CHALLENGES OF FINANCING THE CYBER SECURITY - COMPARISON OF CZECH AND SWEDISH PRACTICE

Tadeáš Pala

Abstract: *The goal of this paper is to assess important challenges of digitalization process. Czech state fails to incorporate both modern technology and useful legislation. Therefore, it lags in the introduction of modern trends especially in the field of cybersecurity. We have analyzed the DESI indicator to identify the state's commitment to developing digitization in general. We used statistical data on financial investments in the NÚKIB (National and Cyber Information Security Agency), the administrative body in charge of cybersecurity. For comparison, we presented an example of good practice, which we consider to be Sweden ranking high in DESI.*

Keywords: *Cybersecurity; DESI; NÚKIB; Comparison*

JEL Classification: *F52; F53; H56; L86*

1 INTRODUCTION

In the last decade, the issue of cyber security has been repeatedly mentioned in all strategic state security plans (Ministry of Defense, 2011). Cyber threats themselves are, of course, much older and date back to the beginning of the development of cybernetics. They gain in importance especially with the advent of the Internet as a global network. The development of digitization and electronization in all aspects of the functioning of society has become one of the framing trends of the new millennium. This trend can be used to demonstrate some basic economic tendencies related to the development of society and progress as such. The initial impulse of "cybernetics" can be identified already during the Second World War, when this segment significantly helped the Allies to win over Nazi technology. During the Cold War, the cybernetics sector fell under the jurisdiction of state authorities, mainly due to its complexity and strategic importance in the context of the power struggle in the bipolar world order. It is common knowledge that the "Internet" itself was originally a military network, which was followed by the "World Wide Web" as an instrument of advanced scientific research in Western countries. The privatization and commercialization of the Internet took place in the late 1980s and especially the 1990s, when—in the euphoria of the disintegration of the bipolar world—there was a mass development of technology and therefore of cyberspace. At that time, the control of state and scientific institutions over the organically developing Internet network was slowing down, and private companies and individuals were taking up the reins of development, especially the development of the Internet.

It is the popularity of digital tools among the population that usually makes the state start dealing with this issue and offer its services in a digitized form. At that moment, you can talk about the so-called e-government.

2 CYBERSECURITY AND ITS DEIFFICULT MEASURABILITY

The central theme of this paper is to analyze the level of security in the e-government of the Czech Republic. We will, therefore, talk mainly about cybersecurity whose theoretical and practical aspects we briefly outline in this chapter. Cybersecurity as such has different definitions, but they all try to follow similar principles. It is possible to work with the definition used in the Czech environment:

"Cyber security is a set of organizational, political, legal, technical and educational measures and tools aimed at ensuring secure, protected and resilient cyberspace in the Czech Republic, both for public and private sector entities as well as for the general Czech public."

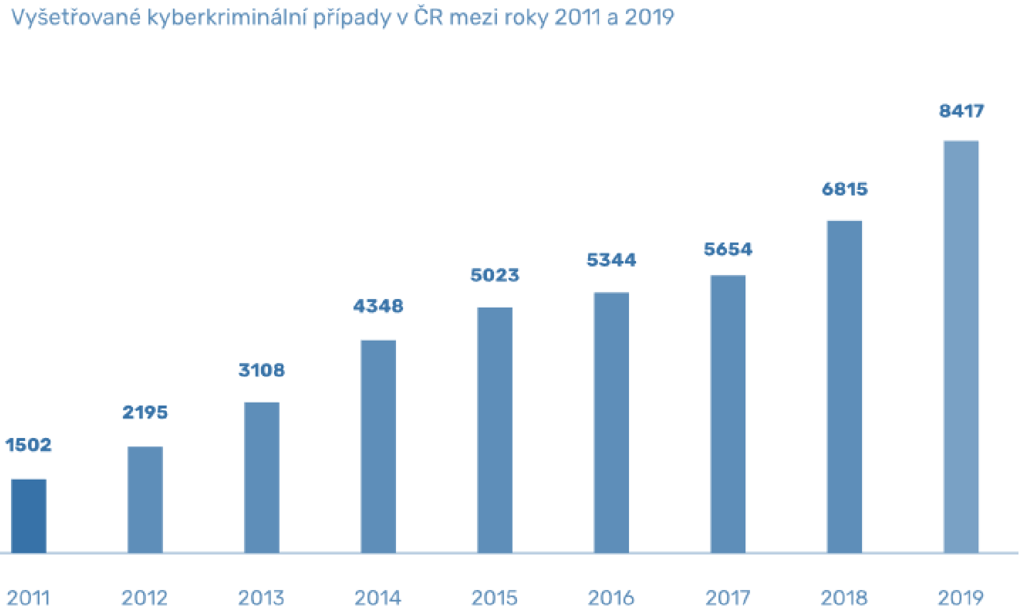
(NCKB, 2015)

The so-called CIA Triad is generally accepted as the key pillars of cybersecurity. It has nothing to do with the secret service, but it is an acronym for the following words: confidentiality, integrity, availability. These three pillars are used in both the private and public sectors (Bašta and Kolouch, 2019).

Conventional indicators of crime have long been based on the incidence and frequency of criminal offenses, with the executive and judicial authorities recording these offenses and producing various statistics. In the Czech environment, statistics from the Ministry of the Interior (the crime map application, which has its shortcomings) (MVČR, 2021) try to report on this. Some indexes seek international comparisons, such as Crime Index by City (Numbeo, 2021) some of the perception indexes. However, they are still more of a rough statistic, given the problematic methodology and, in particular, the different legal frameworks and police procedures. The main shortcoming is the statistical intangibility of crime, which has not been revealed.

In cyberspace, the situation is even more complicated. Efforts to quantitatively measure the number of attacks are lagging behind, mainly due to the fact that it is extremely important to take into account the qualitative impact of the attack.

