Mattila, Juha Kai

Governance of Digital Transformation: As Observed in two Cases of Military Transformations

Published in:
Proceedings of the 18th European Conference on Management Leadership and Governance, ECMLG 2022

Published: 01/01/2022

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Mattila, J. K. (2022). Governance of Digital Transformation: As Observed in two Cases of Military Transformations. In F. Matos, & A. Rosa (Eds.), *Proceedings of the 18th European Conference on Management Leadership and Governance, ECMLG 2022* (pp. 300-309). (Proceedings of the European Conference on Management, Leadership and Governance; Vol. 2022-November). Academic Conferences and Publishing International. https://papers.academic-conferences.org/index.php/ecmlg/article/view/705/861

Governance of Digital Transformation: As Observed in two Cases of Military Transformations

Juha Kai Mattila
Aalto University, Helsinki, Finland
juhakaimattila24@gmail.com

Abstract: The transformation of a modern socio-technical system is challenging. Notably, the digital transformation of an enterprise's business or operational model is an arduous journey toward success. Recent studies illustrate that 70% of business enterprise digital transformations fall short of their objectives. Without revenue-based performance indicators, the digital transformations of military organisations are, if possible, even more challenging. However, governance methods should assist in the complex transformation of interrelated features like human behaviour, business processes, information, data, and technology. Are they applied, and how feasible the standard Information and Communications Technology (ICT) governance methods are in supporting digital transformation in the defence sector? The paper studies how feasible the contemporary ICT -governance methods are for military organisations while executing digital transformation. The research implements the action research method since the researcher has participated in two journeys of military transformation. First, a review of these two cases shows the military utilisation of the governance methods and models. Second, the standard methods are reflected against the most challenging transformation problems to see if they could provide support. Third, the methods are challenged by the range of variety in complex system transformations to test their flexibility. Based on the research on two digital transformations, military enterprises seem to fall short in applying central ICT governance standards and methods. Therefore, they are not getting the best available support. Secondly, the contemporary governance methods do not address all the pain points in military transformation. Hence, the utilisation degree and transformation benefits are not well correlated. Thirdly, modern governance tools are inflexible in addressing various situations, transformation goals, and organisational maturity. In summary, the research surfaces some new gaps within the contemporary ICT governance toolbox when applied to the complex socio-technical transformation in the defence sector.

Keywords: Digital transformation, ICT governance methods, IS management, Action research, Complex socio-technical system

1. Introduction

Digital transformations are not straightforward in any sector. Private enterprises face challenges, according to a Forbes study of enterprise failures in digital transformations (Council, 2021). The study indicates that 70% of transformation projects fall short of their goals and advises organisations to pay attention to their data, onboarding process, the coherency of existing technical foundation, resistance to change, communication and coordination. A Boston Consulting Group survey (Forth; Reichert; de Laubier & Chakraborty, 2020) confirms the failure rate stating that as 80% of companies plan to accelerate their digital transformations, the people dimension is the determining factor in success. The public sector is not doing any better. A study of the EU and national level challenges in digital transformation (Svarc, Laznjak, & Dabic, 2020) shows that social capital and working skills were predictors of success at the national level. The exact correlation emerges from a study of smart city transformations (Kar, Ilavarasan, Janssen, & Kothari, 2019). Since Gartner defines digital transformation as "the process of exploiting digital technologies and supporting capabilities to create a robust new business model" (Gartner, 2004), surely ICT governance methods will help exploit digital technologies and improve the success of transformations.

ICT governance (ISO/IEC, 2015) belongs under the organisation governance (ISO/IEC, 2021), and the ISO/IEC 38500 standard provides guiding principles for "effective, efficient, and acceptable use of IT within an organisation". For the support of transformation, it defines principles for strategy, acquisition, and human performance, among other things. The 38500 also promotes existing good practices to address different approaches for management, in particular, change management, process management, and business model. The ICT governance methods should effectively support transformation programmes since digital transformation has been recognised for over ten years as crucial to performance improvements, business advantages, and even survival in the future (Digital Adoption, 2021).

Military organisations are also seeking operational performance and advantageous capabilities through digital transformations. It seems that they are facing similar challenges to other sectors. This paper uses action research while observing two military transformations to see how feasible the contemporary ICT governance methods are for military organisations while executing digital transformation. The sequenced research sub-questions are:

1. How greatly are armed forces utilising standard ICT governance methods?
2. How well do the methods mitigate the challenges of military DT?
3. How do the methods address the dynamics in different transformation approaches?

The paper is divided into the literature research section to understand how military works, whether they have special challenges in their transformations, how common ICT governance methods map to military line command, and the general difficulties in digital transformations. The research design section explains how the researcher used the action research and provides some essential information about the two use cases that remain otherwise anonymous. The results and discussion section provides causality and answers to the three detailed questions. Finally, the conclusion section summarises the paper.

