ATESTASI: JURNAL ILMIAH AKUNTANSI
Vol 5, Issue 2, (2022), 693 - 709

Personnel Management of The Indonesian National Army Air Force (TNI-AU) In Preparing To Implement Network Centric Warfare

Agus Sudarya [1*]

[*1] Universitas Pertahanan Republik Indonesia

Email
agus.sudarya6795@gmail.com [1*]

Received: August, 04, 2022 **Revised:** August, 31, 2022 **Accepted:** September, 30, 2022

Abstract

This study attempts to describe the management of Indonesian Air Force (TNI-AU) personnel in preparing for the implementation of Network Centric Warfare (NCW). Globally, the military's Information and Communication Technology (ICT) is growing. The war in this digital era makes every country need to prepare itself for the attacks of the digital world. In Indonesia itself, the Indonesian National Army (TNI) has included NCW as one of its programs to deal with possible disturbances in state security stability through the digital world. In addition, NCW is needed by the TNI as a form of a centralized and fast command communication strategy. This study uses a case study strategy involving five informants and written data to complete the integrity of the data. In personnel training management, the TNI-AU has prepared integrated infrastructure development, modeling and simulation, cyber defense management, and personnel management to be specially prepared to occupy crucial positions in the implementation of NCW. This personnel training concentrates on strengthening protection from foreign attacks in the digital world and the technology of unmanned warfare vehicles.

Keywords: Cyber Defense; Network Centric Warfare; Personnel Training; TNI-AU

DOI : https://doi.org/10.57178/atestasi.v5i2.781
p-ISSN : 2621-1963
e-ISSN : 2621-1505

Introduction

In a traditional rule, war can be interpreted as a physical or non-physical action involving two or more groups of people (Suryohadiprojo, 2008). The aim is to dominate a contested area. Along with the development of the times, the tools and tactics used in combat continually develop in tandem with technological developments. Warfare in the Information Age will inevitably embody the characteristics that distinguish this age from previous ages. These characteristics affect the abilities brought into battle and the nature of the environment in which the conflict occurs. Often, military organizations spearheaded the technology development and its application, but that is not the case today. Significant advances in

Information Technology are driven mainly by the demands of the commercial sector. Furthermore, Information Technology is being applied commercially to transform businesses worldwide.

Network Centric Warfare (NCW) is the best term developed to describe how institutions govern and fight in the Information Age. Admiral Jay Johnson, Chief of Naval Operations, called it “a fundamental shift from platform-centric warfare” (Alberts et al., 2000). NCW can be defined as an information advantage operating concept that results in increased combat power by network sensors, decision-makers, and gunners to achieve mutual awareness, increased command speed, higher operating tempo, greater mortality rate, increased survivability, and level of self- synchronization (Guha, 2021; Kang et al., 2018). In essence, the NCW translates information advantage into combat power by connecting knowledgeable entities in the battlespace.

The advantages that network-centric warfare brings to the battlespace are highly relevant to the tactical and operational levels of warfare, but they impact all levels of military activity from tactical to strategic. Although the information gain construct may seem somewhat intangible, it can be measured, and its impact on military operations can be evaluated in terms of mission effectiveness, survivability, and lethality (Garstka, 2003). When adopting the NCW concept, an institution requires a careful analysis of each system to be carried out so that only means (sensor systems and weapons systems) existed before. It is possible to digitize such an entire system as a whole, but it will cost more than creating a new, fully efficient one (i.e., digitizing today’s analog shore radar).

In its military institution, Indonesia has declared NCW a program that needs to be done to deal with various disruptions in the Digital Age. Network Centric Warfare (NCW) as the basis for a communication system to run optimally needs to be manned by qualified and reliable personnel. For this reason, steps to increase professionalism through education and training should be prioritized and adapted to the rapid development of communication technology.

In 2021, the TNI has declared the Policy Principles of the TNI Commander to be used as guidelines in carrying out the tasks of the Communications and Electronics Command (Komlek), namely building a communication system based on satellite technology, the need for Communication and Electronic Equipment (Alkomlek), Electronic Warfare Equipment (Alpernika), the Command and Control System (Siskodal) of the integrated TNI Unit, modernization of the TNI Alkomlek, Cyber and Information Systems and Data Processing (Sisinfolahta) of the TNI as well as preparing development in order to fulfill the Communications and Electronics of the Joint Indonesian Defense Area Command, Materials for the Special Operations Command TNI and TNI Maritime Information Center. Then increase the support for strategic reserve Alkomlek readiness, the role of maintenance and care, HR professionalism, and software fulfillment for the effective and efficient implementation of main tasks.

According to the Chief of the General Staff of the Indonesian National Army, Lt. Gen. Ganip Warsito, in implementing the Integrated Tri Matra Operation System, the TNI still needs cooperation and collaboration with other non-military components in the Komlek sector such as BSSN, Lapan, PT Telkom, PT LEN, the ORARI amateur radio community. and RAPI, as well as the drone pilot community (PUSPEN Markas Besar Tentara Nasional Indonesia, 2021). In practice, this cooperation has existed for a long time and is currently being strengthened by enacting Law Number 23 of 2019 concerning the Management of National Resources for National Defense. This regulation opens up more opportunities for non-military components in the Komlek sector to participate and have a role in National Defense.

So, in carrying out these preparations, the TNI, especially the TNI-AU, needs to prepare its personnel to achieve these goals. In this era of technology, mastery of Information and Communications Technology (ICT) is crucial to fulfilling professional HR's needs immediately. This article will discuss how the TNI-AU prepares its personnel to meet the needs of the Network Centric Warfare program.

