The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2022

Volume 17, Pages 26-37

ICRETS 2022: International Conference on Research in Engineering, Technology and Science

The Role of Project Management in Cyber Warfare with the Support of Artificial Intelligence

Oszkar DOBOS
Obuda University

Agnes CSISZARIK-KOCSIR
Obuda University

Abstract: Cyberspace has a large number of actors and technologies involved that are parts of civil society. The ICT sector professionals and their applied and RDI project technologies are integral and indispensable parts of cyberspace. Project management doctrines and methods can significantly improve the effectiveness of projects, driving organizations towards success. Asymmetric or hybrid warfare clearly extends to the civil sector, and the reverse of this relationship raises interesting questions. The aim of the study is to examine, that what is the role of civilian professionals and technologies in cyber warfare? Narrowing down the question, the focus of this article is on what role project managers and methodologies have in cyber warfare, and in what ways can AI support them? Shall the PM knowledge help and support the efforts. The paper helps to present the issues raised through the eyes of project management by providing a systematic literature review through different aspect of the topic.

Keywords: Project Management, Cyber security, Artificial intelligence

Introduction

The aim of this paper is to determine whether project management has a role in cyber warfare. If there is one, to what extent does artificial intelligence support project management to operate effectively in cyber warfare? We think the ICT sector has surpassed, or at least caught up with, the defence industry in terms of RDI projects. This is understandable, as global skills shortages and capital-intensive developments are concentrating high value-added RDI activity to where large pools of highly skilled personnel and adequate funding is available. These are clearly concentrated in global technology companies, which have a vested interest in continuous improvement, gaining a competitive advantage and achieving ever higher market penetration. This has resulted in an almost unimaginable pace of technological development and the widespread adoption of global products and services. These enable civil society to enter cyberspace and become an active player in it. In response to the impact of digitalisation, global services are also bringing other economic and political actors into cyberspace, so that critical infrastructure and critical information infrastructure owned and operated by civilians also become parts of the network.

In this paper, we will first demonstrate that a significant part of cyber warfare takes place in the civil sector, not only through civilian targets, but also through professionals who take an active role in this activity. Using the structure of the ICT sector, we will illustrate the role of project management in the operation of the sector and in the relevant areas of cyber warfare. We also present ICT technologies and their links to artificial intelligence, and will examine the most commonly used project methodologies in terms of current and potential applications of AI.

Systematic Literature Review

1. Interpreting and Positioning Cyber Warfare

In order to introduce cyber warfare and link it to project management, we first need to define and characterise the concept of cyberspace. There are many definitions and historical overviews available to describe cyberspace, and we will mention only those, which we consider to be definitive and which we think can be applied practically and scientifically, based on our current knowledge and understanding. Therefore, in this article we will present modern approaches through which we illustrate the relationship of cyber warfare with the civil sector and project management. Haig's (2018) detailed, yet concise definition is a good starting point for our present work, which states that "cyberspace is the man-made, dynamically changing artificial domain in which interconnected infocommunication devices and systems operate using the electromagnetic spectrum to collect, store, process, transmit and use information, enabling continuous and global connectivity between people and devices. The above definition corresponds to:

- the need for new forms of interconnectability between people
- the connectivity of physical devices, in line with the Internet of Things principle, and
- the use of the electromagnetic spectrum."

It places a strong emphasis on information as the fundamental driving force of cyberspace. It describes well the technological and logical links between machine-to-machine, human-to-human and human-to-machine, and the flow of information through these links, i.e. the virtual dimension. It also points to the networkisation that is a prerequisite for today's knowledge and technology-based world (Haig, 2018). Taking and strengthening this idea further, it is worth to mention the approach of Laszlo Kovacs, which also suggests a viewpoint appropriate to the modern ICT era. According to Kovacs, cyberspace is an umbrella term that includes everything that comes into contact with information, i.e. processes, actors of these processes, technical and software tools, the systems involved; all of these are directly or indirectly connected to a computer network (Kovacs, 2018a). Having summarized the two definitions, cyberspace is best described as any element, device, process, system, activity, and actor that is networked and directly or indirectly related to the production, processing, transformation, transport, storage or use of data and/or information.

Warfare, as defined, will not be addressed in this article, because one of the characteristics of cyberspace and the virtual world is that it completely blurs the boundaries in the areas that are the defining parameters of this type of action. Thus war and peace cannot be precisely defined in the dimensions of time, space and actors. In terms of actors, in cyberspace warfare, be it defence or counter-insurgency, the actors who carry out actions and those who are targeted are not necessarily military actors. It is safe to say that the majority of potential targets in cyberspace can be identified in civil, economic or political domains. Elements of critical infrastructure or critical information infrastructure, social media systems or events involving large crowds, such as elections or sporting events, are all high-risk areas of cyberspace that do not belong to a country's military forces. This is why civilians and civilian-military cooperation in cyberspace operations have an important role to play in NATO's understanding of cyberspace. Joint activities are complemented by, among other things, joint competence building and capability development (NATO, 2009).