2. Literature Research

The section seeks first to create a general model for military affairs and operational types. Secondly, it defines the nature of a military organisation and its reaction to change. Thirdly, the study tries to recognise the foundational frameworks and methods for ICT governance that makes the most sense for the military. As a result, the section composes a context and model for understanding the ICT branch within military organisations, maps ICT governance to this organisation, and reviews some common failures in military digital transformations.

2.1 How Military Works and Transforms

Military affairs typically comprise force utilisation, generation, and support (Smith, 2005). By tradition, the military is a line command functional organisation with some matrix processes commonly for supplies and long-range fire support. (Mattila & Parkinson, 2018) The history of symmetric battles, i.e., land, maritime, and air, has determined the basic operational model as semi-independent functional stovepipes called Services. (Bosquet, 2009) Nevertheless, many efforts have been made to compose a military organisation that could utilise Joint capabilities (components from different Services used together in operation) (Vego, 2007). Since 1983, the US DoD has operated with global combatant commands for force utilisation, but each force is a construct from components provided by the original Service. (U.S. CENTCOM, 2022) Some armed forces have established Joint logistics and educational functions to support all Services, but force generation typically remains distributed within each Service. (Mattila & Parkinson, 2018)

Military organisations and cultures are optimised to maintain their integrity when the environment is chaotic and lethal on the battlefield. (Dupuy, 1987, pp. 63-74) Hence, transferring fundamental structures or ways of military affairs may be perceived to question the established understanding and the existence of a military organisation. (Kegan & Lahey, 2009, ss. 56-60) Possibly, the hierarchical military organisation possesses immunity or resistance to change, which determines transformation as either adding a new organisation for a new function, consolidating similar functions, distributing parts, or erasing a part from the legacy organisation.

For example, the Defence Forces of Finland has erased units and consolidated functions in their 2008 (Finland, 2009) and 2015 (Prime Minister's Office Finland, 2012) foundational transformations. Conversely, there are several examples of military intentions to transfer their affairs or operational models but failing to reach the end state. (Mattila & Parkinson, 2018) The challenges appear in all layers of the organisational structure. One common nominator for challenges may be the functionally distributed hierarchical power structure, as defined by Otto Scharmer (Wilson, 2017), which resisted all changes except in Sweden, where the change of political agenda halted the digitalisation and integration of the Försvarsmakten (Hartman, 2020). Besides getting the buy-in from generals, each transformation has struggled with the lack of competencies or the speed of transfer for people to keep up.

2.2 ICT Governance Methods for Transformation

A successful transformation requires an organisation to focus its resources and efforts on gaining future value while mitigating risks on the journey. (Cameron & Green, 2012, ss. 117–118) There are several pathways (Eastwood, 2022) for digital transformations, but all of them require strategy, resources, and performance governance. Meanwhile, the enablers (ISACA, 2019), like competency, information, and technology, need to be acquired to support the efforts. The governance of this flux of movement and interrelated enablers is described in the ISO/IEC 38500 (ISO/IEC, 2015) concerning the organisational governance of information technology. The standard could be considered an umbrella framework for information and communications-related governance in an enterprise (Van Haren Publishing, 2013) since it recognises the primary IT business value stream of development and operations together with the core functions of governance, i.e., monitor, evaluate, and direct

(Almaawi, Alsaggaf, & Fasihuddin, 2020). Moreover, the framework connects business and IT strategy, risk management, operations, and change together with the architectural structure of the system (Calder & Moir, 2009), as illustrated in Table 1.

Table 1: A sample of governance and management methods recognised by ISO/IEC 38500

Area of governance	Model or Method	Application
Risk, conformance, and compliance	COBIT (ISACA, 2019)	Framework for governance and management of information and technology in an enterprise. It includes a value stream for managing risks, optimising resources, and creating new value.
Business strategy	Balanced Score Card (Kaplan & Norton, 2001)	Helps in aligning and focusing resources on strategy.
IT strategy	TOGAF (Open Group, 2018)	Enterprise architecture illustrates the structure of the organisation and helps to define the starting point and end state of transformation
Operations	ISO 27001 (ISO, 2018)	Defines an information security management system and how to establish, maintain and continually improve its ability to preserve confidentiality, integrity, and availability of data assets
	ITIL (Axelos, 2019)	Framework for information technology processes covering the life-cycle strategy-design-transition-operation-continual improvement.
Change	P3M3 (PMI, 2022)	Portfolio, Programme and Project management guides help organisational change management.
	CMMI (ISACA, 2022) (Forrester, Buteau, & Shrum, 2011)	Helps in understanding the current level of capability and performance and provides guidelines to optimise or mature them.
Information & Technology	Data Governance and Management (PMI, 2022)	Helps govern data life-cycle strategies and implement processes for collection, access, storage, availability, and security & privacy of enterprise data.