Network Centric Warfare (NCW) theory claims that NCW theory focuses on networks. This focus on networks is based on an understanding of Metcalfe's Law, which states that the 'strength' of a network is proportional to the square of the number of its nodes (Metcalfe, 2013), intending to generate and exploit opportunities within the network, particularly in the battlespace. With this in mind, NCW theory is then presented how the science of probability—creating optimal combinatorial configurations of preformed things/objects subject to the dictates of Metcalfe's Law—is realized. While this approach has undoubtedly given rise to some innovative concept-technology pairs, there are fundamental limitations. The innovation and agility valued by NCW theorists remain locked in the network of relationships constructed between preconceived things/objects. In this sense, NCW theory is far from the ambition of its founding theorists.

Such an understanding of networks—a concept of great importance to NCW theory—allows the recasting of the theory as a conceptual framework within which the individuation and transductive processes exhibited by objects, particularly in the context of war, maybe framed. As expected, this will have profound implications on our understanding of the nature of the relationship between humans, weapons, and combat. It will change the way we think about strategy, tactics and how we conceptualize and design truly innovative operating concepts, concept-technology pairs, and 'sense and respond' architectures, which must increasingly operate as 'edge organizations' (Oros & Nissen, 2010, p. 575). Moreover, it can also help in addressing emerging problems such as the 'tremendous valley problem' (Kioumourtzis et al., 2012; Misselhorn, 2009), which arise in the context of experiments involving human-machine combat teams, advanced robotics, and the application of artificial intelligence, as well as machine learning paradigms in conducting war (Guha, 2021).

The network system focuses on the information system developed and communication, which is crucial in its implementation. Kang et al. (2018) look at the importance of communication in NCW. This communication network is responsible for the flow of information; it is necessary to analyze the performance of this communication against the communication parameters in a high-complexity environment, such as a battlefield. For this reason, many studies have carried out a simulation-based analysis of NCW, which consists of combat systems and network systems to reflect the effects of each other. However, this paradoxically leads to long execution times and difficulties in performing analyzes of various parameters due to timing issues.

Information and Communications Technology (ICT) may play in a military context to warrant a revolutionary label, even at this early date. However, at the heart of NCW lies a fundamental dialectical tension in the concept. NCW promises faster, more precise, and more decisive operations due to information sharing. In this regard, the NCW is oriented towards increasing operational freedom to choose military commanders to avoid or efficiently overcome the barriers to war created through active enemy resistance or ignorance posed by the dangers and chaos of operations (Silfverskiöld et al., 2021). At the same time, because military operations are ultimately carried out to ensure national security, the military context is an environment of strict control and direction. The criticality of this operational dimension is further exacerbated by the quality war, which is dangerous for human life. These two aspects, freedom and control, sharing and security, circle each other carefully like NCW.

As Network Centric Warfare points out, information advantage is gained in part by operating information that protects our ability to collect, process, and disseminate an uninterrupted stream of information when exploiting and/or denying an adversary's ability to do the same. Ultimately, the ability to build collective awareness of the limitations gleaned from platforms and individuals operating in the battlespace is the foundation of a military transformation plan. In other words, IP brings global connectivity to the kill chain (Lu et al., 2021).

Over the past two decades, the level of use of ICT among government employees has increased (Arifin & Tajudeen, 2020). ICTs have changed the way services are provided; it increases productivity and service quality while also reducing operating costs (Fernandez et al., 2017). At the organizational level, the use of technologies such as social media (driven by advances in ICT) helps organizations understand their customers' needs to meet better those customer needs (Tajudeen et al., 2018). Information Systems (IS) continue to impact employees and the organization as a whole significantly. While SI was once used primarily to automate manual processes, it changes the nature of work and the quality of products and services offered (Stair & Reynolds, 2018).

Implementation of new technologies and IS has been explored quite extensively. Rumata & Sakinah (2020) found that successful technology adoption is influenced by users' digital skills and information literacy. Meanwhile, Choshin & Ghaffari (2017) found that user satisfaction, infrastructure, costs, and system performance are factors that can determine the success of e- commerce technology adoption. In another study, Mohd Yusof & Abd Aziz (2015) found that HRMIS was beneficial for users, especially in managing information and monitoring work. Related to this, Ibrahim et al. (2018) noted three factors that will determine the success of HRMIS implementation: user attitudes, readiness to change, and technology readiness.

Similarly, Savoldelli et al. (2014) found that user engagement and self-readiness are vital factors for user satisfaction and net profit. In terms of implementation, HRMIS has been noted to accelerate work processes and efficiency, thereby reducing bureaucracy (Savoldelli et al., 2014). Most users tend to think that the application is ergonomic, and the user scale is simple to moderate. Nonetheless, the implementation of HRMIS certainly requires organizational support, and this can be achieved through ongoing training or more online support (Intra et al., 2016).

Related to NCW, which is closely related to the IT world and networks, TNI-AU personnel need to see this as something that needs to be fulfilled to implement the NCW program, which has become a program of the Indonesian National Army (TNI). NCW, in practice in the TNI and TNI- AU, is a centralized and fast command network system so that it can minimize threats that come from outside, both physical and cyber threats. Training and infrastructure need to be strengthened in this implementation. Personnel recruitment and placement following the capabilities of this personnel are things that need to be underlined because apart from traditional combat skills that have previously been carried out by the TNI-AU, network and IT skills need to be mastered in overcoming threats in this digital era.

Measurement of the success rate of an organization in technology adoption can be done through the technology-organization environment (TOE) framework, which explains three main factors that influence the implementation of technological innovation: technological, organizational, and environmental factors (Yeh & Chen, 2018). In contrast, the measurement of individual success in technology adoption is evaluated through context, attitudes, and behavior factors. Most studies that focus on individual contexts have used theories such as Theory of Planned Behavior (TPB), Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Model of PC Usage (MPCU), Motivational Model (MM), and TAM Extension and Updated Information System Success Model (ISSM) (Arifin & Tajudeen, 2020; Dwivedi et al., 2019). It is the TNI-AU is closely related to infrastructure and human resource management. These conditions of fulfillment are an absolute must by the Indonesian Air Force to maintain the country's stability from various threats both from within and outside the country.

