Information & Security

Published since 1998

V. Shalamanov, V. Monov, I. Blagoev,
S. Matern, G. Vassileva & I. Blagoev
vol. 46, no. 3 (2020): 269-284
https://doi.org/10.11610/isij.4619
ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

A Model of ICT Competence Development for Digital Transformation

Velizar Shalamanov* (✉), *Vladimir Monov*, *Ivaylo Blagoev*, *Silvia Matern*, *Gergana Vassileva*, *Ivan Blagoev

Institute of Information and Communication Technologies,
Bulgarian Academy of Sciences, Sofia, Bulgaria, http://www.iict.bas.bg/EN

ABSTRACT:

The article presents a conceptual framework for development of a model for building of advanced digital competences for digital transformation in cyber resilient environment. It identifies key research areas to support the development and implementation of the model and describes the current results of engaging with the key stakeholders from administration, academia and industry. The focus is on defining the framework for implementing the proposed model in a form of ICT Academy, supported by an e-Platform, governed in most effective way under the COBIT principles and using an innovative e-learning approach. Comparative analysis is made with the development of the NATO Communications and Information Academy (NCI Academy) as an instrument to support the digital endeavour of NATO in order to identify the good practices for the development of a National ICT academy, being able to be part of the trusted collaborative network of the NCI Academy as well.

ARTICLE INFO:

RECEIVED: 04 MAY 2020
REVISED: 12 JUL 2020
ONLINE: 03 SEP 2020

KEYWORDS:

ICT competences, Digital transformation, e-Learning, ICT taxonomies, ICT Personnel development

✉ E-mail: shalamanov@acad.bg

1. Introduction: Competences Challenges in Digital Transformation and Cyber Resilience

In the process of digitalization, considered as a change management (transformation) endeavour in the context of long-term strategic plan for technology transition, we offer a model of digital competence development. *Digital transformation is putting together processes, organization, technology and people to achieve maximum effectiveness, efficiency and cyber resilience of the resulting ICT environment (Cyber space).*

We consider the technology as an objective set of tools to be available and continuously enlarged and improved. Most critical limitation for success is related to people – their selection, development, employment and retirement and even use after retirement from active duties in ICT organizations. Two elements we could manage actively are processes and organization in the Cyber space.

Specific focus of this publication is on the processes and organization for HR management of cyber specialists (in general – ICT specialists) and more specifically development and employment of the Cyber (advanced and regular digital) competences.

In order to develop the model for continuous improvement we run 5 parallel studies, described in the paper. *First* is a study on *ICT competences* taxonomy required by ICT organizations – in our case we use the requirements of the State Agency e-Government in Bulgaria (SAeG) and in particular the *requirements to the Chief Information officers* (CIO). *Second study* is on available *technologies and tools from the industry* and, in our case, we seek cooperation with BAIT (Bulgarian association of IT) to develop a taxonomy and catalogue of solutions for digital space. The *third research area* is about available knowledge and skill development courses (mostly requirements to develop good *e-courses*) for ICT specialists and as a use case we use the community around the National Research Program ICT in Science, education and Security (mostly Institute of Information and Communications Technologies in the Bulgarian Academy of Sciences – IICT-BAS). The focus here is to develop an ICT knowledge / skills taxonomy for development of training courses to transfer this to ICT specialists the most effective way. The *fourth research area* is about the *current status of the human capital* in the country to be used for selection and development of specialists for the public Cyber space. We use as a study case the pool of people in Public Administration in cooperation with the Institute of Public Administration (IPA). The *fifth area* of study to *integrate all elements* in a model for optimization of the process of selection, development, employment and use of retired specialists in Cyber domain. Our assumption is that there is an opportunity to develop an e-Platform to support integrated and comprehensive way these processes with all stakeholders involved and to optimize the processes and organization of this platform (its architecture) in maximizing effectiveness, efficiency and cyber resilience of the supported ICT organizations from the human capital point of view.

