INTERDEPENDENCE BETWEEN E-GOVERNANCE AND KNOWLEDGE-BASED ECONOMY SPECIFIC FACTORS

Mihai Alexandru Botezatu [1*]
Claudiu Pirnau [2]
Radu Mircea Carp Ciocardia [3]

ABSTRACT

The fast expansion of Internet has prompted the introduction of e-Governance at all levels. The main issue with the services introduced through e-Governance (as well as m-Governance) is represented by the lack of a technically safe infrastructure. The connection between services and security involves the development and introduction of internal governance reforms designed to offer a more citizen-oriented approach through better integration and coordination between involved organizations/institutions. Due to the increase of online interactions compared with the offline ones, the pressure for greater openness and accountability intensified. Its result is formalized by the extension of e-democracy implementation. This paper is structured in six chapters: introduction; e-Governance and cybersecurity; e-Governance and e-reputation; e-Governance development with Microsoft Power BI; the use of Power BI in the analysis of e-Governance implementation at regional level; case study and conclusions.

KEYWORDS: *e-Governance, Cybersecurity, Power BI, Knowledge Society, Big Data*

1. INTRODUCTION

E-Governance is "the process of reinvigorating the public sector through digitization and new information management techniques, a process whose ultimate goal is to increase the degree of political participation of citizens and the efficiency of the administrative apparatus." The approach for implementing e-Governance is always top-down, from state to citizen. (Figure 1).

Digital development offers a new perspective on the future directions of the Knowledge Society development. This can only happen in the case of interaction between e-Governance and the major components of society - state organizations, private enterprises, academia and civil society organizations [1].

Knowledge society and e-Governance are closely connected, as the latter is one of the major pillars of the knowledge-based society.

[1*] corresponding author, Lecturer PhD, Romanian-American University, botezatu.mihai.alexandru@profesor.rau.ro
[2] PhD Engineer, Politehnica University of Bucharest, claude.pyr@gmail.com
[3] Associate Professor, Politehnica University of Bucharest, radumirceacarp@gmail.com

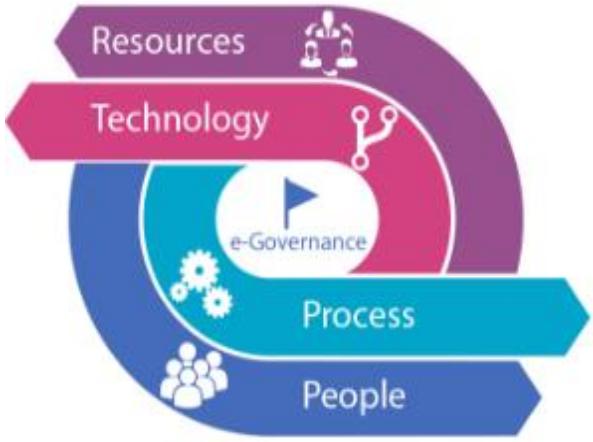

Figure 1. The sense of e-Governance

The Digital Single Market is one of the top 10 European Commission priorities. The Digital Single Market Strategy was adopted on 6 May 2015, setting out 16 initiatives to help consumers, small businesses and industry to fully benefit from the digital single market, including the digital healthcare development and the uniform implementation of telemedicine service in Europe.

Knowledge transfer and assessment processes are responsible for the typical association and relationship between e-Governance, knowledge society and citizens of smart cities. To this end, it is obvious that government support is provided by private enterprises for endowment with hi-tech technologies. The growth intervals of e-Governance in the knowledge-based economy are assessed through specific elements such as: the channels needed to transmit the knowledge flows, the factors that influence the development of e-Governance, the specific knowledge regarding processes that require e-Governance, the regional development of knowledge-based society using "its own capital", the benefits and impact of e-Governance for the knowledge based economy [2].

This type of evaluation allows differentiation of e-Governance and m-Governance development between rural and urban, as well as between countries with different development levels. The "adoption of e-Governance" variable is composed of the following indicators:

- Percentage of individuals using the Internet in relation to public authorities in order to get information;
- Percentage of persons who download forms;
- Percentage of persons who use electronic services to return the completed forms to the competent public authorities [3].

In this context, the maturity levels of e-Governance are:

- Level 1. Web presence - citizens need to find all the necessary information on the site. Thus, the government can initiate effective actions through the virtual environment;

- Level 2. Interaction - citizens must be able to contact their own government through its site, for example by using the e-mail service. Public interest items must be available for download by taxpayers;
- Level 3. Transaction – i.e. online payment facilities;
- Level 4. Transformation (at local, regional and national level) [4];

E-Governance levels have to transform the existing processes into integrated, efficient, unified and personalized services. This level requires the development of internal and external communication processes with the business environment and non-governmental organizations. To prevent cybercrime (more profitable than drug trafficking) and to ensure the security of information systems, procedures and policies are required, and they have to be respected by all user categories of computer system. It is important to note that security policies create a cycle consisting of the following steps: implementation, testing, monitoring and evaluation (Figure 2) [5,6].