Historically, Human Resource Management as we know it today evolved from the nineteenth century in stages. These stages respond to external and internal factors that impact the organization differently. The evolution of the external and internal environment and the response to these changes led to today's human resource management development.

According to Schuler & Jackson (2005), Human Resource Management studies began in the United States in the mid-1970s in response to the increasing professionalization of Human Resource Management by Human Resource Management specialists and the growing recognition of the importance of human resources to corporate success. As a result, businesses in the United States are beginning to see human resource professionals as partners "who must be involved in the company's strategic decision-making process" (Schuler & Jackson, 2005, p. 12). The subject is packaged in two "founder" texts that appeared simultaneously in the early 1980s (Kaufman, 2015). This proposed approach was developed at two of the leading University Schools of Management in the United States: one by Beer et al. (1984), offering a "Harvard model," and one by Fombrun et al. (1984) offer the "Chicago model" of Human Resource Management. The "Harvard" map of the Human Resource Management area, as they call it, takes a broader perspective, giving importance to stakeholder interests, long-term consequences, and "situational factors." Situational factors, or what we call context, are not text features. Instead, it is significantly concentrated on the Human Resource Management chain within the firm as a means of promoting performance and is prescriptive, recommending the systematic use of strategic-based selection, individual performance appraisals, individual performance-related rewards, and outcome-monitored training and development (Mayrhofer et al., 2019). The approach is unitary, in the sense that employers and employees are not seen as having conflicting or disparate interests and the interests of other stakeholders are irrelevant, so companies are, or should be, able to develop their Human Resource Management practices free from industrial relations or government pressure (Mayrhofer et al., 2019; Vernon & Brewster, 2013). Waechter (1996), concerning this Human

Resource Management paradigm, human resources are obtained cheaply, used sparingly, and developed and utilized as much as possible following the demands determined by the overall business strategy.

The Human Resource Management research most likely to address these weaknesses views management actions as nested within enabling and constraining forces, so that management can only maneuver within relatively tight boundaries and lies outside. Therefore, a simple focus on the chain of Human Resource Management policies, practices, and perceptions (van Mierlo et al., 2018) and corporate strategy or company policies miss essential factors. Organizations operate in context. Like Gooderham et al. (2015) noted, the context includes external stakeholders, such as economic actors, governments, local authorities, trade unions, and background factors, such as the size and strength of a country's economy, its history, level of economic development, and the rule of law interacts to govern the framework in which the organization operates. These all impact the Human Resource Management chain in organizations, and the outcomes of those chains lie at different levels of social complexity: outcomes for individual employees; for HRM organizations; for organizational results; for the community; and the country. Human Resource Management has to perform several different functions to find a balance between the external and internal factors of the organization. These functions can generally be described as (1) planning, resourcing, and retention; (2) recruitment and selection; (3) learning, training, and development; (4) remuneration and awards; (5) and employee relations.

The strategic views of military organizations concerning the size of military service and its legal distribution are determined by national policy. These policies generally concern the adopted national defense strategy and the allocated budget. Therefore, military HR planning mainly focuses on matching the available military workforce with those needed by adapting availability. To do HR planning for a military organization, we must define its specificity. Its closed nature and strict hierarchy characterize the military workforce system, i.e., recruiting only at the lowest ranks and filling all higher ranks with internal promotions. A military organization consists of a strict hierarchical structure of job positions occupied by soldiers (Zais & Zhang, 2016). To qualify for a job position, a soldier must meet specific requirements related to their characteristics. Every military human resource soldier has several characteristics, whether or not related to their service in the military organization. Typically, service-related characteristics of soldiers consist of military rank and individual competence. Other characteristics not directly related to their services may also be considered, for example, marital status and foreign language proficiency. Recruitment is possible only at the lowest level of the hierarchical structure of personnel (some minor exceptions can be made for specific jobs) (Jnitova et al., 2017). Military competence is trained within the organization. Therefore, every recruit must undergo training before being ready to fulfill any task in the organization (Hall & Fu, 2015). The promotion system in military organizations only involved progressing one step and did not allow level jumps. It means that the higher levels of the hierarchical structure can only be reached from the levels below them. Advanced job positions or higher HR levels require experience and knowledge of several fields. Therefore, some specific sequence of job positions is required to reach this level. Military regulations generally do not predict the firing of soldiers in mid-career other than for cases of serious misconduct (van Mierlo et al., 2018). Thus, recruited soldiers generally remain in the organization until their retirement or the end of their contract. In terms of developing high skills, training is limited to recruits. Military personnel may follow several training paths during their career to acquire or develop competence, depending on their characteristics.

Military organizations define their targets using HR distribution through different HR classifications. Classification is based on the characteristics of soldiers; for example, we can classify HR based on their military rank. HR distribution lists the number of personnel for different groups according to certain classifications (Zais & Zhang, 2016). To ensure optimal distribution of HR and meet the organization's needs over the following years, two types of HR planning are used: strategic planning and operational planning. On the one hand, strategic planning aims to regulate the evolution of statutory HR distribution on a long-term time horizon, taking recruitment, promotion, and retirement policies into account. According to the law often used, the distribution of human resources is the number of personnel at each level. Strategic planning concerns the achievement and/or maintenance of the distribution of human resources according to the desired legislation (Mazari Abdessameud et al., 2021). The problem of achievement concerns the achievement of the distribution of human resources according to specific laws. The maintenance is to get a stable HR distribution to ensure that the distribution can remain stable for many years to come.