2.3 Mapping the Common Governance Methods to Military Affairs

In a typical enterprise, the business and operation models define governance implementation. Hence, there is a need to determine the essential business and operation model for the ICT-service production within a military enterprise and then arrange the IT-governance practices fitting the model. The Beers (Espejo, 1990) Viable Systems Model provides a structure for ICT business interfaces and levels of decision-making for the start. On top of the structure, the military prefers an in-house service provider and on-premises infrastructure because of autonomy and security reasons, as illustrated in Figure 1, left-hand side. Therefore, there is an in-house service relationship between the ICT provider and units using the software as a service.

Furthermore, the ICT provider may have many sub-providers and vendors to manage in the supply chain. In summary, the value stream (Toivonen & Siitonen, 2016) to support current operations with ICT-related services is composed of end-users, an in-house ICT service provider running service development, delivery, and support functions, and the supply chain connecting vendors and other service providers to support the in-house service provider. Next, there is enterprise information management which focuses on content and knowledge. Finally, at the strategic level, there is an enterprise information governance level focusing on knowledge capital preparedness for future scenarios. Together the ICT value stream and enterprise-level functions establish a generic ICT model for Armed Forces.

Matching the ISO 38500 preferred governance methods to the generic Armed Forces ICT model presented in Figure 1 (left-hand side), the essential tools map looks like Figure 1 (right-hand side). ISO 38500 establishes an umbrella for enterprise information governance at a strategic level, COBIT covers most of the management functions, and P3M3 and TOGAF provide essentials for change management. Furthermore, ICT service development and production are arranged compliant with ITIL and SCM processes within the eTOM business model, and enterprise-wide information and security management should follow the lines of data management and ISO 27001. The ICT model and mapping of governance tools will be used in the paper to establish the required context for the governance tool analysis.

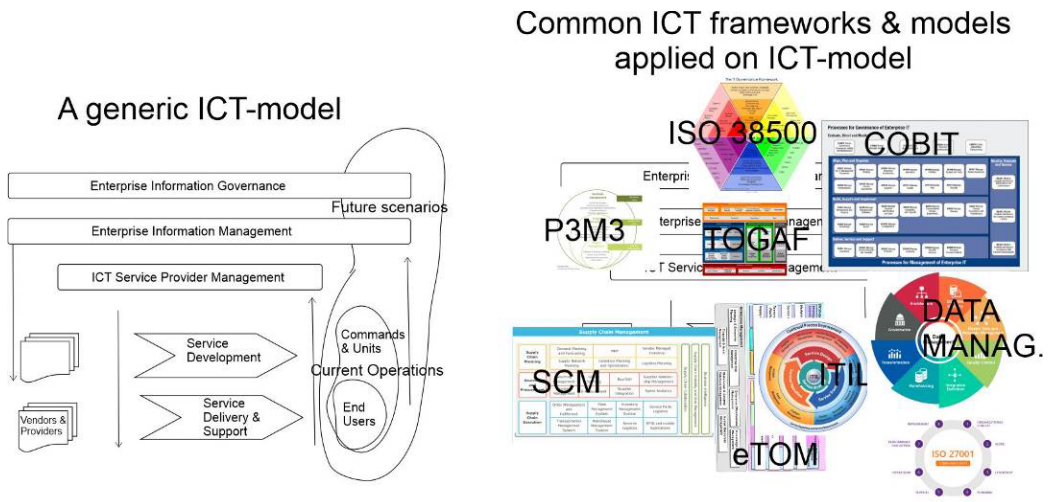

Figure 1: A generic governance, business, and operations model for military ICT and common frameworks of governance frameworks and models matching with ICT-model

2.4 Transformation challenges

For the past decade or so, digital transformation has been the foremost way to accelerate or revolutionise operational performance or business revenue. For example, over the last five years, the end-user experience has improved by more than 70% of cases. However, late surveys point out that 80% of enterprise transformation intentions fail, suffer delays, or be scaled back. (Couchbase, 2022) Nevertheless, with a 30 % annually increased investment, digital transformation continues to be significant pressure from outside or the way to make a difference inside an enterprise. (McKinsey, 2020) Both Couchbase and McKinsey surveys recognise causality between the failures and the following layers of organisation: culture, strategy, processes, human competency, information & data, technology and other resources. A third survey indicates that transformation may fail during the target setting (22%), planning (23%), implementation (35%) and post-transformation (20%) phases. (McKinsey, 2021) The recognised common challenges faced in digital transformations will set the reference to analyse ICT governance tools' abilities in mitigating obstacles along the transformation journey in section 4.2.