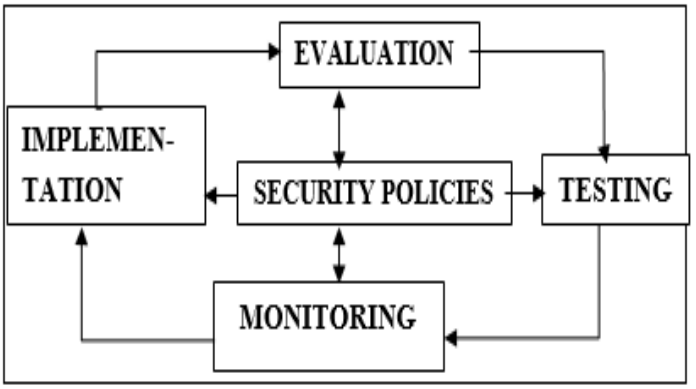

Figure 2. Cycle of Security Policies (*Source: Vasiu, I. & Vasiu, L. 2011*)

The main security policies are:

- Treating information as an asset;
- Controlled access to information;
- Controlled access to IT networks;
- Authorization by login;
- Individual responsibility;
- Functional responsibilities (implementation of security controls and procedures);
- Protection of intellectual property;
- Secure loans;
- Access to external systems;
- Contingency plans;
- Prohibition of unauthorized IT programs;
- Management of exceptional situations.

Factors contributing to the security efficiency are (Figure 3) [5,7]:

- The size of the organization;
- Dissuasive and preventive efforts (administration can play an important role in identifying and targeting organized crime groups, which contribute to money laundering and hide crime financing);
- Collaborative management;
- Category of the organization's activity;
- Risk management.

The main risks identified in the various activities of the e-Governance process (or related to it) are presented in Figure 4 [8].

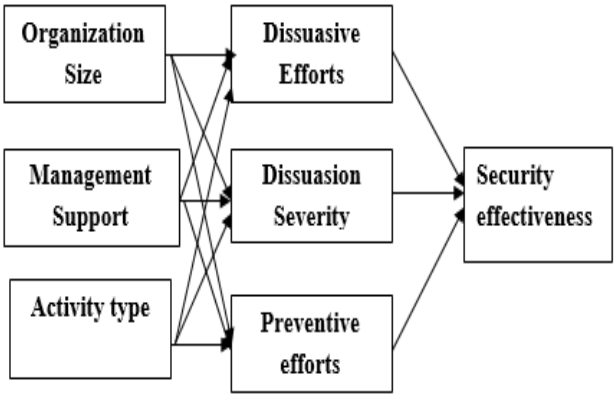

Figure 3. Model of security activity of a computer system
(*Source: Vasiu, I. & Vasiu, L. 2011*)

A study concerning the systemic risk of the Bank of England was published in mid-2014 and showed that 57% of respondents in multinational enterprises assessed geopolitical risk as the main challenge. Significant changes took place during that period in terms of political and military strategies. According to the theory of possibility, every regional power tests what we can call "the extension freedom for the limits of maneuver" [9].

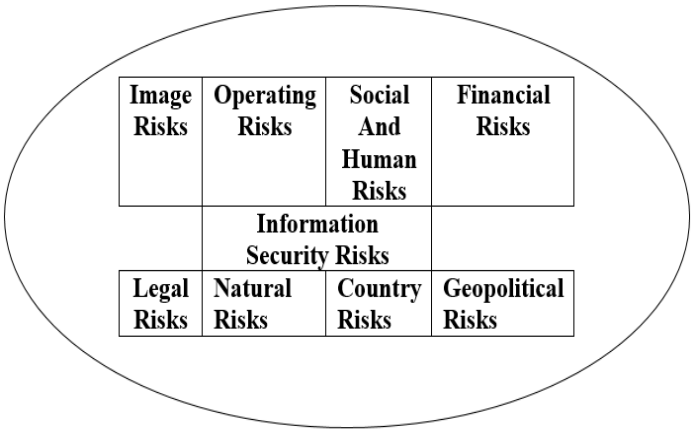

Figure 4. Specific Risks

Continued geopolitical uncertainty could lead to an increase in the complexity of the transition phenomenon from simultaneous crisis management to the implementation of sustainable knowledge based strategies.

