SDA Bocconi
SCHOOL OF MANAGEMENT

SHIELD - STRATEGIC HUB
FOR INTEGRATED EDUCATION
ON LEADERSHIP & DEFENSE

From Defense to Protection: Rethinking National Security in the Age of Hybrid Threats[1]

A.Walter Rauti[2]

Abstract

National security can no longer be understood solely through the outdated paradigm of defense, rooted in military logics and territorial borders. The complexity of the twenty-first century demands a shift toward protection and security, conceived as an integrated, systemic, and managerial approach. This transition is necessitated by the nature of hybrid threats—cyberattacks, energy crises, pandemics, disinformation campaigns, and extreme climate events—which transcend borders, lack a single identifiable enemy, and generate economic, social, and political impacts far more severe than conventional wars. Protection represents a conceptual and operational revolution in the way states address these challenges. It employs instruments of risk management, business continuity, and organisational resilience drawn from corporate management, and it reframes security as a multidimensional public good sustained by the combined efforts of state institutions, businesses, and citizens. At the same time, it redirects attention from the accumulation of military power toward the continuity of essential services and the preservation of social cohesion. The experiences of Germany, Canada, and Japan confirm that this shift is not merely aspirational but already consolidated in advanced contexts, where it has contributed to reducing the costs of crises, strengthening economic competitiveness, and enhancing political legitimacy.

For Italy, adopting such a paradigm means embracing a true national modernisation strategy, one that aligns resilience, economic efficiency, and social consensus within a framework that transforms security from a passive cost into a form of collective capital for the future.

Abstract – IT

La sicurezza nazionale non può più essere compresa esclusivamente attraverso il paradigma ormai superato della difesa, radicato in logiche militari e confini territoriali. La complessità del XXI secolo impone un passaggio verso la protezione e la sicurezza, concepite come approccio integrato, sistemico e manageriale. Questa transizione è resa necessaria dalla natura delle minacce ibride (cyberattacchi, crisi energetiche, pandemie, campagne di disinformazione ed eventi climatici estremi) che superano i confini, non hanno un nemico unico identificabile e generano impatti economici, sociali e politici ben più gravi delle guerre convenzionali.

La protezione rappresenta una rivoluzione concettuale e operativa nel modo in cui gli Stati affrontano queste sfide.

Essa utilizza strumenti di risk management, business continuity e resilienza organizzativa mutuati dal management aziendale, e ridefinisce la sicurezza come bene pubblico multidimensionale sostenuto dallo sforzo congiunto di istituzioni statali, imprese e cittadini. Al tempo stesso, sposta l'attenzione dall'accumulazione di potere militare alla continuità dei servizi essenziali e alla salvaguardia della coesione sociale. Le esperienze di Germania, Canada e Giappone dimostrano che questo cambiamento non è meramente aspirazionale, ma già consolidato in contesti avanzati, dove ha contribuito a ridurre i costi delle crisi, rafforzare la competitività economica e accrescere la legittimazione politica. Per l'Italia, adottare tale paradigma significa intraprendere una vera strategia di modernizzazione nazionale, capace di allineare resilienza, efficienza economica e consenso sociale all'interno di un quadro che trasforma la sicurezza da costo passivo a capitale collettivo per il futuro.

---

[1] *Il contributo sarà pubblicato sul n. 1/2026 della rivista scientifica Azienda Pubblica.*

[2] ***Antonio Walter Rauti*** *is Academic Fellow at the SdA Bocconi, Deputy director di SHIELD and Visiting researcher at the London School of Economics. He is the author of several books on cybersecurity and cybercrime, with his work focusing on the intersection of digital threats, strategic policy, and technological innovation.*

From Defense to Protection: Rethinking National Security in the Age of Hybrid Threats

Introduction

The reflection on the concept of defense in Italy today takes place within a context of profound transformation in international relations, security threats, and risk management strategies. Whereas for most of the twentieth century defense was understood in strictly military and territorial terms — namely, as the capacity of the state to protect its borders from external aggression through the use of the armed forces — in the twenty-first century this paradigm shows serious conceptual and operational limitations. Technological evolution, economic interdependence, globalization, and the growing relevance of non-state actors have made it increasingly evident that defense, understood in its traditional sense, is no longer sufficient to guarantee the overall security of citizens, institutions, and strategic infrastructures (Buzan, Wæver, & de Wilde, 1998).

The European Union and NATO have repeatedly emphasized how new threats are characterized by a hybrid nature, combining military, economic, cyber, and informational instruments (European Commission, 2016). These threats do not respect traditional borders, are not attributable to a single actor, and above all cannot be addressed exclusively with military means. Consequently, Italy, like other advanced democracies, is called upon to rethink its national security strategy, abandoning the idea of "defense" as a separate military function and privileging a paradigm of "protection and security" that includes civil, economic, social, and environmental dimensions (Mumford, 2019). The concept of protection differs from that of defense in that it implies a proactive approach, aimed not only at reacting to a threat but at preventing it and mitigating its effects. Protection is oriented toward resilience, namely the capacity of complex systems (critical infrastructures, energy networks, health services, democratic institutions) to withstand external shocks and to quickly recover their functionality (Boin & Lodge, 2016). In this perspective, security becomes a multidimensional and indivisible public good, concerning not only the survival of the state but the overall safeguarding of society.

The management literature applied to security provides useful tools to understand this evolution. The paradigm of risk management allows the identification, assessment, and mitigation of heterogeneous risks according to systematic methodologies transferable from the private to the public sector (Hopkin, 2018). At the same time, the principles of business continuity management help to ensure the continuity of essential functions even in the presence of severe crises, thus strengthening the resilience of both public and private institutions (Herbane, 2010). The managerial approach to national security therefore requires the integration of military competences with civil, technical, and organizational ones, overcoming the traditional dichotomy between defense and civil protection.

In Italy, the constitutional concept of defense is linked to Article 52 of the Constitution ("The defense of the Fatherland is the sacred duty of the citizen"), historically interpreted in a military sense. However, the increasing frequency of health, energy, and environmental crises has highlighted the need for a broader interpretation that includes the protection of common goods and the safeguarding of fundamental rights. The management of the COVID-19 pandemic, for instance, demonstrated that national security does not depend solely on military capacity but on a complex coordination among public health, civil protection, law enforcement, and local communities (Pisano, Sadun, & Zanini, 2020).

Similarly, the energy crisis following the war in Ukraine revealed the vulnerability of Italian supply chains and the necessity of energy protection strategies as an essential component of national security (IEA, 2022).