The time horizon is also blurred and it is not possible to separate war or warfare from peace, as cyberspace is characterised by the fact that cyber incidents, whether caused by malicious software robots or human actions, can occur at any time, both on the offensive and defensive. The civilian population, accessible through cognitive operations and internet techniques, is a potential target at every moment. As with the previous analogy, the location of a war zone or a specific area of operation cannot be separated or delimited. Anything that exists in cyberspace, i.e. is connected to a network, is accessible from any point on the network regardless of geographical location or distance.

To summarise the above, cyber warfare, given the specificities of cyberspace, is an activity that is constant in time and space, and in which everyone who is directly or indirectly connected to the information network becomes an actor. In line with Laszlo Kovacs, we understand this activity as a deliberate act of military, political, and economic defence in cyberspace. In our interpretation, the use of the word "warfare" is justified because this activity is carried out in pursuit of national interests and, where appropriate, threatening the interests and security of other nations. The fact that NATO identified cyberspace as the fifth theatre of war at the Warsaw Summit in 2016 complements and completes this line of thought (NATO, 2016).

Warfare involves the use of offensive and defensive capabilities alike, and in this case, cyber weapons and cyber defence assets as well. Thus, we should not think of devices that operate in the physical dimension, similar to the mechanism of action of real devices, but of software and hardware tools and their application in cyberspace that inflict some degree of damage on designated targets (Kovacs, 2018b). Indirectly, of course, this damage can be physical, material or even cognitive, but overall, the first target is always some kind of information and the carrying out of an operation involving it. Since this paper aims to focus on the role of civil development project managers in cyber warfare, herein it is appropriate to focus on the information-related areas of cyber warfare, therefore we examine the ICT sector's link to that field.

2. ICT and Cyber Warfare

The definition of cyberspace illustrates the link with the infocommunications industry: networks, especially the internet, information operations, actors, the IoT principle, or wireless communications. Given that the environment for cyber warfare is cyberspace, an indirect link between cyber warfare and ICT can be demonstrated. By interpreting cyber warfare, direct links can also be proven, which is why we consider it necessary to briefly address this issue. Focusing on the ICT sector and civilian use, I will only examine certain cyber-operational capabilities of cyber warfare (Haig, 2018).

- Computer network operations
- Deception
- Psychological operations
- Civilian-military cooperation
- Mass information / mass media.

Computer network operations are operations involving the physical and logical layers of the network. They target network elements, software, hardware, and databases, and include detection, attack, defence, and data manipulation within the network. The term "deceptiveness" covers the communication of any information that is not true, meaning that it can be physical deception, be it electronic or software induced, or even psychological - e.g. social engineering. Deception can occur in all layers of cyberspace. Psychological operations affect people specifically, in the sense of some form of influence, cooperation, or contact. This can apply to any kind of communication channel in cyberspace.

Civil-military cooperation is a capability that is closely related to psychological operations, using the same tools and techniques for communication between the civilian population and the administrative authorities. Mass media is specifically aimed at bringing information to the general public: information via the internet, social media, and news portals. The cyber information capabilities listed above are of course carried out in cyberspace, but it is clear that they have an impact through the products and services of ICT organisations, and in many cases they are the targets themselves.

3. The Technologies and Development of Cyberspace

It is not possible to cover all current and foreseeable technologies due to physical constraints and the dynamics of the ICT sector, so we will focus on those areas that best illustrate the role of ICT and civilians in cyber warfare, and of course, those related to artificial intelligence.The world wide web, or internet, is the basis for all digitisation and data collection: it is virtually what makes cyberspace exist on such a large scale and allows information to be shared quickly and efficiently. Although the Internet was not designed for civilian use, it is now an indispensable tool in the ICT market. Its main purposes and characteristics are (O'Reagen, 2012):

- there is no central management or supervisory body,
- no central control computer,
- billions of computers are connected to each other,
- it is not in a single physically well-defined location,
- not a physically tangible thing.