On the other hand, operational planning targets assigning the right people with the required characteristics for the correct job positions. Must meet operational objectives, namely the optimal distribution of competent human resources. It usually runs with a short-term time horizon. A relevant example of the distribution of operational HR is the number of employees serving in different groups of job positions.

Research Design and Method

In explaining personnel management in the Indonesian Air Force (TNI-AU) in preparation for the fulfillment of credible personnel in Network Centric Warfare (NCW), the researcher uses a constructivism paradigm and a qualitative approach. The researcher wants to see a reality of the readiness of the TNI-AU institution, which has parts for the fulfillment of human resource management as a whole. The author uses cases in particular institutions and follows an interpretive attitude with an abductive research logic; empirical material focuses on actors' experiences, which helps explain the personnel management process when facing a new program. The research strategy that the researcher uses is a case study. The case study method is the most widely used in academia for researchers interested in qualitative research (Baškarada, 2014; Rashid et al., 2019). Researchers chose case study without understanding the various factors affecting their research results. This article aims to present an overview of management within TNI-AU. Due to a significant amount of time and resources required to conduct research (McKenna et al., 2011), any misunderstanding regarding the research objectives and applying the methodology and validation of the findings can lead to unintended negative consequences (Baškarada, 2014). Although case study has been extensively discussed in the literature, little has been written about the specific steps that can be used to conduct case study research effectively (McKenna et al., 2011; Rashid et al., 2019). The data in this study were collected through interviews and literature study. The interview involved several informants, first, the Head of the Center for Information and Communication Technology of Indonesia Defense University, Colonel Lek Ir. Andi Sutomo, S.T., M.Si

(Defense). Furthermore, the researcher conducted interviews with several TNI-AU personnel who, following the consent, mentioned only their initials, namely MT, AF, IKR, and SAF.

Each informant took part in the interview through synchronous mediated communication (telephone or video call) with direct interviews, which was impossible due to the Covid-19 pandemic. Informant interviews were conducted with a semi-structured interview type because they offered flexibility. Then after the interview was transcribed, followed by the coding process. Furthermore, the informants were allowed to review and comment on the final theme obtained by the researcher as a form of re-examination. In addition, researchers also use literature studies to obtain written data related to the implementation of training or management of TNI-AU personnel to fulfill adequate human resources for the implementation of NCW. These written data are secondary data that also complements primary data through interviews. It makes the data presented in this article comprehensive

Results and Discussion

To define the role of humans in the system and capture human operator activities, tasks, communication, and collaboration required to implement the NCW program within the TNI-AU environment and support operational requirements. Therefore, the TNI-AU uses a training approach starting from the basic IT knowledge level, when they have found competent personnel in their fields to be given higher specialized training, as well as collaborating with experts in their fields from outside the military environment (especially Personnel and Selection, Training, and Human Factors Engineering). In TNI-AU training, the role of humans in the system is defined, and task activities are described at a practical level for analysis. Human characteristics, limitations, and constraints that affect performance can be considered. The need for human activity in the system can be weighed against the labor and training costs associated with human presence. Personnel who have been placed in the field should be the driving force for systems and technical views in human-centered design. Without this view, architecture has no basis for analyzing human problems. The hope is that network-centric operations will significantly expand the sovereign options available to Joint and Coalition force commanders—to build a co-integrated grid power projection.

The challenge then is the right mix of innovative technology, organizational change, and new behaviors or competencies that will be combined to achieve the desired end state. Technology is oriented towards easy and fast access to more information on the assumption that information will be better and that there will be a shared understanding and awareness of shared situations, better and faster decision making, and better command, control, and coordination of forces to achieve the commander's goals. What is not clear, of course, is whether the organizational changes and adaptations of human behavior required to take full advantage of the new capabilities made possible by these transformational technologies can be achieved. Human Systems Integration integrates human capabilities and limitations into systems definition, design, development, and evaluation to optimize total system performance in operational environments. It is part of a total systems engineering approach to analysis, design, development, and testing. Human Systems integration has been defined as integrating personnel (skills), labor (workload), training, human factors engineering, safety, survivability, and habitability to inform exchanges during the systems engineering process. Organizational issues are increasingly seen as an integral part of HSI, although there is still some debate about the practical limits.

Modeling and Simulation

TNI-AU proposes that the implementation of NCW is a logical extension of Human Dynamics and can inform Metrics. How this occurs arises from the nature of the simulation used. Following Pew and Mavor (1998), a model is a computational representation of system activity, and simulation is a method for implementing a model, usually in software, to run over some time and under different conditions. It extends the premise of Human Dynamics by focusing on human performance in a system in response to changing environmental conditions. From this perspective, Modeling and Simulation form part of the dynamic view by providing an overview of the state transition threats in which system components interact to pursue a mission. Thus, input for Human Dynamics should be read in the Modeling and Simulation group activity context. Simulations can lead to computer-generated power and similar endeavors. Thus, the model presented in this section offers a proof of concept rather than a full-scale simulation. Overall, the Modeling and Simulation effort has aimed to propose a description that enables systems engineers to analyze and evaluate system dynamics under alternative system configurations. Thus, engineers can weigh design options in a dynamically modeled environment, providing predictions of processing bottlenecks. This strategy provides a different perspective on Network-Enabled Capability (NEC), which poses a challenge for Modeling and Simulation, which is analogous to the challenges faced by the system concept. As noted by Nielsen et al. (2015), “A system consists of multiple, heterogeneous, distributed systems that can and operate independently but also assembled in a network to achieve unique functions.” This idea is critical to the shift in procurement practices from ‘requirements’ to ‘capabilities,’ where stakeholders integrate multiple systems to support capabilities. Stakeholders must provide capabilities to integrate existing, new, and future systems that interact well with individual end-users and meet global needs. Therefore, there is a need for proper systems engineering methodology to represent the system. Beyond this, there is also a need to make predictions (or at least provide informational descriptions) about the performance of different capabilities. From this point of view, Modeling and simulation explore how these abilities can respond to different situations. The researcher proposes that capabilities relate to the skilled integration of humans and technology. TNI-AU begins with a statement of assumptions that inform and influence the panel’s work.

