AARMS Vol. 20, Special Edition (2021) 97–112.

10.32565/aarms.2021.2.ksz.7

Cyber Autonomy Toolbox – Project Management Digital Transformation

Iryna LEROY[1]

There was a time when military technology reinforced and provided added value and expertise to business and government organisations. There are a number of technologies, specific military applications and solutions such as the Internet, GPS or sunglasses, and methodologies like strategic planning and negotiation systems that were developed in the past within military domains and later evaluated and implemented, which brought increases in speed and added business value. There are now many diverse digital transformation projects being implemented in several business domains – ranging from small and medium businesses like an Italian family restaurant to the global oil and gas companies such as Shell or British Petroleum or even executive branches of the European Union/European Commission. All these organisations use different technologies to optimise processes, innovate faster, collaborate efficiently and deliver more value with less effort. Economic defence – like never before – means national security. For that reason, Cyber Security initiatives associated with digital transformations include a "testing mode" period, along with Cyber Autonomy functions that aim to support business critical infrastructures. Different methodologies are in place to optimise for the new data-driven economy and support digital transformation. It is the responsibility of the business to adopt best practices and techniques to reinforce national security and offer effective tool support for effective Cyber Autonomy with digital transformation projects.

Keywords: *project management, cyber autonomy, information security, reputation defence, reputation management, computer security, critical infrastructures, risk management process*

Introduction

The research is based on the principles of a systematic approach and objectivity. The purpose of this form of research is to provide better understanding of the research issues. This paper is divided into four stages, namely:

[1] PhD student, University of Economy and Management, Prague, Czech Republic European Security and Defence College, Brussels, Belgium, Université de Lorraine, France; Head of Core, Western Europe department Wordline Ingenico, e-mail: irynaleroy@hotmail.com

- To answer the research questions, we firstly conducted a systematic literature review of the academic research on Cyber Autonomy. In order to progress with the literature review, a keyword search was done on the largest electronic databases of peer-reviewed literature: Scopus, Web of Science and EBSCO databases and citation databases for peer-reviewed literature, covering scientific journals. We decided to include in the research: official statements of the European Commission, Articles, Reviews and Book Chapters. We identify and describe the Model of Cyber Autonomy and its 7 essential elements.
- To choose different project management methods that can be used for Cyber Autonomy implementation. It includes methodologies, reviews and tools in each methodology and how they differ from each other in terms of structure, types, characteristics, features, target audience and goals.
- To define and describe project management tools that could be useful and suitable for Cyber Autonomy. It includes information regarding project tools and the organisation best suited to deploy the best tools and best practices.
- To define and outline the critical phases of project management and associated tools that could be deployed for Cyber Autonomy. This section presents an overview of best practices and some common steps, based on the type of the organisation and goals of the projects.

The target audience of the study has the following characteristics:

enterprises that belong to the critical infrastructure in the European Union; organisations that work for a large enterprise belonging to high-quality value chains operating in industrialised economies, belonging to the European institutions or related government agencies and having information security departments, engineering teams, research and development departments or belonging to European local member states institutions, having information security departments, engineering teams or research and development departments; Small and medium enterprises (SMEs) in the European Union.

In this paper we discuss about the following hypotheses:

- existing project management tools that can be used in Cyber Autonomy for digital transformation
- different phases of Cyber Autonomy for digital transformation require different project management tools that can be organised in the Cyber Autonomy Toolbox
- there is a specific set of tools that leads to Cyber Autonomy, which can be referred to as the Cyber Autonomy Toolbox

Literature review

Autonomy could help decentralised decision-making processes in hierarchical structures and at the same time provide tangible benefits to information security processes. The concept of Cyber Autonomy is considered from multiple viewpoints by many researchers who are working on the subject of cyber security and defence capabilities.

From a technical point of view some authors believe that the goal of Cyber Autonomy is achieved when any computing user – regardless of his/her technical background – is able to protect himself/herself against cyberattacks and attribute the attack sources. Since 2017, IT vendors have started moving towards 'security automation' (as evidenced by the recent rise in automation vendors at the RSA conferences in 2017 and 2018 – the world's largest cyber security vendor trade show in San Francisco) – the first leap towards cyber autonomy. The holy grail for cyber autonomy is that we can deter attacks and patch vulnerable computing systems in real-time, at scale and without disrupting normal operations.[2] For example, Blasch, Erik & Raz in the article related to traffic management look at Cyber Autonomy as effective positioning in response to various cyberattacks.[3] Lack of effective action in the area of cyberattack could increase vulnerability to cyberattacks.[4] Surely, software systems, particularly those running critical infrastructure, emergency services, and 24/7 manufacturing, have very complex dependencies.[5] Nevertheless, nowadays, the digital economy is no longer just about the tech sector and digital firms, it is increasingly digitising supply chains across all sectors of the global economy.[6] New technologies give a new quality of technological infrastructure, but the same ones raise questions of the security of the different Information and Communication Technologies (ICT) areas. For example, as revealed by the EU's policy documents, 5G technology, as well as its suppliers, represent considerable internal security risks and pose a threat to Europe's technological sovereignty and autonomy.[7]