The role of the internet in networking and the technologies that build on it is important. It is therefore also important in areas such as machine learning and artificial intelligence, which rely on it for data processing and transmission. The next level of networking among Internet-based technologies is cloud technology. As bandwidth has increased, a new approach has become possible. Data is no longer stored and processed on

networked devices, but in a central location in the network. This is an important shift in approach as it fundamentally changes the way digital operations work, enabling complex data processing and the interconnection of independent systems. Another benefit for users is scalability, always using as many resources as needed, so the devices used do not need extreme capacity to meet the infrequently occurring performance peaks. Information and services can be accessed from multiple devices, without the need for duplication/multiplication across them. Tech companies in the ICT sector are constantly developing new technologies based on existing ones through RDI projects. Cloud computing and evolving mobile communications, in contrast to the smart device networks of the past, allow almost any electronic device to be networked and then remotely monitored or even controlled. This means that the condition is reversed and networking can transform anything into a smart device. We call this the Internet of Things (IoT). In many cases with IoT, everything regarding information is actually happening in the cloud. A networked device contains just a sensor and a microchip that enables network connectivity. This is an important milestone for cyberspace, as much of the real physical world can be converted into data through sensors and thus moved into cyberspace. IoT technology forms the basis for the entire smart ecosystem, such as smart cities, smart homes, smart cars and their further development into connected vehicles and the resulting self-driving vehicle technology.

This is a huge amount of data, which is growing exponentially as infocommunications technologies take over. According to Cisco's 2018-2023 projections, the number of internet users will grow from 3.9 billion to 5.3 billion, and the number of networked devices will increase from 18.4 billion to 29.3 billion (Cisco, 2020). This of course implies an increase in data volume, based on a year earlier projections, with personal data traffic rising from 13 gigabytesto to 35 gigabytes from 2017 to 2021. The classical data processing methods used and structured databases are not suitable for processing such volumes and, more importantly, such complexity of data sets, and therefore a new technological development is underway, called Big Data. Big Data works differently from traditional data operations; there is no data processing on the networked device or sensor, it is done in the cloud, where huge amounts of data are collected and connected. Then servers, also with huge resources, have the capacity to perform the operations issued at the endpoints. This, in addition to the advantages of cloud computing, gives the possibility of linking completely independent data, thus making it possible to use and visualise information in ways that have not been used or even known before.

The technologies presented so far allow data to be collected, transformed and processed. Thanks to digitalisation, IoT and broadband communication technology, a lot of data is being accumulated that could not be processed by earlier methods or only with great inefficiency. The trend to address this is Big Data. Along with this, another very important technology is also coming to the fore - artificial intelligence (AI). AI is designed to perform tasks automatically, without human intervention. In the first wave, human knowledge and skills are taught to software, parameterised and, based on certain information and feedback, machines can perform complex tasks, such as making decisions, in a given environment. Data-intensive operations in the last few years have pushed research in a more dynamic, adaptive direction than the earlier approach. This means that, in addition to decisions and predictions made from historical data, these algorithms can also work based on real-time information obtained from the environment. Recent research results go beyond this to endow AI with the ability to learn. This ability called machine learning allows the results of the analysis of incoming data to be incorporated into further operations, i.e. to improve operations - in other words, learning. This is currently a complex and complicated operation, requiring a very large amounts of data, which in many cases is not available, so synthetic data is produced, which makes the process of learning very expensive and time consuming (Negyesi, 2019).

In addition to the technologies already in use and widely accepted, the future is of course also about developing these and similar technical solutions. Although, according to the technological singularity defined by Raymond Kurzweil, we cannot accurately predict the technologies of the future, because we will reach a point in our development where, due to the rapid pace of development, we will not be able to grasp the workings of tomorrow (Kurzweil, 2013). There are estimates, however, and various research institutes are trying to identify trends that show the future in a few years' time. The Gartner research institute is constantly analysing and using a hype curve to identify and determine future trends. The latest available hype curve for 2019 identifies five areas, of which we will only discuss those related to AI in more detail (Gartner, 2019):

- Sensors and mobility: this trend brings together technologies that increasingly enable mobility and the management of associated devices, including 3D sensor cameras and advanced autonomous driving. With advances in sensors and AI, autonomous robots can operate more consciously in the environment around them. For example, new technologies such as lightweight transport drones (both flying and taxiing) will be more advanced in navigating and taking account of objects. This technology is currently hampered by the legal environment, but technological development will continue.

Technologies covered include cloud-based augmented reality (AR), fourth and fifth level self-driving and flying self-driving vehicles.
- Human robotic technologies is a trend to improve human physical and psychological capabilities with biochips and emotional artificial intelligence.
- Post classical computing and communication: classical or binary computing, which uses binary bits, is evolving by modifying existing traditional architectures.
- Digital ecosystems, which are sharing platforms connecting cyberspace actors.
- High-level artificial intelligence (AI) and analytics. Next-generation analytics is the autonomous or semi-autonomous analysis of data or content using sophisticated tools, beyond traditional business aspects. Technologies based on machine learning models will enable the further development of AI and, through it, data analytics. This trend includes adaptive machine learning, AI, and graph analytics.

In addition to the benefits, the new technologies and developments described above also pose increased risks, as they ensure that the entire society and economy is connected to the cyberspace.