Integrated Infrastructure Development

As an effort to support existing Human Resources, the TNI and TNI-AU, in particular, already have infrastructure related to this, such as a laboratory at the Defense University (UNHAN), Sentul. The procurement of this infrastructure is an essential asset for the TNI to remain in a strong guard position even from cyber threats. The TNI-AU has also studied and seen technological developments that exist until now. Rapid technological developments make the TNI-AU never finish updating themselves in the development of existing technology, be it unmanned vehicles or the security of the network systems they use. In addition, the TNI has developed a technology that can form a centralized command network so that whatever instructions and strategies the TNI-AU uses, it starts quickly from the highest ranks to personnel in the field. The procurement of network infrastructure is vital as any strategy used by the TNI to achieve state stability that secures it from existing threats. The infrastructure that the TNI-AU uses is the result of private development tailored to the needs that exist within the TNI so that parties outside the TNI who will carry out threats are unable to penetrate the security level of the existing infrastructure.

The developed infrastructure needs to provide a structure that can help define simulations in the same way as those used for system architecture development. In contrast, Modeling and Simulation provide a means to test the infrastructure's assumptions and interactions. Ultimately, one would anticipate the marriage of infrastructure with simulation tools so that Dynamic Views could be run through various infrastructure combinations to allow testing of 'what-if' architectures under different operational constraints. There are similarities between the Probabilistic approach and Network Topology. Both are based on using simulation models to consolidate data from various existing infrastructures. It is helpful to show that a modeling solution based on a comprehensive infrastructure can strengthen existing Human Resources in the TNI-AU environment. TNI-AU has also covered various simulation tools and modeling techniques for the personnel training process, such as critical path analysis, unrelated to human factors. This broad selection was intentional so as not to favor either approach. The described analysis can be performed with most of these tools (if the problem is redefined to fit the model requirements). The point of Modeling & Simulation, and infrastructure is not to demonstrate the superiority of one approach over another.

TNI-AU Personnel Management in the Implementation of NCW

In carrying out the implementation of NCW, several things need to be fulfilled related to human resources and existing infrastructure. Career advancement is an essential role that can later become individual and institutional progress in the human factor. Roles describe how a person can move from one role to another as he or she acquires skills and knowledge. Roles within personnel may include technician, IT, engineer, administrator/coordinator, manager, soldier, lieutenant, captain. These roles carry tasks that include repairing electrical systems on operated ground systems, designing drones, coordinating and managing projects. In addition, skills may include repairing electrical systems, designing and managing network architectural structures, managing personnel, logistics, and resource allocation. Then, knowledge can include network infrastructure training, military data processing and interpretation experience, human factors skills.

Starting roles starts with fewer general tasks, skills, and knowledge. As individuals progress up the chain, roles become more complex and specific to a particular domain or job. The ever-growing list of tasks, skills, and knowledge illustrates this increased difficulty and specificity. Items under each task, skill, and knowledge category must have the same items as the role below, for example. The IT Manager role will have the same duties, skills, and knowledge as the IT Support role but with additional management qualifications under the category. Furthermore, the chart can be divided into left and right sides where each side moves towards a different area.

Personnel functions include repairing electrical systems, designing IT architecture, software development, flying Class IV helicopters, coordinating and managing projects. Criteria are everything that is needed to perform a task. It can include completing specific tasks, using certain tools or software, and requiring certain types of data to be collected. Knowledge, Skills, and Abilities (KSA) are the knowledge, skills, and abilities needed to perform a task. It can include repairing electrical systems, designing and managing network architectural structures, personnel, military data processing, interpretation experience, human factors skills, network infrastructure training. Roles may include technician, electrical engineer, administrator/coordinator, IT manager, soldier, lieutenant, captain. Task forces are grouped into functions. The flow from top to bottom represents the interdependence between tasks where the top task must be completed before starting the bottom one. Next, another important thing is the involvement of humans and machines. This way, users can easily see the flow and relationships between human and machine interactions between tasks. The criteria and knowledge/skills/ability to complete each task are detailed along with the appropriate role for the task.

Cyberspace and related technologies are essential sources of power in the third millennium. The characteristics of cyberspace, such as low entry prices, anonymity, vulnerability, and asymmetry, have created the phenomenon of power dissipation, which means that if governments have been dividing power games among themselves, then there must be other actors, such as private companies, organized terrorists and criminal groups, and individuals. However, the government still plays a vital role in this. Naturally, this phenomenon will not eliminate the national security of their government. This effect can be evaluated in several ways. First is the concept of security. National security can no longer be defined in terms of the military and internal and external borders, but nowadays, the risk of decreasing citizens' quality of life is a threat to national security. The second is the loss of the geographic dimension of cyber threats. In the past, military threats had a specific geographic location. As a result, it is not difficult to overcome them, at least in identification. The third is the level of vulnerability posed by cyber threats. This threat is sporadic, multidimensional, and because it is associated with sensitive networks and infrastructure, the level of damage is very high. Fourth, these threats cannot be overcome by traditional means alone, such as the use of military and police force, and the government alone is not sufficient to counter them, and practical and bilateral cooperation between the government and the private sector, which has a common interest in dealing with them. With such a threat, he demanded. Fifth, as the previous point, indicated cyber threats are not limited to governments, but individuals and companies will not be immune to the dangers of these threats. Sixth, because security in the information age is not just about governance, the various theoretical approaches to international relations whose theories are based primarily on government are easy to ignore or confuse.