Graph n. 1 Investigated criminal cases in Czech Republic between 2011 and 2019



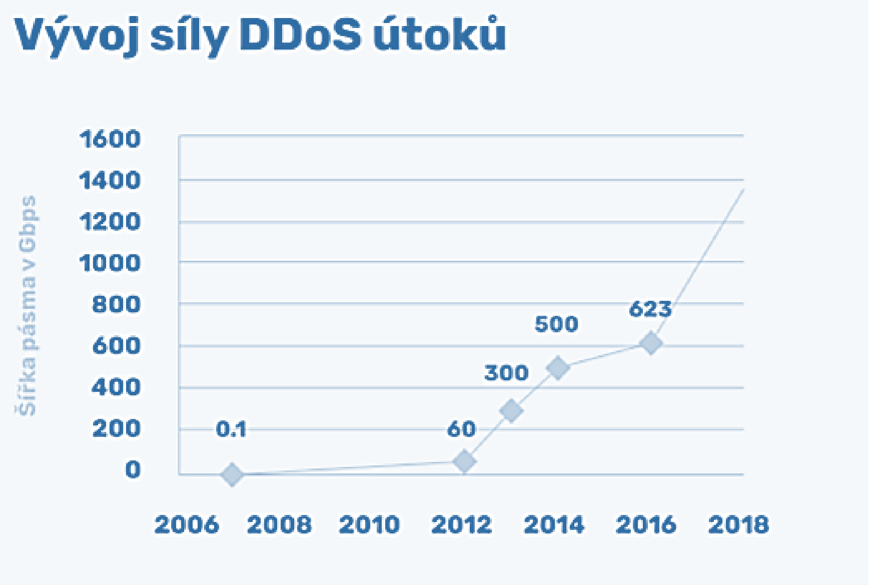
Source: NÚKIB and Policie ČR (2019)

Thus, if we omit the problem of the undetectable ratio between detected and reported cybercrimes, we can look into the graph outlining the increase in the number of cybercrime cases investigated by the Police of the Czech Republic. This graph shows an increasing trend. However, its informative value is limited by the above-mentioned factors. The development of technology marks the intensity of attacks as well as the targets, along with the appropriate methodology for solving and implementing defense and cyber security. This fact can be illustrated by the example of the so-called DDoS attacks. This type of attack is especially dangerous, as it can shut down a state's infrastructure. Typically, these are attacks on the website of the Ministry of Foreign Affairs, or on the operational interfaces of some government. (E15, 2017)

The very logic of the DDoS attacks is based on a large number of network attacks, either in an automated or standard way. In contrast, very frequent recent attacks of the so-called ransomware type can be relatively simple in terms of sophistication. Theoretically, a single penetration is enough to shut down a soft goal of (strategic) infrastructure, such as a regional or university hospital (Český rozhlas, 2020). In the case of an attack on these and similar elements of the strategic infrastructure, it is very difficult to determine the cost of restoring things. The authorities, who try to resolve the situation, are, for logical reasons, reluctant to describe the details because they do not want to do the work of potential future attackers simpler. It is quite possible that in some cases, the extorted money will be paid. In the case of the attack on the hospital in the town of Benešov, the management reported a loss of CZK 59 million, which was certainly not the entire amount but rather a lost profit for non-performed operations. It should be taken into consideration that resolving the situation itself has certainly cost the competent authorities a large amount of money.

It is the change in both the intensity and sophistication of this type of attack that can be demonstrated in the chart presented by NÚKIB (National and Cyber Information Security Agency) in its annual reports.

Graph n. 2 Development of the power of DDos attacks - in Gbps



Source: NÚKIB (2019)

Looking at these data, the hypothesis that quantitative metrics can be helpful in identifying trends is confirmed, but it is insufficient to accurately identify the degree of risk. In the development of the strength of DDoS attacks, we can primarily see the progress of the technology itself. It is necessary to put this information in the context with the development of the Internet, with the speed and the capacity of connections, etc. If we could determine some kind of technological "inflation" in this respect, we would get essentially more accurate data about the real development of cyberattacks. The situation is further complicated by the fact that the global infrastructure is developing rapidly and does not respect national borders. Therefore it is very difficult to relate the real situation to the actions of individual public authorities of the given states. Another factor that complicates objectification is that cyberattacks are subject to current technological trends as well as to the development of the international situation. An already well-known example is the unprecedented cyber campaign against Estonia, which began on August 27, 2007, in response to the sharp deterioration in relations with the Russian Federation. At that time, the Estonian government had removed the controversial bronze statue of a Soviet soldier. Without acknowledging anything, Russia provably and verifiably attacked Estonian e-government structures through a series of massive cyberattacks. This example illustrates the great variability in the number and intensity of attacks (Schmidt, 2013).

Cyberspace has generally become a breeding ground for certain state operations, whether covert or clandestine. Cyberattacks are typical examples of covert operations, where the goal is to carry out the action together with keeping its sponsor secret. Cyberattacks have become part of the hybridization of warfare. This is therefore an example of the above-mentioned concept of "plausible deniability." As mentioned, it is not easy to identify the extent of a cyber threat. Especially for government and decision makers, it is therefore a relatively big challenge to identify the right countermeasures and means to ensure cyber security.

It is also difficult to determine the extent to which states are trying to tackle this problem, as it is a very difficult variable to measure. An objectively determinable level of the development of digitization and electronization in the public sector is practically impossible. So we only have to make do with approximate indicators.