In order to test our approach for the first year we focus on the development of CIO (Chief Information officer) on-line course with all identified test case stakeholders, based on the experience of IT leadership academy experimented in 2018 under the leadership of SA e-Government in partnership between Institute of Public Administration (IPA) and IICT, but involving Defence Institute, European Software Institute for Central and Eastern Europe and Defence Staff College (Military Academy). In 2020 the experiment is aligned with the introduction of the CIO function in IICT-BAS as a pilot for the Bulgarian Academy of Sciences with the support of the established Consultative Council to the President of BAS on effective, efficient and cyber resilient management of ICT resources in the Academy.

The paper presents the initial results in the 5 identified areas with a way ahead in the next 2-3 years with an aim to establish ICT Academy in the IICT-BAS in partnership with involved stakeholders and linked with the National Research Program ICT in Science, education and Security as well as many other projects in IICT-BAS, including Horizon 2020 funded project ECHO.[1]

From the very beginning the work of the team is coordinated with the development of the NATO Communications and Information (C&I) Academy (part of NATO C&I Agency[2]) and similar developments in EU around ESDC (European Security and Defence College, in particular ESDC EAB.CYBER.[3])

The structure of the paper covers in more details the organization and initial results of the introduced five areas of research. First part defines the concept of the ICT Academy. Second part explores the E-Government/CIO requirements taxonomy / status in public administration. The Industry taxonomy / status (technologies and tools) and relation to the body of knowledge maintained in IICT-BAS is presented in the third part as result of joint effort between IICT and BAIT. Fourth part is focused on the Academic Taxonomy / status, based on internal research of requirements of the e-learning platform to the providers of knowledge. The model to optimize the transition from current status to harmonized state is described in the fifth part of the paper.

2. The Concept of the ICT Academy

Development of the concept for the ICT Academy to the IICT-BAS is based on the framework of establishing NATO C&I Academy as part of the NATO C&I Agency. Below are key questions used by the NEDP2020 (NATO Executive Development Program Class 2020) team, developing the concept for further improvement of the NCI academy with answers provided by our team. These answers are driving our specific study in the 5 areas and our intention is to adapt the conclusions of the NEDP2020 team to final design of the ICT Academy to IICT-BAS at the end of 2020 for implementation in 2021/2022.

First question is about the ICT Academy Vision and Business Model, including aspects as i) state of the art education, ii) sustainable business model, iii) consolidation as an academy versus a school. Our view is that the NCI Academy is an instrument of change through education, training, exercises and related research in C4ISR domain. It is a hub of knowledge and excellence for a much larger collaborative, trusted, diversified and adaptable network of National bodies and linked with the key partners - Strategic Commands, HQ, education and training institutions of NATO as key stakeholders. Academy is service based and customer funded as the Agency, with a dominance of non-common funding sources.

The academy benefits from a partnership with industry and attracting on contract base of leading speakers for Cap Stone course on IT leadership.

Cooperation with EU in the area of Cyber and IT leadership / CIO function is attracting additional students and funding to provide a critical mass to be a NATO/European ICT Centre of excellence.

Second question is about areas the NCI Academy should expand its current portfolio to establish itself as a self-sustained, world-class academy (more than just a school). We consider that being a NATO body for C&I E&T the academy should expand to IT leadership, cyber, emerging ICT applications, acquisition, ICT personnel development. Exploring innovative ICT based education and training methodologies as well as studies with involvement of students and guest speakers will provide an additional strength.

Linkages between electronic, cyber and hybrid warfare in a cyber domain is an area to explore too. Role of ICT in transformation is another key area for joint efforts with ACT (Allied Command Transformation).

Accreditation of the courses with universities to add credits for gaining educational degrees will increase the value of the academy. In addition, building trust with Nations could help through E&T type C&I Partnerships to transfer some of the national efforts to the Academy without losing ownership.

Next question is about perceived challenges for the Academy in terms of student attendance; and how can the NCI Academy could address these challenges. For us obviously a hosting problem for students in Oeiras without a dormitory is a problem, so arrangement for at least a limited capacity is required. Long-term arrangements for the accommodation in the region is a must. At the same time most of the E&T could be of distance methods.

Other challenge is the right mixture between organic and temporary staff to provide currency and diversity of knowledge offered. Last two challenges could be overcome by agreement among Nations to send teachers on rotational basis with high quality as VNCs (voluntary national contributions) and establishing a flexible recruitment policy as in the academic institutions.

