Machine Translated by Google
RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.
Year I, v.2 2021. | Submission: October 11, 2021 | Accepted: October 13, 2021 | Publication: October 15, 2021

Integration between Military Doctrine and Private Security: A Study on Models of Risk Management in Corporate Environments

Integration between Military Doctrine and Private Security: A Study on Risk Management Models in Corporate Environments

Author: Rodrigo Hipólito Menezes de Araújo.

Graduated in Law from ULBRA - Lutheran University of Brazil.

Postgraduate student in Public Law at the University of Amazonas - UEA

Summary

Corporate security in the contemporary world faces increasingly complex challenges, demanding sophisticated and adaptable risk management models. In this context, the integration of military doctrine and private security emerges as a strategic proposal, since experiences gained in military operations at borders, in jungle warfare, in migration crises, and in prison rebellions offer a solid foundation for the development of advanced protection protocols. This scientific article seeks to analyze how principles of strategic planning, operational intelligence, and military discipline can be adapted to the corporate environment, increasing organizational resilience in the face of internal and external threats. The study also addresses the legal and ethical limitations of this transposition and proposes pathways for integrated risk management, based on real-world examples and consolidated practices in the defense sector.

Keywords: Private Security; Military Doctrine; Risk Management; Corporate Protocols; Organizational Resilience.

Abstract

Corporate security faces increasingly complex challenges in today's world, requiring sophisticated and adaptable risk management models. In this context, the integration between military doctrine and private security emerges as a strategic proposal, since experiences gained in military operations on borders, in the jungle, in migration crises, and in prison uprisings provide a solid foundation for the development of advanced protection protocols. This scientific article seeks to analyze how principles of strategic planning, operational intelligence, and military discipline can be adapted to the corporate environment, enhancing organizational resilience in the face of internal

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

and external threats. The study also addresses the legal and ethical limitations of this transposition and proposes pathways for integrated risk management, based on real examples and consolidated practices in the defense sector.

Keywords: Private Security; Military Doctrine; Risk Management; Corporate Protocols; Organizational Resilience.

1. Fundamentals of Military Doctrine and its Relevance to Private Security

Military doctrine is a body of knowledge and practices that guides the actions of armed forces in situations of peace, conflict, and crisis. It is based on solid principles of hierarchy, discipline, command and control, as well as consolidated methodologies for scenario analysis and strategic planning. These fundamentals have been developed over centuries of wars, military campaigns, and field experience, giving them a unique value for applicability in complex and high-risk situations. In the context of private security, which faces daily threats such as property invasions, corporate espionage, cybercrimes, and sabotage, the adoption of this doctrine allows for the construction of a robust prevention and response system. The military logic of anticipating enemy movements and structuring alternative plans is directly compatible with the need for companies to protect themselves in a competitive and volatile environment.

Another essential aspect of military doctrine is the importance of discipline and constant training. Military personnel are trained to act under extreme pressure, maintaining rationality and following established protocols, even in chaotic situations. This difference translates, in private security, into highly trained teams prepared to handle incidents of different natures. As Huntington (1996) argues, military professionalization is directly related to the development of leadership skills, rapid decision-making, and resource management under constraint. When such competencies are applied in private companies, standardized and efficient security protocols are created, which reduce the margin of human error and strengthen organizational resilience in the face of crises.

Hierarchy, often criticized in civilian environments, is another element that proves relevant in the field of private security. In critical operations, clarity about who makes decisions and who executes actions ensures fluidity, avoids internal conflicts, and guarantees the effectiveness of the response. In the business sector, where risky situations demand decisions in seconds, this hierarchical model inspired by militarism proves indispensable. According to Janowitz (1971), the cohesion and discipline of a military organization allow it to function as a single organism, even in stressful situations. By adapting this logic to private companies, a structure is obtained in which security professionals act in a coordinated and predictable manner, increasing operational efficiency.

Military doctrine also values the concept of strategic intelligence, that is, the collection and analysis of information to support decision-making. This practice, applied in border military campaigns,

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Whether in jungle or urban operations, it is equally vital for private companies that need to monitor external and internal threats. Predictive risk analysis, now performed with big data software and artificial intelligence, finds its parallel in military intelligence reports that guide preventive actions. As Baylis, Smith, and Owens (2011) point out, success in military operations is directly related to the quality of available information, and the same principle can be applied to the protection of corporate assets.

Another important foundation is logistics management, a pillar of military doctrine that ensures the supply of troops in any scenario. In the business field, private security logistics involves everything from team management to the provision of technological and human resources in strategic locations. Just as a war can be lost due to logistical failures, a company can compromise its operation if it does not adequately structure its security protocols. In this sense, the military lesson is clear: it is not enough to have a contingency plan; it is necessary to guarantee effective means for its execution. This vision expands the responsiveness of companies and strengthens the concept of business continuity.

Furthermore, military doctrine carries a notion of mission that goes beyond the simple execution of tasks. Military personnel are trained to understand the strategic objectives behind their actions, ensuring greater engagement and commitment to results. In the corporate environment, this model can be translated into an integrated security culture, in which all employees understand that asset protection and risk management are collective responsibilities. According to Mintzberg (2009), organizations that cultivate strong values and shared goals are more resilient in the face of crises, a principle that aligns directly with the military logic of cohesion.