4. Extending Cyber Warfare to the Civil Sector

Cyber warfare naturally includes reconnaissance and counter-intelligence activities, but from the perspective of ICT organisations and civilian experts, it is reasonable to narrow the analysis to defence, because in peacetime it is illegal to conduct any kind of reconnaissance or counter-intelligence. To show the civilian dimension of cyber defence, it is also necessary to understand both critical infrastructure and critical information infrastructure as entities that are important for the country, but are operated by civilians, such as telecommunication companies, the banking sector, media, and transport, with a special focus on logistics. Infrastructure elements critical to national security. Article 1, point f. of Act CLXVI of 2012 defines critical infrastructure as follows. *"An asset, facility or system element belonging to one of the defined sectors that is essential for the performance of vital societal functions, in particular health, safety and security of people and property, and the provision of economic and social public services, the loss of which would have significant consequences due to the lack of continuity in the performance of these functions, but which has also become critical information infrastructure as a consequence of digitalisation and the data-driven society."* (CLXVI Act)

It is not possible to give a detailed and comprehensive list in this publication, but one of the main sectors and its sub-sectors is an important part of the subject, and a large part of it also operates in the NGO/civil sector:

Table 1. The types of info communication technologies

Infocommunications technologies	Internet infrastructure and Internet access services
	fixed and wireless electronic communications services, fixed and wireless communications networks
	radio telecommunications
	space telecommunications
	broadcasting
	postal services
	government information technology, electronic networks

Critical Information Infrastructure is defined in a government decree for the following year, the Decree on the Implementation of the Critical Infrastructure Protection Act. *"The networked, physical or virtual systems, devices and methods of society which, due to the need to ensure the continuity of information and the continuity of IT conditions, are essential for the operation of vital system elements by themselves or other identified vital system elements."* (Government Act, 2013).

Critical Information Infrastructure has been defined in a government decree for the following year, the Decree on the Implementation of the Critical Infrastructure Protection Act. *"The networked, physical or virtual systems, devices and methods of society which, due to the need to ensure the continuity of information and the continuity of IT conditions, are essential for the operation of vital system elements by themselves or other identified vital system elements."* (Government Act, 2013).

Beyond these systems, cybersecurity is important for ICT companies' products and services, as high internet penetration puts citizens' data, and through it their assets, at risk. Taking this further, ICT organisations and professionals are indispensable actors in cyberspace and should therefore be an important part of cyber defence. According to Alexander Klimburg, ICT actors are also an integral part of information security. The products and

services of ICT companies, which are accepted and globally distributed, are also a source of vulnerability. Because of the products and services used worldwide, no country is able to secure the entire ICT supply chain on its own, from sources it can entirely trust and control. Areas where the products of multiple suppliers need to be integrated pose a fundamental risk, compounded by cases where products that are unreliable or uncontrollable for the organisation or even the country, are incorporated. The figure below illustrates the role of ICT security in information security (Klimburg, 2012).

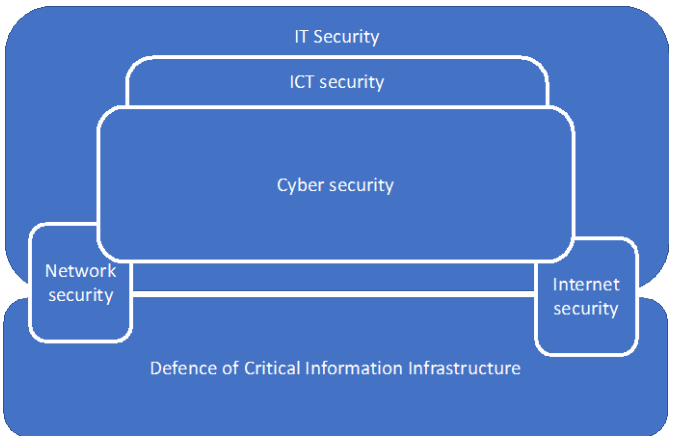

Figure 1. The role of ICT security in information security

So the main link between cyber warfare and the ICT sector is cyber defence and cyber security. In summary, the above shows that a significant part of cyber warfare is taking place in the civilian part of the ICT sector. The majority of civil actors are targets of cyber warfare in relation to the total number of citizens, but professionals in the field appear in important defensive roles. The experts required to develop models, hardware and software tools for defence, their implementation, integration with each other, customisation to the organisation and response and recovery to a given incident are the following:

- technical specialist, typically from several fields
- project manager
- business analyst
- technical analyst/responsible person
- other specialists (legal, economic, political, and communication skills may be required for a specific issue)

A technical specialist and project manager are included in all of the projects listed, while the need for a business analyst, a technical officer or other specialists depends on the type and size of the project and the organisation's processes.