Mobile training teams from NCI Academy and national experts could be developed for addressing urgent needs for exercises and operations as well as to address the needs of partners on the ground.

Defining the ICT Academy Portfolio / Academic Content is linked with a question how can the Academy ensure sufficient flexibility to meet the fast-evolving customer needs and expectations. Our assessment is that the agency has a four type of units: acquisition, service provision, research and academy for E&T. Specific models could be agreed on the ASB level to govern these areas as part of one agency. E&T is very dynamic - in addition to the well-established courses on the current NATO CIS systems and cyber, the academy has to look at the areas actively developing a capable C&I community.

Academy must look more pro-actively to attract more students in order to maintain a critical mass of teachers and support staff, actively to use the experts from other units of the Agency to develop and deliver courses either form distance or on rotational basis.

Support research program, linked with the colleagues in the Hague is an important to provide a quality of training as expected by the customers. Total cost of training could be reduced (that will attract more students) by actively partnering with national E&T centres through an academy accreditation program.

Next question is about the content of the curricula to be extended beyond the CIS areas – for example - acquisition, space, etc. Actually, an acquisition in ICT is not something not related to CIS. Cyber definitely is part of the portfolio by design and Space is there as well - the Agency is working to establish Space tech centre. Most important for us is to add courses on building of C&I community around CIO competences and ICT leadership at large. The school was focused (in the past as a part of NCSA) on preparation of assigned military to serve in NCS/NFS - the academy could go beyond this mission to support the NATO C&I community.

Academic advisory board to the Academy or ASB will be helpful to diversify and adapt the curricula in different areas. Special courses to train representatives from the industry on NATO processes, current NATO systems and related issues with a careful attention to the potential conflict of interests is an area to exploit.

Training Methodology is essential for success and the question about what innovative training methodologies the Academy should explore (e.g. Artificial/Virtual Intelligence, Machine Learning, Big Data Analytics, etc.) is a critical one. Most important is to use technology for active involvement of students - individually and collectively. Opportunity for testing and adapting the courses to the audience could be used as well as adopting certification tests for larger community.

Combining R&D capacity in the Hague, operational capacity in Mons and acquisition expertise in Brussels will require innovative technologies to support it. Intentional exposure of the students to new technologies will drive innovation in C&I community that is a value by itself, but this require and effort.

The Resources dimension could be related to the efforts for the establishment of a NCIA Academy community of teachers, staff, customers, students and alumnae. Definitely, the Academy big value is in building and maintaining the C&I community in NATO, including partners.

Current E&T conference is easy to be extended to stakeholder conference, but there are other interesting initiatives, for example C&I community could use the experience of George Marshall Center in Garmisch-Partenkirchen. It is interesting to explore partnership with AFCEA Int. especially Education foundation. Customer feedback is essential, so specific arrangements with the customers around NCS will be very beneficial.

Question what could be undertaken by the NCI Academy or others, to ensure the continuous availability of a qualified and skilled workforce is at the core of competences of the academy itself. It is very important ASB/C3B (Agency Supervisory Board / Consultation, Command and Control Board) to be involved in order to get attention of the Nations to motivate or directly provide teachers through available mechanisms. Providing good mix of teachers - academic staff, instructors, practitioners is requirement for quality. Some participants in advanced training could deliver lectures to the colleagues as well.

Using the staff from other parts of the Agency and attracting people from NCISG will be helpful as well. It is critical (as in Oberammergau and NDC) the academy to attract C&I leaders for keynote lectures as well as using some conferences of C&I community organized at the Academy to involve participants to deliver lectures.

Last, but not least is the topic of External Relationships. Are there opportunities for partnerships that the Academy should explore - e.g. centres of excellence (CoE, suppliers, other national institutions/academies, etc.). The academy is one really large CoE in CIS/Cyber, but could benefit very much from cooperation with other specialized CoEs – for example CCD CoE in Tallinn and others that are providing training on specific FASes (Functional Area Services).

The Academy is very effective instrument for cooperation between NATO and EU in the area of digitalization and cyber resilience, so partnership with EDA, ENISA, EU MS and in the future the European Center of competence on cyber security will be useful (ESDC as well).

