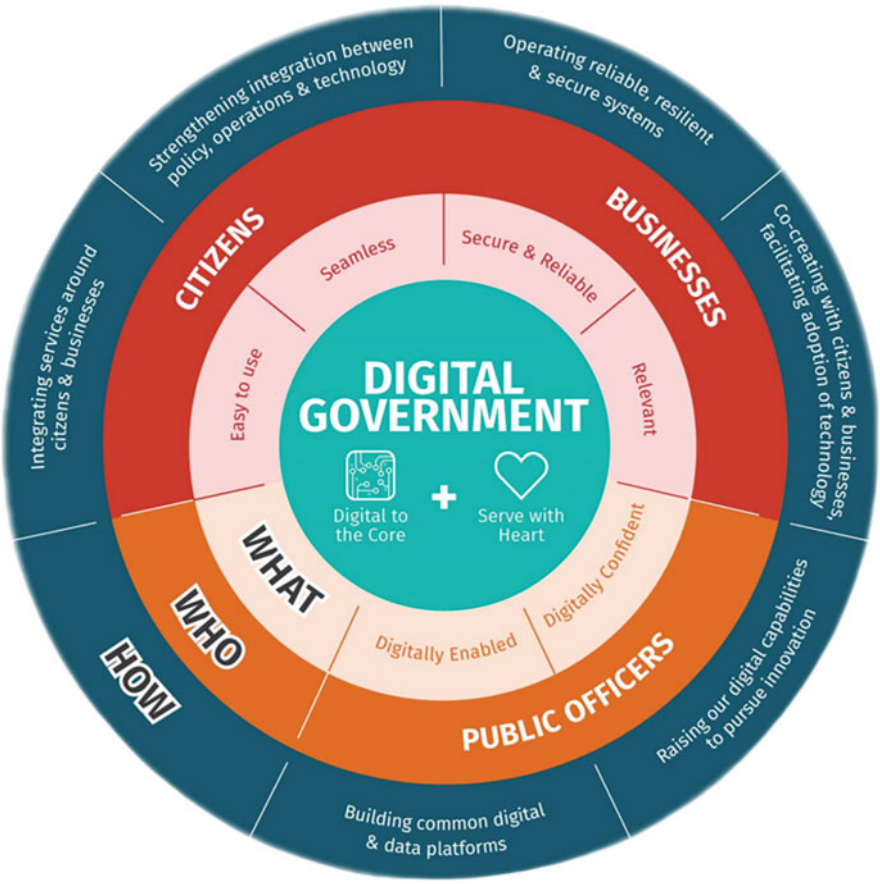

Fig. 10.1 The digital government blueprint [1]

- services that are easy to use, reliable and relevant;
- seamless digital transactions;
- systems and data that are secure;
- digitally enabled and confident service workplaces.

How do we become a digital government?

- the need to strengthen integration between policies, operations, and technologies;
- transforming the government's ICT infrastructure;
- operating reliable, resilient and secure systems;
- raising the digital capabilities to pursue innovation;
- integrating services around citizen and business needs;
- co-creating with citizens and businesses and facilitating the adoption of technology.

A smart nation is a nation where people and businesses are empowered by:

- wider access to data;
- more participation through innovative ideas and solutions;
- a more forward-thinking government that uses technology to serve the needs of citizens better.

This requires the following areas to be transformed:

- health;
- transport;
- urban solutions;
- finance;
- education.

Like Singapore, Estonia has embarked on a similar path of digitization. However, thanks to e-solutions, communicating with the government is fast and convenient for everyone, and the country is operating much more efficiently. The system's success developed there is based on a smart infrastructure that has enabled a secure e-services ecosystem to be built. An important part of this ecosystem is its flexibility and the ability to integrate its different parts while improving e-services and enabling the growth of government systems. Many of the solutions developed there are also similar to the Singapore example. Areas such as healthcare, mobility services (intelligent transport systems, mobile parking), education, financial solutions (e-taxation, e-banking) are also covered.

In addition to analyzing these good practices, the author has also examined reports produced by various professional firms. They also conclude that citizen-centred, universally accessible public services and simple, efficient, and transparent government systems are essential for the development of digital government [2]. The following principles are essential for the development of these systems:

- Decision-making supported by the necessary data, thus building a consensus-based on facts.

