[1] Mário B. Leston
[2]Gajanan Bhole
[3] Manuela M. Oliveira

Portuguese Military Cyber Human Resources Management

Abstract: - The Portuguese public sector institutions, including the Armed Forces, are facing increasing cost reductions due to budget cuts resulting from economic crises and the pandemic scenario. Although Lean thinking aims to reduce waste and improve customer satisfaction through continuous improvement, its implementation often faces challenges. The Portuguese Air Force was a pioneer in applying Lean methodology, achieving positive results in crucial areas, and extending this methodology to other Armed Forces institutions could contribute to better use of national resources. This paper explores the implementation of Lean philosophy in the Portuguese Armed Forces, specifically in the recruitment, integration, and retention of talent in Cyber Security. Centralizing and simplifying processes and resources, as well as resolving challenges inherent to the area, maybe the right approach to respond to the implications on National Security and Defense, providing necessary resources for the capture, training, and maintenance of essential Cyber teams and processes. The mentality based on work processes needs to change to speed up the use of resources and the behaviour of executing elements.

Keywords: Portuguese Armed Forces, Agile Methodology, Cyber Security, Retaining Talent

Introduction

Cyberspace, as we know it, without national borders, coexists simultaneously with a delimited real space, allowing global communication. However, this fullness and speed in communication among all require much more than the technological means where the internet ”flows". This transversal sharing crosses different countries, and cultures with greater or lesser tradition, economic power, and political profile, which constantly seek to suit themselves with the most modern information and communication resources.

However, where too many actors or players coexist, the tendency for anarchy and chaos is high, so the rules must be clear, as well as the appropriate action measures when this is not evident. Additionally, the rapid progress in the development of information, communication technologies, and the Internet, and its growing impact on social phenomena and processes, has led to a greater interest in all phenomena that have emerged from this development. One of these phenomena is cybercrime.

The recognition of the importance of this new phenomenon requires a complex and multidisciplinary approach to developing adequate, original, and efficient principles and norms for the establishment and management of national and collective cybersecurity, not only through technological instruments but also legal and specific ones for its implementation (Spalevi’c, 2014).

Cybercrime

Cyber warfare, the most serious level of cybercrime, distinct from isolated acts perpetrated by individuals with very particular motivations, is characterized by being a form of latent aggression committed by a state, carried out by highly specialized groups, with the ultimate goal of weakening the economic, military, and political resources of the state under attack (Spalevi’c, 2014). In a crisis, the weaknesses and unresolved issues of cybersecurity expose the security of the state and the security of the individuals that comprise it.

Cybercrime per sei is a crime that relates to any type of illicit activities that can be committed with, within, or against computer systems and networks. However, most attacks are made on the network itself (online), using undetectable technologies, which makes it extremely difficult to accurately identify the attackers and the countries of origin, ultimately suggesting that the issue of cybersecurity currently represents a global challenge.

In many countries, the information and communication networks where the Internet operates globally are mostly owned by individuals, and their security can be ensured by the owners or even by the government entities of the country where they are located. It is easy to recognize that one of the main challenges that arise is the need to

[1]Weapons and Electronics BNL, Alfeite Naval School, 2810-001, Almada, Portugal, mario.mpereira@defesa.pt

[2] ECEO, Universidade Lusófona, 1749-024 Lisboa, Portugal,

∗Corresponding author-manuela.oliveira@ulusofona.pt

work together in a transnational solution that goes beyond technology and is capable of neutralizing all threats, ensuring an adequate response to unforeseen events. In this sense, government entities must become partners of the private sector, citizens, and other governments. The risks inherent in the absence of a good cybersecurity policy constitute challenges that go well beyond national borders, compared to the damage caused internally in a state victim of an attack.

However, not all cyber-attacks can be considered cyber warfare (as previously referred to). To better understand the nature of cybercrime and the threat it poses to a state or simply to a governmental or private organization, we can make an analogy with a simple firearm. Just as an unloaded gun by itself does not kill anyone, a bullet without propulsion does not cause damage either. However, when combined, they are an effective means of destruction if they hit the target. In cyberspace, malicious code, computer instructions, or specific data, are equally destructive as a loaded weapon (Spalevi’c, 2014). The digital assets of organizations are constantly under threat from a wide range of more or less dangerous “observers”. When threats materialize, the consequences can be significantly harmful (Ahmad et al., 2020).

In December 2015, a Ukrainian power plant was invaded and nearly one million residents, albeit briefly, experienced a blackout (Zetter, 2016). The year 2017 was particularly prolific, becoming known as the year of ransomware attacks. This type of attack involves a type of virus that “kidnaps” files on infected machines, enabling their “release” (and that of the machine they are on) in exchange for payment. It is estimated that more than 230,000 systems were affected (or infected) just in that year, including personal computers, businesses, and public entities, until an “antidote” was discovered that controlled the progression (Woollaston-Webber, 2017).

The Cybersecurity Challenge

In this context, information technologies and the interconnection of the infrastructures that support them pose new challenges for societies in that they are exposed to new vulnerabilities and risks. Regardless of the perpetrator’s motivation, whether intentional or accidental, cyber incidents have the power to trigger domino effects and seriously or even irreparably disrupt the provision of essential public services.

To avoid situations of this gravity, strategies for improving the security and resilience of systems against external attacks have been drafted since the beginning of the century (Klimburg, 2012). This topic, which deals with the establishment of objectives and strategies on how to achieve them, has garnered attention not only from the business sector but also from academics and politicians. However, any institutional agreement reached only includes the roles and responsibilities of organizations regarding cybersecurity. Crisis management has been a much less addressed topic, despite its relevance (Boeke, 2017).