Results and Discussion

1. Project Management in the AI and ICT Sectors

The organizational structure of today's organisations in the ICT sector is generally twofold. The first is the project organisation, which is explicitly project-based, so the organisation is built around projects, which are at the heart of its operations. The management typically follows the "management by project school", and therefore takes project management to a strategic level: the whole organisation works on a project basis and there is full alignment between project objectives and corporate objectives (strategic goals). Outside the project, colleagues only participate in training, education and internal efficiency improvement projects. Typically, after a project is completed, employees are placed in a so-called resource pool, from where they can be freely involved in a new or ongoing project. In IT, this model is typically used by organisations involved in custom development, systems integration, high value-added RDI consultancy and implementation, and by research laboratories.

Another form of organisation is the matrix organisation, where, if we imagine a matrix, the columns are the functional units and the rows are the projects. Both the functional unit and the project have a manager. In a matrix organisation, the functional unit has core tasks that need to be performed. Projects, on the other hand, are

built up by "hiring" colleagues from several functional units across the organization. Projects form the rows in the matrix. Project approach and project-function are also important in this organisation, which is why temporary organisations and project managers are identified by name within the structure. Between projects, colleagues carry out the core activities of the unit in their respective departments. This model is used by large organisations that have other ongoing core activities, services or products in addition to project activities. Typical examples are multinational companies, centralised international groups and large public organizations (Gaal & Szabo, 2013).

With the proliferation of agile methodologies, a third organisational structure is coming to the fore, similar to a project organisation, however, in this methodology, the project team does not split up after completing a task, but stays together and is dedicated to the next task as a team. This is only possible in a highly agile, flexible environment, which is why even fewer organisations opt for it; these are typically small to medium-sized development companies or organisations with a product of their own that need to respond quickly to customer needs, e.g. start-ups and innovative companies that develop new technologies. Both main organizational structures focus on effective project management, and the vast majority of their operations and work is project-based. In addition to the organisational structure, these bodies strengthen their operations with professional project management at the organisational level. In order to measure and improve this, they use existing methodologies and measure the maturity of the organisation in order to see where it stands in its development.

According to the Project Management Institute (PMI) 2018 survey, 93% of companies use some form of standard project management (PMI, 2018). An earlier survey by Price Waterhouse Coopers in 2007 found a similarly high proportion, with 77% of businesses using some form of documented, company-wide project management methodology (PwC, 2007). The maturity models look at different aspects of project management in an organisation, using different methods, which are described in more detail in the description of the models below.

Paul, one of the researchers of the CMM(R) model, defines PM maturity as "how clearly a specific process is defined, managed, measured, controlled, and how effective it is" (Paul et.al, 1993). According to Skumolski, project management maturity is both a measure of the organisation's receptiveness and openness to project management, and a measurement of the extent to which the organisation is able to fully support and enable its project managers to take the steps necessary for the success of the project (Skumolski, 2001).

In the following, only the most common project management maturity models will be presented, as Pennypacker collected more than 30 existing models in the early 2000s, and their number has been increasing ever since (Pennypacker & Grant, 2003). The three best-known and most used project management models are currently PMI - OPM3, PRINCE2 and the International Project Management Association (IPMA) model. However, the PMI, Prince2 and CMMI models are those that will be presented in this publication, as CMMI was specifically developed for ICT developments and therefore I believe it has more relevance than the IPMA model, and I also think that its penetration is not lower either when looking specifically at the IT domain.

The models are presented without being exhaustive, focusing on areas where they can or could be connected to AI. The main reason for the creation of this model was to manage projects in IT organisations, but it is now considered a much more widespread, almost universal project management methodology. This project management technique, based on a 'de facto' standard, has become a common and frequently used methodology not only in the UK but also in Europe (OGC, 2005).

PRINCE2 is a process-based approach to project management. It describes how a project can be divided into different, separately manageable processes, each with well-defined inputs, outputs, and objectives. The method is based on quality management, which allows the organisation to control the project from its inception to its completion.

Four key elements of the PRINCE2 methodology:

- 8 defined processes that provide the framework for project management
- 8 principles and guidelines used under the different processes
- 3 methods that support the processes
- Precise definition of the components for project verification