In the context of the increasing number of military conflicts, an important role is played by e-Governance, that has to manage not only the issue of the different types of strategies but also the new issue related to the expansion of refugee resettlement and integration phenomenon (depending on their origin, number, gender, qualification, religion, etc.). Implementation of specific programs can only be achieved through new technologies and IT systems, which in turn require solving an extremely complex problem: cyber security [10].

2. E-GOVERNANCE AND CYBERSECURITY

Increasing the complexity of IT systems has transformed the world, becoming a major challenge for e-Governance. The enforcement of specific legislation has evolved, generating ways to protect against internal threats, while military structures have evolved primarily to provide support against external threats (admitting that the extent to which the army is involved in domestic affairs varies from one state to another). Generally, cyber threats come from outside the borders, making it difficult to enforce the law to diminish or punish them. However, such threats rarely amount to the level that would justify a military response. The way governments respond to these challenges can have implications both at national and international level, depending on the nature of the threat. In this context, the first challenge is to "understand the nature of the threat." This includes recognition of the fact that there is a major difference in perspective within the international community among those states that prefer to talk about "information security", including protecting citizens from what we call "harmful content" and other states that focus on "cyber-security" as subset of information security policies [11]. The main steps in ensuring cyber security are shown in Figure 5. Acknowledgement of the fact that not all cyber attacks are motivated in a similar way is also essential to see how a government could address these threats. Specialists in this field use different names to describe the range of cyber attacks, such as "threat", "spying", "subversion", "sabotage" "cybercrime" and, in very few circumstances, "cyber-war". The vast majority of these crimes lie below the threshold of "act of war". Differences between these categories may be minimal, but they prove to be important, both legally and politically. In other words, in the case of a cyber attack, a military response, or even a legal one, is often not the best answer. This does not mean that cyber-threats below the "war" level should not be taken seriously [12]. There are also high-risk situations and critical moments that require the intervention of the army. The military personnel specialized in this area has the cybernetic ability to support combat in theatres of operations as well as to safeguard their own systems during peace time. They provide information and warning signals at national and international level, that usually underpin the most sophisticated cyber operations. Usually, the military is mission-oriented. This type of actions is better sourced and documented than other governmental activities, as it is structured in a way that it would create and develop the needed staff – exactly what would be desirable in order to create an effective cyber defense unit. Moreover, overloading the army generates challenges for at least two reasons. The first is the practical risk of creating a crowding-out effect. Given the "proliferation" of IT systems (IoT, cloud, etc.), cyber security will have to be a discipline

that everybody in a country takes seriously, not just one thing that citizens and private companies can expect to outsource to the military.

Any country that depends too much on the army to ensure cyber security will probably find it in an undesirable situation to reduce incentives that are needed to develop long-term solutions for the private sector.

Figure 5. Seven Steps to Cybersecurity for Control Systems
(*Source: Shrader Engineering Inc. 2015*)

Second, but no less worrying, is the risk of domestic security militarization, which in many countries would be considered a very bad thing. To achieve true cyber-efficiency, it is necessary to operate permanently on the defended systems. Few private sector companies are in a position to receive military assistance in cyber security. The central issue of the role of the army in "defending the nation" against cyber threats is related to the role and capacity of each government. Naturally and necessarily, there must be other cyber-security institutions made up of various competent bodies: the police, national associations to ensure information security, technical centers for computer operations, technical centers to respond to cyber security incidents, etc. These institutions regularly participate in NATO or EU template cyber exercises. To this end, Romania is an integral part of the initiation of the "civil state of cybernetics", mainly based on the Strategy of Cybernetics Security in Romania. Innovative agreements, such as the European Council on Cybercrime in 2001 (with 50 signing parties on all continents), have simplified international legislation on cybercrime. For example, Microsoft and the US Federal Investigation Office are working with international partners to detect and annihilate criminal networks in cyber security. Another potential approach for any government is the role of the private sector in securing its own security. This can be implemented by creating an appropriate incentive structure for sharing information between companies

and raising the standards for cyber security (including through governmental regulations). This could involve the following categories of activities: the exchange of intelligence information between private sector companies (users and Internet service providers) in order to improve defense systems and procedures against cyber attacks; licensing the private sector to respond to intrusions, so-called "hacking back"; creating additional emergency training teams to coordinate feedback on the private sector request. At present, at national level, legislation does not allow hacking-back, as no country wants to take on the risk of rising conflicts for this reason.