Cyber Defense Management

Cyber operations consist of many functions that include cyber management, cyber-attacks, cyber exploits, and cyber defense, all including activities. In their nature, these activities are proactive, defensive, and regenerative. Active Cyber Defense Management focused on integrating and automating multiple services and mechanisms to perform response actions in cyber-relevant time as part of cyber defense. Active Cyber Defense consists of a logical set of functions to capture details from enterprise-level architecture to operational realization. The primary objective is to become a living part of the Ministry of Defense's cyber operations to help defend the country against cyber-based adversaries. Among the many operational needs of warfighters, there is a need for security, which includes the concepts of hardening, protection, assault, and defense among the land, sea, air, space, and cyberspace combatant domains. Cyber is the ability to integrate for other domains and independent domains that have unique needs for cyber defense (Herring & Willett, 2014).

Cybersecurity success is essentially the result of an effective risk management process. However, this process is challenged by the inherent complexity of systems, developed with vulnerable components and protocols and the sophistication of attackers, now supported by well- resourced criminal organizations and states. With scenarios of uncertainty and a high volume of events, cyber resilience capabilities are critical. Cyber resilience is the ability of a system, organization, mission, or business process to anticipate, survive, recover from, and adapt capabilities in the face of adversary conditions, stresses, or attacks against the cyber resources it needs to function. Handling cyberattacks requires the use of appropriate attack models. The attack model makes it possible to recognize the current attack status and its possible future status. The attack model is a hypothetical model that will be used to conclude the possible actions of the attacker. In the management process used, there are at least the following stages:

1) Information Gathering – Collecting target information, such as the technology used and potential vulnerabilities.
2) Weaponry – developing malicious code to explore identified vulnerabilities, combining developed code with unexpected deliverables such as pdf, docs, and ppt.
3) Delivery- Transfers the weapon payload to the target environment.
4) Exploits – The use of vulnerabilities to execute malicious code.
5) Installation – Malware removal software is generally installed, which allows the adversary to maintain its persistence in the targeted environment.

The main issue is the need for much greater consistency in cybersecurity and better training of lecturers across different levels and types of education. People-centric security (PCS) is a strategy that represents an alternative to conventional information security practices. PCS aims to strike a balance between risk reduction and employee agility. It is a strategic approach to information security that emphasizes individual accountability and trust and not restrictive and preventive security controls. The conventional control-centered approach to information security is increasingly untenable in a rapidly evolving and increasingly complex technology, business, and risk environment (Kumar, 2021). Human-centered cybersecurity as a domain is still being developed and not well understood. It was recently founded as an amalgamation of traditional cybersecurity principles and the integration of human-computer interaction, and with an increased focus on collaborative intelligence, with humans and technology working in tandem with one another. This domain holds promise as a socio-cognitive-technical approach to cybersecurity, focusing not only on the role humans play in cybersecurity but developing multiple approaches that can ultimately lead to a balanced cybersecurity perspective, with no one isolated point of failure. It contradicts the adage that "humans are the weakest link in the technical system." In building the foundation for the concept of human-centered cybersecurity, there are three cybersecurity components to consider— the 3Us (user, usage, and usability)—in designing, implementing, and assessing a cybersecurity system. These components are not a complete representation of human-centered cybersecurity but are necessary because they represent a multi-dimensional cybersecurity context (Grobler et al., 2021). In defining this domain, as a starting point, the technical and functional aspects of the system design, the human users who use the system concerning the intended functionality, and the associated thought processes and behavior by humans when interacting with the system for the intended functionality.

PCS is based on critical principles and individual rights and responsibilities. The premise of PCS is that employees have certain rights. However, this is associated with special responsibilities. These rights and responsibilities are based on the understanding that if a person does not fulfill his responsibilities or does not behave in a manner that respects the rights of his colleagues and company stakeholders, that individual will be subject to sanctions.

1) This cohesiveness of rights and responsibilities creates mutual dependence among employees, taking advantage of the social capital that exists within the company.
2) The PCS principle emphasizes detective and reactive controls, and transparent preventive controls, over the use of intrusive preventive controls.
3) PCS supports the maximization of the trust space in which individual autonomy and initiative are encouraged.
4) PCS presupposes an open and trust-based corporate culture and associated executive awareness and support.
5) The PCS principle assumes that individuals have the appropriate knowledge to understand their rights, responsibilities, and related decisions.

Key components and relationships related to cybersecurity management:

1) Cybersecurity breaches Target data, in most cases, confidential data, such as customer records or other valuable information.
2) Data is stored, processed, and communicated on, by, or to Assets, such as software, networks, devices (servers, workstations, and smartphones), websites, people, and third parties.
3) Threat actors, such as organized crime gangs, activists, and nation-states, will deploy Threats, usually targeted at or through Assets to access Data.
4) Threat Defending Controls are primarily applied to Assets and sometimes directly to Data.
5) Some Controls like mobile device encryption protect against specific Threats, like loss or theft of a mobile device, while other Controls, like software patching, protect against some Threats, like crimeware, web application attacks, and cyber espionage.
6) Threats will aim to exploit weaknesses (or vulnerabilities) in Control to access Data.
7) If proper controls are applied to the right Assets and applied effectively relative to the Threat level, the organization will defend against Threats. If this does not happen then, a Data breach will occur.

The TNI-AU explicitly conducts training and education because, in the implementation of NCW, the cyber world is one of the crucial factors to be protected. A war that is no longer conventional makes Human Resource Management, in this case, a significant concern for the TNI- AU to continue to develop and strengthen its personnel well.