Another point worth highlighting is adaptability, a central characteristic of modern military doctrine. Troops in the field need to adjust strategies in the face of sudden changes in the environment, such as climate change, new enemy tactics, or communication failures. This learning proves valuable in the private sector, where companies face emerging risks such as sophisticated cyberattacks, reputational crises on social media, and regulatory changes. The military mindset of "improvise, adapt, and overcome" translates into flexible corporate protocols capable of responding quickly to adversity without compromising the continuity of operations.

Finally, it is important to emphasize that the transposition of military doctrine to private security should not be done mechanically or uncritically. There are fundamental differences between the military and corporate environments, especially in terms of legality, proportionality in the use of force, and social expectations. In this sense, it is up to the security manager to adapt military practices to the demands of the private sector, respecting legal and ethical limits. Authors such as Creveld (1991) remind us that war and security cannot be understood solely as tactical actions, but also as social and political phenomena. This warning should guide the construction of

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Hybrid models that leverage the strengths of military doctrine but adapt them to the specific context of private companies.

2. Experiences in Border Operations and their Application in Corporate Environments

Military operations conducted along borders represent one of the most challenging scenarios for the armed forces. In these regions, the military faces adverse conditions that combine geographical, political, and social elements. The work carried out in these environments requires constant vigilance, the use of monitoring technology, interaction with local communities, and, above all, inter-institutional cooperation with national and international bodies. This set of practices makes it possible to deal with varied threats, such as the smuggling of goods, drug and arms trafficking, irregular immigration, and even situations of transnational terrorism.
When applied to the corporate environment, such experiences offer a robust foundation for the development of private security protocols capable of anticipating risks and ensuring the operational continuity of companies operating in vulnerable contexts.

In the business world, especially in multinational corporations, operating in unstable countries or regions bears a strong resemblance to the challenges faced in border operations.
Companies operating in global supply chains or maintaining branches in geopolitically high-risk areas need to deal with constant uncertainties, such as regulatory changes, transport blockades, local political pressures, or social instabilities. The doctrine acquired in border operations allows for the creation of internal monitoring mechanisms, similar to military intelligence systems, aimed at identifying and neutralizing risks before they become crises. Thus, military practices become strategic tools for governance and organizational resilience, reinforcing the role of private security as a pillar of corporate sustainability.

Experience at the border also reinforces the importance of integration between different forces, such as the army, federal police, and intelligence agencies. This synergy, adapted to the private sector, can be observed in the cooperation between security, compliance, information technology, and legal departments. According to Baylis and Wirtz (2015), the effectiveness of international security is directly linked to the articulation between different actors, and this lesson extends to business organizations, which need to create intersectoral protocols. In the corporate environment, isolation between areas represents a significant vulnerability, since communication failures can compromise the response to incidents. Thus, drawing inspiration from the military logic of the border means developing internal cooperation structures that eliminate organizational silos and favor integrated decision-making.

Another essential element inherited from border operations is the use of technology as a fundamental ally. Reconnaissance drones, heat sensors, satellite systems, and georeferencing software are already part of the military routine in these regions. In the private sector, technologies

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Similar technologies are being incorporated, such as video surveillance systems with artificial intelligence, facial recognition, and predictive analytics platforms. These resources allow for the identification of anomalies in real time and increase the efficiency of security teams. As Gartzke (2007) points out, technology is now a power multiplier in the field of security, both state and private, and its strategic use is indispensable for mitigating risks in global organizations.

Beyond technology, border operations offer lessons in human resource management in high-pressure environments. In these missions, military personnel need to maintain troop morale, manage grueling schedules, and preserve the physical and psychological health of soldiers. This learning is extremely valuable for private companies that employ professionals in adverse contexts, such as regions with high crime rates or operations during critical hours. By adapting military logic, corporate managers can implement intensive training programs, mental health monitoring, and team rotation protocols, ensuring greater operational efficiency and reducing risks associated with the human factor.

Another relevant aspect concerns the cultural and social sensitivity present in military operations on borders. Often, the success of the mission depends on the ability to interact with local communities, understand their demands, and reduce social tensions. This practice, when adapted to private companies, translates into corporate social responsibility policies that contribute to mitigating reputational risks and strengthening institutional legitimacy. According to Nye (2004), soft power is as important as coercive power, and in the private sector this translates into building solid relationships with local stakeholders, which can be decisive in times of crisis.

It is also important to highlight that border operations teach how to deal with unpredictability, since unexpected events, such as intense migratory flows or actions by criminal groups, can occur at any time. This logic of unpredictability is equally present in the global market, subject to financial crises, changes in legislation, and political instability. Applying a military mindset in this context allows private companies to develop more realistic contingency plans and flexible response protocols, capable of minimizing losses and ensuring business continuity. Thus, unpredictability ceases to be an absolute threat and becomes a factor of strategic resilience.