In practice, each country faces different approaches and points of view, the results of which can take various forms depending on the level and type of cyber attack:

- Defense information theft is probably classified as the most serious threat to national security and, as a result, it would fully justify governmental involvement in solving the problem. The motivation of such intrusion may be commercial or strictly military (depending if the intruder is a potential opponent who is willing or not to sell the stolen information).
- Counteracting a potential attack on the critical infrastructure for a nation's existence (energy, communications, transport, finance, etc.) is another serious concern, although it is classified as a less immediate threat than the theft of information concerning national security. Although the army has competencies in this area, in most countries, a part of the critical infrastructure is under the administration of private sector, hence making military approaches less practical or acceptable. The best government approach in this area could be to use economic incentives, including regulations to improve security levels;
- Actions to protect intellectual property, counteracting commercial or industrial espionage represent another area where military approaches may not be appropriate. However, given the potential economic impact, especially where advanced state-of-the-art threat techniques are used, this type of activity has the potential to seriously destabilize international relations. In these situations, most of the time, sanctions against certain countries are imposed;
- Threats concerning cybercrime, although they are not a direct threat, they could turn into one (in the absence of effective control) because of the potential of terrorists or certain states to mobilize criminal networks. In general, the application of specific legislation is very important for this purpose.

3. E-GOVERNANCE AND E-REPUTATION

E-reputation is a fairly recent phenomenon, based on the influence of three elements: Internet services, e-Governance and cyber security. This indicates the trust and perception Internet users have of online services offered by government, public administration, or various organizational categories. This reputation (positive or negative) comes not only from information produced by a particular entity, but also from stakeholders and customers, who can easily express satisfaction or dissatisfaction with the quality of online services and safety in their exploitation.

There is a quote from a famous American businessman, Warren Buffet: "It takes 20 years to build a reputation and five minutes to destroy it. If you think about it, you will act differently."

The repercussions of the e-reputation phenomenon (also known as digital reputation, cyber reputation or web reputation) is not limited only to the individual (employee or client) level but to the image of the entire organization, regions or even countries. All organizations, including governmental organizations, must include in their future strategies the implementation of e-reputation monitoring systems which are as necessary as cybercrime prevention systems.

Also, building a professional reputation must be based on a positive digital reputation. When a person has leading positions, or one is in a sensitive position (as is the case with politicians), one needs to make a clear distinction between the public and private areas on the web (blogs, social networks etc.). In this sense, every individual interested in one's image must build a digital strategy for professional development.

Official statistics indicate that every two years the number of employers conducting Internet surveys on the reputation of future employees has doubled.

According to a poll conducted by the FIPO (French Institute of Public Opinion) - present in Europe and Asia - for VIP reputation on the internet, 85% of consumers make purchases and 80% ask before buying based on the digital reputation. According to the survey, 66% of consumers got recommendations before buying. In 30% of cases, an unfavorable online review led to abandoning the purchase process. Thus, 96% of Internet users are influenced by a brand's e-reputation during a purchase.

Government institutions, following the pattern of a large number of companies, should hire a community manager whose primary duty would be to maintain the digital reputation of an organization or brand.

Such a manager needs appropriate tools to help him/her in problem identification processes, namely finding, filtering, and implementing creative solutions. Microsoft Power BI is a self-service analysis solution (to optimize decision-making), now considered a "democratization" of ERP and CRM solutions.

4. DEVELOPING E-GOVERNANCE WITH MICROSOFT POWER BI

One of the important goals of Power BI projects was also to visualize and monitor the models on the front end for example: Power BI serves this function by displaying data sets drawn directly from cloud sources, Azure HDInsight, and SQL Database on several large screens in Arvato's monitoring center (Arvato Bertelsmann SE & Co – Improving fraud recognition with Microsoft Azure) [13].

Being similar to the SaaS packages, Power BI allows organizing and sharing dashboards, reports, and data sets. Power BI reports can be published within organizational packages specific to each team. These are easy to find - being managed in one location, the content gallery. Because they are part of Power BI, they allow the use of all categories of tools, including interactive data exploration, visualizations, Q & A, integration with other data sources, refresh data, and more [14].

A unique feature of Power BI is the ability to connect directly to on-premise data sources, including SQL Server Analysis Services (SSAS), SQL Server, and so on. Figure 6 shows an example of a live SSAS connection.

The Analysis Services Connector function, integrated with Power BI, allows live queries in SSAS tabular models. Cloud data move or scheduling of previous data updates is not needed- reports and data can be viewed in real-time through dashboards, after which the data management process can continue using various other methods/models specific to the organization [13,14].

Connectivity Services Analyzer is a client agent that enables Power BI to connect to local SQL Analysis Services instances.