3 THE BACKWARDNESS OF PUBLIC ADMINISTRATION AS A MAJOR CHALLENGE

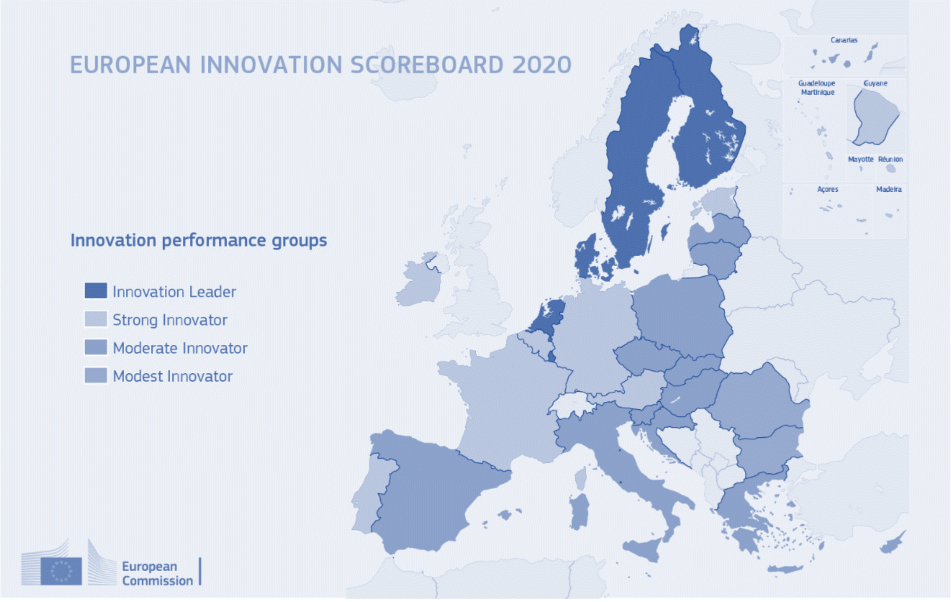
However, in addition to the huge progress made in the services available to internet users, new threats and crime sectors have also been developing. Generally, the mentioned problems are dealt with by various theories, which try to professionally classify and define the dangers in cyberspace. Theories that describe security from the perspective of nation states sometimes work with terms such as "cybersecurity" and "cyberdefence" which merge together into one term "cyberresilience" (Galinec and Steingartner, 2017). This term seems to be a good description of a problem and can function as a hyperonym for other sub-forms of cybersecurity. This term is relevant for issues related to e-government and digitization because security—including the security of the state—is the responsibility of both the government and authorities. These two kinds of security directly or indirectly affect citizens. Cybercrime, as well as cyberattacks carried out by other actors, are logically closely followed by technological innovations. In some cases, both cybercrime and cyberattacks even set new trends of development. Thus, with a certain logical delay, a new discipline—cybersecurity—appears as a reaction to cyberattacks. This chronological development is typical of a large number of evolving technologies.

Within this order, it is also possible to observe the reaction of states, which usually comes only after a more flexible reaction of the private sector. However, the cumbersomeness of the state sector is not only related to the adaptation of modern technologies such as digitization and e-government but it is also related to the issues of cyber security. Some states are trying to create a legal and functional framework for setting the boundaries of new segments, but in the case of such a decentralized and globalized environment as cyberspace, states take the place of the so-called "laggard." The theory of "diffusion of innovations," which first applied the term "laggard," was introduced by Rogers (2003). It works with the various stages of innovation development and identifies the various actors in this process. This theory is widely used in the social sciences or anthropology, but its principles can be applied to the case of the development of innovations in public administration. Therefore, within the framework of e-government, the Czech public administration presently finds itself in the role of “a late adopter” or even the “laggard.”

At the same time, reality shows that it is the state that should ideally play the role of an innovator, early adopter, and, especially in legislative matters, the role of the "trendsetter.” At least, the state should be able to create a suitable environment for innovation and development. However, according to many indicators, it is not possible to achieve this condition in the Czech Republic.

This statement is proved, for instance, by the statistics of international comparison—the European Innovation Scoreboard 2020. In 2020, it included the Czech Republic among the so-called “Moderate Innovators,” which is the penultimate group.

Graph n. 3 European innovation scoreboard 2020



Source: European Commission (2020)

In the following chapters, the degree of the backwardness of the Czech e-government and digitization will be demonstrated on the DESI indicator, which will be one of the key tools for this analysis.

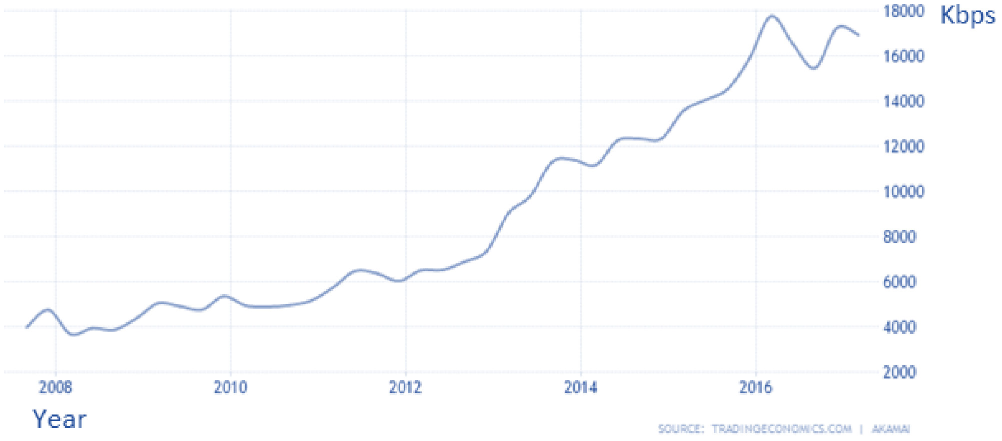
Due to the delay of the public sector behind the private sector, there is a problem in coping with negative and deviant players. As indicated above, the cybercrime actors who closely follow the private sector are in many respects ahead of the slowly adapting public sector. This fact also is to the detriment of public administration. The public sector is also under pressure not only from hackers and cybercriminals, but is also the victim of attacks by other powers that do not share the idea of peaceful coexistence, both in real and virtual space. Cybercrime and cyber "war" are also often intertwined, as foreign powers may hire private hackers for so-called "foreign flag" operations. The attributability and consequent provability and subsequent law (Schmidt, 2013) enforcement related to cyberattacks is therefore very complicated and almost impossible in practice.