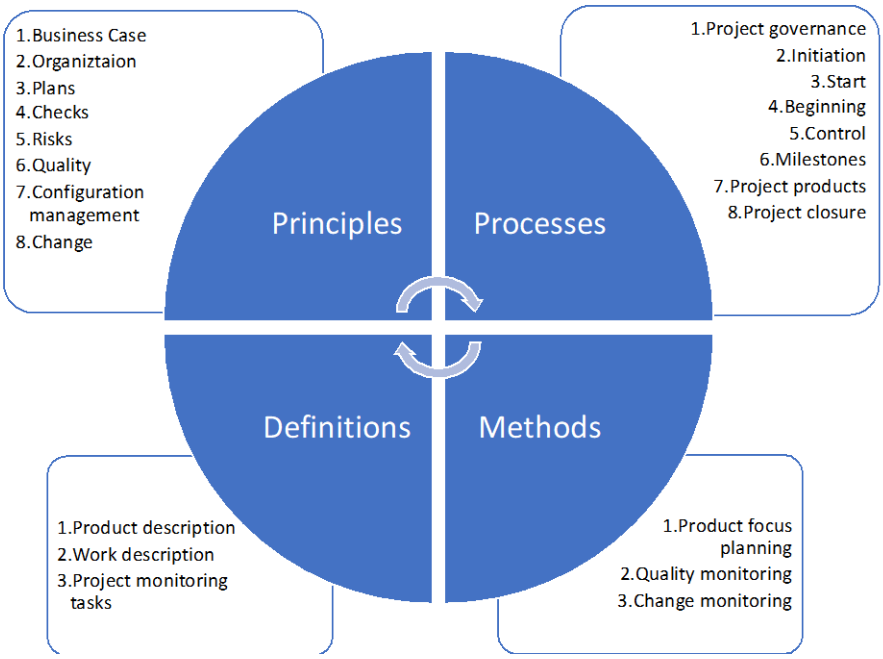

Figure 2. PRINCE2 key features

If an organization chooses this methodology, it allows its managers and project managers to take a unique approach to different projects. The PRINCE2 methodology assumes that the organisation already has well-established project management techniques in place, so it encourages participants to continue using and developing them. The model itself has five levels of maturity, as follows:

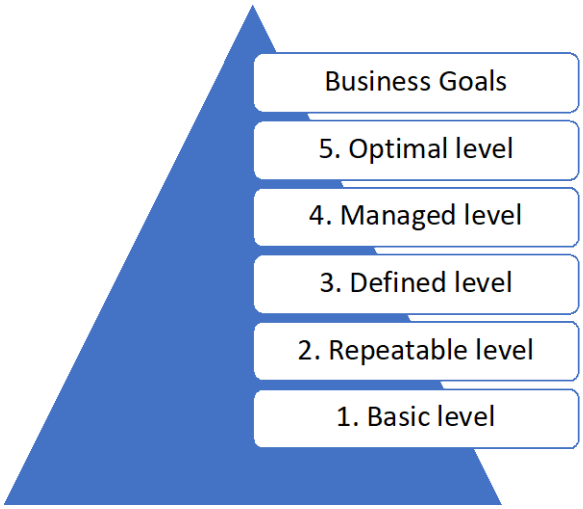

Figure 3. Levels of the PRINCE2 maturity model

On the first and second levels there aren't any controlled processes or procedures, although it is not even neccesary for the execution of ad-hoc tasks. There are agreed guidelines for processes and procedures at the defined level, which apply to all projects. Depending on the organisation, there may even be guidelines on the use of artificial intelligence or related tools. At the managed and at the optimal levels, most processes operate within a controlled framework, but there are procedures in place as well. Here, the organisation performs project management tasks at a professional level.

The PRINCE2 methodology, a tool for effective operational project management, does not currently place primary emphasis on the use of artificial intelligence or any related IT tools. Its general process is to enable a specific/individual focus on the use of AI-based techniques or tools, with a strong mandate from the project manager, there are no specific recommendations or good practices dedicated within the framework of the methodology. By its very design, the model is about providing the project manager with a wealth of accurate

data. Due to digitalisation and strong authorisation, organisations and project managers using the methodology can quickly adopt AI logic and support even for ongoing projects.

2. Capability Maturity Model Integration

The CMMI model can basically be described as a "hybrid" model that has been created by incorporating the strengths of several maturity models. The aim was to develop a model to support the development of processes and products. It consists of two parts, an organisational maturity test part and a process maturity part. The organisational maturity part, known as the "gradual" part, examines groups of key organisational processes that need to be improved in order for the organisation to move to a higher level of maturity. The latter area is the continuum approach, which identifies capability levels for each process [22]. In the case of the CMMI model, we can also speak of 5 maturity levels, with key processes identified at each level. Its creators have also collected tools to help organisations at lower levels to move to higher levels.

- development of organisational rules
- process design
- identifying and making free resources available
- establishing areas of responsibility
- training of employees
- applying performance management to processes
- identification and involvement of relevant stakeholders
- monitoring and controlling processes
- gathering information for development

The highly process-oriented and integrative nature of the CMMI model emphasises the close intertwining of organisational processes and standards with project management, thus facilitating the extension of the artificial intelligence tools and good practices applied by the organisation to the projects. It places less emphasis on identifying and analysing them, thus hiding the potential for their application beyond the organisational use. Project managers are less empowered due to mature and planned processes, and therefore have less opportunity to independently implement new AI applications unknown to the organisation. The methodology focuses on the technical part of project management, on development tasks, and adopts the additional areas and processes from within the organisation.