Conclusions

To define man's role in the system and human operator activities, tasks, communication, and cooperation to implement the NCW program within the TNI-AU environment and support the operating requirements. Human Systems Integration integrates human capabilities and limitations into systems definition, design, development, and evaluation to optimize total system performance in operational environments. TNI-AU proposes that the implementation of NCW is a logical extension of Human Dynamics and can inform Metrics. From this perspective, modeling and simulation are part of the dynamic view by providing an overview of the state transition threats where system components interact to accomplish a mission.

In general, modeling and simulation efforts have proposed a description that will enable systems engineers to analyze and evaluate the system's dynamics under alternative system configurations. It enables engineers to weigh design options in a dynamically modeled environment and predict processing bottlenecks. The strategy provides a different perspective on Network Enabled Capacity (NEC), which presents a modeling and simulation challenge analogous to the system design challenges. A system consists of several heterogeneous and distributed systems that can work independently but are also combined in a network to achieve unique functions.

This realization is central to the shift in procurement practices from 'requirements' to 'capabilities,' where stakeholders integrate multiple systems to support capabilities. Stakeholders need to provide capabilities that integrate existing, new, and existing systems with end-users and meet global requirements. In addition, there is a need to make predictions (or at least meaningful descriptions) about the performance of various skills. The researcher proposes that skills relate to the skillful integration of people and technology. Acquiring network infrastructure is critical to any TNI strategy to achieve state stability to protect it from existing threats. The infrastructure developed should provide the structure to help define the simulations the same way as personnel training.

Reference

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). Network Centric Warfare: Developing and Leveraging Information Superiority (2nd ed.). Washington DC: CCRP Publication Series.

Arifin, M. A., & Tajudeen, F. P. (2020). Impact of human resources information systems in the military environment. Asia Pacific Management Review, 25(4), 198–206. https://doi.org/10.1016/j.apmrv.2020.02.001

Baškarada, S. (2014). Qualitative Case Study Guidelines. The Qualitative Report. https://doi.org/10.46743/2160-3715/2014.1008

Beer, M., Spector, B., Lawrence, P. R., Mills, D. Q., & Walton, R. E. (1984). Managing Human Assets: The Ground Breaking Harvard Business School Program. New York: Free Press.

Choshin, M., & Ghaffari, A. (2017). An investigation of the impact of effective factors on the success of e-commerce in small- and medium-sized companies. Computers in Human Behavior, 66, 67–74. https://doi.org/10.1016/j.chb.2016.09.026

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2019). Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model. Information Systems Frontiers, 21(3), 719–734. https://doi.org/10.1007/s10796-017-9774-y

Fernandez, D., Zainol, Z., & Ahmad, H. (2017). The impacts of ERP systems on public sector organizations. Procedia Computer Science, 111, 31–36. https://doi.org/10.1016/j.procs.2017.06.006

Fombrun, C. J., Tichy, N. M., & Devanna, M. A. (1984). Strategic Human Resource Management. New York: John Wiley and Sons, Inc.

Garstka, J. J. (2003, May). Network-Centric Warfare Offers Warfighting Advantage. SIGNAL. Retrieved from https://www.afcea.org/content/network-centric-warfare-offers-warfighting- advantage/

Gooderham, P. N., Morley, M. J., Parry, E., & Stavrou, E. (2015). National and firm-level drivers of the devolution of HRM decision making to line managers. Journal of International Business Studies, 46(6), 715–723. https://doi.org/10.1057/jibs.2015.5

Grobler, M., Gaire, R., & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. Frontiers in Big Data, 4. https://doi.org/10.3389/fdata.2021.583723

Guha, M. (2021). Technical ecstasy: Network-centric warfare redux. Security Dialogue, 1–17. https://doi.org/10.1177/0967010621990309

Hall, A. O., & Fu, M. C. (2015). Optimal Army officer force profiles. Optimization Letters, 9(8), 1769–1785. https://doi.org/10.1007/s11590-015-0947-7

Herring, M. J., & Willett, K. D. (2014). A Vision for Real-Time Cyber Defense. Journal of Information Warfare, 13(2), 46–55. Retrieved from https://www.jstor.org/stable/26487121

Ibrahim, H., Mohd Shamsudin, F., Mohd Zin, M. L., & Subramaniam, C. (2018). Understanding User Characteristics as Antecedents of Technostress towards HRMIS: A Mixed-Method Study. Jurnal Pengurusan, 53, 37–47. https://doi.org/10.17576/pengurusan-2018-53-04

Intra, G., Alteri, A., Corti, L., Rabellotti, E., Papaleo, E., Restelli, L., et al. (2016). Application of failure mode and effect analysis in an assisted reproduction technology laboratory.

Reproductive BioMedicine Online, 33(2), 132–139. https://doi.org/10.1016/j.rbmo.2016.05.008

Jnitova, V., Elsawah, S., & Ryan, M. (2017). Review of simulation models in military workforce planning and management context. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 14(4), 447–463. https://doi.org/10.1177/1548512917704525

Kang, B. G., Seo, K.-M., & Kim, T. G. (2018). Communication Analysis of Network-Centric Warfare via Transformation of System of Systems Model into Integrated System Model Using Neural Network. Complexity, 2018, 1–16. https://doi.org/10.1155/2018/6201356

Kaufman, B. E. (2015). Evolution of Strategic HRM as Seen Through Two Founding Books: A 30th Anniversary Perspective on Development of the Field. Human Resource Management, 54(3), 389–407. https://doi.org/10.1002/hrm.21720

Kioumourtzis, G., Bouras, C., & Gkamas, A. (2012). Performance evaluation of ad hoc routing protocols for military communications. International Journal of Network Management, 22(3), 216–234. https://doi.org/10.1002/nem.802