The so-called concept of plausible deniability is applied here. This concept has been present in all conflicts since time immemorial, but its factual definition was formulated by former CIA director Allen Dulles in the 1960s. Plausible deniability aims to disguise the activities of particular players so that there is no evidence of their involvement, or that the suspicion is countered by the principle of "claim against claim" (Carlisle, 2003). In the event of a cyberattack, states often use the services of private and criminal organizations, or impersonate them, and ensure that there is no demonstrable electronic trace.

The reality is that the position of state administration and decision makers is therefore quite complex, given that the population under the influence of the demonstration effect requires the development of new technologies. All this is happening in contexts where a number of pitfalls, of both the private and public natures, are already "lurking in the waters." States, including the Czech Republic, must therefore respond to the situation in some way. It is in their interest to create quality defense structures, a legal framework and law enforcement tools in cyberspace.

Cybercrime, like conventional crime, is very difficult to eradicate, especially because of its difficult identification and measurability. If we know that the tools for measuring conventional crime are very "approximate," mainly due to the fact that only detected crime can be measured, then cybercrime is an even bigger problem, due to its technological complexity and virtuality. Legislative frameworks affecting physical or conventional crime have had a chance to evolve over many years and centuries with society, but cyberspace rules must respond to an unprecedented rush. The very definition of cybercrime is problematic. In many cases, it manages to grow old before it is put into functional practice.

Graph n. 4 Czech Republic Internet Speed 2007-2017 - in Kbps.



Source: (Trading Economics, 2021)

A suitable example may be the graph of the development of the average connection speed in the Czech Republic. The increase in speed is quite rapid, as well as other secondary indicators such as transferred data, number of domains, etc. It is clear that the development of cyberspace capacities, at least in the Czech context, has a significant advantage over the state administration. It happens despite the phenomena such as the increase in network quality requirements, larger volumes of transferred data or the development of e-commerce services, which to some extent explain its development capacities.

4 DIGITALIZATION IN THE CZECH REPUBLIC – DESI INDICATOR

One of these indicators is DESI (Digital Economy and Society Index), which is based on Eurostat statistics. It is a relatively complex and sophisticated tool not only in the EU context. Its main advantages are the large number of observed variables, longitudinality, and the comparison of a comparable group of countries. Since 2003, it has been identifying important indicators that have been gradually expanding along with the development of the entire cyber-segment.

The DESI indicator reports an annual summary of statistics, dominated by an overall index for each of the member states. This index has been published since 2014. However, in 2017 the methodology was changed. From the original data, which was presented on a scale of 0 to 1 with a resolution of hundredths, in 2017 it was switched to a scale from 0 to 100 score points. In the statistics, this difference is processed in favor of a newer methodology. The original data are therefore remade on a 100-point scale. Another problem is the recalculation of values for previous years. The DESI annually publishes the main scores for individual states, nevertheless it puts them in the context of previous years. Part of the calculation is the recalculation of the values of previous results. This slightly complicates the coherence of the data within the longitudinal view of the statistics themselves. For comparison purposes, we therefore relied on individual annual reports and used original numbers, not the recalculated ones.

The DESI index score will serve us as a first dependent variable examined, indicating thus the kind of development of digitization in the Czech Republic. Furthermore, this article we will be based on the logical hypothesis that with the growing cyberspace, expanding digitization and electronization, it is in the interest of the state to respond appropriately in the cyber security segment. It was the need for an adequate increase in cyber security capacities that was argued in the introductory part of the article, as were main pitfalls in this area.

In our hypothesis, we therefore observe a growing cyberspace and consider that the state must respond adequately. If we accept the DESI index as an indicator of the development of the digital sector and e-government (albeit with all the limits we are aware of), it is necessary to find the right indicator of an appropriate state response. As mentioned, it was difficult to determine the DESI indicator as “objectively valid”. Given this fact, it is even more complicated to choose the appropriate cyber defense indicator or the appropriate cyber security indicator. According to the arguments presented above, we already know that the number of performed—or rather detected—cyberattacks as a suitable variable fails. Other indicators, such as the robustness of cyber defense, are very difficult to measure or they are classified. What can be done in such a situation? It seems to be inevitable to focus on the available economic data. We assume that the state that takes its cyber security seriously will also invest appropriately in its defense capabilities. This assumption is valid in a conventional environment and therefore we dare to extrapolate this logic to the cyber security segment.

5 THE NEED FOR SECURITY – NÚKIB

The state that is aware of the need to invest in cyber security is taking a wide range of measures to enable it to respond properly and in a timely manner. State cyber security is therefore of interest to many state institutions, namely to police authorities and intelligence, both external and internal. In the case of the Czech environment, cyber security is therefore dealt with by both the Police of the Czech Republic and the internal intelligence of the BIS (Security Information Service), as well as by the VZ (Military Intelligence). There is a reasonable assumption that ÚZSI (Office for Foreign Relations and Information) also deals with this issue. At the same time, cyber security is to some extent addressed at every subsidiary level of state institutions, ministries, administration offices, etc. However, the Czech state also decided to respond to both the situation of rapid cyberspace development and its threats by creating a special professional workplace. In 2011, the so-called NCKB (National Center for Cyber Security) was established within the NBÚ (National Security Authority). In 2017, the independent NÚKIB agency (National Cyber and Information Security Agency) was established, which was based on the Cyber Security Act and its amendment of 2014. It is a central administrative body for cyber security.