3. Research Design

The transformation of a military organisation remains complex because of social relationships, various obstacles on the journey, culture, language, and different perceptions of stakeholders. Hence, the interpretive approach seemed to be an applicable worldview for the research. (Saunders, Lewis, & Thornhill, 2015) Furthermore, Action Research appeared to be the most related method for study since the researcher participated (Reason & Bradbury, 2012) in planning and implementing transformations of two different armed forces (Case A and B). The self-reflective spiral of action research (Kemmis & McTaggart, 2000) followed in both cases the sequence of 1. identifying the competency gaps, 2. consulting the planning team towards applicable methods, 3. applying methods to planning, 4. transferring the organisational behaviour, 5. migrating the ICT infrastructure and data, 6. measuring the short-term outcome and performance, 7. improving the competency of the planning and control team, and 8. adjusting the plan and implementation accordingly.

The self-reflecting spiral ensured opportunities to observe, learn, and adjust the course whilst taking short steps on the transformation journey (Koshy, 2010). Hence, there were several opportunities to introduce ICT governance methods as they became understandable, and the opportunity emerged on the journey. As a result, the main principles of action research (Carr & Kemmis, 1989) were fulfilled as follows:

- The researcher participated in both cases between 2-7 years, providing longevity for the viewpoint.
- The researcher engaged the actors in the senior consultant role, so the relationship's peer nature was as close as possible to typical military culture.
- The action included several spirals of planning, observing, reflecting, and re-planning.

The two digital transformations (A and B), that the researcher participated in this study, were different in their nature. Therefore, the data collected during the action research provides various points along the transformation journeys. The research uses the EA Tool (Mattila J. K., 2020) to analyse the current position (AS-

IS) and intended end states (TO-BE) from the information and ICT technology viewpoint, as presented in Table 2.

Table 2: Nature of the two military enterprises and their transformation journeys of ICT branch as observed during the research

Feature	A Case	B Case
Cultural/Strategic posture during the transformation	The organisation adopts new abilities by minimising risks and optimising investments in a slow evolutionary manner in its strategy.	The organisation aims to acquire the best available platforms following an accelerated evolutionary posture in its strategy.
Affairs/Operations intention during the transformation	The organisation optimises the operational efficiency through coordination of the capabilities of each Service.	The organisation aims for operational efficiency through more independent Services with diversified capabilities.
Information AS-IS	Unstructured information is managed mainly through pages and collaborative workspaces	Unstructured information is managed as files in terminal devices and possessed by individual soldiers. E-mail and physical memories are used for file sharing.
Information TO-BE	Need to improve the use of information and data with business intelligence, real-time analysis, and enable machine learning support in automation and speed of awareness	Need to improve collaboration and sharing of information between units and soldiers in a confidential manner. Also, to digitise some main supporting processes end-to-end.
ICT AS-IS	On-premises cloud infrastructure runs enterprise platforms which support main processes. Accessed through multiple ways of communications, some mobile.	Hundreds of monolithic applications are operated in tens of separate domains and accessed through a fixed network.
ICT TO-BE	Need to become more agile in using edge, on-premises, and public cloud to capture data, process it on time and enable faster collaboration between men and machines.	Need to consolidate applications and services to enterprise platforms operated by a joint service provider.

Naturally, the researcher's language, knowledge, attitude, and perception in every engagement with others impact the observations. Also, long-time engagement evolves understanding and relationships, which naturally affects the observations.

4. Results and Discussion

The section provides first a view of how greatly the two cases recognise and utilise the essential ICT governance methods and tools. Secondly, it shows how the governance methods address the prevalent challenges of digital transformation in military culture. Thirdly, the section approaches governance tools from a dynamic viewpoint and assesses how well the tools manage the transformation from AS-IS to TO-BE. Finally, the section discusses the causality between the usage of governance tools and the ability to navigate the transformation journey and cope with dynamics.

4.1 Degree of Utilisation

While doing the action research, the researcher observed the organisation's policies, proposed improvements to increase the transformation success, and followed some adoption of these proposals. However, since both cases did not transfer their strategy or process postures, the researcher adopted a pragmatic approach of promoting whatever part or feature was feasible in the context of time, competency, and culture. As a result, both cases end up using some viable details of the selected ICT governance methods, as illustrated in Table 3.

Table 3: Utilisation of standard ICT governance methods in observed cases

Tool/Case	A case	B case
ISO 38500	Not applied to the letter, but parts without recognising the framework.	Some policy drafts but not implemented.
COBIT	Parts applied in policies and guidance but not necessarily recognised as COBIT	Parts applied in policies and doctrines.
BSC	Features applied in value measurement, but the method is not recognised	Not utilised, nor recognised.