Cyber infrastructure now plays a significant role in the context of cyber autonomy and could potentially increase the degree of information and data protection as well as fill in the current gaps of the cyber and information security industry.[8] Basically, autonomy is defined as the ability of an entity to structure its own action and environment independently and without unwanted influence from the outside. In Artificial Intelligence, autonomous agents are not dependent upon the goals of other entities.[9] Agent autonomy means that agents have control over both their internal state and over their behaviour.[10] The same could be applied also for Information Security and Cyberspace in the area of Cyber

---

2 Ryan KL Ko, 'Cyber Autonomy: Automating the hacker – self-healing, self-adaptive, automatic cyber defense systems and their impact to the industry, society and national security', in *Emerging Technologies and International Security,* ed. by Reuben Steff, Joe Burton and Simona R Soare (Routledge, 2020), 12–14.

3 Erik Blasch et al., 'Information Fusion as an Autonomy enabler for UAS Traffic Management', *AIAA Science and Technology Forum and Exposition. AIAA SciTech Forum,* 04 January 2021, 1–12.

4 Victor Bolbot et al., 'A novel cyber-risk assessment method for ship systems', *Safety Science* 131 (2020).

5 Ryan K.L. Ko, 'Cyber Autonomy', 12–14.

6 T S Kuprevich, 'Tsifrovyye platformy v mirovoy ekonomike: sovremennyye tendentsii i napravleniya razvitiya', *Ekonomicheskiy vestnik universiteta* (2018), 311–318.

7 Márton Varju, '5G Networks, (Cyber)Security Harmonisation and the Internal Market', *European Law Review* 45, no 4 (2020), 471–486.

8 Bram Vonsée, Wina Crijns-Graus and Wen Liu, 'Energy technology dependence – A value chain analysis of geothermal power in the EU', *Energy* 178 (2019), 419–435.

9 Michael Luck and Mark d'Inverno, 'Formal Framework for Agency and Autonomy', *Proceedings of the First International Conference on Multiagent Systems – ICMAS,* 1995.

10 Bob van der Vecht, Frank Dignum, John-Jules Ch Meyer, Martijn Neef, 'A Dynamic Coordination Mechanism Using Adjustable Autonomy', in *International Workshop on Coordination, Organizations, Institutions, and Norms in Agent Systems III,* ed. by Jaime Simão Sichman, Julian Padget, Sascha Ossowski and Pablo Noriega (Springer, 2007), 83–96.

Autonomy. Therefore, new definitions of autonomy are useful when applied to production systems that include a variety of diverse participants and items: private firms, non-profits, governments, individuals, processes, as well as physical cyber devices, computers and servers, software and communication technologies.[11]

In 2020, the authors of the book *Emerging Technologies and International Security* proposed four phases of maturity for full cyber autonomy. This book also reviews new and emerging cyber security automation techniques and tools, and discusses their impact on society, the perceived cyber security skills shortage and national security.[12] According to the authors, cyber autonomy can be supported by cyber security and used against cyberattack. The role of technology has shifted recently with the result that those who do not (or cannot) keep up experience significant disadvantages. Technology no longer supplements our real-life interactions. Rather, real life supplements our technological interactions in all areas of activities. Dependence on technology has dramatically increased due to Covid-19 in different business areas.[13] Technology dependence has become bottlenecks in the European Union (EU) strategy and for European businesses. The dependence of the industry on external vendors can be seen as a major dependence bottleneck and a major stumbling block to the project towards the digital transformation of both the government and private organisations. It could jeopardise the future of information security for small and medium enterprises (SMEs) and the adoption of technologies in the EU.[14]

Building Cyber Autonomy should include a project management phase to ensure that the system achieves the desired result. Information security forums and practices are at their peak with digital transformation of organisations all around the world. A project management approach for cyber security is more comprehensive and effective for implementation of these practices. Project managers can help in the following ways: streamline project execution, enable strategic alignment, optimise continuous resource allocation, resolve problems and effectively manage risks.[15]

An effective Cyber Autonomy Toolbox would help to reduce risks and attain data security and solid data strategy through effective and professional management. With a Cyber Autonomy Toolbox, insights can be provided into the choice between traditional planning methods and agile project management methods which could increase the speed of digital transformation implementation, if risks are clearly assessed, then planning complexity can be reduced.

---

11 Norbert Gronau, 'Determinants of an Appropriate Degree of Autonomy in Cyber-physical Production Systems', *CIRP Journal of Manufacturing Science and Technology* 26 (2016), 70–80.

12 Reuben Steff, Joe Burton and Simona R Soare, *Emerging Technologies and International Security* (Routledge, 2020), 174–189.

13 Jeffrey Allen, 'Increasing Dependence on Technology in the Law Practice in the Time of COVID', *American Journal of Family Law* 34, no 4 (2021), 160–164.

14 Katie Reveno, 'Technological dependency in a post-COVID-19 society', *Stanford Daily*, 19 November 2020.

15 Bhavyatta Bhardwaj, 'Project Management: Changing the way Cyber Security works in an organization', *PM World Journal* 8, no 9 (2019), 1–11.