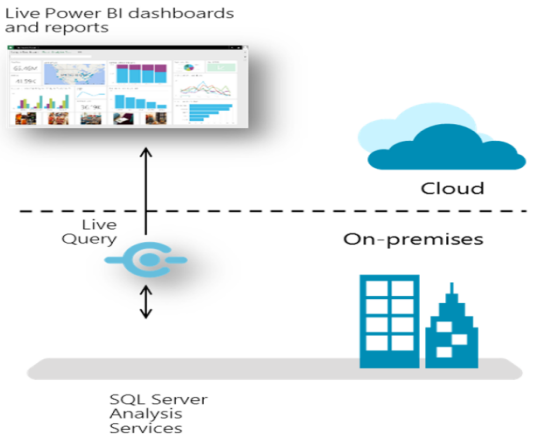

Figure 6. Example of Live Connection to Power BI

When a user browses a Power BI based on SSAS data, Power BI issues queries about data expression analysis (DAX) to the connector, which acts as a proxy between Power BI and SSAS. The connector transmits the name of the new user to an authorized user through the Azure Active Directory service and applies the existing SSAS security permissions, based on roles. The connector then interrogates the local SSAS cube to return the data, and the cached connection optimizes the performance of the query [15].

Communication between the connector and Power BI is achieved through the Azure Service Bus, which creates a secure SSL channel between the Power BI service and local area data through an output port. This process does not require the opening of an entry port in the local protection system.

Before users can access data from an SSAS database, the Analysis Services Connector must be installed in that location. The connector can be installed on any server that has access to the web and to the relevant instance for analysis services.

When a company's Active Directory is federated with Azure the authentication process works automatically. If there is no federation with Azure, activation of authentication is possible via an additional configuration.

With Microsoft Power BI, Desktop or Microsoft Excel, business analysts can import data from a wide range of localized data sources, and then publish them in Power BI. Microsoft Power BI Personal Gateway enables data management and synchronization so that reports and dashboards in Power BI could be always up to date.

Power BI integrates with other cloud services, including Azure SQL Database, Azure SQL Database Auditing, and Azure Stream Analytics. By expanding Azure-specific capabilities in Power BI, integrated BI solutions can be created without interruption. For example, we can use Azure Stream Analytics to process streaming data, after which they can be exported to Power BI, allowing the dashboard to be updated in real time.

Excel and Power BI Desktop files can be published directly into Power BI, simplifying the generation of dashboards and real-time reports. When uploading a file, Power BI can automatically improve data by detecting key features. For example, if a table in a loaded Excel file includes a data field, Power BI can automatically create columns of the month and year type to facilitate reporting based on these elements.

Uploading Excel files can be done from a computer or by connecting them to OneDrive for Business or OneDrive Personal. The advantage of connecting to the OneDrive workbooks is that any changes to a workbook will automatically appear in the dashboard and reports connected to the Power BI workbook.

Power BI supports files with advanced data models, such as Power BI Desktop files and Excel files with Power Pivot data models. When an Excel workbook is loaded with a Power Pivot data model, Power BI loads the entire data model to increase the level of complexity of the applications. The same is true for Power BI Desktop files [16].

Uploading files from Power BI Desktop allows overlapping data from a variety of sources that do not connect directly to Power BI. For example, when using Power BI to explore data from Facebook, a SharePoint list or its own SAP system, data can be accessed through Power BI Desktop, and then a report can be generated and published later in Power BI. Similarly, Power BI Desktop allows you to connect to data from multiple sources.

5. USING POWER BI TO ANALYZE THE IMPLEMENTATION OF E-GOVERNANCE AT REGIONAL LEVEL. CASE STUDY.

In the EU, according to Eurostat statistics, filling in and submitting income tax returns, looking for job vacancies and online visits to public libraries are the services with the highest percentage of users. However, in general, citizens' interest in online income tax forms and job search is lower than interest in other categories of e-services [17,18].

In this case study, conducted on November 11, 2017, we analyzed the issues related to job vacancy offered through www.posturi.gov.ro. They are part of the category of jobs belonging to public institutions.

The positions occupied in public institutions and authorities are classified as follows:

I. Central public administration, out of which:
1. Institutions fully financed by the state budget;
2. Institutions fully funded by social security budgets;

3. Institutions subsidized by the state budget and the unemployment insurance budget;
4. Institutions fully financed by their own income.

II. Local public administration, out of which:
1. Institutions fully funded by local budgets;
2. Institutions fully or partially funded by their own income.

Using Microsoft Power BI, we imported a csv. file which contains the job vacancy status in each county, as shown in Figure 7.

To make various charts on vacancies status, we used the specific tools provided by Power BI as shown in Figure 8. The existence of such diagrams can help us in the development and implementation of HR model strategies.