Historical and cultural evolution of the concept of defense in Italy

Historically, the notion of defense has been intertwined with the construction of national identity. In the post-war period, Italy's alignment within NATO and the memory of World War II reinforced the centrality of the armed forces as an instrument of security. However, as early as the 1970s, with the beginning of European cooperation in the field of security and the first major energy crises, the limits of a purely military concept became evident. The rise of both domestic and international terrorism (the so-called *Anni di piombo* and subsequent Islamist attacks) showed that threats to citizens' security did not originate solely from external actors, but also from transnational and internal networks that were difficult to address through traditional means (Ignazi, 2017).

Hybrid threats and complexity

Today, the category of hybrid threat represents the clearest example of the inadequacy of traditional defense. Cyberattacks, such as those suffered by Italian infrastructures in the healthcare and energy sectors, demonstrate the vulnerability of a highly digitalized national system (Rid, 2020). Disinformation, fueled by campaigns orchestrated by foreign powers, threatens democratic stability and citizens' trust in institutions. Climate change, finally, generates extreme events requiring integrated responses from civil protection, the military, and territorial governance (OECD, 2019).

Comparative approaches: Germany, Canada, Japan

When comparing the Italian experience with that of other advanced countries, more mature models of security management emerge.

- **Germany**: In its *Weißbuch 2016*, Germany introduced the concept of "comprehensive defense," placing cyber and energy resilience at the center. The Bundeswehr operates in synergy with civil protection, overcoming the traditional division of roles (Bundesministerium der Verteidigung, 2016).
- **Canada**: Through its *Emergency Management Strategy*, Canada has adopted a whole-of-government model that integrates various institutional levels and recognizes the centrality of local and Indigenous communities (Public Safety Canada, 2018).
- **Japan**: With its doctrine of *Comprehensive Security*, Japan has included economic security, cyber protection, and disaster management as fundamental pillars of national security. The experience of Fukushima strengthened the link between energy security and civil protection (Hook, Gilson, Hughes, & Dobson, 2018).

These comparative models demonstrate that security is no longer solely a state function but a multilayered process requiring resilience, participation, and inter-institutional coordination.

Objectives of the paper

This paper therefore aims to:

1. analyze the limits of the traditional concept of defense in Italy,
2. examine the characteristics of hybrid threats and the managerial implications of their management,
3. propose a new model of protection and security for Italy, based on resilience, multi-level governance, and integrated public-private approaches,
4. discuss comparative experiences from Germany, Canada, and Japan as sources of inspiration.

With this approach, the paper seeks to contribute to the academic and political debate on the transformation of Italian national security, proposing an innovative paradigm capable of responding to the challenges of the twenty-first century.

1. Literature Review

The conceptual transition from traditional defense to integrated protection and security is not only a problem of political science or international relations, but also a theoretical and practical challenge that involves the literature of management, economics, and public governance. Hybrid threats and the growing interconnection among military, economic, technological, and social dimensions require an interdisciplinary approach, capable of drawing from paradigms typical of managerial sciences such as risk management, crisis management, organizational resilience, and multi-level governance.

1.1 Security as a public good and economic externalities

A first strand of literature focuses on the nature of security as a public good. According to Olson (1965), public goods are characterized by non-excludability and non-rivalry: everyone benefits from them and no one can be excluded from their consumption. National defense has often been cited as a classic example of a public good, but this traditional approach shows significant limitations. Hybrid threats and systemic risks produce negative externalities that do not only affect the state as a whole but have direct impacts on markets, businesses, and local communities (Sandler & Enders, 2004).

The economic literature on security therefore suggests considering protection as a complex public good, one that includes civil (healthcare, environment), digital (cybersecurity), energy, and infrastructural dimensions. These hybrid public goods require new forms of governance that go beyond state monopoly and include public-private partnerships (Kaul, Grunberg, & Stern, 1999).

1.2 Risk management and national security

A second key strand is risk management, developed initially in the corporate world and later transferred to the public sector. Hopkin (2018) argues that risk management allows heterogeneous threats to be identified and mitigation instruments to be prepared. Applying such methodologies to national security makes it possible to treat hybrid threats not as exceptional events but as predictable and manageable phenomena according to managerial criteria.

From this perspective, traditional defense (centered on military deterrence) appears too rigid and insufficiently adaptive, whereas the protection paradigm allows the development of resilience strategies that reduce the overall vulnerability of the country system. As Kaplan and Mikes (2012) highlight, organizations must distinguish between preventable risks, strategy risks, and external, uncontrollable risks. The same distinction applies to states: conventional military risks correspond to "preventable risks," while cyberattacks, pandemics, and climate crises belong to the category of systemic risks, to be addressed through protection and adaptation strategies.

1.3 Business continuity and organizational resilience

The literature on business continuity management has emphasized the importance of maintaining the continuity of operations even in the face of disruptive events. Herbane (2010) demonstrates that resilient organizations are not only able to survive crises but also to transform them into opportunities for learning. This approach has been progressively extended from the private to the public sector: governments and administrations must guarantee the

continuity of essential services (healthcare, energy, transportation, communications) even under conditions of stress.

For Italy, this implies a radical shift: the focus can no longer be the defense of borders but rather the system's capacity to ensure vital services to citizens in the presence of global shocks. The COVID-19 pandemic and the 2022 energy crisis represented true stress tests of business continuity for the state, demonstrating the urgency of a managerial approach to security.

1.4 Multi-level governance and institutional coordination

Another fundamental contribution from the managerial and economic literature concerns multi-level governance. Hooghe and Marks (2003) argue that complex problems require coordination that cuts across different levels of government: local, national, and supranational. Protection and security, due to their hybrid and transnational nature, cannot be guaranteed by a single institutional level.

In Italy, this translates into the need to strengthen coordination among the central state, regions, municipalities, and European institutions. The "whole-of-government" model adopted in Canada and the Japanese "comprehensive security" model are significant examples of how multi-level governance can improve overall resilience. In managerial terms, this corresponds to developing network governance systems capable of integrating public, private, and civil society actors (Rhodes, 2012).

1.5 Security economics and sustainable growth

The economic literature also highlights the close relationship between security and development. Collier (2007) underscores how countries affected by instability or conflicts experience deep economic losses. Conversely, investing in security and resilience can generate significant economic returns by reducing the future costs of crises and disasters.

Security should thus be understood as a form of collective capital that sustains long-term economic growth. In this perspective, the concept of protection integrates with theories of sustainability: security concerns not only conflict prevention but also the safeguarding of natural resources, the environment, and social cohesion. The literature on security economics (Anderson & Moore, 2006) demonstrates, for example, how cybersecurity is a strategic investment for a country's competitiveness rather than a mere cost.