Tool/Case	A case	B case
TOGAF	The EA method is applied throughout the organisation, but decision-makers do not recognise its value.	Tools and methods applied at a technical level but not utilised further.
ISO 27001	A national variation is applied widely in Armed Forces and Defence industry	Some features are applied mainly to each unit.
ITIL	Widely followed in ICT service provider organisation	Some features implemented with ISMS.
P3M3	Widely followed at a project level, but the programme and portfolio levels are merged in the engineering & acquisition process	Followed at project level depending on the project manager. Not recognised at other levels.
CMMI	Used in measuring the current status of process implementation	Used in measuring the quality of some process implementation
Data Governance and management	A long tradition of content management gradually extended to information and data levels.	Traditional document management alongside individual efforts in the areas of files and information.

Neither of the cases used the standard ICT governance methods entirely, purely, nor necessarily acknowledged. Nevertheless, the researcher and transformation programmes used parts of methods as either a seed for knowledge that hopefully will sprout in the future or a tailored tool to address a recognised challenge. Hence, the research does not measure the maturity of the governance tool utilisation but their feasibility in governing the transformation.

4.2 Feasibility in Mitigating Transformation Challenges

The feasibility of the governance methods depends on the challenges, utilisation of the tools and the journey of transformation. The research combines the challenges detected from military and private organisations into themes reflected in the standard governance tools in Table 4. The reflection of the challenge theme defines how much practical support the research observed from each tool or method.

Table 4: How well do standard governance methods address the typical ICT transformation challenges organisations observed using a three-step scale (green = match; yellow = something; red = no match)

Challenge Themes/ Tools	ISO 38500	COBIT	BSC	TOGAF	ISO 27001	ITIL & eTOM	P3M3 & CMMI
Culture – resistance to change							
Strategy – Non-disruptive							
Process - stovepipes							
Human Competency – slowly evolving							
Information & Data – security controlled							
Technology – complex integration							
Other resources – competition between cost units							

There is no one method to manage all typical challenges of military ICT transformations, but a need to combine them for a purpose. The need for combination supports the researcher's intent to apply whatever mitigates commonly recognised problems. For example, transferring and building up the social structure and human competencies receive weak support from the standard tools. This weakness requires help from other methods, like systems thinking, organisational behaviour, and business dynamics. The assistance in understanding organisational dynamics in the transformation does not appear in the above reflection. Since the transformation is about the migration of data and technology, the transition of individual competencies and habits, business transformation, and the organisational dynamics viewpoint (Burke & Litwin, 1992) ask for a separate assessment.

4.3 Governing the Dynamics of Transformation

Next, the research assesses the dynamics along the evolutionary path by applying the EA Tool (Mattila J. K., 2020) but simplifying the study by focusing on three layers within the main focus, i.e., ICT business, ICT operations, and technology. Table 5 samples the most critical gaps in the ICT governance methods found when managing the dynamics of migration, transition, and transformation. Nevertheless, the paper does not analyse more complex powers and forces between organisational components in motion.

Table 5: Transformation dynamics challenge the existing ICT governance methods

Transformation dynamics/ support from methods	A Case	B Case	Dynamic features challenging the existing ICT governance methods
ICT business transformation	From a Joint ICT service provider to a supply chain of multiple providers	From embedded ICT units to a Joint ICT service provider	Case A does not receive much support, but Case B could use the methods ideally. Unfortunately, they do not support the transition of culture and competencies.
ICT operations transition	From service management to value chain management	From element management to service management	Enterprise-oriented methods do not recognise the challenges of value chains for case A. However, the service management is well covered, but the ambitious transfer asks for more support.
IC technology migration	From cloud provided through roaming connections to software-defined everything	From domain computing on fixed connections to cloud computing with mobile access.	The latest ITIL recognises DevSecOps integration required in software-defined everything for case A. Cloud computing and mobility migration can be orchestrated in support of existing methods.

The dynamics of the ICT transformation challenge the existing governance methods in three areas:

1. Transformation goes beyond the range – methods follow progress with a delay. However, they do not define the behaviour on the edge of development.
2. Transformation fast forwards – methods presume a level of understanding and maturity between the slow steps of evolution.
3. Social and cognitive immunities to change – the focus is on managing things and transactions rather than the transition of interrelationships.

4.4 Discussion

Based on these two cases, the military does not systematically utilise the common ICT governance frameworks and methods. Whether this is because officers' training does not include these subjects or military command and control culture is too strong to tolerate frail matrix governance methods, remains outside of this research. Nevertheless, the ability of military personnel with various backgrounds to adopt applicable parts of these methods was remarkable once the challenge was recognised and ownership shared. Therefore, the complete application of ICT governance methods does not guarantee effortless transformation, but shared challenges and applied remedies make the success more predictable.