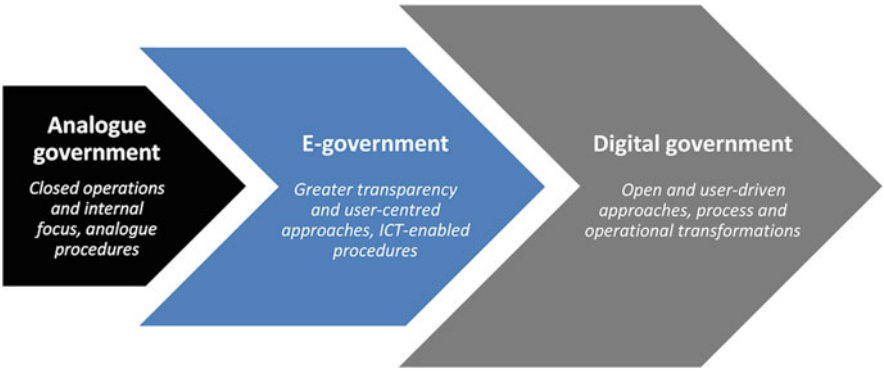

Fig. 10.2 Transformation from analogue to digital government. [4]

- Making transparency and access to information possible, even by default, thus ensuring openness.
- Develop a knowledge-driven cyclical system that follows the cycle of discovery, prototyping and implementation.
- Develop a user-centric approach to user needs through continuous testing.
- Establish and maintain the ability to share data and functions between systems, thereby creating interoperability.
- Restricting unauthorized access to systems and data, thereby ensuring appropriate data protection and security [3].

This is a multi-stage process, which the Organisation for Economic Cooperation and Development (in the following: OECD) explains in more detail in a 2019 report. The figure below shows the steps required to develop digital governance, which is the basis for the report (Fig. 10.2).

Based on the above studies and reports, the author was able to identify the characteristics that describe the information systems of smart nations in terms of security [5].

10.4 Results

The research has identified the key information security threats and risks, attack vectors and vulnerabilities that threaten the secure operation of smart nations and the integrity of the data they handle. In parallel, the security activities that can contribute to ensuring the security of systems, networks, and services, and creating an appropriate operating environment were also identified.

10.4.1 Information Security Challenges in the Smart Nation

The different types of attacks that threaten digital governments very often depend on the vulnerability and/or susceptibility of devices and systems. Vulnerabilities are security weaknesses in systems that attackers can exploit. The most important vulnerabilities are easily available on the Internet to security professionals and criminal hackers alike [6]. Targeted attacks are more time consuming, but they also allow the attackers to rely on tools designed to exploit vulnerabilities. Typical types of vulnerabilities that may appear in the smart nations include:

- Network vulnerabilities: are caused by insecure operating systems and network architecture. This includes server and host (endpoint) failures, misconfigured wireless network access points and firewalls, and insecure network protocols.
- Hardware vulnerabilities: exploitable weaknesses in computer hardware that affect almost all systems and system components, including desktops, laptops, servers, and smartphones.
- Vulnerabilities in software and applications: this includes coding errors or software that does not respond to certain requests in the expected way. Software vulnerabilities are often caused by a bug, flaw, or weakness in the software.
- Zero-day vulnerabilities: security flaws that have been discovered by criminals but are not known to software developers and therefore have not been patched. The term refers to the number of days the vendor has to patch the vulnerability (Zero-day exploits are code that compromises zero-day vulnerabilities) [7].

Information security threats can basically be divided into three main categories, namely network threats, client threats and user threats.

10.4.1.1 Threats to Networks

Misconfiguration of network devices provides a possible route for attackers to get into the systems. Common vulnerabilities leading to exploitation include open access control, weak encryption and passwords, devices using default installation settings, and devices without the latest security patches [8]. The most common network threats that can compromise information and communication systems operating in the digital state are:

- sniffing;
- eavesdropping;
- session hijacking;
- IP spoofing;
- ARP poisoning;
- DNS poisoning [9].