The model of Cyber Autonomy and supportive process-based methods for effective project management during digital transformation

The matrix approach to the modelling of Cyber Autonomy allows us to determine the structural elements, and functional capabilities of this system. Cyber autonomy could be envisioned as a multi-layer defence system with several elements and functionalities in each layer for Information Security Strategy (ISS). Analysis of the increasing frequency of cyberattacks and threats leads to the need to supplement each structural element of cyber autonomy with new functions (clarify functions of these elements). Thus, without changing the existing structure of a company or organisation and management "traditions" that belong to it, it is possible to set up effective functionality in conditions of increased cyber danger and increased threats to enhance organisational resistance and reinforce ISS. In our opinion, the traditional structural model of the organisation from the point of view of Cyber Autonomy can be represented in Figure 1.

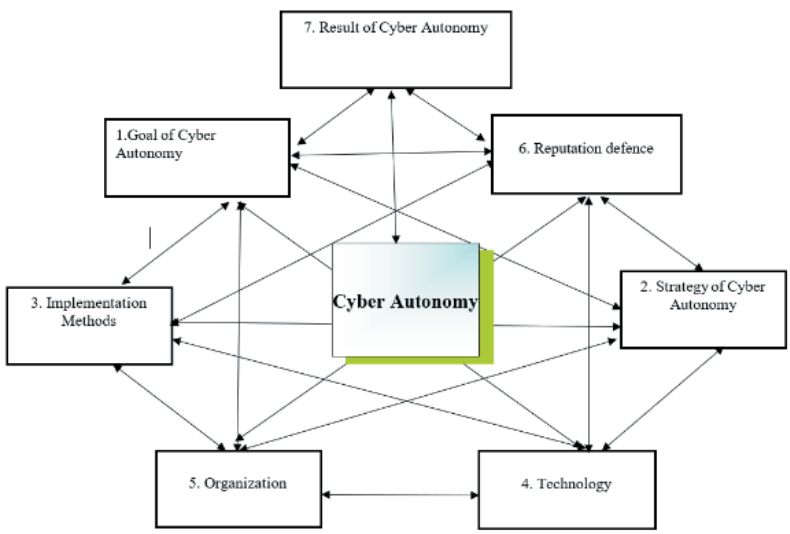

Figure 1: Model Elements: Seven elements of the Cyber Autonomy model

Source: Compiled by the author.

At the company or organisation, Cyber Autonomy aims the development of opportunities and rights to determine, prevent, defend and develop sovereignty, and the creation of the resilience of infrastructure to the atmosphere; such a system is stable. Based on the described model above, Cyber Autonomy includes the following elements:

1. Goal of Cyber Autonomy
2. Strategy of Cyber Autonomy
3. Implementation Methods
4. Technology

5. Organisation
6. Reputation defence
7. Result of Cyber Autonomy

With the purpose of ensuring Cyber Autonomy and the uninterrupted functioning of Cyber Autonomy, these structural elements should provide the following functions indicated. The Cyber Autonomy functions described below are aimed at supporting the Cyber Autonomy model with detailed descriptions of the functions that Cyber Autonomy elements perform. The seven structural elements of the Cyber Autonomy model are supported by seven main functions.[16] Below are listed the seven main functions:

1. Create "Autonomy of IT infrastructure"
2. Ensure "Autonomy of suppliers"
3. Follow "Autonomy of directives, frameworks and guidelines"
4. Secure "Autonomy of professionals"
5. Increase "Autonomy of communication"
6. Develop "Autonomy of processes"
7. Protect "Autonomy of territory"

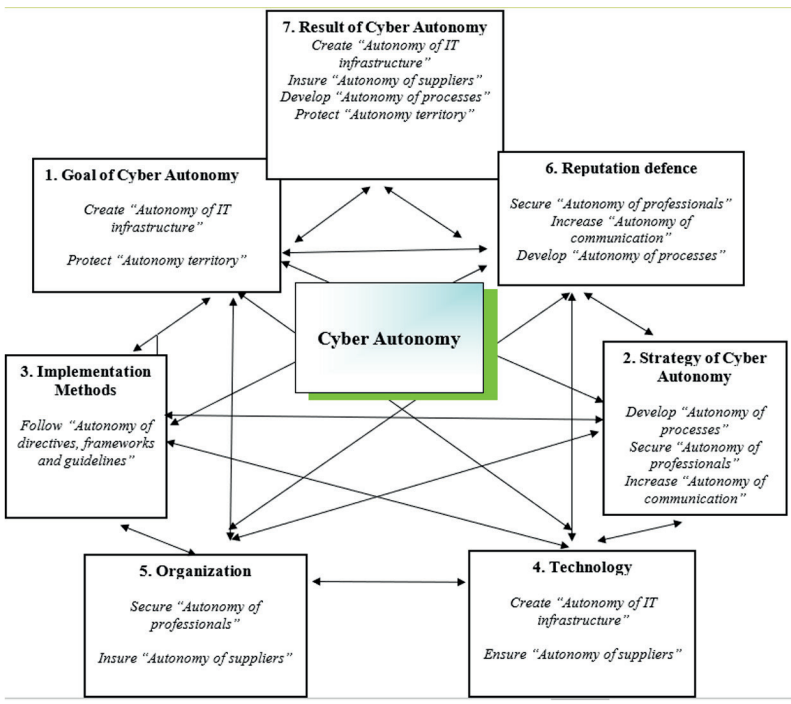

Figure 2: Supportive functions of Cyber Autonomy

Source: Compiled by the author.