From a cultural perspective, the military organisation seems more prone to stability than agility (Kale, 2020). Thus, military digital transformations should be slow-paced or short steps and well within the scope of existing ICT governance methods for improved outcomes. Similarly, some ICT transformations in academic organisations have benefitted from applying good practices when consolidating university ICT. (Toleman, Cater-STeel, Kissel, Chown, & Thompson, 2009) Sometimes, the military transformations do not recognise their cultural heritage but launch ambitious programmes to gain an advantage or fast forward to meet the adversary's capabilities. Consequently, the culture of society and the competencies of individuals often hold down the realisation of transformation programmes and existing ICT governance methods do not support mitigating these problems. Hence, understanding enterprise sub-cultural structure is essential for the success of any transformation. (Pew & Mavour, 1998)

The ICT governance methods recognise all essential components (technology, information, competency) and aspects (performance, resources, strategy, value/risk) for transformation, but they remain enterprise-focused. Therefore, they require extensions from supply chain, value stream, and digital and knowledge economy management methods. (Kale V., 2020) Furthermore, good ICT governance practices seem to fit well for consolidated, hierarchically managed enterprise ICT services. In contrast, the fitting may be less feasible when ICT is distributed into autonomous business units or spread over the length of the value chain. (Loukis, Janssen, Dawes, & Zheng, 2016)

The strategy should focus on utilising organisational resources to achieve an advantage, but, except for balanced scorecard and portfolio management, centralised ICT governance methods do not support the acquisition and orchestration of resources within distributed, hierarchical, and functionally separated military organisations. (De Vries, 2010) Hence, the alignment of effort remains loose, and cooperation between military Services is challenging. At least, the importance of consolidating strategic alignment and ICT governance mechanisms has been proven productive in private sector organisations. (Wu, Straub, & Liang, 2015) The military has the challenge of valuating their ICT performance and investments since their ”business value” does not reflect on the financial figures as clearly as the private sector. (De Haes & Van Gremberg, 2015)

In conclusion, there is no one ICT governance tool to master digital transformation in military organisations. The feasibility of methods depends on the pace, length of the leap, and ambition of the transformation. Since the ICT governance methods often evolve behind the edge of evolution, they may not be the best practice to seek support for fast-forwarding or edge advantage-seeking transformations. In any case, it seems that successful orchestration of digital transformation requires a combination of governance methods tailored to the particular posture and target of the organisation.

5. Conclusions

The statistics show that 70% or more of digital transformations are falling short of their initial goals. Nevertheless, over 80% of organisations plan to gain performance or business advantages. Military organisations are also facing challenges in their transformations to gain advantages. The ICT governance and management methods should provide support in utilising digital technology and improve the success of the transformation. Is the military not using good practices? Are good practices not addressing the challenges of military transformation? Are good practices unable to manage the dynamics of a digital transformation?

The ISO 38500 promoted principles and management methods map well onto the Armed Forces’ general ICT business model. However, none of the two cases fully recognised or utilised any governance or management methods. Nevertheless, both cases could use parts of the toolbox to improve their success in transforming the ICT branch once the challenge was recognised and the tool was identified and shared. On the other hand, there is no evidence that full compliance with the good practices would even enhance the transformation’s success. The results indicate that sub-cultures of organisation, competency of people, and arrangements of military affairs significantly affect the application of good governance practices.

Based on the action participation, there is no one governance method to address the usual challenges of digital transformation. Moreover, even utilising the complete toolbox promoted in ISO 38500 does not provide full coverage as social structure, human competencies and acquisition of resources remain weakly supported. Hence, the governance toolbox requires an extension of, at least, systems thinking, organisational behaviour, business dynamics, and supply chain management. Transformation may need more leadership than good practices in management.

The transformation dynamics, interrelating forces between organisational components, affect the outcome of digital transformation. However, the toolbox of good governance did not support when transformation reached further towards the edge of development, when the intention was fast forward the organisation, or when social structure was exceptionally immune to change. Therefore, it requires a tailored approach to apply good governance practices in a wide variation of ICT transformations.

The lack of public data concerning military digital transformations makes this research relatively unique from an academic viewpoint. Action research may be one of the best ways to gather reliable data with the proper context from military transformations that extend over several years and have many rotating stakeholders. Transformation practitioners should be relieved as there are no signs that full implementation of the governance toolbox makes transformation successful. On the contrary, tailored application of tools to mitigate recognised challenges seems to create a better impact.

The focus of the research is limited only to ICT transformations and does not observe a broader transformation of military affairs. Moreover, the information concerning affairs and operational performance transformations would be further constrained for operational security reasons. Nevertheless, the in-house transformational experts, who have access to confidential information, may extend and build on this research. Furthermore, the

constrained understanding of one researcher engaging in two transformations can be mitigated in the future by a multi-discipline research team that composes observations from several viewpoints, i.e., sociology, psychology, business, information, and engineering, and even create a better governance framework for digital transformations.

References

Almaawi, A., Alsaggaf, L. & Fasihuddin, H., 2020. The Application of IT Governance Frameworks in Saudi Arabia: An exploratory study. *International Journal of Computer Applications, Vol 176, 30.June.*

Axelos,2019. *What is ITIL.* [Online] Available at: https://www.axelos.com/certifications/itil-service-management/what-is-itil

Baev, P., 2015. *Ukraine: a test for Russian military reforms,* Paris: Ifri.