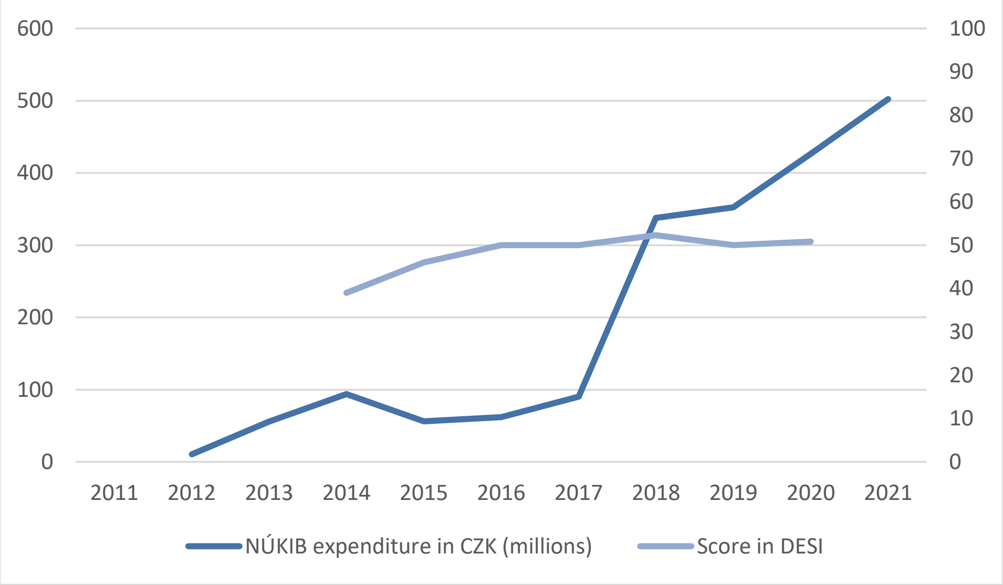
"NÚKIB is the central administrative body for cyber security, including the protection of classified information in the field of information and communication systems and cryptographic protection. It is also in charge of the issue of publicly regulated services within the Galileo satellite system. It was established on 1 August 2017 on the basis of Act No. 205/2017 Coll., which amended Act No. 181/2014 Coll., On Cyber Security and on Amendments to Related Acts (the Cyber Security Act)."

(NÚKIB, 2018)

It is this body, with its central powers, that is at the center of our attention. It is at this point that we will try to measure, at least approximately, the determination, activity and ability of the state to respond to the expanding threats in cyberspace. The Agency does not function as a part of executive power, or does not have a police role. However, in practice, its task is to gather information, create strategies and legislative frameworks for Czech cyberspace. Therefore, apart from all other national cyber activities, which are either scattered and cannot be properly consolidated or are subject to secrecy, all that remains is to focus on the NÚKIB.

NÚKIB's activities are diverse and many of them are logically inaccessible to the public, but what is accessible is budget information. It is a separate chapter of the state budget number 378, which belongs to NÚKIB, which will enable us to at least roughly identify the state's determination to invest in cyber security. Of course, the factor of "efficiency" or qualification of the competent authority remains aside, which limits the informative value of budget information. However, for the purposes of our analysis, the information on the budget increase will tell us to what extent the state apparatus considers cyber threats to be a danger.

Graph n. 5 Relation between NÚKIB expenditure and DESI score of the Czech Republic – in CZK (millions)



Source: Author based on NÚKIB and DESI (2021)

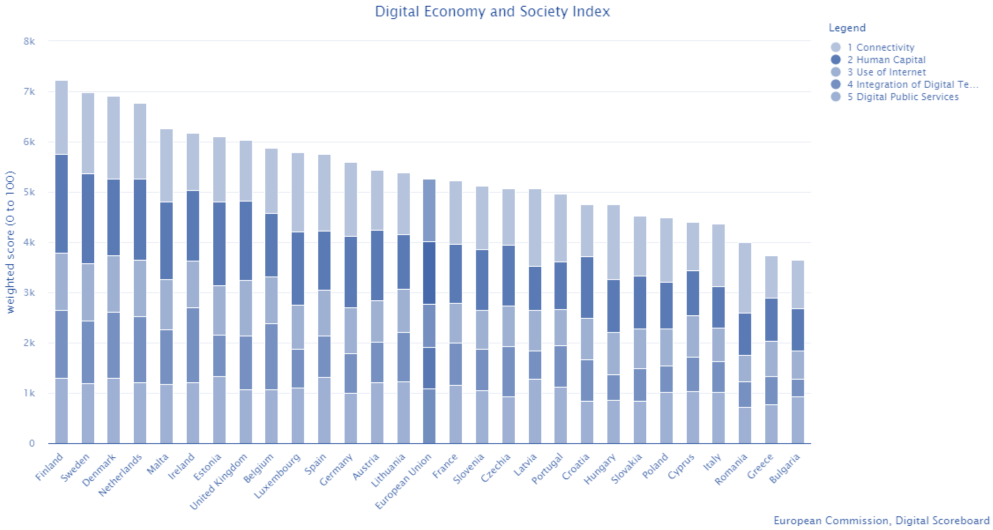
There were some complications in interpreting the collected data related to the budgets allocated for the NÚKIB. These were mainly due to the transformation of the institution between 2016 and 2017, given that until 2016 this institution had been called the NCKB (National Center for Cyber Security) and operated under the NBÚ (National Security Authority). The data were therefore drawn from the annual reports of the NBÚ, and since 2017 from the annual reports of the independent NCKB. It was therefore slightly complicated to find relevant data for 2016, when the transition took place. Another problem, which is probably related to the initial phase of the organization's operation, was the issue of budget spending. In the first years of operation of the independent NCKB, it was not possible to use up all the resources allocated for this chapter of the state budget. In statistical data, we therefore publish values that were actually spent and are reported as real expenditures.

Thus, the main focus of this article is as follows: it is the relationship between the development of digitization in the Czech Republic (the development being measured by the DESI indicator) and the willingness of the state to address issues related to cyber security (the willingness being measured by expenditure on the relevant central administrative office of cyber security).