The challenges in managing this type of attack go far beyond the technique of the area’s operatives. Finding concerted tools and approaches that are transversal to public and private organizations and even more difficult among different states makes this topic of utmost importance and urgency, considering the scope of its effects when security is breached. According to Ahmad et al. (2020), most large organizations invest in a preventive approach, with Information Security Management (ISM) specialists whose objective is to ensure the protection of digital assets. The ISM function conducts risk assessments, develops strategies, provides appropriate policies and training to define procedures and guide behaviors, as well as implementing technological controls such as firewalls, antivirus, and encryption to restrict unauthorized access. Despite all these measures, security breaches occur simply by providing the right opportunity, knowledge, and motivations. Along with information security management, many organizations have already implemented Incident Response (IR) functions to minimize the possible damage from a cyber-attack and quickly restore the normalcy and availability of digital services.

However, despite all the attacks taking place around the world, few organizations learn from incidents and integrate what they have learned into their daily activities, operating proactively rather than reactively. It would also be worrying to find a “simple" process for sharing incidents through a database with lessons learned, to reduce the attack surface. The strong integration of ISM and IR functions creates opportunities for learning that ultimately lead to organizational security benefits, creating greater awareness of security risks, a reliable mapping of threats, allowing constant re-evaluation of security vulnerabilities implemented, and promoting an assertive and effective response.

The Human Factor

Recruitment and Requirements

At the center of all issues related to security, and in particular, cybersecurity in the armed forces, are people. The recruitment of individuals for cybersecurity or cyber defense teams should occur through an evolutionary process that is attentive to the current state of the art in IT and training. Initially, the recruitment model should obtain its members internally, i.e., qualified military personnel with aptitudes for integrating cyber teams.

In the second phase, military schools should incorporate appropriate training into their academic programs and define a career specifically associated with cyberspace. Finally, a current process should be established for the operations of cyber teams that involve all sectors of the armed forces. It is recommended that the recruitment process establish an exit procedure for cyber team members from the beginning, with the perspective that they carry with them the values and principles of the military institution and defence, as well as their personal development to other sectors of State activity.

Commitment Factors

When we ask ourselves about the best measures to adopt for talent retention in a particular organization or project, we should start by asking ourselves what people expect from the work they have. This simple question or its answer can clarify and help to design any human resources appreciation and retention strategy more thoughtfully (Reynolds, 2019).

On the one hand, it is especially difficult to create an attractive and challenging environment capable of attracting, developing, and retaining the best human resources, particularly in industries or services whose competition and talent hunting are fierce, while remaining competitive in an increasingly global market. On the other hand, individuals are redefining what they understand as a career, as well as their expectations and their relationship with the employer.

There is an indisputable awareness that the employee-employer relationship has become more balanced in the sense that the employee recognizes that they are as important to the employer as the employer is to their professional development. If in the not-too-distant past, an individual expected to derive from their profession the income necessary to realize their projects, currently, work (or work activity) goes further. Those who work value not only the monetary return but also flexibility, personal development, appreciation and training, and the “pleasure” that can be derived from the activity carried out.

All of these changes represent additional challenges and can even be problematic for traditional human resources departments, with special emphasis on military institutions – by definition, less flexible. This rigidity causes them to lose human resources to private organizations that adapt and understand the importance of focusing on employee-centred approaches.

Thus, the whole issue of talent retention boils down to the answer to a simple question: What do individuals want from their work activity? The matter of talent retention can be effectively addressed by addressing a fundamental question: What are the specific desires and expectations that individuals have from their employment? This question holds particular significance in the context of military organizations, as it necessitates not only a response but also the active engagement and dedication of the organization itself. Nevertheless, all decisions regarding human resources are made at a higher level; the direct military hierarchy plays a very important role not only in the productivity of the unit but also in how each member sees themselves in its success and development. Returning to the question, what do individuals want from their professional activity?

The International Coaching Federation (ICF) uses five distinct categories to answer this question: compensation, identification, balance, personal development, and recognition. Even before we develop each of these dimensions, it is important to recognize that Millennials, compared to previous generations, are characterized as detached, disinterested, and with little resilience in the face of adversity. Many factors contribute to this characterization, but without losing sight of the discussion, let us return to the presented dimensions, and on these, it is important to add that individuals generally want each one. The priority each gives to them varies, but ultimately, most employees seek a mix of all of them. The consideration of these attributes by the institution will dictate to what extent the employee will embrace a commitment and remain as such. Although not guaranteeing the right retention of the desired talents by itself, the use of the ICF is considered to provide institutions with a mechanism to improve productivity and commitment, regardless of the decisions the employee may make along their professional path.

Compensation

Compensation (or remuneration in the form of salary, overtime, bonuses, commissions, subsidies, insurance, paid vacations, and even retirement plans) is an important, if not the most important, dimension. According to Reynolds (2019), "compensation is important to 99% of Millennials and very or extremely important to 81% of older employees, confirming that compensation remains at the top of employees' priorities regardless of age, although with the different impact depending on the age group."

Military personnel are no different. The United States Army recognized as early as 1970 that "adequate pay alone will not attract, but inadequate pay can certainly deter" (Tagarev et al., 2021). In the US Army, compensation is also a valuable tool often used to influence recruitment and retention goals, offered to recruits in the form of university tuition, medical insurance, paid vacations, and housing to attract them to serve the nation. A performance bonus is added to the monthly salary to keep members in critical career areas.

Spousal housing and facilities are also offered to support and retain families.