[16] Iryna Leroy, *Cyber autonomy for business: building a European cyber resilience. Views on the progress of CSDP* (Luxembourg: Publications Office of the European Union, 2021).

Following the extensive literature review we analysed different project management methods from the different angles such as the target audience (type of organisations), the structure of a method, types, characteristics, features, capability to handle IT and non IT projects for SMEs and government institutions, scalability and applicability for Cyber Autonomy digital transformation. After analysing in-depth, we estimate that four of them would match essential parameters for Cyber Autonomy.

Project management methods and tools in the context of Cyber Autonomy

Currently, none of the world's top 15 digital companies is European. There is no significant European operating system, browser, social media network or search engine, meanwhile the investment gap compared to the USA and China is estimated at 190 million euro per year.[17] There is a growing interest in Europe for the concepts of "digital sovereignty" and "strategic autonomy in cyberspace".[18] In our opinion, digital transformation projects of an organisation to ensure Cyber Autonomy should have some parameters that help improve processes in an organisation. There are no universal solutions in the creation of Cyber Autonomy and in the IT sector. We propose to choose a set of methods focused on ensuring Cyber Autonomy, which avoids the need to have more resources or spare time at each stage in case of any complications or increased risks. We cannot define one or other methodologies that are of the most frequently used methodology and involve all necessary parameters and elements for Cyber Autonomy which are suitable for both business organisations and government organisations. As Cyber Autonomy aims the development of opportunities and rights to determine, prevent, defend and develop sovereignty in an organisation, to mitigate threats and maintain resilient infrastructures – such a system must be stable. Therefore, it is important to choose combinations of tools from different project management methods of which one would be appropriate for these organisations.

Table 1: Tools of reputation management relative to cyberattacks

Essential parameters for Cyber Autonomy	**Agile Yes/No**	**Lean Six Sigma Yes/No**	**PM² Yes/No**	**PRINCE2 Yes/No**
Meet the goal of Cyber Autonomy that refers to the technological area and describes it as technological capabilities and rights of an organisation to determine, prevent, defend and develop sovereignty to mitigate threats and the resilience of infrastructure.	Y	Y	Y	Y
Be suitable for business and government domains.	Y	Y	Y	Y

[17] Axel Voss, 'Digital autonomy', *The Parliament Magazine*, 17 March 2020.

[18] Didier Danet and Alix Desforges, 'Digital sovereignty and strategic autonomy in Europe: From concept to geopolitical reality', *Hérodote* 177–178, no 2–3 (2020), 179–195.

Essential parameters for Cyber Autonomy	Agile Yes/No	Lean Six Sigma Yes/No	PM² Yes/No	PRINCE2 Yes/No
Have an average project duration from 1 up to 6 months.	Y	Y	Y	Y
Include risk management evaluation.	Y	Y	Y	Y
Include compatibility with process transformation.	Y	Y	Y	Y
Be suitable for SMEs and startups.	Y	Y	Y	Y
Enable collaboration between different functional and business teams.	Y	Y	Y	Y
Correspond to Information Security standards.	Y	Y	Y	Y

Source: Compiled by the author.

Various authors describe project management tools. Nicolai Andler has the list of the most important tools for the workshops and evaluation offered by tools and concepts for projects that are characterised by complexity and uncertainty.[19] It becomes essential to identify the areas of IT project streamlining, as applications developed by employees and enterprises can much more efficiently perform their tasks, achieve their goals and create value for their clients. There are many IT tools on the market which can be useful in the process of managing IT projects.[20] One of the most famous project management books on software project management is *The Mythical Man-Month.* It describes tools, practice of suggestions on factors affecting success of software development projects. Author Frederick P Brooks provides information especially about estimation, resources and overall planning, not just for software projects. Brooks emphasises that for an optimal work specialists should have their own specific set of tools that are highly customised and suitable for the type of job that the team is doing, and all tools should be built and maintained by a common tools team, led by a project manager.[21] Kim Helaman offers the basic principles and tools of project management as well as revised material on project management methods and practices from different methodologies such as Agile or PMP.[22] Author Hugo pays special attention to the levels of use of quantitative risk management tools and the benefits gained from their use, and describes critical success factors.[23] The combination of tools helps achieve the final result. Below is a list of the most effective and commonly used tools in project management methodologies.[24]

---

19 Nicolai Andler, *Tools for Project Management, Workshops and Consulting: A Must-Have Compendium of Essential Tools and Techniques* (Erlangen: Publicis, 2020), 36.

20 Jolanta Pondel and Maciej Pondel, 'Stages and Areas of the Use of IT Tools Supporting the Management of IT Projects', *Management Sciences/Nauki o Zarzadzaniu* 23, no 1 (2018), 45–57.