Finally, the integration of lessons learned from border military operations with corporate practice must be conducted critically and adapted to the legal requirements of the private sector. While the military can operate with greater leeway in the use of force and state authority, private companies must respect labor, civil, and criminal laws that restrict their operations. Therefore, it is up to the security manager to interpret military principles, adjusting them to the business context and balancing operational efficiency with legal compliance. This transposition not only strengthens corporate security protocols but also enhances the credibility of companies with clients, shareholders, and regulatory authorities.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

3. Jungle Operations and the Adaptation of Strategies to the Private Sector

Military operations in the jungle represent some of the most hostile and challenging environments for any armed force. In these regions, combatants face not only human enemies but also natural threats such as wildlife, tropical diseases, difficult terrain, and adverse weather conditions. Survival and success in such operations depend on a specific set of tactical skills, meticulous planning, and a resilient mindset. When these experiences are applied to the private sector, especially in companies operating in complex and unstable environments, a clear parallel emerges: the need for rapid adaptation, efficient use of limited resources, and constant monitoring of the external environment. The logic of the jungle, where small failures can result in major tragedies, inspires the creation of much more rigorous and realistic corporate safety protocols.

One of the main lessons learned from jungle operations is the importance of preparation and specialized training. Military personnel operating in these scenarios undergo intensive programs in survival, navigation, physical and psychological endurance, as well as camouflage and ambush techniques. This preparation ensures that, in the face of any unforeseen event, soldiers are able to react with discipline and efficiency. In private companies, this can be translated into recurring training for security teams, evacuation drills, fire prevention programs, first aid training, and protocols for responding to technological emergencies, such as cyberattacks. According to Salas et al. (2006), highly trained teams exhibit greater cohesion, a lower failure rate, and a greater capacity for decision-making under pressure —fundamental characteristics in both the military and corporate environments.

Another essential aspect inherited from jungle operations is the notion of adaptive logistics. In regions where access is limited and resources are scarce, the military needs to improvise solutions to ensure the supply of food, ammunition, medicine, and equipment.
This mindset of logistical flexibility can be applied to the private sector in the form of resilient supply chains, capable of adapting quickly to unexpected disruptions or crises.
Companies that rely on single suppliers or operate in hard-to-reach regions can apply military lessons regarding route diversification, strategic inventory, and alternative transportation options, minimizing the risk of operational disruption.
In this sense, the jungle teaches that one should not depend on a single path or resource, but rather structure redundant systems capable of sustaining the mission even in adverse scenarios.

Adaptability is also evident in team management. In jungle operations, leadership needs to be able to inspire confidence, make quick decisions, and maintain high morale, even in the face of extreme hardship. This resilient leadership skill is equally necessary in the private sector, especially in companies undergoing organizational crises, structural changes, or financial restructuring. The leader, like a military commander, needs to balance firmness with sensitivity, conveying security to subordinates while striving for success.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Practical solutions to problems. As Yukl (2013) argues, leadership in crisis contexts is marked by the ability to communicate a clear vision, make decisions under uncertainty, and maintain team motivation—principles aligned with the logic of military operations in hostile environments.

Another relevant point is the emphasis on teamwork and the interdependence of group members. In the jungle, each soldier depends directly on the competence and vigilance of their comrades, and the failure of one can compromise the safety of all. This model of collective cohesion, when applied to private companies, translates into the need to create an organizational culture where security is not just the responsibility of a specific department, but a collective commitment. Awareness programs, educational campaigns, and integrated security policies reinforce the idea that each employee is a key player in protecting company assets. Thus, the logic of military interdependence inspires corporate practices that increase collective vigilance and reduce internal vulnerabilities.

Furthermore, experience in jungle operations highlights the importance of environmental intelligence.
Military personnel constantly need to interpret signals from nature, from wildlife behavior to subtle climate changes, to anticipate risks and ambushes. This ability to read the environment can be applied to the private sector through data analysis, market trend monitoring, and the use of predictive tools. Companies that can proactively interpret these external signals are better able to anticipate economic crises, identify competitor moves, and adapt their security strategies. As Porter (1999) points out, competitive advantage is directly related to the ability to interpret the environment and act proactively, a principle already established in jungle military practices.

Another key lesson concerns psychological resilience. Operating in conditions of isolation, deprivation, and constant threat requires military personnel to possess a mental resilience far above average. In the private sector, security professionals, risk managers, and even executives face similar pressures, albeit in different contexts, such as long hours, critical decisions, and a high level of responsibility. Resilience development programs, inspired by military training, can help companies prepare their employees to handle intense pressure without compromising the quality of their decisions. According to Bonanno (2004), resilience is a determining factor in maintaining performance in stressful situations, and its corporate application can represent a strategic advantage.

Finally, it is important to highlight that the transposition of jungle experiences to the private sector should not be literal, but adaptive. While in the military field physical survival is the central objective, in the corporate environment the goal is business continuity and asset protection. However, the logic of resilience, adaptability, leadership, and strategic intelligence remains the same, only adjusted to new legal and social parameters. In this way, jungle operations not only offer a repertoire of techniques useful for private companies, but also a

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

A mindset model that values preparation, discipline, and the ability to thrive in uncertain and challenging environments.

4. Crisis Management in Prison Riots and its Relevance to Private Security

Prison riots are among the most complex and risky events for security forces, as they involve a set of variables including extreme violence, delicate negotiations, public opinion pressure, and the need to preserve lives. In such situations, military or police action is frequently activated in support of prison administrations, which demands strict protocols for containment, negotiation, and regaining control. The experience accumulated in riots offers valuable lessons for the private sector, especially regarding crisis management in highly critical corporate environments, such as energy companies, banks, hospitals, and airports. The logic is similar: there is a collapsing environment, divergent interest groups, risks to physical and property integrity, and the urgent need to restore order with the least possible damage.