Segmentation and specific engagement with partners will be required - with academia and industry. Such a partnership will help the Academy to be involved in the EU research and education community as well as US/Canada from NA side.

Such a partnership program will require first to prove success of the core mission and good support from the Nations through ASB.

Question of the NCI Academy potential gain of value by obtaining additional accreditations deserves special attention. Being a trans-Atlantic alliance, the accreditation of the key courses has to be with both European and North American universities that will provide academic reputation and opportunity for students to get credits for their degrees. Accreditation is to be anticipated in the beginning, but obviously is not a priority right now – first key courses and serious enlargement of the students' constituency is required to have this effort economically sound.

There is a need for building of hierarchy of training modules - basic C&I training, advanced C&I training, Capstone level. After internal audit and proven maturity some courses could be accredited. Accreditation could be by decision of Nations to establish courses in this system over and above National programs with focus on IT governance and interoperability, cyber security.

Above questions and agreed views in our team are the base for further consultations with NEDP2020 team on improving of the NCI Academy, in order to transfer experience from NATO in development of ICT Academy to the IICT-BAS in relation to the National Research Program ICT in Science, Education and Security.

3. E-Government / CIO Requirements

In this section we analyse the current status and challenges facing the development of digital competences in public administration. Data are taken from The Bulgarian Institute of Public Administration (IPA),[4] State of the Administration Report of the European Commission[5] and State e-Government Agency of Republic of Bulgaria.[6] Matching the current situation and requirements of the ICT organizations is defining the HR challenge in support of the digital endeavour. This is important for the analysis and defining the requirements to the e-Platform for competence management, its processes and organization.

Advances in the digital transformation of the administration and emerging technologies pose significant challenges for administrations. Data from the 2018 State of the Administration Report[5] shows that the total number of ICT administration staff is 2,987, which is 120 more than in 2017, but remains very small as a share of the total employees employed (about 2 %). According to their functions, they are allocated as follows: ICT support staff - 1 913, planning - 627 and development - 447. This indicates a lack of planning and management capacity for information resources in administrations.[6]

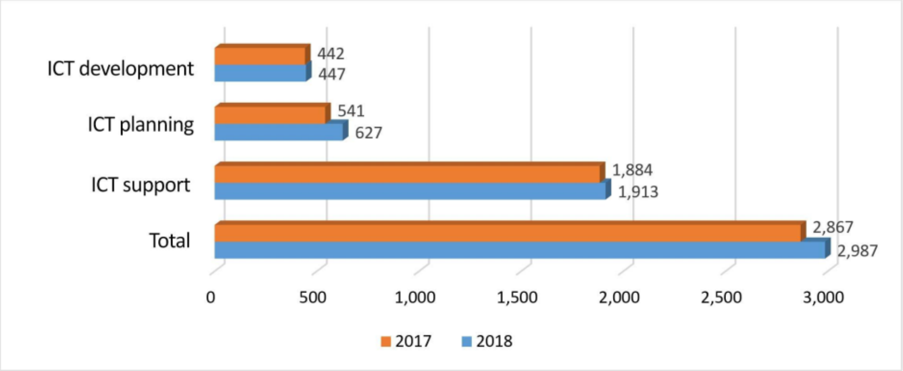

Figure 1: Number of ICT officials in the public administration.

About 30% of the administrations indicate that they do not have the necessary administrative capacity to work in e-government, the main reasons being the lack of qualified or under-trained staff, low pay, insufficient staffing, lack of budget.

Aggregated data received from administrations on the remuneration of ICT employees indicate that the highest average monthly remuneration in administrations is for the position of State Expert - BGN 2 012.