1.6 Organisational learning and adaptive security

Finally, an emerging area of literature concerns organisational learning applied to security. Argyris and Schön (1996) emphasize that organizations must develop double-loop learning capacities, revising not only their actions but also the underlying assumptions that guide them. Applied to national security, this means that Italy must move beyond the traditional defense paradigm and learn to consider protection as a dynamic, adaptive, and continuously learning process.

Protection therefore requires a managerial approach capable of integrating monitoring, feedback, and innovation. In this sense, digital technologies, big data, and artificial intelligence can become fundamental tools for the predictive management of hybrid threats (Brynjolfsson & McAfee, 2017).

The management and economic literature confirms that traditional defense is no longer adequate to confront complex and hybrid threats. On the contrary, an integrated approach to protection and security allows states to:

- treat security as a multidimensional public good,
- apply risk management and business continuity methodologies,
- develop multi-level governance and network governance systems,
- integrate security with sustainable development,
- foster organisational learning and adaptive security.

Within this framework, Italy is called upon to position itself in a modern, managerial, and resilient perspective that connects national security to global economic and organizational dynamics.

2. The Limits of the Defensive Paradigm: From Defense to Protection

The debate on national security in the twenty-first century is characterized by an unprecedented tension between continuity and rupture. On one side, the legacy of the Cold War and the centrality of the state monopoly on legitimate violence continue to shape strategic doctrines, military budgets, and public expectations. On the other, the emergence of hybrid threats—cyberattacks, energy crises, pandemics, disinformation campaigns, and extreme climate events—has profoundly transformed the nature of risks and the conditions of governance. These threats are not limited to military confrontation, but are systemic, transnational, and multidimensional, producing economic, political, and social impacts of greater scope and intensity than conventional wars (Boin & Lodge, 2016; Nye, 2017).

In this context, defense understood as deterrence and protection of borders appears conceptually and operationally inadequate. The Italian case is emblematic: a country strongly integrated into European and transatlantic alliances, but simultaneously exposed to vulnerabilities deriving from energy dependency, fragile digital infrastructures, demographic imbalances, and institutional fragmentation. The very logic of defense, historically centered on territorial sovereignty, collides with threats that undermine the continuity of essential services, the resilience of communities, and the trust of citizens in institutions.

2.1 The inadequacy of the defensive paradigm

The defensive paradigm rests on three fundamental assumptions: the identification of an external adversary, the centrality of military power as an instrument of deterrence, and the territorial border as a line of defense. Each of these assumptions is challenged by hybrid threats. The adversary is often elusive, decentralized, or even non-human (as in the case of pandemics or climate events). Military power, though necessary, is insufficient to counter cyber threats, misinformation, or systemic vulnerabilities. Borders, finally, are permeable to phenomena that move through global networks of energy, finance, and information.

Italy, like other European countries, continues to structure its defense policy around NATO commitments, historically focused on the 2% of GDP threshold for military spending In 2025, Allies signalled a new spending ambition of 5% of GDP, comprising 3.5% for core defence and 1.5% for defence-related investment in infrastructure and resilience, aligned with the updated capability targets under the NATO Defence Planning Process. While Italy has reached the 2% floor, the 5% signal poses additional fiscal and political challenges and, if pursued via unselective budget expansion, risks entrenching inefficiencies rather than addressing structural vulnerabilities.

2.2 From defense to protection

It is in this context that the concept of protection acquires relevance. Protection does not replace defense but redefines its scope, integrating it into a broader framework in which the objective is not only to repel external aggression, but to guarantee the continuity of vital systems and the stability of society. Protection is not a purely military paradigm, but a managerial and systemic approach, based on principles of resilience, risk management, and value for money.

Resilience refers to the ability of a system to absorb shocks, adapt, and rapidly restore functionality (Boin & Lodge, 2016). Risk management implies the capacity to allocate resources flexibly, in proportion to the probability and impact of threats (Kaplan & Mikes, 2012). Value for money, finally, requires evaluating every public expenditure in terms of social and economic benefits, transforming security from a passive cost into an active investment.

These principles, largely derived from the corporate management literature (Herbane, 2010; Hopkin, 2018), are applied here to national security, highlighting the possibility of overcoming the rigidities of the defensive model. The aim is not to reduce the role of the armed forces, but to complement it with a systemic vision in which military deterrence is only one element of a broader strategy of protection.

2.3 Security as a multidimensional public good

The protection paradigm can also be framed within the theory of public goods. According to Kaul, Grunberg, and Stern (1999), public goods are characterized by non-excludability and non-rivalry: their enjoyment cannot be limited, and their consumption by one individual does not reduce availability for others. Security, understood as protection against systemic threats, fully falls within this category. All citizens benefit from resilient energy infrastructures, efficient health systems, and secure digital networks, regardless of their individual contribution to financing them.

This perspective has significant managerial and political implications. First, it justifies the central role of the state in providing security, since private actors alone cannot guarantee it. Second, it highlights the need for participatory governance, in which businesses and citizens are also involved in the production of security. Third, it legitimizes the reallocation of public spending toward sectors that produce positive externalities across the economy and society.

2.4 Italy in comparative perspective

The Italian case highlights the urgency of adopting the protection paradigm. The pandemic reduced GDP by more than 9% in 2020 (Pisano, Sadun & Zanini, 2020), an economic loss greater than any military conflict in recent history. Cyberattacks on hospitals and public administrations have demonstrated the vulnerability of the digital system. Energy crises have shown the strategic dependence of the country on external suppliers. Disinformation campaigns have undermined social cohesion and trust in institutions.

Other countries have already moved in this direction. Germany has adopted the concept of Sicherheitspolitik, integrating defense, civil protection, and resilience. Canada has developed a whole-of-society resilience strategy, emphasizing collaboration between state, businesses, and citizens. Japan has articulated a model of Comprehensive Security that includes economic, technological, and social dimensions (Bundesregierung, 2016; Public Safety Canada, 2018; Ministry of Defense Japan, 2020). These experiences demonstrate that protection is not an aspirational concept, but a consolidated practice in advanced contexts.

2.5 Towards a new national modernization strategy

For Italy, adopting the protection paradigm means embarking on a true modernization strategy. Protection is not only about ensuring security, but about aligning resilience, economic efficiency, and social consensus in a single framework. It means overcoming the fragmentation of policies and institutions, adopting managerial tools for risk

management and performance evaluation, and developing a culture of accountability and innovation. In this sense, protection represents a conceptual and operational revolution. It shifts attention from the accumulation of military power to the continuity of essential services, from the logic of emergency to that of prevention, from security as cost to security as capital. It is a paradigm that combines effectiveness, efficiency, and legitimacy, transforming national security from a defensive expenditure to a collective investment in the future.