One of the main lessons learned from prison riots is the importance of preventative intelligence. Many riots, as Adorno and Salla (2007) point out, could be avoided through more robust monitoring systems, identification of criminal leaders, and tracking of internal tensions. In the corporate environment, this translates into periodic audits, communication channels for detecting dissatisfaction, and the use of data analysis tools that allow for the identification of risk patterns before they materialize. Just as in a prison, where small signs can precede a major crisis, companies also have vulnerability indicators that, if correctly interpreted, can prevent major collapses. This preventative culture, inspired by military logic, strengthens internal compliance and corporate security mechanisms.

Another crucial lesson learned from rebellions is the role of leadership in times of chaos. In the prison system, when a rebellion occurs, the absence of clear leadership can result in misguided decisions, escalation of violence, and increased damage. In private companies, crisis situations such as cyberattacks, executive kidnappings, or industrial sabotage require leaders capable of remaining calm, conveying security, and coordinating effective responses. As highlighted by Boin et al. (2005), crisis management requires leaders who can simultaneously provide immediate responses and plan long-term solutions. Military experience in rebellions demonstrates that prepared leaders can transform chaos into an opportunity for institutional strengthening, while unprepared leaders tend to exacerbate the crisis.

Negotiation is another key element. In rebellions, resolution often comes through mediation between criminal leaders and authorities, requiring a balance between firmness and diplomacy.
This logic also applies to the private sector, where security crises often involve multiple stakeholders, such as shareholders, customers, suppliers, the press, and regulatory bodies. The ability to negotiate under pressure, while maintaining institutional principles and at the same time

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Avoiding greater harm is a skill derived from military and police experience in extreme contexts. According to Fisher and Ury (1991), principled negotiation—which seeks to address essential interests without abandoning structural values—is the most effective in conflict environments.

Another lesson learned from prison riots is the importance of communication. The absence of a clear communication strategy, both internally and externally, can generate rumors, panic, and loss of institutional credibility. In the military field, teams are trained to manage information strategically, avoiding contradictions and ensuring troop cohesion. In private companies, crisis communication must be equally planned, with trained spokespeople, transparent messages, and well-defined official channels. As Coombs and Holladay (2010) argue, crisis communication is as important as the operational response, as it preserves reputation and maintains stakeholder trust even in the face of adversity.

Logistics management also proves essential during riots. Maintaining supplies, perimeter control, evacuating the wounded, and mobilizing reinforcements are critical aspects in prison collapse situations. This learning can be applied in the private sector in the form of contingency plans to ensure the continuity of critical operations. Transportation, energy, and telecommunications companies, for example, cannot interrupt their services even in crisis situations, under penalty of generating social collapses. The military logic of anticipating support resources, alternative routes, and strategic stockpiles translates into corporate protocols that ensure operational resilience in times of instability.

Furthermore, prison riots demonstrate the need for integration between multiple institutions. No crisis of this magnitude is resolved in isolation: police, firefighters, medical teams, justice agencies, and even armed forces need to work together. In private companies, this translates into the importance of creating cooperation networks with suppliers, regulatory bodies, outsourced security companies, and local authorities. This integrated model

It expands response capacity and legitimizes actions taken in critical moments. As Comfort and Kapucu (2006) argue, interdependence between institutions is one of the pillars for the effective management of complex crises.

Finally, the experience gained from prison riots demonstrates that every crisis, however devastating, can be transformed into an opportunity for learning and institutional strengthening. In the private sector, security crises can be milestones for improving protocols, reassessing policies, and training teams. The military logic of post-action, based on detailed reports and failure analysis, is an example of how to transform negative experiences into sources of innovation and resilience. Thus, crisis management inspired by prison riots is not limited to putting out fires, but seeks to build organizations better prepared for the future.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

5. Migration Crises and the Development of Advanced Security Protocols

Migration crises represent social phenomena with a significant impact on both states and private institutions. They generally occur as a result of wars, economic crises, political persecution, environmental disasters, or social collapses, resulting in massive and disordered flows of people seeking better living conditions. In border regions, the military is frequently called upon to manage these situations, operating in screening posts, providing humanitarian aid, controlling borders, and often conducting containment operations to prevent confrontations. This experience is extremely relevant to the private sector, especially for companies that deal with intense flows of people, such as airports, hospitals, shopping centers, and large industries. The military logic applied to migration crises provides support for the development of protocols that guarantee security without neglecting human rights and international norms.

One of the main lessons learned from migration crises is the need to combine security measures with humanitarian actions. At borders, the military must deal with vulnerable populations, including women, children, and the elderly, while simultaneously combating potential threats such as the entry of criminals or infiltrated terrorist groups. This balance between protection and care can be transposed to the private sector, where companies face the challenge of maintaining security without compromising the well-being of clients and employees. According to Betts and Collier (2017), an efficient response to migration should integrate security and reception, a principle that can be applied to corporate crowd management protocols and emergency response at large events.

Another crucial aspect of migration crises is the importance of screening and risk classification.
Military personnel in the field conduct identification processes, document verification, health monitoring, and interviews to separate vulnerable groups from potential threats. This screening model can be adapted for private companies in contexts of large flows, such as airlines, financial institutions, and technology companies that handle a large volume of users. The use of technological tools, such as biometrics, artificial intelligence, and predictive analytics, allows for the identification of anomalies and the reduction of risks more efficiently. As Andreas and Snyder (2000) argue, intelligent surveillance is one of the pillars for the effective management of transnational flows, and this logic can be applied to the corporate environment.