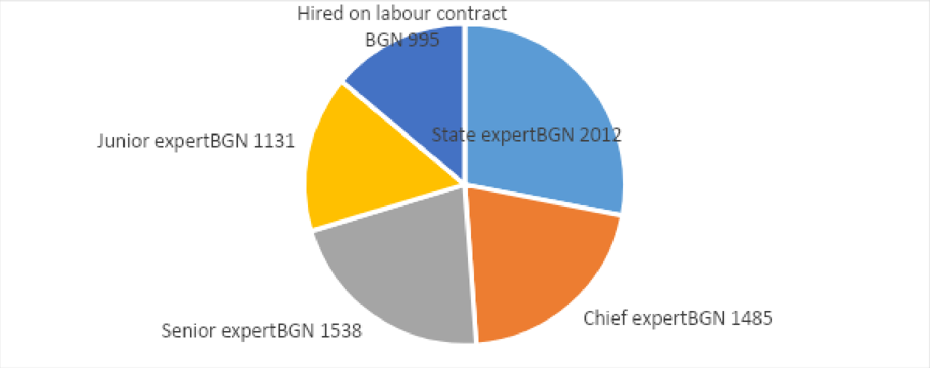

Figure 2: Average monthly salary of ICT employees.

The data on the remuneration of ICT employees in the public sector show that their average monthly remuneration lags far behind those in the private sector. This, combined with intense competitive pressure from the private sector, makes it impossible to attract and retain highly qualified personnel from the public administration.

High staff turnover continues, including due to non-competitive pay to the private sector, lack of career opportunities and incentives and mechanisms to acquire and maintain real hands-on experience and knowledge of the most sought-after and up-to-date technological solutions. The lengthy selection procedures for civil servants, as well as the lack of **f***lexible forms of remote working*, also contribute to the low interest of qualified experts in employment in public administration.

The shortage of skilled Chief Information Officers (CIOs) has a major impact on the ability to plan and manage information resources and reengineer processes, the quality of projects being developed and technical specifications, financial planning and the provision of network and information security. The role of the CIOs is crucial for the success of the public administration.

The CIOs of leading organizations describe a consistent set of six key principles of information management that they believe contribute to the successful execution of their responsibilities, according to a research made by the United States General Accounting Office.[7] These principles touch on specific aspects of their organizational management such as formal and informal relationships among the CIO and others, business practices and processes, and critical CIO functions and leadership activities. The CIOs interviewed considered these principles instrumental because they address critical organizational and operational aspects of the CIOs role.

These six fundamental principles and key characteristics of CIO Management in leading organizations described by the CIOs with a summary of the practices and comparing them with practices in the federal CIO environment are presented in the table below.

Table 1. Comparison of Leading Practices and Federal CIO Management Practices.[7]

Principle	*What a Leading Organization Does*	*What the Public Administration Does*
Recognize the Role of Information Management in Creating Value	● CEOs and governors ensure that the CIO organization is a key business player ● CIO is a full participant in the executive decision-making process	● Information management generally still viewed as a support function instead of a strategic activity ● CIO is not always involved in strategic and policymaking decisions
Position the CIO for Success	● Defines clear CIO role and authorities ● Matches CIO type and skills set with business needs ● Forges CIO partnership with CEO and other senior executives	● Does not always clearly define CIO role or authority ● Does not always match CIO selection with organisation's needs ● Does not always provide executive support for the CIO position
Ensure the Credibility of the CIO Organization	● CIO builds credibility through effective leadership, good working relationships, track records, and partnering with customers and peers	● Uses practices similar to leading organizations
Measure Success and Demonstrate Results	● Strong links exist between business objectives and performance measures ● Performance management structure still evolving	● Weak links between organization's goals and information technology and management performance measures ● Required annual performance plans still in early stages
Organize Information Resources to Meet Business Needs	● Reassigns staff as needed to best serve interests of customers ● Structures the organization along business lines as well as information management functional areas	● Tries to meet needs of customers with a fixed organizational structure ● Structures the organization primarily along information management functional areas
Develop Information Management Human Capital	● Maintains up-to-date professional skills in technology management ● Outsources entry-level positions but largely hires at all levels of experience	● Provides limited amount of training in technology management ● Assumes entry-level staff will remain in federal service as a career

Table 1 indicates that a gap exists between the practices of the CIOs in public administration and CIOs of leading organizations. Areas in which gaps exist should be examined carefully to understand the basis for the differences as well as opportunities for greater implementation of the principles.

The conclusion is made that an understanding of the information technology and management practices of leading organizations could contribute to the development of improved CIO management practices in the public sector. Increasing the capacity and responsibilities of ICT staff is essential for the successful implementation of eGovernment policy, information security and for building effective digital administration.