Accommodations for spouses and facilities to support and maintain families are also provided, bearing in mind that pay is an important variable but certainly not the only one to consider if you choose a lifelong military career. However, regardless of the career chosen, the person will certainly consider the working environment and the relationships between colleagues and direct managers. These often dictate the individual's performance, as they relate directly to their job satisfaction, as well as their willingness to continue collaborating with an organization or institution

A dissonant relationship with the direct supervisor or poor relationships with colleagues is not particularly constructive. Regardless of the hierarchy in which the employee operates or the role they play, all confirm that the existence of trust and support from team members or structures is extremely important. Of course, a poor work environment can be compensated for by other attributes, but it does not always compensate for the "damage" it causes in the medium/long term.

Identification

Another dimension not to be overlooked is the identification of the employee with the philosophy of the organization or institution. In general, people want to belong to organizations that play their role in society, meaningfully and intentionally. It is no coincidence that there is currently so much attention paid to concepts such as Corporate Social Responsibility (CSR). According to Pricopi (2012), "People want to feel that what they do is important and that their contribution counts towards achieving something bigger... We increasingly see organizations doing something significant that also interests society, through the community in which they operate." In this context, more and more organizations are focused on the "purpose" of motivating their employees, by offering volunteer opportunities, directing direct profits to charity organizations, among other similar activities (Pricopi, 2012).

Balance

The post-pandemic reality has confirmed the already tenuous separation between work and personal life, long blurred by the advance of technology that connects people and latitudes more and more. Being constantly connected "to work" becomes the norm admired by all those who defend the flexibility of the functions they perform. Although the younger generation is indeed quite favourable to flexibility, this is another phenomenon not exclusive to this age group. However, a healthy balance between work and personal life, with all this flexibility, requires sufficient resources, competent leadership, and well-defined organizational policies.

All organizations, military or civilian, state or private, that do not have these resources and good management, will use the same workforce to fill in all the gaps that arise. And in this way, the balance between work and personal life is usually the first to be affected, resulting in extended working hours, work on weekends, and vacations. In some geographies, military personnel and their families also have additional unique challenges, including long deployments, lack of predictability, high-stress environments, and the possibility of temporary or permanent physical injuries. Most people tolerate these imbalances to a certain point, often ending up in increasingly frequent burnout situations.

Personal Development

Another relevant factor, with particular emphasis on the military, is career opportunities (or the lack thereof). According to Deal and Levenson, Millennials "attach high priority to development" but once again, the vast majority of the workforce seeks career opportunities regardless of their experience and age. Personal development within an organization is one of the most important reasons why individuals enter specific companies, while the lack of it is one of the most common reasons for leaving a job.

Career opportunities can mean not only new and more satisfying jobs, but also specialized training and retraining, and above all open communication between the employee and the institution. It is equally important for organizations to recognize how important it is for individuals to "see" their future and how they can fit into the structure in the medium and long term. The formalization of goals motivates change and learning. The best organizations are aware of this and value career opportunities, development programs, promotions, professional requalification, and leadership positions - and are open and transparent in their processes.

All career and personal (professional) development opportunities should always be aligned with leisure, compensation, and recognition programs. This blend of work and leisure has proven to be a fundamental pillar for commitment between the employee and the organization. Military personnel have the same professional expectations. With promotions come more responsibility, better pay, opportunities for career advancement, compensation for hard work as well as the risk often associated with one's rank. The missions to which they are subject provide in some cases, opportunities for leadership, experience, and adventure, but also unpredictability and stress. However, it does not always result in professional development, provide certifications, or open doors for greater opportunities.

Recognition

With or without formality, all individuals seek recognition for their work and dedication. While on one hand, many individuals seek responsibility and autonomy, these same individuals also need recognition and feedback to be able to evaluate whether they are on the right track or should adjust their performance. In their book "The Human Capital", Pfau and Kay (2002) emphasize that people seek recognition for their work and parity in their remuneration.

Although military personnel cannot expect to see their performance recognized on their paychecks, the expected feedback should be reflected in their superiors' performance reports to obtain greater levels of responsibility and access to future career promotions.

Challenges of Talent Retention

Organizations exist far beyond meeting the needs of their employees and their mission is to create wealth for their shareholders, regardless of the metier they dedicate themselves to. For them to be successful in their purposes, they need collaborators, but this relationship is not always seen as a two-way street. In this context, the development of policies, procedures, and programs that adapt to the wishes of employees requires a profound paradigm shift.

What we often see are organizations putting their priorities ahead of the employee if they intend to fulfill their simple missions or objectives, by reducing rest times, extending the teams' working hours to meet an imminent deadline, or satisfying an order.

As a rule, organizational priorities prevail over individual desires, and employees are sensitive to these situations. However, if they persist indefinitely, the balance in the relationship is lost. However, reality dictates that personnel needs in organizations can change rapidly. Commercial competitiveness is complex and remains constantly in flux, adding pressure on reducing turnover and find new and experienced employees. If they have the necessary flexibility to respond to market demands, organizations can hire individuals directly to fill seasonal positions or offer training to redirect existing employees to an emerging career field, for example.

Additionally, all organizations still deal with different degrees of influence from external and internal agents. At the level of military institutions, these deal with the internal governance of the institution, the government in office, budgetary constraints, and international partnerships with other military institutions. The lack of authority, in the sense of the absence of decision-making power, is also a significant challenge in talent retention. Hierarchical institutions – such as the military are characterized by - retaining and delegating authority in their organizational structure in a different way from other organizations.