3. Hybrid Threats and Managerial Challenges

Hybrid threats are defined by their capacity to combine heterogeneous instruments—military, economic, technological, informational, and environmental—within a unified strategy aimed at destabilizing adversaries without resorting to open conflict. Their peculiarity lies in their ability to exploit the interdependencies of modern societies, transforming vulnerabilities into vectors of instability. Cyberattacks, energy crises, pandemics, disinformation campaigns, and climate events are not isolated phenomena: they propagate through networks that connect infrastructures, markets, and communities, generating cascading effects of potentially catastrophic magnitude (Miller, 2020; Rid, 2021).

Unlike conventional threats, hybrids lack a clearly identifiable enemy. In many cases, attribution is uncertain or deliberately ambiguous, as in the case of cyber operations conducted by actors shielded behind proxies. Moreover, hybrid threats transcend territorial borders, exploiting global flows of capital, data, and energy. Their impacts are not limited to the security domain, but affect the economy, politics, and society, producing costs that far exceed those of traditional wars.

3.1 The Italian vulnerabilities

Italy represents a particularly exposed case due to a set of structural vulnerabilities. Energy dependence, digital fragmentation, demographic imbalance, and institutional weakness make the country fertile ground for systemic crises. The energy crisis following Russia's invasion of Ukraine demonstrated the strategic dependence of Italy on external suppliers, while cyberattacks on hospitals and public administrations revealed the fragility of digital infrastructures. The COVID-19 pandemic exposed weaknesses in the healthcare system, with shortages of personnel, outdated infrastructure, and territorial inequalities that amplified the impact of the crisis (Pisano, Sadun & Zanini, 2020).

Institutional fragmentation further aggravates these vulnerabilities. Competences in security are distributed among ministries, agencies, regions, and local authorities, often without adequate coordination. This dispersion of responsibilities reduces the ability of the system to respond in a coherent and timely manner, as demonstrated by delays in the management of cybersecurity and climate emergencies.

3.2 Managerial challenges posed by hybrid threats

The first managerial challenge posed by hybrid threats concerns the construction of resilience. Unlike traditional defense, which focuses on deterrence and immediate response, resilience implies the capacity of a system to absorb shocks, adapt to new conditions, and restore functionality rapidly. As Boin and Lodge (2016) argue, resilient institutions are not those that avoid crises, but those that transform them into opportunities for learning. In Italy, the pandemic highlighted how the absence of robust healthcare resilience plans dramatically increased the social and economic costs of the crisis. The integration of mechanisms of organizational learning (Argyris & Schön, 1996) thus becomes a necessary condition for addressing complex and evolving threats.

3.2.1 Risk management and value for money

A second challenge lies in adopting risk management logics. Unlike traditional defense spending, oriented toward large multiyear programs, risk management entails flexible allocation of resources according to the probability and impact of threats. Kaplan and Mikes (2012) propose a risk management model that distinguishes between preventable, strategic, and external risks: applied to national security, this approach allows the prioritization of investments in areas with the highest expected return, not only in economic terms but also in terms of social and political value for money. For Italy, this means redirecting resources from costly weapon systems with limited social spillovers to sectors such as cybersecurity, critical infrastructure protection, and renewable energy, where benefits are both immediate and widely distributed.

3.2.2 Multi-level governance and institutional coordination

Hybrid threats challenge the centralized architecture of traditional defense. Protection requires the involvement of diverse actors—state, businesses, local governments, and citizens—and a governance system capable of coordinating their interests. Hooghe and Marks (2003) describe this model as multi-level governance, in which competences and responsibilities are distributed across different institutional levels. In Italy, the fragmentation of competences among ministries, agencies, and regions has often hindered the construction of unified strategies, as seen in delays in the development of cybersecurity frameworks and responses to climate emergencies. Effective governance must therefore overcome bureaucratic rigidities and promote flexible cooperation networks that integrate public and private capabilities (Rhodes, 2012).

3.2.3 Innovation and organizational flexibility

Another critical challenge is institutional capacity for innovation. Hybrid threats evolve rapidly, rendering rigid models and long-term planning obsolete. The Ukrainian experience, with its extensive use of drones and artificial intelligence, demonstrates how rapid innovation can compensate for disparities in resources with adversaries. For Italy, this implies adopting financing and procurement models closer to those of venture capital, capable of supporting high-risk, high-reward technological projects and start-ups. This entrepreneurial logic contrasts with the traditional slowness of military procurement processes, but represents an essential condition for responding effectively to continuously changing hybrid threats.

3.2.4 The role of organizational culture

Finally, hybrid threats pose a cultural challenge. Italian institutions tend to privilege compliance and adherence to procedures, while hybrid crisis management requires flexibility, creativity, and rapid decision-making. Herbane (2010) stresses that many organizations fail in crisis management not for lack of resources, but because of cultural resistance to innovative strategies. For this reason, the transition from defense to protection cannot be reduced to formal reorganization: it must involve a profound change in organizational culture, promoting a proactive, integrated, and results-oriented approach.

3.3 Implications for public management

The managerial challenges posed by hybrid threats have profound implications for public management. They require the adoption of instruments from corporate management, adapted to the institutional context: cost-benefit analysis, risk management, performance evaluation, and accountability. The objective is not only to increase efficiency, but to build a governance model capable of ensuring protection in a context of limited resources and constantly evolving threats. In this sense, the protection paradigm is not merely a conceptual innovation, but a managerial one, requiring institutions to adopt practices of learning, flexibility, and continuous adaptation.

The next chapter will outline the principles and objectives of the protection paradigm, presenting it not as an abstract alternative but as an operational strategy consistent with Italy's institutional and economic context.

4. From the Concept of Defense to Protection and Security

The concept of protection represents a paradigmatic shift compared to the traditional notion of defense. Whereas defense is rooted in the military logic of deterrence and the repulsion of external aggression, protection emerges as a systemic and managerial approach aimed at ensuring the continuity of essential services, the resilience of communities, and the stability of the economy. Protection does not abolish defense, but rather repositions it within a broader framework, in which security is conceived as a multidimensional public good.

The literature on public goods offers a useful theoretical framework for understanding this specificity. Kaul, Grunberg, and Stern (1999) argue that global public goods are characterized by non-excludability and non-rivalry, which means that their enjoyment cannot be limited and that consumption by one individual does not diminish availability for others. Security, understood as protection against hybrid and systemic threats, clearly falls into this category: all citizens benefit from resilient infrastructures, robust healthcare systems, and secure digital networks, regardless of individual contributions. Protection is therefore the modality through which the state ensures the provision of goods that no private actor could guarantee alone.