3. Organization Project Management Maturity Model – OPM3

The Project Management Institute aimed to create a 'good practice' resource in the area of project/programme/portfolio management, which could also be used to standardise and assess these capabilities of the organisation. OPM3 is also a generic model that can be implemented across different industries, sizes and geographies.

With the model, users will be able to identify which good practice belongs to which area, and thus match theory with practice, increasing the efficiency of implementation. Hundreds of case studies are available in the field of organisational project management, showing which specific skills need to be developed and how to develop them to reach the desired level of maturity. Furthermore, OPM3 supports the organisation in its self-assessment. Based on these results, the strategic prioritisation and resources of the organisation, it helps to create a development plan. This plan enables the development of the necessary project management skills, thus leading to a higher level of maturity.

The basic components of OPM3 (PMI, 2003):

- A collection of good practices
- Collection of skills
- Observable outputs
- Key performance indicators.
- Development plan.

The structure of OPM3 (PMI, 2003):

- Standardisation: repeatable processes and activities are used by the organisation.
- Measurement: it can measure its processes, activities and their effectiveness.
- Management: it can analyse and evaluate measurements. It can react to them and thus control the output, i.e. the efficiency.
- Continuous development: the need for improvement is established. The emphasis shifts from reactive to proactive behaviour, with problems and performance issues not aimed to be solved but to be prevented and eliminated.

In addition to the maturity levels, there are three levels of management that make up project management at the organisational level: project, programme, and portfolio. These areas are divided into five project life cycles: identification, design, implementation, monitoring and management, and closure. From this we can draw the structure of the OPM3. These good practices (represented by arrows) lead through the maturity levels, which are broken down into project lifecycle (rings). The rings contain the skills required for the level (points within the rings).

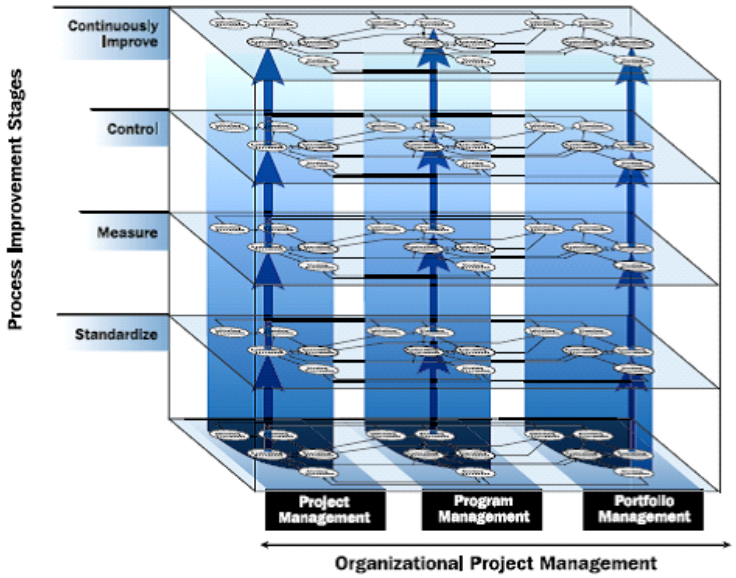

Figure 4. OPM3 structure

3. OPM3 model summary

The PMI model, while often referring to organisational policies and processes in general, does not mention AI as a specific area of maturity or project management. It is important to note, however, that PMI in his recent research names AI as an important and indispensable organisational capability. [24] It relies on a strong matrix or project-oriented organization for its operation, a very strong empowerment for project management. It provides the opportunity to identify areas for improvement or even project risks where the application of MI could be a solution. This is important because it gives you the authority to allocate resources within the project. This could mean specialist staff, extra time for certain tasks, or even financial resources for tools or training for colleagues. So there is a certain degree of freedom for project management in this model, although the client's needs and risk apportionment must of course be taken into account. That said, it is of course not a sustainable method if each project needs to introduce MI individually, but the model is structured so that it can easily become good practice, then become legitimate to use and can be adopted by the whole organisation's project management in a spirit of continuous improvement.

Although current methodologies do not name and dedicate processes or tools for the use of AI, it is clear from the trends that, like all fields, project management will become data-driven as a result of digitalisation, and this also means the use of AI. Currently known AI applications could be used for data processing, decision making, forecasting based on data patterns, important reporting and administration tasks, risk occurrence and assessment, and of course instant status reporting. According to PMI's 2019 research, 85% of organisational leaders predict that AI will change the way they do business within five years. The organisation has defined PMTQ, project management technology quotient, as a capability for future project management. It summarises knowledge of technologies such as AI or cyber security (PMI, 2019).