Kumar, S. (2021). The missing piece in human-centric approaches to cybernorms implementation: the role of civil society. Journal of Cyber Policy, 1–19. https://doi.org/10.1080/23738871.2021.1909090

Lu, T., Chen, K., Zhang, Y., & Deng, Q. (2021). Research on Dynamic Evolution Model and Method of Communication Network Based on Real War Game. Entropy, 23(4), 487. https://doi.org/10.3390/e23040487

Mayrhofer, W., Gooderham, P. N., & Brewster, C. (2019). Context and HRM: Theory, Evidence, and Proposals. International Studies of Management & Organization, 49(4), 355–371. https://doi.org/10.1080/00208825.2019.1646486

Mazari Abdessameud, O., Van Utterbeeck, F., & Guerry, M.-A. (2021). Military Human Resource Planning through Flow Network Modeling. Engineering Management Journal, 1–12. https://doi.org/10.1080/10429247.2021.1900660

McKenna, S., Richardson, J., & Manroop, L. (2011). Alternative paradigms and the study and practice of performance management and evaluation. Human Resource Management Review, 21(2), 148–157. https://doi.org/10.1016/j.hrmr.2010.09.002

Metcalfe, B. (2013). Metcalfe's Law after 40 Years of Ethernet. Computer, 46(12), 26–31. https://doi.org/10.1109/MC.2013.374

van Mierlo, J., Bondarouk, T., & Sanders, K. (2018). The dynamic nature of HRM implementation: a structuration perspective. The International Journal of Human Resource Management, 29(22), 3026–3045. https://doi.org/10.1080/09585192.2018.1443957

Misselhorn, C. (2009). Empathy with Inanimate Objects and the Uncanny Valley. Minds and Machines, 19(3), 345–359. https://doi.org/10.1007/s11023-009-9158-2

Mohd Yusof, M., & Abd Aziz, K. (2015). Evaluation of Organizational Readiness in Information Systems Adoption: A Case Study. Asia-Pacific Journal of Information Technology and Multimedia, 04(02), 69–86. https://doi.org/10.17576/apjitm-2015-0402-06

Nielsen, C. B., Larsen, P. G., Fitzgerald, J., Woodcock, J., & Peleska, J. (2015). Systems of Systems Engineering. ACM Computing Surveys, 48(2), 1–41. https://doi.org/10.1145/2794381

Oros, C. L., & Nissen, M. E. (2010). Designing Complex Organizations Computationally. In M. Wang & Z. Sun (Eds.), Handbook of Research on Complex Dynamic Process Management: Techniques for Adaptability in Turbulent Environments (pp. 573–598). New York: Business Science Reference.

PUSPEN Markas Besar Tentara Nasional Indonesia. (2021). Kasum TNI : Network Centric Warfare Perlu Diawaki Personel Yang Andal. Retrieved from https://tni.mil.id/view-195172-kasum-tni-network-centric-warfare-perlu-diawaki-personel-yang-andal.html

Rashid, Y., Rashid, A., Warraich, M. A., Sabir, S. S., & Waseem, A. (2019). Case Study Method: A Step-by-Step Guide for Business Researchers. International Journal of Qualitative Methods, 18, 160940691986242. https://doi.org/10.1177/1609406919862424

Rumata, V. M., & Sakinah, A. M. (2020). The Impact of Internet Information and Communication Literacy and Overload, as Well as Social Influence, on ICT Adoption by Rural Communities. Asia-Pacific Journal of Rural Development, 30(1–2), 155–174. https://doi.org/10.1177/1018529120977250

Savoldelli, A., Codagnone, C., & Misuraca, G. (2014). Understanding the e-government paradox: Learning from literature and practice on barriers to adoption. Government Information Quarterly, 31, S63–S71. https://doi.org/10.1016/j.giq.2014.01.008

Schuler, R. S., & Jackson, S. E. (2005). A Quarter-Century Review of Human Resource Management in the U.S.: The Growth in Importance of the International Perspective. Management Revu, 16(1), 11–35. https://doi.org/10.5771/0935-9915-2005-1-11

Silfverskiöld, S., Andersson, K., & Lundmark, M. (2021). Does the method for Military Utility Assessment of Future Technologies provide utility? Technology in Society, 67, 101736. https://doi.org/10.1016/j.techsoc.2021.101736

Stair, R. M., & Reynolds, G. W. (2018). Principles of Information Systems. Massachusetts: Cengage Learning.

Suryohadiprojo, S. (2008). Pengantar Ilmu Perang. Jakarta: Pustaka Intermasa.

Tajudeen, F. P., Jaafar, N. I., & Ainin, S. (2018). Understanding the impact of social media usage among organizations. Information & Management, 55(3), 308–321. https://doi.org/10.1016/j.im.2017.08.004

Vernon, G., & Brewster, C. (2013). Structural spoilers or structural supports? Unions and the strategic integration of HR functions. The International Journal of Human Resource Management, 24(6), 1113–1129. https://doi.org/10.1080/09585192.2012.703416

Waechter, H. (1996). Book Reviews : Paul R. Sparrow and Jean-M. Hiltrop: European Human Resource Management in Transition. Organization Studies, 17(2), 343–345. https://doi.org/10.1177/017084069601700211

Yeh, C.-C., & Chen, Y.-F. (2018). Critical success factors for adoption of 3D printing.
Technological Forecasting and Social Change, 132, 209–216. https://doi.org/10.1016/j.techfore.2018.02.003

Zais, M., & Zhang, D. (2016). A Markov chain model of military personnel dynamics.
International Journal of Production Research, 54(6), 1863–1885. https://doi.org/10.1080/00207543.2015.1108533