Another distinctive element of the protection paradigm is its systemic nature. Hybrid threats do not affect isolated sectors but exploit interdependencies across different domains: digital, healthcare, energy, and social. Protection must thus be conceived not as a set of sectoral policies, but as an integrated strategy that considers the national ecosystem as a whole. This requires governance tools capable of coordinating diverse actors—public and private, central and local—and managing interconnections across sectors. The literature on multi-level governance (Hooghe & Marks, 2003) and network governance (Rhodes, 2012) underscores the importance of flexible, reticular, and collaborative decision-making models, able to respond to threats that disregard institutional boundaries.

Finally, protection distinguishes itself through its managerial approach, drawing upon practices of risk management and business continuity developed in the private sector (Kaplan & Mikes, 2012; Hopkin, 2018). Whereas traditional defense relies on long-term plans rigidly tied to military procurement programs, protection demands flexibility, adaptability, and the ability to reallocate resources swiftly in response to evolving threats. This perspective implies a more efficient use of public funds, guided by the principle of value for money, namely the maximization of social and economic benefits for every unit of expenditure.

4.1 Defense and protection compared

The difference between defense and protection is not merely semantic but substantive. Defense aims at preventing or repelling external aggression, while protection focuses on the capacity to maintain systemic functionality in the face of shocks of any nature. In terms of objectives, defense pursues territorial integrity, whereas protection pursues the continuity of essential services and the preservation of social cohesion. In terms of instruments, defense relies primarily on military force, while protection uses a heterogeneous set of tools—healthcare, cybersecurity, energy security, and strategic communication—integrated within a preventive and resilient logic.

International experiences confirm this difference. In Germany, the concept of Sicherheitspolitik integrates military defense with civil protection and social resilience (Bundesregierung, 2016). In Canada, the paradigm of whole-of-

society resilience emphasizes collaboration among state, businesses, and citizens (Public Safety Canada, 2018). In Japan, the notion of Comprehensive Security includes the protection of critical infrastructures and economic resilience as fundamental components of national strategy (Ministry of Defense Japan, 2020). These examples demonstrate that the protection paradigm is already consolidated in advanced countries, where it reduces crisis costs, strengthens competitiveness, and enhances political legitimacy.

4.2 Protection and economic sustainability

An often-overlooked dimension of protection is its coherence with economic sustainability. The defensive paradigm, with its high costs and limited returns, generates fiscal pressures that threaten budgetary stability. Protection, by contrast, transforms security expenditure from a passive cost into an active investment. Investments in healthcare, digital, and energy resilience not only mitigate the costs of crises but generate broad economic benefits, fostering innovation, competitiveness, and employment. In this sense, protection represents not only a security strategy but also a modernization strategy, aligned with the United Nations Sustainable Development Goals (SDGs).

4.3 Toward a new paradigm

The transition from defense to protection implies a profound cultural and institutional shift. It is not merely about redistributing resources but about redefining the very conception of national security. Protection demands the adoption of preventive rather than reactive logics, the integration of diverse competences, and the construction of trust between institutions and citizens. For Italy, this transition is not simply desirable but necessary: without a paradigm shift, the country risks remaining trapped in an inefficient model, unable to respond to the systemic challenges of the twenty-first century.

4.4 Principles of the protection paradigm

Resilience constitutes the first pillar of the protection paradigm. It does not coincide with the mere ability to resist a shock, but with the capacity to absorb it, adapt to change, and restore system functionality rapidly. As Boin and Lodge (2016) argue, institutional resilience lies not only in preventive preparation but also in the ability to learn from experience and transform crises into opportunities for innovation. In the Italian case, the COVID-19 pandemic revealed the economic and social costs of lacking healthcare resilience: shortages of protective equipment, insufficient emergency plans, and weak coordination mechanisms amplified the crisis (Pisano, Sadun & Zanini, 2020).

Nevertheless, resilience entails trade-offs. Investing in redundancy and backup capacity involves immediate costs that may appear inefficient in normal times. A healthcare system with surplus staff and hospital beds, for example, may seem costly in ordinary conditions but becomes invaluable in emergencies. The managerial challenge is to balance efficiency and redundancy, avoiding waste without compromising the capacity to respond to shocks.

4.4.1 Risk management

The second principle is risk management. Unlike traditional defense, oriented toward rigid, long-term procurement programs, risk management demands a flexible allocation of resources, based on the probability and impact of threats. Kaplan and Mikes (2012) propose distinguishing between preventable, strategic, and external risks, each requiring different instruments: compliance mechanisms for preventable risks, innovation and experimentation for strategic risks, and resilience for external risks.

Applied to national security, this model means allocating resources not simply according to external commitments—such as NATO's 5% target—but based on systematic assessments of actual threats. For Italy, this implies prioritizing cybersecurity, energy resilience, and climate adaptation, which pose concrete risks with potentially devastating impacts. The danger, however, is to fall into a purely reactive approach, over-prioritizing visible threats while neglecting low-probability but high-impact risks. Once again, the trade-off lies between efficient allocation and long-term vision.

4.4.2 Value for money

The third principle is value for money, which implies efficient use of public funds. The traditional defensive model tends to justify military spending through quantitative benchmarks—such as GDP share or the number of systems acquired—without precise evaluation of social returns. Protection, by contrast, requires that each investment be assessed in terms of distributed benefits: crisis cost reduction, improved quality of life, strengthened trust in institutions, and enhanced competitiveness.

Investments in cybersecurity, for example, have been shown to generate significant savings. IBM Security (2022) estimates that every dollar invested in digital prevention can save up to 14 dollars in incident management costs. Similarly, investments in renewable energy reduce external dependency while generating employment and technological innovation (IEA, 2022). These data demonstrate that protection spending can maximize economic and social returns. Yet here too trade-offs exist: focusing excessively on short-term returns risks sidelining sectors whose benefits emerge only in the long run.

4.4.3 Critical discussion of the principles

The selection of resilience, risk management, and value for money as guiding principles is not arbitrary, but reflects their coherence with the strategic objectives of contemporary security. The fundamental goal is to ensure the continuity of essential services and social stability, for which resilience is indispensable. The scarcity of public resources demands rigorous prioritization, hence the centrality of risk management. Political legitimacy, finally, depends on citizens' perception that resources are used efficiently and fairly, thus the importance of value for money.

These principles are also interconnected. Resilience requires investments that must be prioritized through risk analysis, while their political acceptance depends on value for money. The trade-offs involved do not undermine the principles but highlight their dynamic nature: protection is not a fixed state but a continuous process of adaptation, balancing, and learning.