21 Frederick P Brooks, 'The Mythical Man-Month: After 20 Years', *IEEE Software* 12, no 5 (1995), 57.

22 Kim Heldman, *Project Management JumpStart* (Wiley, 2011),16–17, 258–279.

23 Francois D Hugo, Leon Pretorius and Siebert J Benade, 'Some Aspects of the Use and Usefulness of Quantitative Risk Analysis Tools in Project Management', *The South African Journal of Industrial Engineering* 29, no 4 (2018), 116–128.

24 Maneesh Kumar, Jiju Antony and Byung Rae Cho, 'Project selection and its impact on the successful deployment of Six Sigma', *Business Process Management Journal* 15, no 5 (2009), 669–686; Eldon Larsen, 'Adapting project management principles and tools for research and development', *AIChE Annual Meeting Conference Proceedings*, 2014, 1–8; David Hinde, *PRINCE2 Study Guide, Second Edition Overview of PRINCE2* (Wiley, 2018), 391–413, 345–390; Six Sigma Qualtec, 'The Importance of Project Selection: Why Six Sigma Projects Falter, How to Assure Success and Sustainability', *White Paper,* 2020.

Table 2: Project management tools for Cyber Autonomy

Method	Tools of the project	Description	Domain
Agile	• Scrum/Kanban • Lessons learnt • Risk assessment	• Source: to achieve incremental growth • Source: to promote disciplined project management • Source: frequent inspection and adaptation • Source: self-organisation and adaptability	IT, manufacturing, software development, etc.
Lean Six Sigma	• Brainstorming • Process mapping • Project chapter • Root cause analysis • The 5 whys • Voice of the customer (VOC) • SIPOC (suppliers, inputs, processes, outputs and customers) • Kaizen (continuous improvement) • Value stream mapping	• Source: skill to predict, prevent and control defects in a process • Source: understanding the elements of waste • Source: skills to achieve sustainable quality improvement through process improvement • Source: understanding of variation in processes	IT, manufacturing, software development, retail, airline industry, etc.
PM²	• PESTEL analysis risk • Likelihood/impact matrix • Work Breakdown Structure (WBS) • Deliverable Breakdown Structure (DBS) • Effort and cost estimates • Decision trees • Gantt charts • Critical Path Method (CPM) • Critical Chain Method (CCM) • Earned Value Management (EVM)	• Source: improving communication and the dissemination of information • Source: clarifying expectations as early as possible in the project lifecycle • Source: defining the project lifecycle (from initiating to closing) • Source: providing guidelines for project planning • Source: introducing monitor and control activities • Source: proposing management activities and outputs (plans, meetings, decisions) • Source: providing a link to agile practices (Agile PM²)	IT, manufacturing, software development, retail, healthcare, government, etc.

Method	Tools of the project	Description	Domain
PRINCE2	• Effort and cost estimates • Decision trees project • Scheduling resource • Levelling Gantt charts • Pareto analysis risk • Assessment Lean/ Kaizen • Lessons learned	• Source: continued business justification • Source: a project must make good business sense • Source: learn from experience • Source: project teams should take lessons from previous projects into account • Source: define roles and responsibilities • Source: manage by stages • Source: manage by exception • Source: focus on products • Source: tailor to the environment	IT, manufacturing, software development, retail, healthcare, government, etc.

Source: Compiled by the author.

It is apparent that the use of project management tools (25%), and that of a project management methodology (25%) are the most common measures to increase comfort levels to achieve successful project execution.[25] The iSixSigma Magazine benchmarking study of the project selections sought to characterise how companies identify, prioritise and approve projects in their Six Sigma programs.[26] According to the study, 84% of the Lean Six Sigma Master Black Belt respondents reported that they "always" used Project management tools, 81% always used Project chapter and 55% always used SIPOC (suppliers, inputs, process, outputs and customers). PRINCE2 themes and processes also include a host of study tools, case studies.[27] PRINCE2 studies show that PRINCE2 includes seven principles, seven topics and ten knowledge areas.[28] Within the European Union institutions and agencies, PM^2 is often used. The result of the integration demonstrates that it is possible to advance management and raise the level of project success. PM^2 methodology is often used by government institutions and organisations. The PM^2 project management methodology has been developed and actively supported by the European Commission as a project management standard. The European Commission recommends PM^2 for the management of projects funded under the Horizon 2020 program. It is important to note

[25] Project Success Survey, *Driving project success in Belgium* (PwC, 2018), 17–18.
[26] iSixSigma Magazine, 'Six Sigma Project Selection', 2005.
[27] David Hinde, *PRINCE2 Study Guide, Second Edition Overview of PRINCE2* (Wiley, 2018), 1–45.
[28] Roman R Veynberg, Nikita A Moiseev and Sofja M Sakharova, 'Applying project management standards in IT industry: PRINCE2 PMBoK', *Vestnik of the Plekhanov Russian University of Economics* 17, no 1 (2020), 56–66.

that PM^2 provides for the integration with agile methods and Lean Six Sigma tools, etc. Thus, the methods complement each other.[29]

Phases of project management and tools that could be used and suitable for Cyber Autonomy

The most obvious way to make your project more manageable is to break down the execution process into successive steps. It is on this linear structure that traditional project management is based on. Project management is strictly tied to the execution time of tasks, which are, as a rule, predetermined at the planning stage; tools are excellent for the implementation of projects within this approach. Our suggestions for the phases are described below.[30]