Bosquet, A., 2009. *The scientific way of warfare.* New York: Columbia University Press.

Burke, W. W. & Litwin, G. H., 1992. A causal model of organizational performance and change. *Journal of Management 18.3,* pp. 523-545.

Calder, A. & Moir, S., 2009. *IT Governance.* Cambridgeshire: IT Governance Publishing.

Cameron, E. & Green, M., 2012. *Making sense of change management 3rd edition.* London: Koga Pace Ltd.

Carr, W. & Kemmis, S., 1989. Becoming critical: Education, knowledge and action research. *The Journal of Educational Thought,* pp. 209-216.

Chizek, J. G., 2003. *Military transformation: Intelligence, surveillance and reconnaissance,* Washington DC: US Foreign Affairs, Defence and Trade Division.

Clark, C., 2020. Gen. Hyten On The New American Way of War: All-Domain Operations. *Breaking Defence.*

Conetta, C., 2010. *More of Less? The limits of defence reform and military transformation.* [Online] Available at: http://www.comw.org/pda/fulltext/Limits-Defense-Reform-130529.pdf [Accessed 18 July 2020].

Couchbase, 2022. *Digital transformation - Lessons learned and strategic setbacks,* Santa Clara: Couchbase Inc.

Council, F. T., 2021. *Forbes Innovation.* [Online] Available at: https://www.forbes.com/sites/forbestechcouncil/2021/06/15/13-industry-experts-share-reasons-companies-fail-at-digital-transformation/

De Haes, S., Van Gremberg, W. (2015). *Enterprise Governance of Information Technology.* Cham: Springer

Deptula, D. A., 2016. Evolving technologies and warfare in the 21st century - Introducing the "Combat Cloud". *Mitchell Institute Policy Papers, vol 4.*

De Vries, P. (2010). The resilience principles: A framework for new ICT governance. *SSRN Electronic Journal*, 137-186

Digital Adoption, 2021. *Gartner Digital Transformation 101: Research, Perspectives, Services, And More.* [Online] Available at: https://www.digital-adoption.com/gartner-digital-transformation/

Dupuy, T. N., 1987. *Understanding war.* New York: Paragon House Publishers.

Eastwood, B., 2022. *How to coordinate multiple pathways to digital transformation.* [Online] Available at: https://mitsloan.mit.edu/ideas-made-to-matter/how-to-coordinate-multiple-pathways-to-digital-transformation

Espejo, R., 1990. The Viable System Model. *Systemic Practice and Action Research 3(3),* pp. 219-221.

Finland, P. M. O., 2009. *Finnish Security and Defence Policy 2009,* Helsinki: Prime Minister's Office Publications.

Forrester, E. C., Buteau, B. L. & Shrum, S., 2011. *CMMI for services 2nd Ed.* New Jersey: Pearson Education.

Forth, P., Reichert, T., de Laubier, R. & Chakrabrty, S., 2020. *Flipping the Odds of Digital Transformation Success.* [Online] Available at: https://www.bcg.com/publications/2020/increasing-odds-of-success-in-digital-transformation

Gartner, 2004. *Digital Transformation.* [Online] Available at: https://www.gartner.com/en/information-technology/glossary/digital-transformation

Hamberg, U., 2010. *NBF - Förmågan att se på andra sidan kullen eller "Kejsarens nya kläder".* Stockholm: Swedish National Defence College.

Hartman, C., 2020. *Försvaret som försvann: berättelsen om varför det moderna nätverksbaserade totalförsvaret aldrig realiserades.* [Online] Available at: http://www.diva-portal.org/smash/get/diva2:1442332/FULLTEXT01.pdf

ISACA, 2019. *COBIT 2019 Governance and management objectives.* Schaumburg: ISACA.

ISACA, 2022. *CMMI Performance Solutions.* [Online] Available at: https://www.isaca.org/enterprise/cmmi-performance-solutions

ISO/IEC, 2015. *38500.* [Online] Available at: https://www.iso.org/standard/62816.html

ISO/IEC, 2021. *37000 Governance of organisations,* Geneva: ISO/IEC.

ISO, 2018. *27001:2018: Information technology - security techniques - information security management systems - requirements,* s.l.: ISO/IEC JTC 1/SC 27, 2018-02.

Kale, V., 2020. *Digital transformation of enterprise architecture.* Boca Raton: CRC Press.

Kaplan, R. S. & Norton, D. P., 2001. *The strategy focused organisation.* Harvard: Harvard Business School Publishing.

Kar, A. K., Ilavarasan, V., Janssen, M. & Kothari, R., 2019. Moving beyond smart cities: Digital nations for social innovation & sustainability. *Information Systems Frontiers 21, no.3,* pp. 495-501.