4.5 Focus: comparative applications of the principles

Germany has embodied the principle of resilience through its approach to energy security. The Russian invasion of Ukraine in 2022 exposed the vulnerability of German dependence on Russian gas and pushed Berlin to accelerate diversification strategies. Massive investments in LNG terminals, renewable energy, and efficiency programs were implemented not only as economic or environmental policies but as instruments of national security (Bundesregierung, 2022). This case shows how resilience requires upfront redundancy costs, such as the construction of LNG infrastructure, but generates systemic benefits by reducing exposure to geopolitical shocks.

Canada has operationalized risk management by decentralizing resilience strategies to provincial and municipal levels. Public Safety Canada (2018) developed frameworks that assess the probability and impact of different risks, including climate events, cyber incidents, and pandemics, and allocates funds accordingly. Provinces particularly exposed to floods receive dedicated resilience financing, while others prioritize wildfire protection. This selective allocation maximizes efficiency but creates heterogeneity: wealthier provinces with stronger fiscal capacity can complement federal funding, while weaker regions remain more exposed. The Canadian experience illustrates the trade-off inherent in risk management between allocative efficiency and territorial equity.

Japan has emphasized value for money by investing in dual-use technologies with both security and economic returns. The Ministry of Defense has supported start-ups working on artificial intelligence, robotics, and cybersecurity systems that can serve both civilian and military purposes (Ministry of Defense Japan, 2020). This strategy ensures that every yen spent on security also stimulates innovation, job creation, and competitiveness. However, the Japanese model relies heavily on public debt, raising concerns about long-term fiscal sustainability. The lesson is that value for money must be evaluated not only in terms of returns but also in relation to fiscal constraints.

The comparative evidence demonstrates that resilience, risk management, and value for money are not abstract principles but operational logics already implemented in advanced contexts. For Italy, adopting them means learning from Germany the importance of redundancy in strategic sectors such as energy, from Canada the benefits and risks of decentralized risk management, and from Japan the role of innovation in linking security with economic competitiveness. The challenge lies in adapting these lessons to Italy's structural vulnerabilities, its fragmented governance, and its fiscal limitations.

4.6 Objectives of the protection paradigm

The first strategic objective of protection is to guarantee the continuity of essential services. In contemporary societies, security is measured less by the ability to repel external attacks than by the ability to ensure that hospitals, schools, energy networks, and digital systems function without interruption. A blackout, a hospital network outage, or a disruption of water supply can generate social and economic damage greater than that of many conventional military attacks. Italy, with its high dependence on critical infrastructures and its exposure to natural and technological risks, must prioritize continuity as the cornerstone of its security policy.

4.5.1 Safeguarding social cohesion and trust

A second objective is safeguarding social cohesion and trust in institutions. Hybrid threats such as disinformation campaigns, cyberattacks on public services, or poorly managed emergencies undermine the legitimacy of the state. Protection, by ensuring transparency, accountability, and the reliability of services, becomes a lever for reinforcing the bond between citizens and institutions. In Italy, where social trust is traditionally fragile, investing in protection means consolidating the very foundations of democracy.

4.5.2 Innovation and economic competitiveness

A third objective concerns innovation and competitiveness. Investments in protection sectors such as cybersecurity, renewable energy, and healthcare infrastructures generate positive externalities across the economy. They stimulate technological innovation, create employment, and enhance international attractiveness. The Japanese case demonstrates how security policies can be integrated with industrial policies to strengthen competitiveness. For Italy, a country with a strong industrial base but limited investment in high-tech sectors, protection can become a catalyst for modernization and growth.

4.5.3 Alignment with the Sustainable Development Goals

Finally, protection aligns with the objectives of sustainable growth codified in the United Nations Sustainable Development Goals. Energy security, climate adaptation, and health resilience are simultaneously components of national security and elements of sustainable development. By investing in these areas, Italy not only improves its security but also strengthens its capacity to attract international funding and private investment. Protection thus represents a strategy that reconciles security, sustainability, and economic efficiency in a single framework.

4.7 Financing protection

One of the most critical issues in the Italian transition toward the protection paradigm lies in financing. The defensive model is marked by rigidity, path dependency, and diminishing returns. Large military procurement programs, often initiated decades ago and politically difficult to revise, continue to absorb substantial resources even when their strategic contribution is marginal (Dunne & Tian, 2013). The defense budget is structured primarily around armaments and personnel, while crucial components of protection such as cybersecurity, energy resilience, and healthcare infrastructures remain chronically underfunded.

Recent analyses confirm the distortion created by this model. Gilli and Rauti (2025) have shown that many European countries, including Italy, are caught in a trilemma between the need to increase military capabilities, maintain fiscal stability, and preserve democratic legitimacy. Indiscriminate increases in military expenditure, driven by external commitments such as NATO's new 5% of GDP target, risk consolidating inefficiencies and eroding political consensus. In Italy, this dynamic has translated into chronic underinvestment in civilian infrastructures essential for resilience, while defense procurement programs continue to benefit from inertia and political protection.

4.7.1 Toward a National Resilience Fund

To overcome these inefficiencies, Italy should adopt an innovative financing model capable of integrating defense and protection into a coherent strategy. A plausible solution would be the creation of a National Resilience Fund, conceived as a permanent instrument capable of mobilizing resources from multiple sources: the state budget, European funds, public-private partnerships, and innovative financial instruments.

Such a fund would allow investments to be targeted toward sectors with the highest social and economic multipliers, including cybersecurity, renewable energy, healthcare, and protection of critical infrastructures. Allocation criteria should be based on cost-benefit analyses and evidence-based assessments, ensuring transparency and accountability. The logic must be one of portfolio diversification, similar to venture capital, in which a share of investments is directed to high-risk, high-potential projects, such as start-ups and SMEs developing dual-use technologies. Experiences in Japan demonstrate that such an entrepreneurial approach, though riskier than traditional procurement, can generate innovation and competitiveness that benefit both security and the broader economy (Ministry of Defense Japan, 2020).

Public-private partnerships represent another indispensable instrument, particularly in sectors such as energy and digital infrastructures that are predominantly in private hands. By sharing risks and benefits, the state can attract private capital, reduce the fiscal burden, and ensure that investments align with national security objectives. The Canadian experience confirms the effectiveness of PPPs when inserted into a clear and transparent regulatory framework, preventing the risks of opportunism or inefficiency (Public Safety Canada, 2018).