6 SWEDISH GOOD PRACTICE

Within the comprehensive DESI index 2020 indicator, the Czech Republic is in the 12th place from the bottom and in the 3rd place below the EU average as a whole. The generally recognized leaders in e-government issues in the European environment are mainly the Scandinavian countries. For the needs of our analysis, the example of Sweden was chosen. Sweden has long been ranked in the DESI statistics at the top. It is particularly important for comparison with the Czech Republic due to almost the same population (according to the Eurostat the Czech Republic had a population of 10 693 900 of the 1st of January 2020. According to available figures, Sweden has a population of 10 327 600). Even though the population is about the same, Sweden manages to maintain its reputation as a state with a highly developed cyber and virtual environment. For 2020, the DESI indicator ranked it second in the EU as a whole. The Swedish approach to e-governance can therefore be considered an example of good practice.

Graph n. 6 Digital Economy and Society Index 2020



Source: European Commission, (2020)

In this analysis, we will take a closer look at how Sweden approaches cyber security issues and what importance it attaches to it. We will use the similar model to the one applied for the Czech Republic. We will be interested in the development trends of the DESI index and expenditures on the main national administrative body dealing with cyber security. In the case of Sweden, this is the so-called: Försvarets radioanstalt, FRA (Försvarets radioanstalt in english - National Defence Radio Establishment)

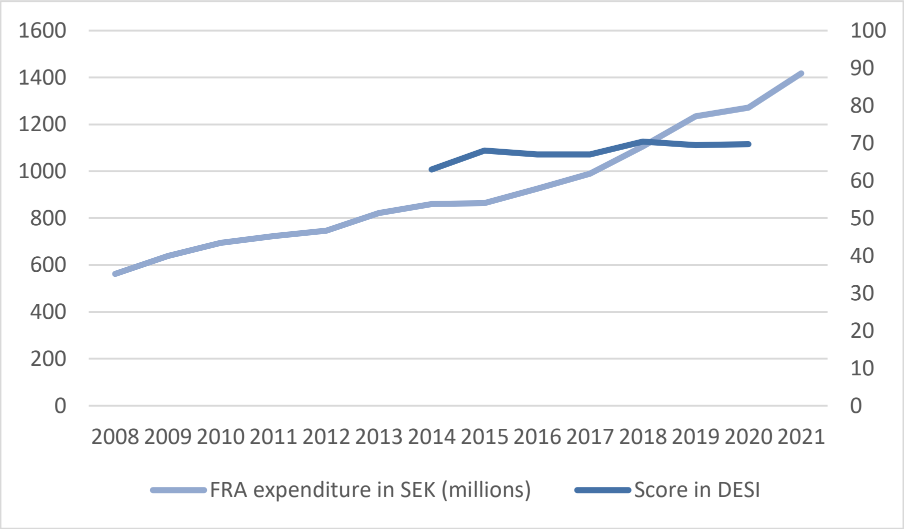
This is the office originally focusing on SIGINT, which has its roots in the period of the Second World War. It is therefore necessary to say in advance that the entire budget is not allocated for the needs of cyber security but also for the operation of radio equipment. In any case, the information on expenditure on this institution is of certain telling value. As for the Czech Republic, the NCKB also shields other than cyber security activities. It is, for example, responsible for the administration of the Galileo satellite navigation system project.

The situation analyzed in Sweden is diametrically different from that of the Czech Republic. From the available data, it is clear that investments in the office responsible for cybersecurity are significant and have a long-term and continuous growing trend. From the first available data from 2008, we can see a steady annual increase. The fact that the data are available and consistent retrospectively over 12 years indicates that Sweden considers this issue to be important. It thus tries to respond to the above-mentioned rapid development of cyberspace systematically. Behind these steps, it is possible to recognize an effort to reduce the significance of the gap between cybercrime and the reaction of the state. It should, of course, be noted that Sweden has long been at a higher level of living standard than the Czech Republic, which may in some respects slightly reduce the importance of the absolute values of the funds invested.

However, it is possible that apart from investing in human resources, technology prices in the global IT market do not vary much across countries. It is known from the experience of some tenders that some contracts are even more expensive in poorer countries, mainly due to the presence of corruption, the backwardness of legislation, or a weaker market position. It is, therefore, not possible to determine whether the prices for IT services are definitely more expensive in Sweden than in the Czech Republic. What can be said is the fact that Swedish investments have been several times higher in the long run. In the first graph, we can see the budgets of the relevant Swedish administrative authority in absolute values of the Swedish kronor.

In the context of the DESI indicator, which is also shown in the graph, it is evident that it is stable between 60 and 70 points. This is approximately 20 points more than the Czech Republic in a comparable period.

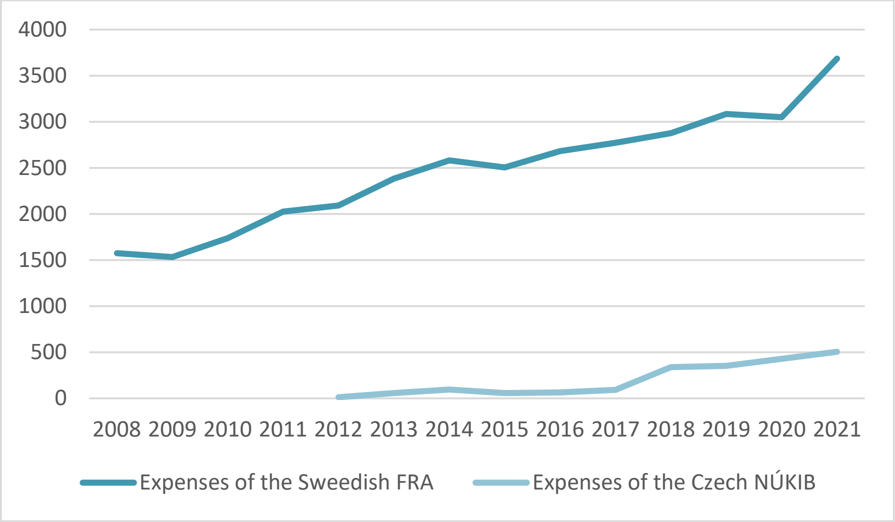
Graph n. 7 >> Relation between FRA expenditure and DESI score of Sweden - in SEK (millions)



Source: (Author based on DESI and FRA 2021)

If we compare the purely financial dimension of the two countries, as indicated in the next graph, it can be seen that the numbers are indeed very different. Despite the increased efforts of the Czech Republic, a multiple difference is still visible. On the chart, Swedish values are converted into Czech crowns for each year according to the then-relevant exchange rates.