Communication, both internal and external, also plays a central role in migration crises. In refugee camps or border crossings, information needs to be transmitted clearly, in different languages, and adapted to diverse audiences. This practice, when applied to private companies, reinforces the importance of crisis communication protocols that consider the cultural diversity of clients and employees. Multinational companies, for example, need to structure accessible and multilingual channels to guide audiences in emergency situations. According to Coombs (2007), clear and transparent communication is a

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

one of the most crucial elements for preserving trust during complex crises, in both public and private institutions.

Logistics management is also a valuable lesson from migration crises. Ensuring shelter, food, healthcare, and transportation for thousands of people in transit requires efficient coordination, prior planning, and strategic resources. This logistics model, adapted to the private sector, can be applied in situations of corporate evacuation, natural disasters affecting production units, or pandemics that disrupt supply chains. The military experience in creating alternative routes, emergency stockpiles, and inter-institutional partnerships serves as a guide for companies that wish to strengthen their resilience. According to Heaslip (2011), humanitarian logistics in migration situations provides valuable lessons for organizations seeking to improve their business continuity plans.

Another essential point is conflict management. In migration crises, the crowding of people in precarious conditions often results in tensions, disputes over resources, and even violent confrontations. In this context, military personnel are trained to apply crowd control techniques, conflict mediation, and the gradual use of force. These practices find parallels in private companies that manage large concentrations of people, such as stadiums, shopping centers, and corporate events. Training private security teams to handle crowds proportionally and strategically can prevent escalations of violence and protect the institutional image. As Reicher et al. (2004) remind us, the way authorities deal with crowds directly influences the level of cooperation or resistance, which also applies to the corporate environment.

Interinstitutional cooperation is another lesson learned from migration crises. No military force or government agency can handle the complexity of this phenomenon alone; coordination with NGOs, international agencies, and local communities is necessary. This logic can be applied to private companies in the form of strategic partnerships with suppliers, authorities, and civil society organizations, expanding the support network during times of crisis. Companies that build this type of network tend to provide faster and more effective responses in emergency situations. According to Kapucu (2006), network governance is one of the keys to organizational resilience in uncertain scenarios.

Finally, migration crises demonstrate that risk management cannot be limited to technical protocols, but must consider social, cultural, and political factors. The private sector, while drawing inspiration from military practices, must adapt these lessons to a context that values social responsibility and compliance with international law. Companies that treat crises merely as operational problems tend to lose legitimacy, while those that demonstrate social sensitivity and respect for human rights strengthen their institutional image. In this sense, the military logic applied to migration provides a basis for private companies to develop more humanized, integrated, and sustainable security models capable of balancing protection, efficiency, and social responsibility.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

6. Integration of Military Intelligence in the Private Sector

Military intelligence is one of the strategic pillars for success in defense operations, as it allows for the anticipation of threats, the analysis of vulnerabilities, and the creation of plans based on reliable data. Traditionally, this practice involves gathering information through surveillance, interceptions, undercover agents, and analysis of geopolitical scenarios. When applied to the private sector, the logic of military intelligence significantly expands the ability of companies to predict risks, protect assets, and prepare for contingencies. Private security, when based on intelligence systems, ceases to be reactive and becomes preventive, reducing costs and strengthening corporate resilience. Thus, the integration of military intelligence represents a competitive advantage in increasingly unstable and complex markets.

One of the central elements of military intelligence is the intelligence cycle, which comprises the stages of planning, collection, processing, analysis, and dissemination of information. This cycle, described by Lowenthal (2017), can be perfectly adapted to private companies, where risk management requires systematized information for decision-making. For example, in a multinational company, collection may involve monitoring social networks, analyzing local news, customer feedback, and internal audits. Processing and analysis allow this dispersed data to be transformed into strategic reports that assist corporate leadership.

Dissemination, in turn, ensures that the correct information reaches the appropriate department in a timely manner. This model, inspired by the armed forces, makes corporate security management more scientific and less intuitive.

Another relevant point is the use of advanced technologies to enhance intelligence work. In the military field, satellites, drones, encryption software, and big data systems are widely used. In private companies, these resources can be adapted in the form of electronic monitoring, information security software, predictive behavior analysis, and artificial intelligence applied to asset protection. As Zegart (2019) and Clarke (2017) point out, technology is no longer just a support tool, but an indispensable component for the effectiveness of intelligence in any sector. Companies that invest in risk analysis technology tend to reduce losses, anticipate crises, and protect their market reputation.

Counterintelligence is also a crucial aspect inherited from military doctrine. If, on the battlefield, the objective is to prevent the enemy from accessing strategic information, in the private sector the goal is to prevent industrial espionage, data leaks, and malicious infiltrations. Cases of corporate espionage, such as those observed in the technology and pharmaceutical sectors, demonstrate that the absence of counterintelligence mechanisms can compromise years of investment in research and development. Inspired by the military model, private companies can adopt secrecy protocols, vulnerability testing, and internal access monitoring, reducing the likelihood of insider attacks. This military learning strengthens not only information security but also the trust of clients and investors.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Another relevant lesson is scenario analysis. The armed forces are accustomed to working with multiple hypotheses, developing contingency plans for different situations, even those with low probability. This prospective reasoning model can be applied to private companies through methodologies such as risk scenario analysis, threat mapping, and the development of impact and probability matrices. According to Godet (2000), prospective analysis does not seek to predict the future absolutely, but to prepare institutions to react to different possibilities. By bringing this military logic to the corporate environment, security managers can structure more robust and realistic responses to emerging crises.