Posturi dupa judet	numar posturi
Alba	45
Arad	40
Arges	33
Bacau	34
Bihor	27
Bistrita-Nasaud	13
Botosani	19
Braila	13
Brasov	55
Bucuresti	138
Buzau	19
Calarasi	17
Caras-Severin	11
Cluj	52
Constanta	57
Covasna	11
Dfmbovita	21
Dolj	34
Galati	32
Giurgiu	11
Gorj	20
Harghita	24
Hunedoara	32
Ialomita	18

Figure 7. Importing data into Power BI

For the purpose of smart and sustainable development, job openings subject needs to be matched with elements such as human resource planning, number of people able to work, human resource crisis, flexibility in employment, demographic statistics (the age pyramid), the role of episodic memory (the link between memories and future plans), etc.

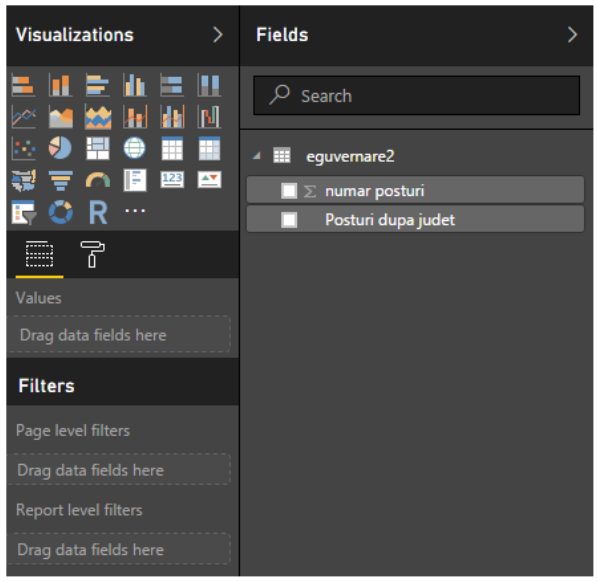

Figure 8. The main graphical representations in Power BI

The diagram in Figure 9 shows the variation of job openings in public institutions, depending on the type of employer. As it can be seen, the highest number of new employments happened in local institutions (representing about 60% of total new employments), followed by those in city halls (approximately 30%). Employment according to the required level of qualification (figure 10) shows an exponential increase in the technician positions (1046), compared to the management positions (147).

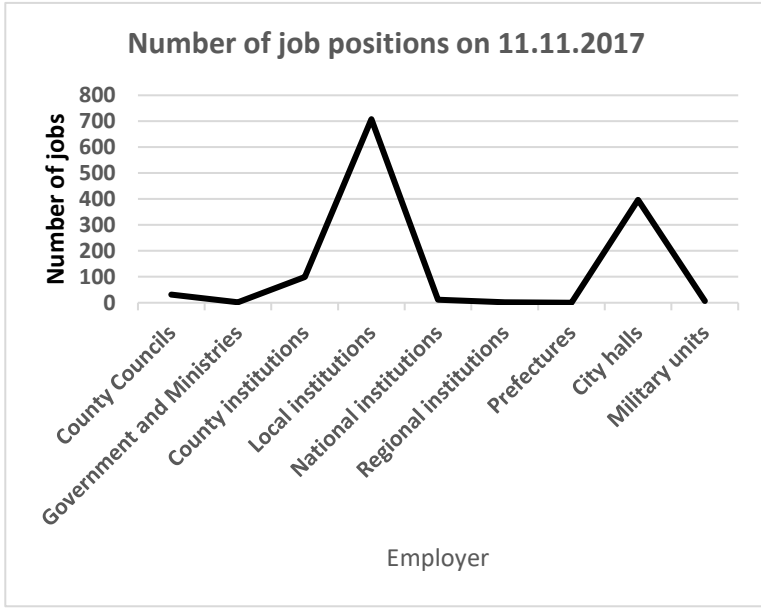

Figure 9. Variation in job positions by employer

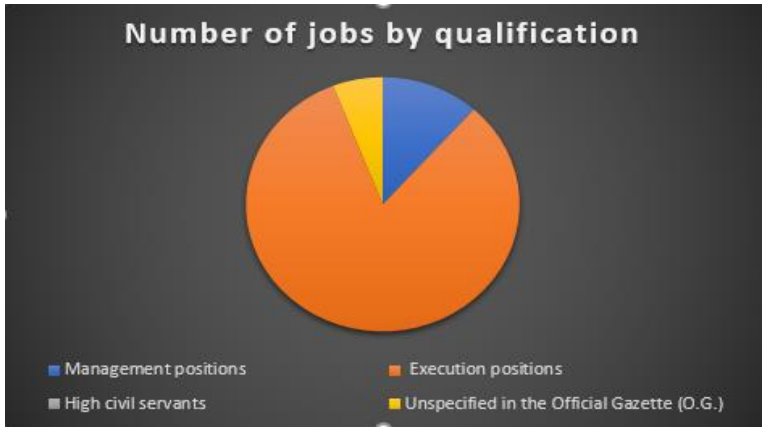

Figure 10. Employment by qualification

When considering variation in the number of job openings in the public system by county (Figure 11), the top leaders are Bucharest, Timis and Constanta, while the employment in the private sector (dominated by the auto and food industry) is lead by Ilfov, Bistrita-Nasaud and Timis counties.