The main focus which is central to the project is to deliver specialist products. This chapter explores how the project manager controls the staging process to manage each delivery stage. It provides a fixed point in time at which acceptance of the main outputs of the project can be confirmed. Acceptance is the formal act of acknowledgement by the client, user or operation team that the project has met agreed acceptance criteria as defined in the project product description. The project manager creates the end project report which focuses on how the project is performed against its planned targets concerning time, cost, quality, scope, benefits and risk.[31] Results show that while Agile methods are being adopted across a wide range of industries and sizes of organisations, if you look at the teams within those companies practicing Agile, they are predominantly within the IT, software development/engineering and project management departments. The majority of Agile users (19%) are in IT/Software Development and Financial Services.[32] In comparison to PM^2, the description of the processes is separate from the description of the tools, which is rendered in the Project Management Tools 7 Techniques application.[33] The principles of project management in Cyber Autonomy should be adequate, flexible, coherent and iterative. Different stages of a software project life cycle should identify competence and development gaps and opportunities.[34] Projects are divided into several phases to provide better management control and appropriate links to the ongoing operations of the organisation. The phases generally comprise an initiation phase, a planning phase, an implementation or execution phase, a monitoring and control phase, and lastly, a closure

---

29 European Commission, *PM² Project Management Methodology. Guide 3.0* (Luxembourg: Publications Office of the European Union, 2018).

30 Z Marketer, Z Guay and Z Callahan, 'Top-7 metodov upravleniya proyektami: Agile, Scrum, Kanban, PRINCE2 i drugiye', 08 July 2016.

31 David Hinde, *PRINCE2 Study Guide, Second Edition Overview of PRINCE2* (Wiley, 2018), 47–88, 391–413.

32 Eileen O'Loughlin, 'Agile Project Management Software User Report: 2020', *Project Management*, 05 February 2020.

33 European Commission, *PM² Project Management Methodology. Guide 3.0.*

34 Jonghyuk Cha and Eunice Maytorena-Sanchez, 'Prioritising project management competences across the software project life cycle', *International Journal of Managing Projects in Business* 12, no 4 (2019), 961–978.

phase.[35] In addition to project planning and control, it also covers the topics of teamwork, communication and the integration of projects into organisations.

When considering the impacts of an anthropogenic project, the expected life cycle needs to be considered.[36] Experts cite five major elements that define a project: creation, planning, execution, monitoring and completion, each tackled in a logical sequence. The creation has to do with defining a scope of work that is to be performed along with major goals that are to be accomplished.[37] Table 3 describes the phases of the project management.

Table 3: Phases of the project management

Phase	Goal	Domain
Initiating	• Make sure that the project can actually be implemented before investing in planning and follow-up tasks	All domains
Planning	• Project strategy • Project definition, including planning stakeholder relations, environmental impacts • Identification of project risks • Work planning • Key roles and responsibilities • Success rates • Potential risks and barriers to efficiency • Expectations for intra-team communication • Project timetable	All domains
Executing	• Execution equates to working the plan • Coordinate the execution of project plans • Act in real time • Produce deliverables • Measure progress and activities • Coordinate the team work • Evaluate potential obstacles • Implement necessary changes	All domains
Monitoring and control	• Monitoring, or command as some call it, entails updating the plan as it is worked. • Actively reviewing the status of your project • Reviewing proceeds	All domains
Closing and controlling	• Collection and evaluation of progress data • Integrated control of quality, time, resources, costs, financial means • Completion means closing out all open tasks required to reach the desired end	All domains

Source: Compiled by the author.

35 Gerrit van der Waldt, *The Project Administrator: Perspectives to Project Support Services* (New York: Nova, 2019).

36 Cristina Cosma and Francis Hopcroft, *Environmental Project Management* (New York: Momentum Press, 2021).

37 Jeff Davidson, *Everyday Project Management* (Oakland: Berrett-Koehler Publishers, 2019); James Taylor, *Project Scheduling and Cost Control: Planning, Monitoring and Controlling the Baseline* (*J Ross Publishing, 2018);* David Hinde, *PRINCE2 Study Guide, Second Edition Overview of PRINCE2. Identifying PRINCE2 Risk – Part 2* (Wiley, 2012).

Conclusion

Growing demand in the digital domain increases interest in Cyber Autonomy Project Management for Digital Transformations. A Cyber Autonomy Toolbox with defence tools should also focus on reversing the asymmetry between the power of the possibly exclusive different suppliers or company departments, the asymmetry between the rate of attacks and efficiencies of defence. Tools used by an organisation should be aligned with all phases of implementation to support the ongoing digital transformation processes.