Table 10.1 illustrates the most typical characteristics of each threat.

Table 10.1 Key characteristics of network threats

Attack vectors	Characteristics and features
sniffing	Interception of data by recording network traffic.
eavesdropping	Intrusion, when an attacker attempts to steal sensitive information transmitted over the network.
session hijacking	Exploiting a valid session.
IP spoofing	Creating Internet protocols with a fake IP address.
ARP poisoning	The attacker forwards ARP messages to a local network.
DNS poisoning	Inject incorrect domain name system information into the resolver cache.

Table 10.2 Key characteristics of threats to clients

Attack vectors	Characteristics and features
overload attacks	Attackers seek to make a machine or network resource inaccessible to intended users.
targeted attacks	A covert and continuous series of attacks, typically against a specific person, persons, or organization.
backdoor attacks	Disables the normal authentication methods for accessing the system.
man-in-the-middle attacks	The attacker covertly takes over and changes the relationships between the communicating parties.
malware attacks	Attackers create and deliver malicious software to a victim's device or system for the purpose of gaining access to personal data or causing damage to the device, usually for financial gain.
IoT attacks	An attacker exploits the vulnerability of IoT devices to take control of them or turn them into a zombie network.

10.4.1.2 Threats to Clients

Increasingly sophisticated cyber-attacks such as malware, phishing, machine learning and artificial intelligence, or cryptocurrencies, are exposing companies, governments, and individuals' data and assets at constant risk [10]. This is especially true in the digital nation, where all information and data are exchanged, stored, and processed online. Moreover, these attacks are not only directed against networks; in many cases, they are directed against the hosts (clients) running on the systems. The most common attacks on clients are:

- overload attacks;
- targeted attacks;
- backdoor attacks;
- man-in-the-middle attacks;
- malware attacks;
- IoT attacks. [11]

Table 10.2 illustrates the most typical characteristics of each threat.

10.4.1.3 Threats to Users

In the digital state, users have a particularly heavy responsibility to handle sensitive data properly. As a result, they and/or the data and systems they manage may be exposed to several external and internal threats, which have already been mentioned above. However, some methods rely explicitly on the users' good faith or even inattention. The most common attacks against users, in addition to those mentioned above, are some attacks that can also be directed against users:

- social engineering attacks;
- deepfake;
- fake news [12].

Table 10.3 illustrates the most typical characteristics of each threat.

10.4.2 Information Security Solutions in the Smart Nation

The research has also identified the most typical solutions to these threats, which can be applied to several different areas. Accordingly, the author has compiled a matrix that illustrates the areas in which each protection solution can help to protect information and systems in the context of the smart nation. These protection solutions and their potential application in each area are listed in Table 10.3.

The above table shows that there is a huge need for information security professionals, both on the regulatory and technical side, in the context of digitalization and thus the development of the smart nations. Public organizations, businesses, and even users cannot afford to ignore the increasingly sophisticated threats emerging in their private lives and working environments. This is the reason why continuous training and upgrading sessions are essential to develop and maintain digital literacy (Table 10.4).

Table 10.3 Key characteristics of threats to users

Attack vectors	Characteristics and features
Social engineering attacks	Social engineering attacks typically involve some form of psychological manipulation, and exploitable human traits that the attackers are trying to abuse. The aim is to manipulate unsuspecting users to provide confidential or sensitive information.
deepfake	A person who wants to influence a user creates a fake image or video using deep learning technology, which may be used to threaten the victim, force him or her to perform an action that is harmful to the system's operation or provide sensitive information.
Fake news	*They are* articles or stories that are created to misinform or mislead readers deliberately. Fake news is typically created to influence public opinion, for example, to influence the population's political views, thereby undermining public confidence in political leadership and thus affecting the proper functioning of the smart nation.