4.7.2 Integration with NATO and European commitments

The 5% spending signal can be operationalised by counting, within the 1.5% defence-related investment share, verifiable projects in cyber, energy grids, logistics and other resilience-enabling infrastructures that directly support collective defence commitments. For Italy, the challenge lies in interpreting this target not as a purely quantitative

constraint but as an opportunity to redirect a portion of resources toward protection sectors consistent with NATO's broader objectives of collective resilience. Investments in cybersecurity, energy infrastructures, and logistics can legitimately be included within the 1.5% dedicated to infrastructures, provided they are linked to defense purposes.

The European Union also plays a central role, both through structural funds and through programs such as Horizon Europe, which finance innovation and resilience projects. Aligning the National Resilience Fund with European instruments would multiply available resources and integrate Italian protection policies into a continental framework. In this way, financing protection would not be limited to reallocating domestic resources but would become a lever for attracting European and private capital, enhancing fiscal sustainability and political legitimacy.

4.8 Managerial implications

The protection paradigm requires a profound reorganization of governance. Hybrid threats cut across the boundaries of ministries and sectors, demanding coordination among multiple levels of government as well as collaboration with private actors. Hooghe and Marks (2003) describe multi-level governance as a model in which competences and responsibilities are distributed rather than centralized, creating flexible and reticular decision-making processes. For Italy, where institutional fragmentation has often led to inefficiencies, this implies shifting from a hierarchical model to a networked system in which the state assumes the role of facilitator and coordinator rather than exclusive decision-maker.

4.8.1 Accountability and performance measurement

Another crucial managerial implication is accountability. Traditional defense policies have been evaluated through input indicators such as the percentage of GDP allocated to defense or the number of systems procured. These measures, however, say little about the actual security experienced by citizens. The protection paradigm requires the development of new performance indicators capable of measuring reductions in vulnerabilities, continuity of essential services, and the social and economic benefits of investments. Kaplan and Mikes (2012) emphasize the importance of evidence-based monitoring tools, which allow strategies to be adapted based on concrete outcomes. In the Italian case, creating a robust system of accountability is essential not only for technical reasons but also to build the political legitimacy of protection policies.

4.8.2 The cultural transformation of institutions

Protection cannot be implemented without a cultural shift in public institutions. Italian bureaucracy is traditionally oriented toward compliance and adherence to procedures, while hybrid threats demand adaptability, rapid decision-making, and organizational learning. Argyris and Schön (1996) distinguish between single-loop learning, which corrects errors within established rules, and double-loop learning, which questions the underlying assumptions. Adopting the protection paradigm requires the capacity for double-loop learning, enabling institutions to question their own routines and embrace innovation. This cultural change is as important as financial investment, because without it, resources risk being absorbed by rigid structures incapable of adapting.

4.8.3 Innovation and organizational flexibility

Hybrid threats evolve at a pace that traditional procurement and bureaucratic cycles cannot match. The Ukrainian conflict has demonstrated how rapid innovation in drones and artificial intelligence can radically change the battlefield in a matter of months. Italy must learn from this lesson, introducing procurement and financing models inspired by entrepreneurial logics, capable of supporting high-risk and high-reward projects. Public venture capital, accelerators for dual-use technologies, and fast-track procurement procedures are examples of instruments that can make institutions more flexible and innovative. Herbane (2010) stresses that many organizations fail in crisis management not for lack of resources, but because of their inability to experiment with new solutions. Organizational flexibility, therefore, is a strategic asset as much as financial capacity.

4.8.4 The international dimension

Managerial implications cannot be limited to the national level. Italy is part of NATO and the European Union, frameworks that impose obligations but also offer opportunities. The new NATO target of 5% of GDP requires careful negotiation to ensure that investments in protection are recognized as contributions to collective security. At the same time, EU programs such as Horizon Europe and the European Defence Fund provide opportunities to finance projects that combine security, innovation, and sustainability. Managing protection therefore requires not only internal reform but also the ability to leverage international governance structures to mobilize resources and strengthen legitimacy.

4.9 Conclusion of the chapter

The protection paradigm emerges as both a conceptual and operational revolution compared to the defensive model. Its foundations lie in three interrelated principles: resilience, which guarantees continuity of essential services and the capacity to adapt to shocks; risk management, which enables the efficient allocation of scarce resources; and value for money, which ensures that every unit of expenditure produces measurable social and economic returns. The objectives of protection are equally clear: safeguarding the continuity of critical infrastructures, consolidating social cohesion and trust in institutions, stimulating innovation and competitiveness, and aligning security with sustainable development.

Financing this paradigm requires overcoming the inefficiencies of traditional defense spending and creating innovative instruments such as a National Resilience Fund, supported by diversified resources and governed by evidence-based criteria. International experiences show that protection is not a theoretical aspiration but a consolidated practice in advanced contexts such as Germany, Canada, and Japan, where investments in resilience and innovation have produced tangible benefits in terms of security, competitiveness, and legitimacy.

The managerial implications are equally decisive. Protection demands a shift from hierarchical and bureaucratic models to multi-level and networked governance, from rigid procurement programs to flexible and innovative financing mechanisms, and from a culture of compliance to one of organizational learning and experimentation.

Italy's ability to adopt this paradigm depends not only on financial choices but also on institutional and cultural transformation.

Finally, the international dimension confirms that protection is not in contradiction with Italy's commitments to NATO and the European Union. On the contrary, the new 5% GDP target approved in 2025 can be reinterpreted as an opportunity to channel resources toward infrastructures and sectors that strengthen both national resilience and collective security. In this sense, protection represents not an alternative to defense but its evolution: a paradigm capable of responding to hybrid threats, modernizing institutions, and transforming security from passive expenditure into collective capital.

5. Focus: Germany, Canada, Japan, and Italy

5.1. Germany: resilience through energy and infrastructure

Germany has integrated the protection paradigm into its national security strategy primarily through investments in resilience. The energy crisis triggered by the Russian invasion of Ukraine accelerated Berlin's commitment to diversification, with over 200 billion euros allocated to renewable energy, LNG terminals, and digital infrastructures (Bundesregierung, 2022). These measures demonstrate how protection is framed not only as an economic or environmental policy, but as a national security imperative. Germany has also developed federal mechanisms of coordination that, despite political fragmentation, allow the central government to align resilience policies with regional initiatives. The main limitation lies in the high fiscal cost of these programs, which have sparked debates on sustainability in the long term.

5.2. Canada: risk management and decentralized resilience

Canada has distinguished itself through a whole-of-society approach that emphasizes decentralized risk management. Public Safety Canada (2018) developed frameworks for allocating resources based on risk assessments at the provincial and municipal level. This model has increased efficiency, allowing investments to focus on the most pressing vulnerabilities, such as floods or wildfires. The Canadian experience illustrates both the potential and the risks of decentralization: while efficiency has improved, territorial inequalities persist, since wealthier provinces can complement federal funding with their own resources, while poorer areas remain more exposed.