Table 4: Cyber Autonomy Toolbox

Elements (all 7 above)	**Supportive functions (for each element)**	**Phase according to project management method**	**Cyber Autonomy Toolbox (that included in proposed Tools)**
1. Goal of Cyber Autonomy 2. Strategy of Cyber Autonomy	• Create "Autonomy of IT infrastructure" • Protect "Autonomy territory" • Develop "Autonomy of processes" • Secure "Autonomy of professionals" • Increase "Autonomy of communication"	Initiating	• Brainstorming • Process mapping project chapter • Root cause analysis • The 5 whys • Effort and cost estimates decision trees • Gantt charts • Critical Path Method (CPM) • Critical Chain Method (CCM)
3. Implementation methods 4. Technology	• Follow "Autonomy of directives, frameworks and guidelines" • Create "Autonomy of IT infrastructure" • Ensure "Autonomy of suppliers"	Planning and executing	• Value Stream Mapping • Work Breakdown Structure (WBS) • Deliverable Breakdown Structure (DBS) • Scrum/Kanban • Voice of the Customer (VOC) • Deliverable Breakdown Structure (DBS) • Likelihood/Impact matrix
5. Organisation 6. Reputation defence	• Secure "Autonomy of professionals" • Ensure "Autonomy of suppliers" • Secure "Autonomy of professionals" • Increase "Autonomy of communication" • Develop "Autonomy of processes"	Monitoring and control	• SIPOC (suppliers, inputs, process, outputs and customers) • Pareto analysis risk • Levelling Gantt charts • Assessment Lean/Kaizen • Lessons learned • PESTEL Analysis Risk

Elements (all 7 above)	Supportive functions (for each element)	Phase according to project management method	Cyber Autonomy Toolbox (that included in proposed Tools)
7. Result of Cyber Autonomy	• Create "Autonomy of IT infrastructure" • Insure "Autonomy of suppliers" • Develop "Autonomy of processes" • Protect "Autonomy territory"	Closing and controlling	• Risk assessment • Earned Value Management (EVM) • Kaizen (Continuous improvement) • Lessons learnt

Source: Compiled by the author.

The effectiveness of Cyber Autonomy and proposed tools will also depend on its complementarity with the seven elements described above and supportive functions (for each element of the Toolbox). Generally, the success of project management for digital transformation will depend on the implementation of the Cyber Autonomy Toolbox. Through a set of elements, supportive functions and respective phases of project management (Initiating, Planning, Executing, Monitoring and control, Closing and controlling) described in Table 4 are designed to assist general management and support strategic digitisation projects. The Cyber Autonomy Toolbox and associated tools such as the approach should be used as a guideline in the design, construction, operation and modification of an organisation's cybersecurity operations and digital project management transformation. The Cyber Autonomy Toolbox could be also part of business recovery or continuity plans for ongoing digital transformation process for an organisation.

References

Allen, Jeffrey, 'Increasing Dependence on Technology in the Law Practice in the Time of COVID'. *American Journal of Family Law* 34, no 4 (2021), 160–164.

Andler, Nicolai, *Tools for Project Management, Workshops and Consulting: A Must-Have Compendium of Essential Tools and Techniques.* Erlangen: Publicis, 2020.

Bhardwaj, Bhavyatta, 'Project Management: Changing the way Cyber Security works in an organization'. *PM World Journal* 8, no 9 (2019), 1–11.

Blasch, Erik, Ali Raz, Roberto Sabatini and Carlos Insaurralde, 'Information Fusion as an Autonomy enabler for UAS Traffic Management'. *AIAA Science and Technology Forum and Exposition. AIAA SciTech Forum*, 04 January 2021, 1–12. Online: https://doi.org/10.2514/6.2021-0658

Bolbot, Victor, Gerasimos Theotokatos, Evangelos Boulougouris and Dracos Vassalos, 'A novel cyber-risk assessment method for ship systems". *Safety Science* 131 (2020). Online: https://doi.org/10.1016/j.ssci.2020.104908

Brooks, Frederick P, 'The Mythical Man-Month: After 20 Years'. *IEEE Software* 12, no 5 (1995), 57–60. Online: https://doi.org/10.1109/MS.1995.10042

Cha, Jonghyuk and Eunice Maytorena-Sanchez, 'Prioritising project management competences across the software project life cycle'. *International Journal of Managing Projects in Business* 12, no 4 (2019), 961–978. Online: https://doi.org/10.1108/IJMPB-11-2017-0145

Cosma, Cristina and Francis Hopcroft, *Environmental Project Management.* New York: Momentum Press, 2021.

Danet, Didier and Alix Desforges, 'Digital sovereignty and strategic autonomy in Europe: From concept to geopolitical reality'. *Hérodote* 177–178, no 2–3 (2020), 179–195. Online: https://doi.org/10.3917/her.177.0179

Davidson, Jeff, *Everyday Project Management.* Oakland: Berrett-Koehler Publishers, 2019.

European Commission, *PM² Project Management Methodology. Guide 3.0.* Luxembourg: Publications Office of the European Union, 2018. Online: https://doi.org/10.2799/755246

Gronau, Norbert, 'Determinants of an Appropriate Degree of Autonomy in Cyber-physical Production Systems'. *CIRP Journal of Manufacturing Science and Technology* 26 (2016), 70–80. Online: https://doi.org/10.1016/j.cirpj.2019.05.001

Heldman, Kim, *Project Management JumpStart.* Wiley, 2011. Online: https://doi.org/10.1002/9781119549109

Hinde, David, *PRINCE2 Study Guide, Second Edition Overview of PRINCE2.* Wiley, 2018.