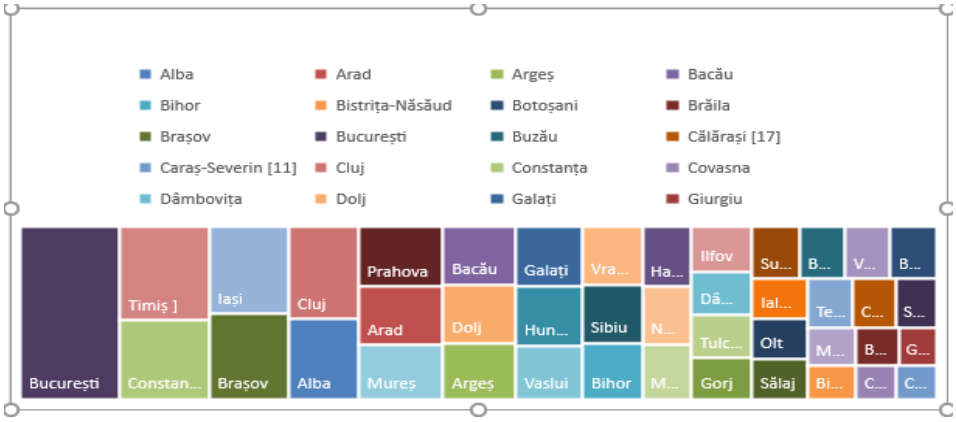

Figure 11. Variation in job positions by county

The regional map of vacancies on 11.11.2017, according to www.posturi.gov.ro, is presented in Figure 12. Thus, we can see that the counties with the most vacancies (in the public system) are: Constanta, Iasi, Brasov, Cluj and Alba.

In each development region there are statistics regaarding the correlations between number of jobs and income [19]. For example, in the Center Region, in 2016, Sibiu County was number one in the top of the highest salary earners - 1.997 RON, followed by Brasov - 1.827 RON, Mures -1.708 RON, Alba -1.689 RON, Harghita -1.373 RON and Covasna -1.420 RON. At the national level, Bucharest, Ilfov, Cluj, Timis and Sibiu are the counties where the employees earned the highest net salaries in 2016, between 2.138 and 2.857 RON net per month.

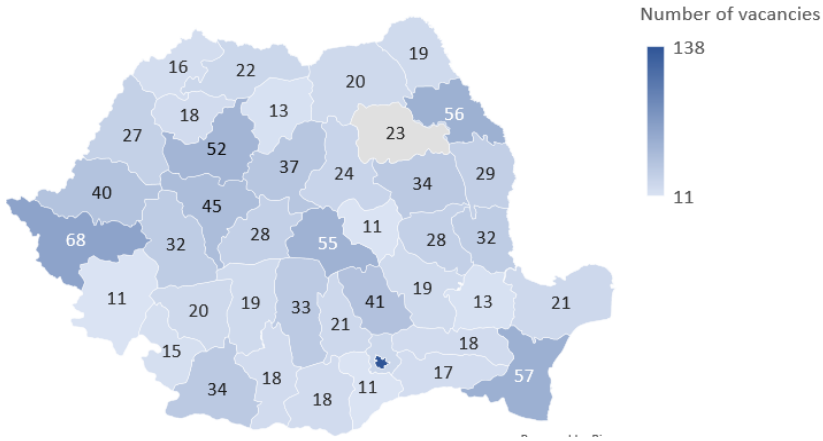

Figure 12. Regional map of vacancies on 11.11.2017
(*Source: www.posturi.gov.ro*)