Although unit-level leaders have direct interaction with their personnel and know their performance better than anyone, they may not have (which is a fact most of the time) the necessary authority to satisfy individual aspirations, such as better pay, more benefits, and career promotions. In addition to this "lack of authority," there is the burden of the hierarchical superiors themselves. To lead teams efficiently, it is necessary to take time and energy to support each one, listen to their issues, give them feedback, and at the same time, think of effective ways to increase productivity or commitment in their functions, not forgetting the need to report any developments to their peers and hierarchical superiors.

Factors of Change

All these challenges are already present when everything goes according to plan. However, in the constantly changing and tumultuous world we live in, it is increasingly difficult to anticipate times of change or at least have the necessary flexibility to keep up when called upon. The pandemic that the world has faced since 2020 (because it is still part of our lives three years later) has been one of the biggest challenges for private organizations and state institutions around the world. Almost overnight, we were all forced to adjust to a completely different reality, and even remote work (long advocated) came to stay, showing that with dynamism, responsibility, and willingness, there are many ways to carry out the activities assigned to us and still be highly successful. Thus, the ability to react and the speed with which it was felt proved to be the difference between "who cries and who profits from selling tissues".

Returning to individuals and their role in this whole process, it is important to assume that people are not open or entirely honest with their superiors about their current and future aspirations. However, whether or not they have the authority to make a difference, whether or not they believe that their members' aspirations are achievable, team leaders must have an open attitude and provide honest feedback, allowing employees to decide what is best for their future. Keeping employees on "standby" can result in discouragement in the very short term and in an entrenched dissatisfaction that will lead to the search for another occupation.

In all these challenges, culture and education (or training) will certainly play a preponderant role. By culture, we mean values, priorities, and behaviours. The organizations themselves with common pillars operating in different countries, hold in each geography, a very unique and conditioned mix and adaptation of these same pillars, very much dependent on the cultural values of their employees. This cultural and training aspect is especially applicable in military institutions. The rigidity of the hierarchy and the usual promotion by seniority (and not by merit) contrast with the adaptable nature of a military person. Any paradigm shift in this environment with years of entrenched norms and traditions will not be impossible, but it will certainly take longer than ideal.

These are just some of the reasons why it is difficult to use the knowledge we have about what an employee expects from the organization in which they are involved and, on the other hand, how difficult it can be to retain talent in more traditional institutions. Nevertheless, despite all the difficulties and constraints presented, to truly improve recruitment, commitment, and retention, any military or non-military organization/institution must take an active role, especially at the team or unit level. Commanders and direct superiors have - as already mentioned - a huge influence on the motivation, productivity, commitment, and retention of their members, and the dimensions presented can represent an added value to better direct attention to the factors that most impact individuals and promote their commitment to the institution.

In the United States Navy and Marine Corps, it was recognized in 2018 (Kroger, 2020) that the intellectual capacity of its members (military and civilian) and a permanent passion for continuous learning would constitute the basis of any credible deterrent against war. In the same report, organizational and functional changes were recommended designed to elevate education to a strategic and budgetary priority at the same level as the modernization of weapons systems themselves. It also identified the need for a comprehensive education strategy to unify the most disparate elements within the units, integrating talent management initiatives equally. In this way, and concert with high-level leaders and throughout the hierarchy, the goal is to align the policies and resources necessary to produce a more educated and agile naval force.

A situation of war or the threat of war, such as the one we are currently living in, is the toughest auditor for military institutions (and indeed for civilian institutions, given the repercussions for civil society). The best way to deter future conflicts and win those that we cannot avoid is to operate at our maximum or near-maximum theoretical potential. However, we cannot reach this level of maximum effectiveness without sustained education for the entire military force. Intelligence will increasingly lead over strength, although this may seem like an implausible truth given the current situation in Eastern Europe.

However, only intelligence can prevent the escalation of conflicts or even avoid them altogether through diplomatic negotiation that best serves all parties involved. Thus, one of the best talent retention strategies in the military institution is a solid formation of its personnel, aimed at their excellence. All factors important to employees and challenges to talent retention are especially applicable to the technology sector in the various branches of the armed forces not only in Portugal but worldwide. As is commonly known, the private sector has a strong advantage in negotiating and retaining talent in these areas and can even lure the best professionals to work in the public sector (which includes military institutions) in exchange for higher pay and work flexibility.

Yet, the importance of this sector in particular, and considering the threats to cybersecurity and the magnitude of damage from successful attacks, requires exceptional and even "out of the box" measures to retain the best for the most critical positions. Without the freedom or even budget availability enjoyed by the private sector, retention measures could involve special incentives for critical positions or even specialized training and qualification plans for the position held. Remuneration or incentives could also reward those who, on their initiative, decide to invest in their profession, such as obtaining linguistic proficiency. Incentives could reward those with the highest demonstrated proficiency, requiring that these "levels" obtained are clear to all involved.

Nonetheless, remuneration is not everything for those who spend all day in front of a screen and who are expected to have an alert, shrewd, and alternative mind (as only then can they be one step ahead of the threat in prevention). The best talents in cybersecurity are unconventional "characters" who like to enjoy flexibility (within the possibilities that firewalls and proxies currently provide) in an informal work environment. Despite unorthodox this may prove to the military chain of command, such an environment free of formality and protocols, through an inevitable paradigm shift, could reverse the exodus of the best professionals to the private sector.

In addition to incentives or merit-based remuneration (and promotions) rather than seniority, a pleasant and challenging work environment, there is also a factor with which the private sector cannot compete - the sense of mission. Just as not all individuals choose to be military, territorial security agents, or even peace soldiers, despite the remuneration involved, there is a commitment to the homeland. A call to a mission that only a few follows. This is an unbeatable factor that should not be exploited lightly but rather rewarded through top training for members of this special defense force, as well as a sense of belonging and a solid and cohesive team where the sense of mission far outweighs the individualism present in private organizations.