Hinde, David, *PRINCE2 Study Guide, Second Edition Overview of PRINCE2. Identifying PRINCE2 Risk – Part 2.* Wiley, 2012.

Hugo, Francois D, Leon Pretorius and Siebert J Benade, 'Some Aspects of the Use and Usefulness of Quantitative Risk Analysis Tools in Project Management'. *The South African Journal of Industrial Engineering* 29, no 4 (2018), 116–128. Online: https://doi.org/10.7166/29-4-1821

iSixSigma Magazine, 'Six Sigma Project Selection', 2005. Online: www.isixsigma.com/store/project-selection-research-report/

KL Ko, Ryan, 'Cyber Autonomy: Automating the hacker – self-healing, self-adaptive, automatic cyber defense systems and their impact to the industry, society and national security', in *Emerging Technologies and International Security,* ed. by Reuben Steff, Joe Burton and Simona R Soare. Routledge, 2020. Online: https://doi.org/10.4324/9780367808846

Kumar, Maneesh, Jiju Antony and Byung Rae Cho, 'Project selection and its impact on the successful deployment of Six Sigma'. *Business Process Management Journal* 15, no 5 (2009), 669–686. Online: https://doi.org/10.1108/14637150910987900

Kuprevich, T S, 'Tsifrovyye platformy v mirovoy ekonomike: sovremennyye tendentsii i napravleniya razvitiya'. *Ekonomicheskiy vestnik universiteta* (2018).

Larsen, Eldon, 'Adapting project management principles and tools for research and development'. *AIChE Annual Meeting Conference Proceedings,* 2014, 1–8.

Leroy, Iryna, *Cyber autonomy for business: building a European cyber resilience. Views on the progress of CSDP.* Luxembourg: Publications Office of the European Union, 2021.

Luck, Michael and Mark d'Inverno, 'Formal Framework for Agency and Autonomy'. *Proceedings of the First International Conference on Multiagent Systems – ICMAS,* 1995.

Marketer, Z, Z Guay and Z Callahan, 'Top-7 metodov upravleniya proyektami: Agile, Scrum, Kanban, PRINCE2 i drugiye', 08 July 2016. Online: www.pmservices.ru/project-management-news/top-7-metodov-upravleniya-proektami-agile-scrum-kanban-prince2-i-drugie/

O'Loughlin, Eileen, 'Agile Project Management Software User Report: 2020'. *Project Management*, 05 February 2020. Online: https://blog.capterra.com/agile-project-management-software-user-report/

Pondel, Jolanta and Maciej Pondel, 'Stages and Areas of the Use of IT Tools Supporting the Management of IT Projects'. *Management Sciences/Nauki o Zarzadzaniu* 23, no 1 (2018), 45–57. Online: https://doi.org/10.15611/ms.2018.1.06

Project Success Survey, *Driving project success in Belgium.* PwC, 2018.

Reveno, Katie, 'Technological dependency in a post-COVID-19 society'. *Stanford Daily,* 19 November 2020. Online: www.stanforddaily.com/2020/11/19/technological-dependency-in-a-post-covid-19-society/

Six Sigma Qualtec, 'The Importance of Project Selection: Why Six Sigma Projects Falter, How to Assure Success and Sustainability'. *White Paper,* 2020. Online: www.ssqi.com/breakthroughs/whitepaper-pdfs/Project_selection_WP.pdf

Steff, Reuben, Joe Burton and Simona R Soare, *Emerging Technologies and International Security.* Routledge, 2020. Online: https://doi.org/10.4324/9780367808846

Taylor, James, *Project Scheduling and Cost Control: Planning, Monitoring and Controlling the Baseline. J Ross Publishing, 2018.*

Van der Vecht, Bob, Frank Dignum, John-Jules Ch Meyer, Martijn Neef, 'A Dynamic Coordination Mechanism Using Adjustable Autonomy', in *International Workshop on Coordination, Organizations, Institutions, and Norms in Agent Systems III,* ed. by Jaime Simão Sichman, Julian Padget, Sascha Ossowski and Pablo Noriega. Springer, 2007, 83–96. Online: https://doi.org/10.1007/978-3-540-79003-7_7

Van der Waldt, Gerrit, *The Project Administrator: Perspectives to Project Support Services.* New York: Nova, 2020. Online: https://doi.org/10.52305/TETP8786

Varju, Márton, '5G Networks, (Cyber)Security Harmonisation and the Internal Market'. *European Law Review* 45, no 4 (2020), 471–486.

Veynberg, Roman R, Nikita A Moiseev and Sofja M Sakharova, 'Applying project management standards in IT industry: PRINCE2 PMBoK'. *Vestnik of the Plekhanov, Russian University of Economics* 17, no 1 (2020), 56–66. Online: https://doi.org/10.21686/2413-2829-2020-1-56-66

Vonsée, Bram, Wina Crijns-Graus and Wen Liu, 'Energy technology dependence – A value chain analysis of geothermal power in the EU'. *Energy* 178 (2019), 419–435. Online: https://doi.org/10.1016/j.energy.2019.04.043

Voss, Axel, 'Digital autonomy'. *The Parliament Magazine,* 17 March 2020. Online: www.theparliamentmagazine.eu/news/article/digital-autonomy