4. Industry Technologies and Tools Status

In this area, the research effort of the team is in the initial phase and process of establishing a partnership with the Bulgarian Association of Information Technology (BAIT) and Innovation centre – Bulgaria, development of questionnaires and analysis of the existing technology taxonomies in ICT sector. Mapping of these classifications with the competence map of the IICT-BAS as well as other institutes in the Academy of sciences and the universities, involved in the National Research Program ICT in Science, Education and Security will inform in comparison with the requirements for the e-Government / CIO function the competence / technology requirements for the e-Platform for management of digital competences.

Initial study of required tools and competences for distance working and the role of CIO to select and manage these tools and competences in IICT is presented by Borissova et al.[8]

Recognized world class expertise in IICT–BAS [9] is in the areas of:

- HPC, incl. parallel algorithms and scientific computations
- Computer networks
- AI/NLP, especially Linguistic Modelling and Knowledge Processing
- Signal processing and Mathematical Methods for Sensor Data Processing
- Robotics and embedded intelligent systems
- Information processes, decision support systems, modelling & simulation, etc.

Cooperation with industry is studied along the following projects, related to Cyber security:

- Secure, safe and reliable email service compliant with the modern Cyber security concept and integration with different systems like web browsers, desktop computers, smart devices and automated system platforms;
- Solution for distance working: VPN corresponding to modern requirements for Cybersecurity, resting on a high security concept with Public key infrastructure concept with multi factor authentication. This service works with crypto algorithms and mechanisms which is compliance with all modern Cybersecurity laboratories. This high-performance solution

can service all organization users even if they work at the same time. In addition, this VPN service has no subscription fees and is affordable for every company and is completely under the control of the organization;

- Virtualization plan for workstations that are critical to the organization: It's includes all workstations which must be all time available and protected. The users can access their workstations from Intranet and Internet, but the second only through high secured VPN service. All time users will work from terminals. This eliminate efforts to upgrade and servicing a lot of critical workstations which is placed and accessed only from one working location. The new approach also solves the problems with viruses and other ways of information loss. Virtualized machines will be placed over RAID massive and additionally their data can be backup any time;
- Establishing of Web services which will correspond with approved standards for Cybersecurity and high performance of web services. This solution is designed to be hosted from new concept of high-performance web service solution. The service will be protected with two security layer protocols TLSv1.2 and TLSv1.3 and it will be verified by SSL server certificates. The users will reach file system only through Secure FTP. All web contents and databases can be automatically backup from system tasks. The designed service will be high-performance and reliable for the needs of both ours and any other organization;
- An online learning platform: Selected Moodle platform will be hosted, managed and system administrated on infrastructure of our organization.

All IT solutions offered in IICT can be built and deployed at a value that is possible for any medium to large organization. It will combine the best amount of cost, high performance and high level of cyber security.

We believe that if more organizations accept our applied technological solutions and take from our experience, in the future all will be ready to enter the inevitable era of digitalization.

Cooperation with industry is tested around cases, to mention the one with Evrotrust – Bulgarian start-up innovation company which accepted the challenge to be one of the first companies in the world to provide services like a certified provider of remote signature and remote identification. All of this to be in compliance with European regulation eIDAS and first standard for remote signature.

5. Requirements for Building Interactive Online Courses for ICT Competence Development

Essential for development of the e-learning platform and building interactive online courses that engage the learners in maximizing online learning is the process of transforming standard learning content into one that is appropriate for conducting online self-paced courses.[10, 11]

The main purpose of the described requirements is to bring out all the components of an online course through which the training content is presented in a manner that is as close as possible to the traditional training.

At the heart of the requirements is the provision of an online course on the assumption that the learner and the author of the course do not have any communication opportunity, which requires that all issues that would arise in the learner be foreseen and provided with relevant information.

In addition to the detailed requirements, the possible means of providing additional information, communication and feedback to the trainees are described.

Some of the information only serves to better orient the entire content creation team and to clarify the expected end result.