However, all these suggested changes imply a basic restructuring of cybersecurity services in the various branches of the armed forces. The suggestion of this work is based on reducing the basic structure, betting on the centralization of services, retaining the best and most qualified personnel, and developing the necessary measures to establish a satisfactory compromise for all parties involved. The suggested restructuring should follow the Lean philosophy (Womack et al., 1991), which allows for an analysis of where and what can be reduced (eliminating waste of resources).

Addressing a new approach

The Lean Philosophy

Historically, moments of deep crisis often open the way to great opportunities. In 1950, after World War II, when most Japanese companies were plunged into a serious economic crisis, Toyota recognized the need to adapt Ford's production model (until then the leader in automobile production) to the reality of Toyota and the country. This adaptation established the basis of what we know today as Lean Methodology. Toyota's production then evolved over the next forty years and in the 1990s gave rise to "Lean Thinking" - a philosophy of long-term growth and continuous improvement of the organization.

This growth and continuous improvement are revealed through the creation of value for the customer, society, and the economy, with cost reduction, improvement of delivery times, and quality, through the systematic elimination of waste or MUDA (a Japanese term) (Wilson, 2009). Lean Thinking is, therefore, an integrated approach to providing products and/or services to achieve superior quality, just-in-time production, and competitive cost, culminating in customer satisfaction (Khadem et al., 2006).

However, despite the proven results in different areas, this methodology is not without criticism. These criticisms range from the negative impact of the entire process on the brand if it does not result in what was expected, to the ability of organizations to innovate and even to the blocking of creativity of their collaborators, since the operation becomes rigid to alternative execution methods that are not properly foreseen and tested. Criticisms also refer to a lack of sensitivity to human aspects and interactions between organizations.

The Lean principles that constitute the mechanism for the improvement process we know today were developed by Womack et al. (2007), based on the original work of Ohno of the Toyota Motor Corporation, which had a clear objective of optimizing production through the elimination of waste (Askin et al., 2001).

The Toyota strategy was based mainly on the following methods: Kanban methods, elimination of waste, investment in the value of quality, continuous improvement, human resource development, integration of material orders and suppliers, specialized and efficient layouts with balanced material flows, among others (First National Toyota, 1998; Haque, 2003). In the 1980s, the MIT Automobile Institute conducted a detailed study of production processes based on Lean methodology in the automotive industry, and all applied developments were properly documented in the book "The Machine that Changed the World" (Womack et al., 2007). The most relevant results of this work were later discussed by Koskela (1992) in a report from Stanford University entitled "Lean Construction."

Although this work philosophy emerged from the automotive industry and is essentially applied to production processes in a factory environment, Lean Thinking can be generally considered a business strategy based on the principle of optimizing an organization's production process by eliminating any waste of resources, to maximize profit (through cost reduction, whether related to materials, labour, or others). Companies and organizations that consider adopting this "slimming" philosophy of the production structure have methodologies and tools with proven efficiency (Sinha and Matharu, 2019), of which the following stand out:

Kaisen: originating from Japan, the word Kaisen means continuous improvement, assuming the collaboration of the entire team involved, allowing them as a whole to improve processes and performances through the adoption of better work practices that involve low or no investments (Garza-Reyes et al., 2022).

5S methodology: Is a workplace organization method originated in Japan, based on five principles: Seiri (sort); Seiton (set in order); Seiso (shine); Seiketsu (standardize) and Shitsuke (sustain).

Kanban (or Pull System): It is a simple method that involves providing each work cell or process with the necessary materials based on instructions received from the previous cell or process, ensuring just-in-time operations, avoiding delays or unnecessary stock formation (Demir and Paksoy, 2021).

5M+Q+S: A technique used to identify the main sources of waste from a specific point analyzed in the operation developed. The 5M stands for Man (human resources), Machine, Method, Mission (objective), and Management. The Q identifies Quality, and the S corresponds to Safety. All these concepts are then combined to find the waste of resources.

Jidoka: This technique involves the standardization of work, also known as the standardization of the process. It assumes the identification of the best way to perform a particular task. This standardization of instructions (procedures) for performing the task in question aims to ensure that it is performed most efficiently and is properly documented, making it possible for anyone to perform it by following the procedures.

Heijunka or Level Programming: This practice aims to level all production, not just producing order by order but responding to several orders, making it possible to satisfy different customers at the same time, promoting production stabilization.

Value Stream Mapping: This methodology aims to analyze activities and segment them into subclasses according to their value: if the analyzed activities add a lot of value to the project, if they add little value, if they are essential, or if they are completely dispensable. The initial mapping of activities and their value is often elaborated using brainstorming sessions involving the entire work team, where future actions can also be discussed.

The implementation of Lean Thinking (and any other methodology) involves appointing a work team with the primary objective of conducting a thorough survey of all operations, seeking to define each process where it can be improved through the elimination of unnecessary tasks or other resource losses.

Agile methodology

This methodology, imported from the software industry to the management universe, emerged in 2001 through the initiative of 17 software developers who sought to improve performance by implementing new processes and work techniques (Jim Highsmith, Ken Schwaber, and Martin Fowler). Work models based on the Agile methodology aim to promote planning, results, and continuous improvement. Targeted at software development and IT solutions, it incorporates values where Individuals and interactions are considered over processes and tools. The pursuit of an effective response to the needs of the "customer" and constant adaptation to change more efficiently drives a process of faster development and delivery, with quality products/services and satisfied recipients.