Graph n. 8 >> Expenditures of NÚKIB and FRA compared – in CZK (millions)



Source: Author based on DESI and NÚKIB (2018)

The Czech Republic is not doing very well compared to the best ones, but it is trying to improve.

In further research, it would be worth analyzing other indicators and deciphering more detailed data.

7 TRUST (AT RISK) AS A KEY ELEMENT

It is crucial for our article to understand the link between the development of e-government and cybersecurity. The arguments presented in the following chapters will help us to understand this interconnectedness. However, one of the most important arguments related to the state’s ability (or inability) to innovate is discussed in the article Mitigating e-governance avoidance (Abdelhamid and Kisekka, 2019). Its authors emphasize a simple but important idea, which works with the fact that some failures in development and innovation are caused by non-acceptance on the part of the population. This non-acceptance can be caused by many factors, one of the most significant being the fear of insufficient security. The birth pangs of a chaotic implementation can lead to the "sinking" of the whole innovation. Even in the case of the Czech Republic, this phenomenon is very well known.

It is the issue of trust in the state and its services that prove to be a very important factor. It will be discussed in the next chapter on several specific examples. From a theoretical point of view, the loss of trust and relationship on the citizen-politics axis is increasingly mentioned in current theories that deal with the fission lines that divide society. Society has been very sensitive to any other potential divisions recently, and this fact is aided by the considerable incorporation of both new media and digitization into everyday life. That is why it is important to set high standards for the developing e-government sector. In fact, it is possible to both gain and lose a lot with the help of new technologies. Choejey (2015) concisely defines the goals of e-government as: "The main goal of the e-government implementation is to improve the effectiveness, efficiency and quality of public service delivery using Information and Communication Technologies (ICT). However, its success is dependent on the provision of information security goals such as confidentiality, integrity, availability and trust. Therefore, cybersecurity is vital for the successful adoption of e-government systems."

In addition to the theoretical dimension, there is also a purely practical one: Despite good intentions, it is extremely important that the individual e-government programs are user-friendly and secure. In particular, safety is crucial, and it needs to be combined with a comfortable solution to the problem. It is this combination that proves to be essential for gaining trust. Well-secured but complicated systems do not have to gain popularity with users at all, and the whole investment may prove useless. Even worse and more common scenarios may occur: security compromises are made in favor of convenient use. After a short phase of popularity, there may be some leakage or mass problem that can damage users' approach to the platform for a long time. An important aspect, which manifests itself not only during the coronavirus crisis, is the lack of shared data and valuable information. In the framework of cybersecurity, it is absolutely necessary that the so-called "spillover" effect be applied, which will enable quality information about potential threats. The use of these procedures has also proved successful in the private sphere, as evidenced by the analysis (Yang and Kwon and Lee, 2020).

However, the dissemination of information must be subject to logical control. A robust network must first be set up to prevent the misuse of such shared information.

8 CONCLUSION

For the Czech process of digitization and e-government, the lesson learned is as follows: Based on the findings of this paper, the Czech Republic needs the intensive strengthening of the digital infrastructure that would not be precipitous but systematic. It is extremely important that development takes place equally at the technological, administrative, legislative, and security levels. It is the appeal to follow security procedures and standards that is the main message of this paper. In the first place, it is necessary to increase investments in both strengthening the relevant institutions and disseminating good practice. The next step, which must take place at the same time, is the creation of quality legislation. In the Czech Republic, it has not been permanently possible to create a functional and efficient administrative system that would not be burdened by growing bureaucracy. In the context of the Czech Republic, we are increasingly getting into the situation described by the controversial Russian politician Viktor Chernomyrdin. After the failures of monetary reform in 1993, he declared the legendary statement: “We wanted the best, but it turned out as always.”

This observation is confirmed by the current practice in the development of e-government as well as by other administrative challenges. This practice convicts the Czech system of both inefficiency and exibility. In the context of the Czech Republic, excessive bureaucracy is an issue that is often discussed. However, according to the author of the thesis, the highest risk is characterized by the threat of neglecting the security aspect of e-governmental development. There is a legitimate suspicion based on previous practice that the established trend will continue, with digitization and e-government progressing very slowly and being user-unfriendly. Due to this disadvantage, the dissatisfaction of citizens will increase and the demonstration effect may prevail. This trend will not receive support from the population and will not assert itself. The second option, which is perhaps even more risky, is to try to hastily “bridge the gap,” but without robust security pillars based on well-thought-out legislation.

A certain hope is represented by the activities of NÚKIB, which continuously strives to develop security tools in cyberspace. It does so to a limited extent in dealing with individual cyberattacks as well as in creating the basis for effective cyber legislation. Finally, it is important to mention that the development of e-government can work as a means of excellent economic savings and, in particular, as a helpful step to make mechanisms for the citizens more efficient. Here, however, it is necessary to remember one of the essential disputes of democracy: the conflict between freedom and security. In the case of e-government, it is particularly the conflict between "comfort and security." In the environment of the Czech state, which is characterized by problems with bureaucracy rather than by the issues of efficiency and innovation, it is necessary to pay attention to the following imperative: security must precede comfort, or comfort must be especially safe, even in cyberspace.