Table 10.4 Protection solutions and their application areas

Security solutions	Networks	Clients	Users
24/7 monitoring	X	X	X
Access management	X	X	X
Avoiding suspicious links	X	X	X
Encryption	X	X	
Intrusion detection	X	X	
Network monitoring and firewalls	X	X	
Network segmentation	X		
Physical security	X	X	
Practicing basic safety hygiene	X	X	X
Regular (encrypted) backups	X	X	
Safety training	X	X	X
Software update and patches	X	X	
Spreading awareness	X	X	X
Use of multifactor authentication	X	X	X
Use of protected communications	X	X	
Use of security software	X	X	
Use of VPN	X	X	X
Use reliable anti-malware software	X	X	
Use secure authentication methods	X	X	X

10.5 Conclusion

The author has looked at the challenges digital states face in protecting their data and the potential threats to protecting data, networks, and the smart nation's functioning. Personal data protection, including sensitive personal data, is of paramount importance from a data protection perspective. A compromise of such data could result in serious financial and emotional damage or a significant loss of prestige for some actors in the digital state. On the other hand, adequate data protection can increase trust among the public and encourage the use of established e-services and applications, thus enhancing the development of the digital ecosystem, contributing to the development of digital competencies and the digital economy. These are essential today if a state wants to keep pace with the digital economy and maintain stability, for example, within the European Union. Subsequent paragraphs, however, are indented.

The answer to the second question, which are the most effective security solutions for smart nations, cannot be clearly defined. There are several potential threats from cyberspace that affect the security of the networks, the devices used and the population (users). These vulnerabilities and threats pose serious challenges to cyber security professionals, as the accelerating pace of digitalisation and development brings new attack vectors that are very difficult for the defence community to track. By the time a countermeasure is found for a given type of attack, attackers

have developed a more sophisticated, harder to detect method that exploits possible zero-day vulnerabilities in the devices, creating previously unknown problems for the operator.

References

1. The Singapore Government: Digital government blueprint (2018)
2. Nyikes, Z., Kovács, T.A., Tokody, D.: In situ testing of rail damages in accordance with Industry 4.0. J. Phys. Conf. Ser. (1742-6588 1742-6596) **1045**, 1–6 (2018). https://doi.org/10.1088/1742-6596/1045/1/012032
3. Observatory of Public Sector Innovation: Digital Transformation. https://oecd-opsi.org/guide/digital-transformation/. Last accessed 25 Sept 2021
4. OECD: The Path to Becoming a Data-Driven Public Sector OECD digital government studies. OECD Publishing, Paris (2019). https://doi.org/10.1787/059814a7-en
5. Nyikes, Z.: Digital competence and the safety awareness base on the assessments results of the Middle East-European generations. Proc. Manuf. (2351-9789) **22**, 916–922 (2018). https://doi.org/10.1016/j.promfg.2018.03.130
6. Balázs, Á., Nyikes, Z., Kovács, T.A.: Building protection with composite materials application. Key Eng. Mater. (1013-9826 1662-9795) **755**, 286–291 (2017). https://doi.org/10.4028/www.scientific.net/KEM.755.286
7. Sándor, M.: The interfaces of IT operation, development and cyber security, approached from the point of view of technical toolsets. Natl. Secur. Rev. **2**, 73–85 (2019). 13 p
8. Nyikes, Z.: Contemporary digital competency review. Interdiscip. Descr. Complex Syst. (1334-4684 1334-4676) **16**(1), 124–131 (2018). https://doi.org/10.7906/indecs.16.1.9
9. Sinha, P., Kumar Rai, A., Bhushan, B.: Information Security threats and attacks with conceivable counteraction. In: 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), vol. 1, pp. 1208–1213 (2019, July). https://doi.org/10.1109/ICICICT46008.2019.8993384
10. Nyikes, Z.: Creation proposal for the digital competency framework of the middle-east European region. Key Eng. Mater. (1013-9826 1662-9795) **755**, 106–111 (2017). https://doi.org/10.4028/www.scientific.net/KEM.755.106
11. Szádeczky, T.: Security of E-government website encryption in Germany and Hungary. Acad. Appl. Res. Military Public Manag. Sci. **17**(2), 127–138 (2018). ISSN 2498-5392
12. Péter, B.: A közösségi média lehetőségei és kihívásai a védelmi szférában, Biztonság és honvédelem : Fenntartható biztonság és társadalmi környezet tanulmányok 2, Budapest, Magyarország : Ludovika Egyetemi Kiadó pp. 587–602 (2020)