Among some of the 12 principles that define this methodology (Agarwal, 2019), the following stand out developing projects around motivated individuals by creating a trusting environment that supports the necessary collaborators for the execution of different tasks and trusts them to do the work; giving priority to a face-to-face conversation as the most efficient and effective method of transmitting information to and within a development team; regularly measuring the progress of work done; maintaining a constant and sustainable development pace indefinitely; maintaining process simplicity; reflecting and regularly adapting behaviour for continuous improvement. By following these guiding values and principles (among others), the team prioritizes flexibility and adapts to change in an uncertain environment of constant change. The main differences between Agile methodology and traditional HR practices can be summarized in:

Iterative Approach: Agile HR breaks down HR processes into smaller, manageable increments, allowing for continuous improvement and adjustment. Traditional HR practices, on the other hand, often involve rigid, inflexible processes that are difficult to change.

Collaboration and Cross-Functional Teams: Agile HR strongly encourages bringing together individuals with diverse skills and expertise to work on projects. Traditional HR practices often involve siloed departments and a hierarchical structure.

Customer Focus: Agile HR places a strong emphasis on understanding and meeting the needs of employees and stakeholders, treating them as "customers", while traditional HR usually prioritize the needs of the organization over the needs of their employees.

Continuous Feedback and Improvement: Agile HR promotes regular feedback and evaluation to identify areas for improvement and make necessary adjustments. Traditional HR practices may rely on annual performance reviews and infrequent feedback.

Adaptability and Flexibility: Agile HR can quickly respond and adapt to new situations and requirements. Traditional HR practices may be slow to change and resistant to new ideas.

In summary, Agile HR is designed to be more responsive, adaptive, and people-centered, while traditional HR practices may be more rigid and hierarchical.

Downsizing versus Rightsizing

Workforce reduction has become a popular human resource management practice over the last few decades, and according to Lean philosophy, one of the possible approaches for streamlining operations to reduce waste is to cut unnecessary labour that does not add value. However, its application does not always result in positive impacts on the organization, and the “saved” costs may not materialize into additional innovation (Mellahi and Wilkinson, 2010).

In the last decade, unprecedented levels of workforce reduction have been witnessed in many industrialized countries, and few organizations have not undergone some form of downsizing in restructuring processes (Brockner et al., 1987; LeCun et al., 2015; Amabile and Conti, 1999; Jalajas and Bommer, 1999). When a company is already in crisis, this technique is often a viable solution, although it is considered a negative measure as it is often associated with layoffs, causing frustration, uncertainty, and even indignation among employees (Chadwick et al., 2004).

In a structure such as the military institution, the challenges for competitive productivity also include an overload of human resources or a repetition of services in different branches of the armed forces, among other factors. Often, there is an inverse relationship between quantity and quality, which in certain areas of special relevance such as cybersecurity can have disastrous consequences. Thus, the proposed restructuring for certain structures such as the one addressed in this paper should involve rightsizing approaches instead of mere cost reduction. It should be understood that Lean philosophy does not advocate blind reduction of resources with a view to optimization but rather the elimination of waste. Is it more wasteful of time and resources to invest in and train an individual for a key position for years and then lose them to another organization? The high direct and indirect costs of turnover in organizations are well-known to human resource managers. On the other hand, rightsizing aims to prevent crisis scenarios rather than being a response to an already installed scenario. It is a proactive, not reactive, approach that seeks to adjust available human resources not only to meet immediate needs but also to project future needs. In a department responsible for the cybersecurity of the armed forces, with the importance that this may represent at the level of Portuguese national security, reducing staff as a reactive response to crisis times cannot continue to be the answer (Dougherty and Bowman, 1995; Freeman, 1994).

This is an area of the utmost importance, where specialized training must be top-notch, where quality standards must be met daily as a work philosophy, and not just as compliance with audits. Combining these factors with an area where turnover reveals low remuneration and absence of prospects or career advancement as main reasons, more than an oversizing problem of teams, the military institution frequently faces impoverished teams that are poorly updated in training and dispersed across different branches to perform often-similar procedures with different designations.

The proposal presented here is to create a single central cybersecurity management area, divided into distinct areas only when and for specific area requirements. A crisis management approach that is transversal to different branches and highly specialized teams that divide their time between constant work and training. Far from duplicating positions, there will be a permanent action force to ensure personnel failures (vacations, absences, and sick leave) while constantly training in the latest cybersecurity technologies and methodologies. The investment in constant training of staff could prove to be a factor of commitment between the parties, accompanied by a sense of purpose to serve the country with the best possible technical conditions.

Cybersecurity in the Armed Forces (FFAA)

Current Structure

The Strategic Directive of the Portuguese General Staff of the Armed Forces (EMGFA) for 2021-23 is the structuring document that establishes the strategic objective of strengthening priority joint capabilities and defines a line of action to reinforce Cyber Defense, with a focus on the training and retention of human resources, doctrinal and technological consolidation, and the increase of interoperability. This work aims to summarize the legislative framework, and the developments in the doctrinal field of NATO and the European Union (EU), attentive to the metamorphosis of society and all its surroundings in the coming years (Marinos, 2019).

Thus, currently, the creation of a Cyber Defense Corps is under study within the General Staff of the Armed Forces (EMGFA), which integrates elements of the Computer Incident Response Capability (CIRC) of the EMGFA and the branches (Navy, Army, and Air Force), which constitute the Cyber Defense Operations Command for the consolidation of a national strategy to respond to cyber threats. Additionally, a School and a Data Center are created. These are articulated and shared information with the National Cybersecurity Center (CNCS).

Strengths and Weaknesses

Given the current context, it is considered essential to restructure the higher structure of the state system to face current and future cyber threats. On the one hand, new generations seem to be developing a greater capacity to deal with emerging technological challenges, but on the other hand, it is important to ensure that the most relevant bases of technology and ethical principles are preserved so that changes are better accepted.