The integration of military intelligence into the private sector also reinforces the importance of cooperation. No military agency operates in isolation, and the exchange of information between different bodies is fundamental to building a comprehensive view of the threat. In the corporate sector, this logic can be adapted through partnerships between companies, trade associations, government agencies, and security service providers. The creation of shared intelligence networks allows for the identification of common threats, such as cyberattacks, fraud, and organized criminal groups. This cooperation model expands collective protection and strengthens the sector as a whole, rather than limiting security to fragmented solutions.

Another aspect inherited from military intelligence is the need for constant updating and learning. Threats change rapidly, whether in the military or corporate field, and outdated protocols can compromise overall security. Private companies, by incorporating military logic, need to invest in continuous training, technological updates, and periodic reviews of their security plans. This process ensures that corporate intelligence is not static, but dynamic, adapted to new challenges. As Castells (2010) reinforces, we live in the age of networked information, and only institutions capable of continuous learning can remain resilient.

Finally, it is important to highlight that adapting military intelligence to the private sector must consider legal and ethical aspects. While armed forces can use invasive and far-reaching methods, private companies need to respect privacy laws, labor rights, and international data protection standards, such as the LGPD in Brazil and the GDPR in the European Union. Therefore, it is up to the security manager to apply the principles of military intelligence in a way that is adjusted to the corporate environment, ensuring efficiency without infringing on rights. In this way, the integration of military intelligence strengthens private security, but also increases its legitimacy before society and its stakeholders.

7. Advanced Risk Management Protocols in Corporate Environments

Risk management protocols in corporate environments represent the practical consolidation of all military knowledge applied to private security. They are responsible for structuring preventive measures, establishing incident response flows, and ensuring business continuity.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Businesses thrive even in the face of severe crises. Military doctrine, throughout history, has demonstrated the importance of clear and replicable protocols capable of guiding actions in highly complex scenarios. In companies, this learning translates into corporate security plans that involve everything from vulnerability audits to disaster simulations, ensuring that all employees know exactly what to do in critical situations. As Kaplan and Mikes (2012) state, effective risk management does not eliminate uncertainty, but prepares organizations to respond with resilience.

A central aspect of risk protocols inspired by military logic is scenario-based planning. Just as troops in the field prepare different responses for offensives, ambushes, or strategic retreats, private companies need to structure action plans for diverse incidents, such as cyberattacks, financial crises, industrial accidents, or threats to the physical integrity of executives. The key difference in military experience lies in the discipline of constantly testing these scenarios, ensuring that the protocols are realistic and functional. In the corporate sector, this materializes in periodic training, penetration tests, internal audits, and evacuation drills. These practices, far from being mere exercises, strengthen the company's ability to react under real pressure.

Another essential element is the continuous analysis of vulnerabilities. Armed forces operate under the logic that no position is impenetrable, leading to the constant review of defenses and adaptation to the enemy. This principle, applied to companies, means periodically reviewing physical, digital, and organizational security systems, always considering that threats evolve. The use of methodologies such as ISO 31000 or COSO ERM, combined with the military mindset of constant vigilance, enhances the maturity of risk management. In this sense, companies stop treating security as a cost and begin to see it as a strategic investment, since failures can compromise financial and intangible assets, such as reputation and customer trust.

Risk communication is another fundamental point. In the military environment, the clarity of orders and the speed of information dissemination are crucial for the success of an operation. In the private sector, risk protocols should include internal and external communication strategies, ensuring that all levels of the organization are informed and prepared. This includes everything from communication with employees to relationships with the press, clients, and regulatory bodies. According to Coombs (2010), crisis communication must be transparent, precise, and timely, as the absence of clear information can generate panic, rumors, and irreversible damage to the institutional image. Therefore, corporate risk protocols should integrate communication as an inseparable part of the strategy.

Organizational resilience, inspired by military principles, is another structuring axis of corporate protocols. Armed forces are trained to operate even in adverse conditions, ensuring mission continuity regardless of obstacles. This philosophy, when transposed to companies, translates into business continuity plans.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Business Contingency Plans (BCP) and Disaster Recovery Plans (DRP). These instruments allow organizations to face crises without interrupting essential services, ensuring stability in critical moments. As Sheffi (2007) and Hiles (2010) point out, business resilience is directly related to prior preparation, and well-structured risk protocols represent the core of this preparation.

Another important aspect is the integration between departments. Military protocols work because all sectors of the force—logistics, intelligence, command, and operations—act in a coordinated manner. In the private sector, risk protocols are only effective when different areas, such as security, IT, legal, compliance, and communication, work in an integrated way. Companies that maintain isolated sectors tend to present fragmented and ineffective responses in crises. Therefore, risk management should be treated as a corporate responsibility and not as a task restricted to one department. This integrated vision ensures greater efficiency and legitimacy of the responses adopted in the face of internal and external stakeholders.