In the last decade, the issue of cyber security has been repeatedly mentioned in all strategic state security plans. Cyber threats themselves are, of course, much older and date back to the beginning of the development of cybernetics. They gain in importance especially with the advent of the Internet as a global network. The development of digitization and electronization in all aspects of the functioning of society has become one of the framing trends of the new millennium. This trend can be used to demonstrate some basic economic tendencies related to the development of society and progress as such. The initial impulse of "cybernetics" can be identified already during the Second World War, when this segment significantly helped the Allies to win over Nazi technology. During the Cold War, the cybernetics sector fell under the jurisdiction of state authorities, mainly due to its complexity and strategic importance in the context of the power struggle in the bipolar world order. It is common knowledge that the "Internet" itself was originally a military network, which was followed by the "World Wide Web" as an instrument of advanced scientific research in Western countries. The privatization and commercialization of the Internet took place in the late 1980s and especially the 1990s, when—in the euphoria of the disintegration of the bipolar world—there was a mass development of technology and therefore of cyberspace. At that time, the control of state and scientific institutions over the organically developing Internet network was slowing down, and private companies and individuals were taking up the reins of development, especially the development of the Internet.

It is the popularity of digital tools among the population that usually makes the state start dealing with this issue and offer its services in a digitized form. At that moment, you can talk about the so-called e-government.

REFERENCES

[1] ABDELHAMID, M., KISEKKA V., SAMONAS S.: Mitigating e-services avoidance: the role of government cybersecurity preparedness. Information & Computer Security. 2019. 27(1), p. 26–46.

[2] CARLISLE, R.: The Complete idiot's guide to spies and espionage. Indianapolis: Alpha. 2003

[3] CHOEJEY, P. FUNG, C.C., WONG, K.W., MURRAY, D., XIE, H.: Cybersecurity Practices for E-Government: An Assessment in Bhutan. ICE-B 2015 2015. [online]. Available at: https://www.semanticscholar.org/paper/ Cybersecurity- Practices-for-E-Government%3A-An-in-Choejey-Fung/7fa082bd6407f3502933f89c27d2b5212ab971d1

[4] ČESKÝ ROZHLAS.: Kyberútok na nemocnici v Benešově způsobil škodu přes 59 milionů. Pachatele se vypátrat nepodařilo. Irozhlas.cz 2020 [online]. Available at: https://1url.cz/YKl6p

[5] ČTK.: E15.cz. Za pád webu Účtenkovky mohou hackeři, tvrdí náměstkyně Schillerová. E15.cz. 2017 [online]. Available at: https://1url.cz/9Kl6B

[6] EUROPEAN COMMISSION.: Digital Economy and Society Index (DESI) 2020. cz Luxembourg: Publications Office of the European Union, 2020 [online]. Available at: strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020

[7] EUROPEAN COMMISSION.: European innovation scoreboard. Luxembourg: Publications Office of the European Union, 2020 [online]. Available at: https://ec.europa.eu/docsroom/documents/42981

[8] EUROSTAT.: EU population in 2020. Ec.europa.eu: 2020[online] Available at: https://1url.cz/5Kl6G)

[9] GALINEC, D., STEINGARTNER W.: Combining Cybersecurity and Cyber Defense to achieve Cyber Resilience. 2017 IEEE 14th International Scientific Conference on Informatics. 2017 87-93.

[10] KOLOUCH, J., BAŠTA, P.: CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC.

[11] MOČR: Bílá kniha o obraně. Praha: Ministerstvo obrany České republiky - odbor komunikace a propagace, 2011.

[12] MVČR.: Mapa Kriminality Policie ČR. Ministerstvo vnitra České republiky. 2021 [online] Available at: (https://kriminalita.policie.cz)

[13] NCKB.: Národní centrála kybernetické bezpečnosti - Národní strategie kybernetické bezpečnosti ČR 2015-2020. Brno: NBÚ, 2015 [online] Available at: https://1url.cz/RKl6q

[14] NÚKIB.: Národní úřad pro kybernetickou bezpečnost - Zpráva o činnosti Národního úřadu pro kybernetickou bezpečnost za rok 2017. Brno: NÚKIB, 2017. [online]. Available at: https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-cinnosti-nukib-2017.pdf

[15] NÚKIB.: Národní úřad pro kybernetickou bezpečnost - Zpráva o stavu kybernetické bezpečnosti ČR – 2019. Brno: NÚKIB, 2019 [online] Available at: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

[16] NUMBEO.COM.: Crime Index by Cities 2021. numbeo.com. 2021 [online] Available at: https://www.numbeo.com/crime/rankings.jsp

[17] ROGERS, E.M.: Diffusion of innovations. 5th ed. New York: Free Press, 2003

[18] SCHMIDT, A.: The Estonian Cyberattacks. Atlantic Council, 2013, 1-29. [online] Available at: https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks

[19] SNFMA.: The Swedish National Financial Management Authority. Regleringsbrev. 2021. [online]. Available at: https://www.esv.se/statsliggaren/regleringsbrev/?RBID=21218

[20] TRADING ECONOMICS.: Czech Republic Internet Speed2007-2017 Data: 2020-2021 Forecast: HistoricalCzech Republic Internet Speed | 2007-

2017 Data | 2020-2021 Forecast |. Trading economics, 2021[online] Available at: https://tradingeconomics.com/czech-republic/internet-speed

[21] YANG, A., KWON J.Y., LEE, S.T.: The impact of information sharing legislation on cybersecurity industry. Industrial Management & Data Systems. 2020, vol. 120(9), p.1777–1794.

AUTHOR

Mgr. Tadeáš Pala, Department of Public Economics, Faculty of Economics and Administration, Masaryk University in Brno, Czech Republic; email: 415056@mail.muni.cz.