Kegan, R. & Lahey, L. L., 2009. *Immunity to change.* Boston: Harvard Business Review Press.

Kemmis, S. & McTaggart, R., 2000. Participatory action research. In: *Handbook of qualitative research 2nd ed.* Thousand Oaks: SAGE, pp. 567-607.

Kofman, M. & Lee, R., 2022. Not built for purpose: The Russian military's ill-fated force design. *War on the Rocks*, 02 June.

Koshy, V., 2010. *Action research for improving educational practise.* London: SAGE Publishing Ltd.

Lavrov, A., 2018. *Russian military reforms from Georgia to Syria,* Washington: CSIS.

Lindström, J., 2005. *Natverksorienterat forsvar.* [Online] Available at: https://docplayer.se/17352815-Natverksorienterat-forsvar.html

Loukis, E., Janssen, M., Dawes, S.,& Zheng, L. (2016). Evolving ICT and governance in organisational networks - Conceptual and theoretical foundations. *Electron Markets*, 7-14

Mattila, J. K., 2020. *Engaging a Moving Organisation - Modelling a military enterprise with architecture tools.* Helsinki: Aalto University.

Mattila, J. K. & Parkinson, S., 2018. Quo Vadis, Militare? Evolution of Military Affairs from a Business Architecture Viewpoint. *Kungliga Krigsvetenskapsakademien Hanglingar och Tidskrift,* pp. 151-172.

Matila, J.K. & Parkinson, S., 2018. Enterprise Architecture as a Tool in Military Change Management. In *Proceedings of the 6th International Conference on Management, Leadership and Governance, ICMLG 2018.* pp. 194-202

McKinsey, 2020. *Managing the fallout from technology transformations,* Chicago: McKinsey Digital.

McKinsey, 2021. *Losing from day one: Why even successful transformations fall short.* [Online] Available at: https://www.mckinsey.com/~/media/mckinsey/business%20functions/people%20and%20organizational%20performance/our%20insights/successful%20transformations/december%202021%20losing%20from%20day%20one/losing-from-day-one-why-even-successful-transformations-fall

Open Group, 2018. *The Open Group Standard for TOGAF version 9.2.* [Online] Available at: https://www.opengroup.org/

Pew, R.W., & Mavour, A.S. (1998). *Modeling human and organisational behaviour - application to military simulations.* Washington: National Academy Press.

PMI, 2022. *Data management practices.* [Online] Available at: https://www.pmi.org/disciplined-agile/process/data-management/data-management-practices

PMI, 2022. *Foundational standards.* [Online] Available at: https://www.pmi.org/pmbok-guide-standards/foundational

Prime Minister's Office Finland, 2012. *Government's Defence Report,* Helsinki: Prime Minister's Office Publications 7/2012.

Reason, P. & Bradbury, H., 2012. *The SAGE Handbook of Action Research, Edition 2nd.* SAGE Publications Ltd.

Saunders, M., Lewis, P. & Thornhill, A., 2015. *Research methods for business students, 7th Edition.* Edinburg: Pearson Education Ltd.

Smith, R., 2005. *The Utility of Force: The Art of War in the Modern World.* London: Allen Lane.

Svarc, J., Laznjak, J. & Dabic, M., 2020. The role of national intellectual capital in the digital transformation of EU countries. Another digital divide?. *Journal of Intellectual Capital.*

Toivonen, T. & Siitonen, J., 2016. Value Stream Analysis for Complex Processes and Systems. *Procedia CIRP,* Volume 39, pp. 9-15.

Toleman, M., Carter-Steel, A., Kissel, B., Chown, R., & Thompson, M. (2009). Improving ICT Governance: A radical restructure using COBIT and ITIL. In a Cater-Steel, *Information technology governance and service management* (pp.178-191). IGI Global.

U.S. CENTCOM, 2022. *U.S. Central command history.* [Online] Available at: https://www.centcom.mil/ABOUT-US/uscentcom-history/

Van Bladel, J., 2022. The unprofessional Russian soldier. *Egmont.*

Van Haren Publishing, 2013. *ISO/IEC 38500 for IT governance.* [Online] Available at: https://www.vanharen.net/blog/isoiec-38500-for-it-governance-in-3-minutes/

Vego, M.N., 2007. *Joint Operational Warfare. Theory and Practice*. Newport: Naval War College

Wilson, P. A., 2017. Otto Scharmer and the field of the future. In: *Palgrave Handbook of Organizational Change Thinkers.* Palgrave Macmillan, pp. 1129-1146.

Wu, S.P-J., Straub, D.W., & Liang, T-P. (2015). How information technology governance mechanisms and strategic alignment influence organisational performance: Insights from a matched survey of business and IT managers. *MIS Quarterly*, 497-518