Conclusion

The publication confirmed our hypothesis that the ICT sector has a very high involvement in cyberspace, and thus in cyber warfare. This means that ICT professionals, including project managers, can be active participants in cyber warfare. In this paper, this is only confirmed for cyber defence, but knowing the project characteristics, projects can also be considered as reconnaissance or counter-intelligence type tasks. As these are also carried out in the civilian part of cyberspace, and since the actors, environment and tools are the same, the methodology could be the same too.

The project management methodologies used do not currently use AI in a standardised way. Therefore, it cannot be stated formally that AI makes professional project methodologies more effective or in any way assists professional project methodologies in cyber governance. Developers of project management methodologies appear to be putting a lot of emphasis on moving towards AI, and companies producing various project management tools and software are currently using AI for certain tasks. While these facts somewhat nuance the picture, overall the use and integration of standardised AI into formal methodologies is still in its infancy.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Acknowledgements or Notes

This article was presented as an oral presentation at the International Conference on Research in Engineering, Technology and Science (www.icrets.net) conference held in Baku/Azerbaijan on July 01-04, 2022.

References

Act CLXVI of 2012. *On the identification, designation and protection of critical systems and installations*. Wolters Kluwer. Retrieved June 28 2021 from https://net.jogtar.hu/jogszabaly?docid=a1200166.tv.

Cisco. (2020). *Cisco annual internet report (2018–2023).* White Paper. Retrieved June 28 2021 from https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html,

Gaal, Z.. Szabo, L. (2013). *Segedlet a projektmenedzsmenthez II. Megoldasok, modszerek, technikak*. Veszpremi Egyetemi Kiado.

Gartner (2019). 5 trends appear on the gartner hype cycle for emerging technologies, Retrieved June 28 2021, from https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/.

Government Act. *Implementing Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Installations*. Wolters Kluwer. Retrieved June 28 2021 from https://net.jogtar.hu/jogszabaly?docid=a1300065.kor.

Haig, Z. (2018). *Informacios Muveletek A Kiberterben*. Dialog Campus Kiado. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12651/web_PDF_Informacios_muveletek_a_kiberterben.pdf;jsessionid=97D3B77EE69E4C11F4B0AE1A46544334?sequence=1,

Klimburg, A. (2012). *National cyber security framework manual*. NATO CCD COE Publication.

Kovacs, L. (2018a). *A kiberter vedelme.* Dialog Campus Kiado.

Kovacs, L. (2018b). *Kiberbiztonsag es –strategia.* Dialog Campus Kiado.

Kurzweil, G. (2013). *A szingularitas kuszoben.* Ad-Astra.

NATO. (2009). Allied Joint Doctrine for Information Operations, Retrieved June 22 2021, from https://info.publicintelligence.net/NATO-IO.pdf.

NATO. (2016). *Warsaw Summit Communique*, Retrieved June 22 2021, from https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

Negyesi, I. (2019): A mesterseges intelligencia es a hadseregek, *Hadtudomany*, *2019*/3., 71-79.

O'Reagen, G. (2012). *A brief history of computing*. 2nd ed. Springer.

Office of Government Commerce (2005). *Managing successful projects with PRINCE2*,

Paul, M.C.; Curtis, B.; Chrissis, M.B.; Weber, C.V. (1993). *Capability maturity model for software, version 1.1*, Software Engineering Institute, Carnegie Mellon University. Retrieved May 16 2021, from https://resources.sei.cmu.edu/asset_files/technicalreport/1993_005_001_16211.pdf,

Pennypacker, J.S.; Grant, K.P. (2003). Project management maturity: An industry benchmark. *Project Management Journal, 34*(1), 4-11.

PMI (2003). *Organizational project management maturity model, opm3 knowledge foundation*

PMI. (2018). P*ulse of profession – succes in disruptive times* Retrieved May 16 2021, from https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2018.pdf, downloaded: 16.05.2021.

PMI. (2019). *Pulse of profession – the future of work – leading the way with pmtq*, Retrieved May 16 2021, from https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2019.pdf?v=ff445571-0b23-4a2b-a989-44eb20df55bd&sc_lang_temp=en.

PwC. (2007). *Insights and trends: current programme and project management practices - the second global survey on the current state of project management maturity in organisations across the world*. Retrieved May 16 2021, from https://www.pwc.com/cl/es/publicaciones/assets/insighttrends.pdf.

Skumolski, G. (2001). Project maturity and competence interface. *Cost Engineering; Morgantown, 43*(6),11-18.

Author Information

Oszkar Dobos
Obuda University
1034 Budapest, Becsi út 96/b.
Contact e-mail:*dobos.oszkar@xiagency.hu*

Agnes Csiszarik-Kocsir
Obuda University
1034 Budapest, Becsi út 96/b.
kocsir.agnes@uni-obuda.hu

To cite this article:

Dobos, O. & Csiszarik-Kocsir, A. (2022). The role of project management in cyber warfare with the support of artificial intelligence, *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 17, 26-37.*