The application of technology in risk protocols is another point of convergence between military doctrine and corporate practices. Big data tools, artificial intelligence, predictive analytics, and blockchain can strengthen protocols by predicting attack patterns, identifying vulnerabilities before they are exploited, and recording data in an inviolable way. Just as the modern army cannot do without satellites and drones, companies cannot forgo advanced technological resources for risk management. According to Brynjolfsson and McAfee (2014), the digital age has transformed how organizations deal with threats, making the combination of human intelligence and automated response systems indispensable.

Finally, risk protocols inspired by military logic must consider not only the technical aspect, but also the human and ethical aspects. Modern armed forces recognize that missions cannot ignore the impact on civilians and on institutional legitimacy. Similarly, private companies need to align their protocols with values of ethics, social responsibility, and legal compliance. This means respecting regulatory standards, preserving labor rights, and ensuring that security measures do not compromise the dignity of employees or customers.
Thus, advanced risk management protocols, while increasing operational efficiency, strengthen the legitimacy and reputation of organizations in a highly competitive market.

Conclusion

This study sought to analyze how military doctrine, built from centuries of experience in extreme risk environments, can be integrated into private security for the development of advanced risk management protocols in corporate environments. The analysis covered diverse scenarios—from border and jungle operations to migration crises and prison riots—demonstrating that, although the military and corporate natures share similarities, these principles can be applied to private security.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Despite fundamental differences, both share the need for discipline, planning, adaptability, and resilience. The results suggest that the transposition of military practices, when properly adjusted to legal and ethical parameters, significantly strengthens the capacity of private companies to prevent, manage, and overcome crises.

One of the most relevant points identified was the centrality of **prevention.** In both military and corporate contexts, crises rarely occur without prior warning signs. Prison riots, migration crises, and border attacks could, in many cases, have been avoided with robust monitoring, intelligence, and communication systems. This lesson applies to private companies, which frequently underestimate small signs of dissatisfaction, operational failures, or technological vulnerabilities, allowing latent problems to turn into catastrophes. Thus, investing in preventive intelligence ceases to be optional and becomes an essential element for organizational survival.

Another important finding relates to **leadership in times of crisis.** The study demonstrated that military doctrine confers upon leaders distinct skills to operate in chaotic environments, inspiring confidence and maintaining team cohesion under extreme pressure. In the corporate sector, crises such as cyberattacks, internal sabotage, or logistical collapses require managers who combine firmness, rationality, and sensitivity. Management literature (Boin et al., 2005; Yukl, 2013) reinforces that effective crisis leadership is that which manages to balance the need for immediate responses with a long-term vision, a central characteristic of military commanders and highly applicable to the private sector.

Strategic communication has also proven to be a cross-cutting element, essential for both military and business operations. Experience in rebellions and migration crises has shown that the absence of clear information can exacerbate chaos, while transparent and well-targeted messages reduce tensions and preserve institutional legitimacy. In the private sector, risk communication should be seen as an inseparable part of crisis management, involving not only employees but also clients, suppliers, and regulatory bodies. By aligning with the military principles of clarity and timeliness, companies strengthen their credibility and avoid irreversible reputational damage.

The analysis also highlighted the role of **technology** as a power multiplier. Just as satellites, drones, and encryption systems have transformed military operations, artificial intelligence tools, big data, and blockchain are revolutionizing corporate security. The use of these technologies not only expands the ability to anticipate risks but also strengthens real-time operational response. Companies that understand this convergence between technology and security become better prepared to face emerging threats, whether physical or digital. In this sense, integrating the military mindset of constant technological modernization is vital for business competitiveness.

Another key point is the **importance of inter-institutional cooperation.** Border operations, migration crises, and prison riots have shown that no single institution is capable of...

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

Responding in isolation to large-scale challenges is not an option. The same applies to private companies, which must build support networks involving suppliers, associations, regulatory agencies, and even competitors in certain contexts. The logic of cooperation, inspired by military doctrine, enhances the resilience of the private sector and strengthens the collective capacity to confront systemic threats.

Ethics **and legality** emerge as central axes in adapting military doctrine to the corporate sector. While the military environment may operate with its own rules of exception, private companies are subject to labor, civil, criminal, and data protection laws. In this sense, the transposition of military practices must be judicious, ensuring that security protocols respect human dignity and are aligned with standards of social responsibility.

This compliance not only avoids legal sanctions, but also legitimizes the company's actions in the eyes of its stakeholders, reinforcing its institutional reputation.

Another element to highlight is **organizational resilience.** Military operations in jungles and hostile environments teach us that survival depends on the ability to constantly adapt to new threats. This mindset, applied to the private sector, implies the creation of business continuity plans (BCP) and disaster recovery plans (DRP) that ensure operation even in unstable contexts. Resilience, therefore, ceases to be a desirable characteristic and becomes a strategic prerequisite for organizations that aspire to longevity.

From an academic standpoint, this study contributes to broadening the debate on the **interdisciplinarity between public security, national defense, and corporate governance,** demonstrating that military knowledge is not limited to the field of warfare, but can be legitimately and effectively applied to the private sector. This perspective expands research horizons and stimulates the development of new risk management methodologies based on established practices, but adapted to contemporary demands.