5.1. Basic Information Applicable to the Entire Training Course:

- **Learning content information** - includes basic components of the course that aim to inform and motivate the learner to complete the course.
  - Name of the training
  - Brief description of the training
  - Detailed training description
  - Learning Objectives
  - Training Needs
  - Teaching methodology
  - Name of all training topics
  - Prior knowledge and skills required of the trainees
  - Terms with definitions required to start the training
  - Practical applications
  - Author(s)
  - Administrative support
- **Method of conducting, duration and completion:**
  - Form of training (self-paced, virtual classroom supported or blended learning)
  - Duration of training
  - Requirements for successful completion of training
  - Information about creating and configuring a final test

5.2. Information about Each of the Individual Training Topics

- Title of the topic Summary of the topic
- Benefit to learners after completing the topic
- Objectives of the topic
- Introduction

- Content of the topic
- Presentation on the topic
- Topic extension
- Supporting story
- Example
- Content that usually makes it difficult for learners
- Complex to present content
- Terms with definitions used in the topic
- Key knowledge to be acquired after completing the topic
- Key skills to be acquired after completing the topic
- Competences
- Knowledge assessment questions
- Cases and Tasks
- Embedded video / audio files
- Additional files for download
- Useful links / additional literature
- Summary

Not all of these components are required, but the more enriched the content is with elements interacting with the learner, the greater the degree of mastery of the competences in the course will be.

It is good practice when working with content writers who are not experienced in preparing online courses to provide illustrative examples from other courses already built to more clearly illustrate the meaning of the individual components of the online course.

Practice shows that the development of online courses usually takes several iterative cycles, until the authors, together with the team of developers, have an understanding of the nature of each of the team members.

Creating online courses is not an easy process and the motivation of the team should be the benefit that the course will reach a much larger group of students than in-person training.

6. Integration and Transition to Digital Transformation

Digital transformation is commonly recognized [12] as the cultural, organizational and operational change of an organization, industry or system through a smart integration of digital technologies, processes and competences across all levels and functions of the organization. The need for digital transformation appears in response to the rapid change of digital technologies and employs their capabilities to create new value and competitive products.

Based on our concept of ICT Academy and e-Platform for competence management, we are considering the digital transformation in several rapidly developing areas by an extensive use of advanced ICT competences and skills. At this stage of development, the focus is on the ICT competences taxonomy in the following areas where digital transformation becomes increasingly important:

- ICT competences required by organizations;
- ICT competences required by E-government;
- ICT competences for Information security.

The model of digital transformation involves the three main phases [13]:

- *Digitization* is the process of converting analogue information into digital information and the change of analogue tasks to digital tasks. It allows for a computerized storage, processing and transmitting of the encoded digital information.
- *Digitalization* is the process of employing digital and IT technologies to improve existing processes and enhance customer capabilities.
- *Digital transformation* is the phase that encompasses the overall change of organizations profile and leads to the development of new operation models and innovative products.

Digital transformation facilitates technologies to create new value for customers and increased digital competitiveness and acquire the capabilities to rapidly adapt to changing circumstances. Organizations aiming to transform digitally not only need to have digital assets, but also acquire or develop capabilities related to digital agility, digital networking and big data analytics.

Following the best practices to ensure successful digital transformation, the implementation of the model includes several fundamental steps.

- *Identification of digital transformation objectives.* At this step it is necessary to determine the organization's level of digitization and try to align the current state and long-term digital goals.
- *Building a digital transformation strategy.* The strategy should be based on a clear objective and a feasible plan which involves selecting areas of improvement and integrating digital systems from those areas.
- *Choice of the necessary technological tools.* Tools such as IoT, Analytics, Cloud, VR, and AI are vital drivers for a successful digital transformation. Organizations should decide which technological tools would be the most beneficial for their operation.
- *Establishing competent technology leadership*. The leadership support provided by a Chief Information Officer must research new technologies, strategize how technology can provide new value and address the risks associated with digital information.
- *Establishing Key Performance Indicators.* The indicators should give a measurable value that demonstrates how effectively the organization is achieving key strategic objectives. They also can show how successful or unsuccessful is the transformation.

- *Training the staff and integrating a digital culture among the organization.* At this step the staff should accept the change and adapt to the digital transformation.