6. CONCLUSIONS

E-Governance tasks and decisions are generated, transmitted and implemented, first and foremost, depending on the efficiency (models, procedures, schemes, etc.) with which governments use their own leadership to develop national cyber security strategies. The main approaches to this end must answer the following questions: Given the number and complexity of the variables, how involved should be a government official to define cover cyber security at national level? Given the involved factors (the rule of the game), how should governments balance their investment in cyber security and law enforcement both in the state and the private sector? What would be the most effective methods of involving military specialists in supporting the private sector in the event of cyber attacks (when required)? What would be the most effective ways of facilitating international civil society cooperation in the field of cyber security? How can diplomatic initiatives reduce the need to use the army to ensure internal cyber security? What are the methods that can be used by a government to avoid international disputes over cyber issues that would undermine IT security cooperation? The political dimension of a conflict (military or not military) is an unremitting challenge for all the institutions involved. Effective implementation of e-Governance contributes to increasing the level of cooperation and the number of interactions between policy decision-makers, thus increasing the chances of diplomatic settlement of conflicts. At local level, the increase in public sector employment has enhanced the level of taxpayers' satisfaction in their interaction with civil servants. Currently we are witnessing a paradox of e-Governance: in rural localities, where the number of Internet users is reduced, customer satisfaction increases as long as the number of interactions at the counter increases between the taxpayer and the civil servant; in the case of urban localities, customer satisfaction increases with the emergence of new e-services, which implicitly leads to a decrease in the number of interactions at the counter between the two parties involved. The increasing or decreasing number of employees in the public sector may generate fluctuations depending on: the variation in the number of institutions (management of change may lead to the establishment or termination of some public bodies); the degree of implementation of e-Governance; salary

increases or decreases generated by changes in the five factors that govern the economy: ownership, information, demand law, substitutes and inflation. Digital transformation involves the interaction of four dimensions: service, security, transparency and trust. The implementation of the seven dimensions of Big Data (variety, volume, velocity, value, variability, visualization and veracity) in the context of the seven dimensions of sustainable development (human being, culture, political life, economy, nature, society and spirit) is the determining factor of digital transformation through e-Governance.

REFERENCES

[1] Barbara, A.A. Luc, J. Gilles, P. Jeffrey, R. E-Governance & Government Online in Canada: Partnerships, People & Prospects*, Centre on Governance, University of Ottawa*, Canada, 2001.

[2] Khanh, N.T.V. The critical factors affecting E-Government adoption: A Conceptual Framework in Vietnam, *School of IT Business, SOOGSIL* University, Seoul, South Korea, 2014.

[3] *** E-Government and E-Democracy in Switzerland and Canada. Using online tools to improve civic participation. *Summary report of a roundtable discussion*, Ottawa, Ontario, April 8, 2011.

[4] Finger, M. Pécoud, G. From e-Government to e-Governance? Towards a model of e-Governance, *Swiss Federal Institute of Technology,* Lausanne, Switzerland, 2010.

[5] Vasiu, I. Vasiu, L. Criminalitatea în cyberspaţiu, *Editura Universul Juridic*, Bucureşti 2011.

[6] Kelvin, J.B. Stephen, M. Digital Solutions for Contemporary Democracy and Government, *IGI Global*, USA, 2015.

[7] Fang, Z. E-Government in Digital Era: Concept, Practice, and Development, *School of Public Administration, National Institute of Development Administration*, Thailand, 2002.

[8] Wirtz, B.W. Daiser, P. E-Government. Strategy Process Instruments, *German University of Administrative Sciences Speyer*, ISBN 978-3-00-050445-7, 1st edition, September 2015.

[9] Didraga, O. Managementul riscurilor în proiectele de e-guvernare din România, *Colecţia Cercetare avansată postdoctorală în ştiinţe economice*, Editura ASE Bucureşti, 2015.

[10] Ailioaie, S. Hera, O. Kertesz, S. Ghidul de e-Democrație și Guvernare Electronică, *Ghid realizat pentru Parlamentul României*, Octombrie 2001.

[11] Tăbușcă, A. Established Ways to Attack Even the Best Encryption Algorithm, *Journal of Information Systems & Operations Management*, Vol.5, No.2.1/2011, Ed. Universitară, ISSN 1843-4711, 2011.

[12] "Electrical, Communications and Technology Systems for critical infrastructure projects" http://www.shrader.net (consulted in November 2017).

[13] Lachev, T. Applied Microsoft Power BI (2nd Edition): Bring your data to life! *Microsoft Data Analytics*, 2017.

[14] https://powerbi.microsoft.com/en-us/documentation/powerbi-desktop-getting-started.

[15] https://community.powerbi.com /t5/ Data- Insights-Summit- 2017-On/Take-Power-BI-Visualization-to-the-Next-Level/m-p/197936.

[16] Căruțașu, G. Pirnau, M. Facilities and changes in the educational process when using Office365, *Journal of Information Systems & Operations Management*, Vol. 11 Issue 1, pp. 29-41, May 2017.

[17] http://ec.europa.eu/eurostat/ statistics- explained/ index.php /Archive:E-government_ statistics#Use_ of_e-government_services_by_employment_situation.

[18] http://statistici.insse.ro/shop/index.jsp?page=tempo3&lang=ro&ind=FOM104B.

[19] Botezatu Mihai Alexandru, "Modele de analiză în studiul forței de muncă din România", Editura Pro Universitaria, ISBN 978-606-26-0308-3, București, 2015