In short, the integration of military doctrine and private security represents not only a viable alternative, but a growing necessity in a world marked by uncertainties, global threats, and complex crises. Companies that know how to adapt the lessons of military operations to their corporate reality will have a greater capacity to anticipate risks, protect assets, and sustain their competitiveness in turbulent markets. In this way, the critical and adapted transposition of the military mindset contributes not only to private security, but also to the strengthening of corporate governance and social stability.

References

ADORNO, Sérgio; SALLA, Fernando. **Organized crime in prisons and the attacks of the PCC.** *Estudos Avançados,* v. 21, n. 61, p. 7-29, 2007.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

ANDREAS, Peter; SNYDER, Timothy. **The Wall Around the West: State Borders and Immigration Controls in North America and Europe.** Lanham: Rowman & Littlefield, 2000.

BAYLIS, John; WIRTZ, James. **Strategy in the Contemporary World.** 5. ed. Oxford: Oxford University Press, 2015.

BAYLIS, John; SMITH, Steve; OWENS, Patricia. **The Globalization of World Politics: An Introduction to International Relations.** 5. ed. Oxford: Oxford University Press, 2011.

BETTS, Alexander; COLLIER, Paul. **Refuge: Transforming a Broken Refugee System.** London: Penguin, 2017.

BOIN, Arjen et al. **The Politics of Crisis Management: Public Leadership under Pressure.** Cambridge: Cambridge University Press, 2005.

BONANNO, George. **Loss, Trauma, and Human Resilience.** *American Psychologist,* vol. 59, n. 1, p. 20-28, 2004.

BRYNJOLFSSON, Erik; MCAFEE, Andrew. **The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies.** New York: WW Norton, 2014.

CASTELLS, Manuel. **The Network Society.** 8th ed. São Paulo: Paz e Terra, 2010.

CLAUSEWITZ, Carl von. **On War.** São Paulo: Martins Fontes, 1989.

CLARKE, Richard. **Cyber War: The Next Threat to National Security and What to Do About It.** New York: Ecco, 2017.

COOMBS, W. Timothy. **Ongoing Crisis Communication: Planning, Managing, and Responding.** 3rd ed. Los Angeles: SAGE, 2007.

COOMBS, W. Timothy. **Crisis Communication and Reputation Management.** London: Routledge, 2010.

COOMBS, W. Timothy; HOLLADAY, Sherry J. **The Handbook of Crisis Communication.** Chichester: Wiley-Blackwell, 2010.

COMFORT, Louise; KAPUCU, Naim. **Inter-organizational Coordination in Extreme Events: The World Trade Center Attacks, September 11, 2001.** *Natural Hazards,* v. 39, p. 309–327, 2006.

CREVELD, Martin van. **The Transformation of War.** New York: The Free Press, 1991.

FISHER, Roger; URY, William. **Getting to Yes: Negotiating Agreement Without Giving In.** 2nd ed. Boston: Houghton Mifflin, 1991.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

GARTZKE, Erik. **The Capitalist Peace.** *American Journal of Political Science,* vol. 51, no. 1, p. 166–191, 2007.

GODET, Michel. **Creating Futures: Scenario Planning as a Strategic Management Tool.** Paris: Economica, 2000.

Heaslip, Graham. **Challenges of Logistics in Humanitarian Aid.** *Proceedings of the 9th International Conference on Humanitarian Logistics,* Dublin: Trinity College, 2011.

HILES, Andrew. **Business Continuity Management: Global Best Practices.** New Jersey: Wiley, 2010.

HUNTINGTON, Samuel. **The Soldier and the State: The Theory and Politics of Civil-Military Relations.** Cambridge: Harvard University Press, 1996.

JANOWITZ, Morris. **The Professional Soldier: A Social and Political Portrait.** New York: The Free Press, 1971.

KAPLAN, Robert S.; MIKES, Anette. **Managing Risks: A New Framework.** *Harvard Business Review,* vol. 90, no. 6, p. 48-60, 2012.

KAPUCU, Naim. **Interagency Communication Networks During Emergencies: Boundary Spanners in Multiagency Coordination.** *The American Review of Public Administration,* vol. 36, no. 2, p. 207-225, 2006.

LOWENTHAL, Mark M. **Intelligence: From Secrets to Policy.** 7. ed. Washington: CQ Press, 2017.

MINTZBERG, Henry. **Managing.** San Francisco: Berrett-Koehler Publishers, 2009.

NYE, Joseph. **Soft Power: The Means to Success in World Politics.** New York: Public Affairs, 2004.

PORTER, Michael. **Competition: Essential Competitive Strategies.** Rio de Janeiro: Elsevier, 1999.

REIHER, Stephen et al. **Self and Social Identity in Collective Action.** In: REES, D.; STOTT, C. (org.). *Crowd Dynamics, Security and Public Order.* London: Routledge, 2004.

SALAS, Eduardo et al. **Teamwork in Multiteam Systems.** *Journal of Applied Psychology,* vol. 91, no. 2, p. 269–280, 2006.

SHEFFI, Yossi. **The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage.** Cambridge: MIT Press, 2007.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

SUN TZU. **The Art of War.** São Paulo: Martins Fontes, 2002.

YUKL, Gary. **Leadership in Organizations.** 8. ed. Boston: Pearson, 2013.

ZEGART, Amy B. **Spies, Lies, and Algorithms: The History and Future of American Intelligence.** Princeton: Princeton University Press, 2019.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.