Characterizing work processes faces enormous challenges due, essentially, to the fear of changes at all levels of hierarchical structures. It is easier to keep things as they are. And changes always cause some disruption and service performance breaks, which is why the creation of pilot projects and task forces is proposed to validate all procedures in a secure environment. The adoption of new and challenging methodologies such as Agile would allow for continuous process improvement, thus keeping up with technological advancements, both in hardware and software programming, creating unique opportunities to “shake up” the culture and status of current social compliance, which prevents the renewal and anticipation of threats to weaker democratic states and the general population.

Restructuring Process Proposal with Task Forces

Starting from the structures of the General Staff of the Armed Forces and the branches, with the creation of the Cyber Defense Corps, the formation of Task Forces should be implemented, initially, as pilot teams with broader objectives than the regular structures, with the ability to react to new threats and events that require extraordinary measures and that may affect the integrity of the State and/or the population. Guidelines should, as far as possible, follow Agile methodologies, to reduce response times to threats and the number of personnel involved. In general, processes should be more efficient, both in financial terms (costs) and operational terms (mission fulfilment).

Nonetheless, any implementation of one or more Lean techniques (including the Agile methodology) assumes the existence of a continuous improvement team, specifically trained for this purpose and dissolved after a predetermined period or once the expected results are achieved (whichever comes first). From a review of the literature, a conceptual implementation model can be described in the following stages: The selection of the activity(ies) to be intervened in usually takes one of four forms. It can result from a careful analysis of the entire process, hierarchical indication, the need for organizational restructuring, or even employee suggestions. Once the activity/area is decided, the "project" is defined and a team member is appointed to lead it. This is the person who shares the project status with the rest of the team and decides on the next steps.

With the formation of the change agent team and the definition of the project, the Preparation Stage begins. In addition to the leader, who works closely with the activity coordinator and is responsible for implementing all initiatives in the field, the team includes production elements that collaborate in finding solutions and implementing them effectively in daily practice. Whether or not they perform the role of leader, the team must have a connection to the intervened area. The existence of this element is crucial as any improvement process does not work in the field if it is not receptive to change. It also requires total commitment from all those who are part of the tasks or activities being optimized and who will ultimately be directly responsible for maintaining that optimization.

In this case, this change agent team should incorporate the maximum responsible officials of all "similar" areas in the different branches of the Armed Forces, so that together with the leader, they could arrive at a unique structural model, capable of responding to all needs. Once the preparation stage is completed, the Diagnostic Stage begins, in which an assessment of the state of the art is made, including the definition and KPIs (Key Production Indicators) that represent the current process performance. In the next stage, the "new" process is designed, changing everything that represents a positive impact on the previously identified indicators. A transformation plan is driven by everyone with a view to the desired changes, followed by its effective implementation.

With the implementation of the transformation plan, the Implementation Stage defines verification or validation dates for the functioning of the "new" process, where the KPIs are re-estimated and compared with the corresponding initial indicators. If the results are satisfactory, the project is considered complete, and the improvement team is dissolved or changed to a new project (and consequently, some of its members). Otherwise, the previously planned solution is restructured. When the solution found can have applicability in another area, the key elements in the team (representatives of the area in question) are replaced, and the implementation phase of the transformation plan is repeated.

Despite the performance improvement and cost reduction scenario, all organizations face risks when embracing a project of this size, and its impact - when not properly anticipated, and the teams not adequately informed and motivated - can be fatal and seriously damage the operational stability of processes and eventually result in serious setbacks throughout the operation.

Expected Return

It is difficult to quantify the expected value of adopting the Lean philosophy in the context of the Armed Forces, particularly in the area of Cyber Defense. However, there are high expectations, as option ZERO, of not advancing, could create a very high-risk exposure, given that certain states have invested in and operated concerted and well-crafted cyber-attacks intending to alter the world order. Adopting these models would allow for constant verification of the state of measures, making it possible to correct their developments. Thus, the greatest return is expected to come from the training of its members and the generation of a new culture of efficiency and technical knowledge.

Conclusions

The Agile methodology, among many other Lean tools, is proven to be a technique that adapts to various work processes and allows for almost constant evolution, which is considered useful for government agencies and, in this particular case, for the Armed Forces. Culturally, enormous challenges will be required to overcome some barriers that impose changes in behaviours and expectations that will improve the functioning of various structures, allowing for the assurance of vital goods and services.

In conclusion, adopting the Lean philosophy in the context of the Armed Forces is expected to result in the training of its members and the creation of a new culture of efficiency and technical knowledge. However, it is important to note that all organizations face risks when embracing a project of this magnitude, and its impact can be fatal and seriously damage the operational stability of processes, resulting in serious setbacks throughout the operation. Therefore, an effective implementation should always consider different phases and contingency plans to mitigate any setbacks in the process.

Limitations of the Study

The development of this work took place in a very particular context of security or threat - the exit from a pandemic state with all the underlying limitations and the invasion of Ukraine by the Russian army and other conflicts with an emphasis on the disruption of infrastructures and entities through cyber-attacks. Such events led to the suspension of work several times, with some planned meetings canceled and not rescheduled due to difficulties in coordinating the schedules of those involved.

Additionally, the scope of the topic proved to be a challenge in that delving deeper into each topic addressed here would in itself require an extensive report. Therefore, the authors consider that different perspectives were left unexplored and specialized opinions from current experts, should be considered in future developments in this area.

Competing interests

No competing interest is declared.

Author contributions statement

Both authors wrote and reviewed the manuscript.