In IICT-BAS we investigate a synergy between 4 parallel initiatives for successful digital transformation:

- Establishing a CIO function (CIO/CISO/DPO) to develop vision, strategy and plan for transformation, to lead its implementation;
- Development of ICT academy to support internal training in support to digital transformation and to provide a multi-stakeholder e-Platform with e-courses for the development of digital competences, based on the body of knowledge in the institute and its partners;
- Implementing a modern portfolio, program, project (P3) management system to support the main activities of the institute fully digitized way;
- Introducing of digitized risk management system to identify and mitigate important risks in the process of transformation.

As we put people in the centre of the transformation process [14, 15] the evolutionary improvement of the personnel performance assessment system in support of the digital transformation (and of course fully digitized by itself) is used to drive the change.

7. Conclusion

In this paper we have studied the current status, challenges and perspectives for digital transformation of Bulgarian academic institutions, industry and business companies as well as organizations in the public sector operating in cyber resilient environment. A conceptual model for building of advanced ICT competences for digital transformation is developed including several integral parts. At first, the model includes an ICT academy as a fundamental tool for change through education, training and collaborative research with NCI Academy and Bulgarian scientific institutions. As a second part the model involves development of an E-Government/CIO requirements taxonomy in public administration and the third element is the Industry taxonomy/status with technologies and tools. An important part of the model is e-Platform for building interactive online courses and enhancing the knowledge and digital skills of the learners. At present the model is at an early stage of development and future collaborative research and efforts involving academia, industry and public sector are necessary for its further elaboration and implementation.

Acknowledgement

This paper is supported by the National Research Program ICT in Science, Education and Security and the budget project of the IICT in digital transformation.

References

1. ECHO project, 2020, www.echonetwork.eu.
2. NATO Communications and Information (C&I) Academy, last modified 2020, www.ncia.nato.int.
3. ESDC (European Security and Defence College), last modified 2020, https://esdc.eu ropa.eu/.
4. The Bulgarian Institute of Public Administration (IPA), last modified 2020, https://www.ipa.government.bg/bg/cifrovizaciya-i-publichnata-administraciya.
5. "2018 State of the Administration Report," adopted by Decree No. 273/20.5.2019, https://ec.europa.eu/.
6. State e-Government Agency, "Republic of Bulgaria, August 2019," 2020, https://www2.e-gov.bg/en/1.
7. Chief Information Officer, "Executive Guide," GAO-01-376G, 2020, www.gao.gov/assets/80/76558.pdf.
8. Daniela Borissova, Zornitsa Dimitrova, and Vasil Dimitrov, "How to Support Teams to be Remote and Productive: Group Decision-Making for Distance Collaboration Software Tools," *Information & Security: An International Journal* 46, no. 1 (2017): 36–52.
9. "Expertise in IICT–BAS," 2020, http://www.iict.bas.bg/EN/index.html.
10. Ivan Blagoev and Vladimir Monov, "Criteria and Methodology for the Evaluation of e-Learning Management Systems based on the Specific Needs of the Organization," *International Journal of Education and Information Technologies* 12, North Atlantic University Union (NAUN), (2018): 134-141.
11. Gergana Vassileva, Vladimir Monov, and Ivan Blagoev, "E-learning model for personalised online education based on data analysis and competence profile," *Proc. of the International Conference on Education and New Learning Technologies "EDULEARN19", Palma de Mallorca Spain*, July, 2019, pp. 3726-3732.
12. Natalja Verina and Jelena Titko, "Digital transformation: Conceptual framework," *Proc. of the Int. Scientific Conference "Contemporary Issues in Business, Management and Economics Engineering'2019", Vilnius, Lithuania*, 9–10 May 2019*,* pp. 719-727.
13. Peter C.Verhoef, Thijs Broekhuizen, Yakov Bart, Abhi Bhattacharya, John Qi Dong, Nicolai Fabian, and Michael Haenlein, "Digital Transformation: A Multidisciplinary Reflection and Research Agenda," *Journal of Business Research*, 2 November 2019.
14. Velizar Shalamanov, "Institution building for IT governance and management," *Information & Security: An International Journal* 38 (2017): 13–34.
15. Silvia Matern, Gabriela Savova, Denitsa Goleva, and Velizar Shalamanov, "Human Factor in Digitalization and Cyber Resilience of Public Administration," *Computer and Communications Engineering* 13, no. 2 (2019): 3-14.