Acknowledgments

The authors thank the anonymous reviewers for their valuable suggestions. This work isn't supported by any funds.

References

1. Agarwal, A., 2019. *The Basics Of Agile and Lean – Develop an Agile Mindset and Lean Thinking*. Amazon Digital Services LLC - KDP Print US.
2. Ahmad, A. et al., 2020. *How the integration of cyber security management and incident response enables organizational learning*. Journal of the Association for Information Science & Technology, 71(8), 939–953.
3. Amabile, T.M. and Conti, T., 1999. *Changes in the work environment for creativity during downsizing*. In Academy of Management Journal, 42(6):630–640.
4. Askin, R.G. and Goldberg, J.B., 2001. *Design and Analysis of Lean Production Systems*. Wiley. ISBN: 9780471115939.
5. Boeke, S., 2017. *National cyber crisis management: Different European approaches.* Governance, 31.
6. Brockner, J. et al., 1987. *Self-esteem and reactions to negative feedback: Toward greater generalizability*. Journal of Research in Personality, 21(3), 318–333.
7. Cardash, S.L. et al., 2013. *Estonia's Cyber Defence League: A Model for the United States?* Studies in Conflict & Terrorism, 36(9), 777–787.
8. Chadwick, C. et al., 2004. *Effects of downsizing practices on the performance of hospitals*. Strategic Management Journal, 25(5):405–427.
9. Dougherty, D. and Bowman, E.H., 1995. *The effects of organizational downsizing on product innovation*. In California Management Review, 37(4), 28–44.
10. First National Toyota, 1998. McKinsey Quarterly.
11. Freeman, S.J., 1994. *Organizational Downsizing as Convergence or Reorientation: Implications for Human Resource Management*. Human Resource Management, 33(2), 213–238.
12. Garza-Reyes, J.A. et al., 2022. *Deploying Kaizen events in the manufacturing industry: an investigation into managerial factors*. Production Planning & Control 33.5, pp. 427–449. DOI 10.1080/09537287.2020.1824282.
13. Haque, B., 2003. *Lean engineering in the aerospace industry*. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture 217.10, pp. 1409–1420. DOI: 10.1243/095440503322617180.
14. Jalajas, D.S. and Bommer, M., 1999. *The influence of job motivation versus downsizing on individual behaviour*. Human Resource Development Quarterly, 10(4):329–341.

15. Khadem, M. et al., 2006. *Efficacy of Lean Metrics in Evaluating the Performance of Manufacturing Systems*. International Journal of Industrial Engineering-theory Applications and Practice 15, pp. 176–184.
16. Klimburg, A., 2012. *National cyber security framework manual*. Tallinn, Estonia: NATO CCD COE.
17. Koskela, L., 1992. *Application of the New Production Philosophy to Construction*. Technical Report No. 72, Center for Integrated Facility Engineering, Department of Civil Engineering, Stanford University.
18. Kroger, J., 2020. *Education for Seapower Strategy 2020*. Naval War College Review, 73(3).
19. LeCun, Y. et al., 2015. *Deep learning*. Nature, 521(7553):436.
20. Marinos, N., 2019. *CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*. GAO Reports.
21. Mellahi, K. and Wilkinson, A., 2010. *Slash and burn or nip and tuck? Downsizing, innovation, and human resources*. International Journal of Human Resource Management, 13(21), 2291–2305.
22. Okay-Somerville, B. and Scholarios, D., 2019. *A multilevel examination of skills-oriented human resource management and perceived skill utilization during a recession: Implications for the well-being of all workers*. Human Resource Management, 58(2), 139–154.
23. Pfau, B.N. and Kay, I.T., 2002. *The Human Capital Edge: 21 People Management Practices Your Company Must Implement (or Avoid) to Maximize Shareholder Value*. McGraw-Hill.
24. Pricopi, M., 2012. *Military Integration - A Fundamental Condition for European Security and Stability*. Revista Academiei Fortelor Terestre, 17(2), 122–127.
25. Reynolds, B., 2019. *What Do People Want from Work? The Simple Question that Can Transform Unit Engagement and Retention*. Air & Space Power Journal, 33, 4–18.
26. Sercan, D. and Paksoy, T., 2021. *Lean management tools in the aviation industry: New wine into old wineskins*. International Journal of Aeronautics and Astronautics 2.3, pp. 77–83.
27. Sinha, N. and Matharu, M., 2019. *A Comprehensive Insight into Lean Management: Literature Review and Trends*. Journal of Industrial Engineering and Management 12.2, pp. 302–317. DOI: 10.3926/jiem.2885
28. Spalevi’c, Z., 2014. *Cyber Security as a Global Challenge of The Modern Era*. Sinteza 2014 - Impact of the Internet on Business Activities in Serbia and Worldwide, 687–692.
29. Tagarev, T. et al., 2021. *AI-driven Cybersecurity Solutions, Cyber Ranges for Education & Training, and ICT Applications for Military Purposes*. Information & Security, 1, 5–8.
30. Wilson, L., 2009. *How To Implement Lean Manufacturing*. McGraw-Hill Education. ISBN: 9780071625081. URL: https: / / books. google. es/books? id = gJFJ1A7aR-8C.
31. Womack, J.P. et al., 1991. *The Machine that Changed the World: The Story of Lean Production*. USA.
32. Womack, JP. Et al., 2007. *The Machine That Changed the World: The Story of Lean Production*. Free Press. ISBN: 9781416554523.
33. Woollaston-Webber, V., 2017. *The NHS trusts and hospitals affected by the Wannacry cyberattack*. WIRED.
34. Zetter, K., 2016. *Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid*. WIRED.