5.3. Japan: value for money and technological innovation

Japan has adopted a model of Comprehensive Security that integrates defense with economic and technological dimensions. The Ministry of Defense has invested in dual-use technologies, including artificial intelligence, robotics, and cybersecurity, supporting start-ups and SMEs with strong innovation potential (Ministry of Defense Japan, 2020). This approach embodies the principle of value for money, ensuring that security spending simultaneously stimulates industrial competitiveness and job creation. The limitation of the Japanese model lies in its reliance on public debt, raising concerns about fiscal sustainability and long-term resilience.

5.4. Italy in comparative perspective

Compared to these countries, Italy remains anchored to the defensive paradigm, with a budgetary structure concentrated on military procurement and personnel. Although Italy has already achieved the NATO 2% target and now faces the new 5% benchmark, the share of resources devoted to protection sectors such as cybersecurity, renewable energy, and healthcare remains marginal. The pandemic, energy crises, and cyberattacks have shown the systemic vulnerabilities of the Italian system, exacerbated by institutional fragmentation and limited investment in innovation.

The comparative evidence highlights the path Italy must take: from Germany, the importance of resilience in strategic sectors; from Canada, the selective allocation of resources based on risk management; from Japan, the integration of security spending with technological innovation and competitiveness. The challenge lies in adapting these models to Italy's structural constraints, including high public debt and weak governance capacity. Protection, in this sense, is not an alternative but the only way to reconcile international commitments, fiscal sustainability, and democratic legitimacy.

Table 1 - Comparative overview of national security paradigms in Italy, Germany, Canada, and Japan.

COUNTRY	STRATEGIC APPROACH	MANAGERIAL TOOLS ADOPTED	ECONOMIC IMPLICATIONS	MAIN CHALLENGES
ITALY	Defensive paradigm still prevalent, with a slow transition toward protection (cyber, energy, health)	Initial applications of risk assessment; creation of dedicated agencies (e.g., National Cybersecurity Agency)	High energy dependence, digital lag, high opportunity costs of traditional military spending	Weak social consensus on military expenditure; incomplete multilevel governance; delays in public-private integration
GERMANY	*Gesamtverteidigung*("comprehensive defense") oriented toward energy and cyber resilience	National risk mapping; business continuity planning; PPPs with technology and energy companies	Strengthened competitiveness through investments in digital and energy resilience	Tension between NATO obligations and domestic preference for civil protection
CANADA	*Whole-of-Government*and inclusive multilevel governance	Stakeholder engagement; performance management with resilience indicators; federal-provincial coordination	Investments in climate and energy resilience conceived as assets for economic growth and attractiveness	Coordination challenges across federal levels; institutional complexity
JAPAN	*Comprehensive Security* (integrati on of defense, economic resilience, and disaster management)	Crisis management; disaster risk reduction; adaptive leadership; PPPs for supply chain protection	Reduced economic impacts of natural disasters; resilience conceptualized as collective capital	High energy dependence; significant climate risks; constitutional constraints on armed forces use

The table highlights the strategic approaches, managerial tools, economic implications, and main challenges of each country. Data and concepts are based on national policy documents and relevant academic literature, including the *Weißbuch 2016* (Bundesministerium der Verteidigung, 2016) for Germany, the *Emergency Management Strategy for Canada* (Public Safety Canada, 2018), and the Japanese doctrine of *Comprehensive Security* as discussed in Hook, Gilson, Hughes, & Dobson (2018).

6. The Benefits of the New Paradigm and Concluding Perspectives

For Italy, adopting the protection paradigm requires redefining its national security objectives. The traditional emphasis on territorial integrity, while still relevant, no longer captures the primary sources of vulnerability. The real risks to the Italian system stem from energy dependence, cyber fragility, climate instability, and public health crises. The new 5% NATO target, which combines standard defense, core military spending, and defense-related infrastructure, risks reinforcing a quantitative logic disconnected from these vulnerabilities. Reorienting objectives means placing the continuity of essential services, the resilience of infrastructures, and the cohesion of communities at the center of national strategy.

Redefining policy principles

Italy must anchor its security strategy in the principles of resilience, risk management, and value for money. Resilience ensures redundancy in strategic sectors such as energy and healthcare. Risk management allows scarce resources to be allocated based on the probability and impact of threats. Value for money guarantees the legitimacy of spending, ensuring that investments translate into tangible benefits for citizens and businesses. Yet each of these principles entails trade-offs: redundancy conflicts with efficiency, risk prioritization can leave some sectors underfunded, and value for money may favor short-term projects over long-term resilience. The managerial challenge lies in balancing these tensions through evidence-based evaluation and adaptive governance.

6.1 Financing protection in Italy

The Italian defense budget remains dominated by armaments and personnel, with limited resources devoted to protection sectors. This allocation reflects path dependency and political inertia rather than strategic priorities. As Gilli and Rauti (2025) have shown, indiscriminate increases in defense spending risk generating inefficiency and eroding democratic legitimacy. The new NATO target accentuates this problem: if the additional 3% of GDP is absorbed by traditional programs, opportunity costs will be enormous, undermining investments in cybersecurity, renewable energy, and healthcare resilience.

Toward a National Resilience Fund

A structural response would be the creation of a National Resilience Fund, designed to mobilize resources from the state budget, European programs, and public-private partnerships. This fund should prioritize investments in high-multiplier sectors, combining short-term benefits with long-term resilience. Inspired by venture capital models, it could finance innovative projects and start-ups in dual-use technologies, accepting a degree of risk in exchange for high potential returns. Transparent criteria and evidence-based evaluation would ensure legitimacy, while the involvement of private actors through PPPs would reduce fiscal pressure and broaden the resource base.

Integration with NATO and the EU

Financing protection must also align with Italy's international commitments. The 1.5% of GDP earmarked for infrastructures under the new NATO target can legitimately include investments in energy grids, digital

infrastructures, and logistics hubs that strengthen both national resilience and collective defense. Similarly, European Union programs, from Horizon Europe to the Recovery and Resilience Facility, offer substantial resources that can be integrated into a coherent national strategy. In this way, Italy can transform external constraints into opportunities, aligning protection with both transatlantic and European frameworks.

6.2 Managerial and institutional implications

The shift to protection demands governance reform. Multi-level coordination is indispensable in a country marked by fragmentation among ministries, agencies, regions, and municipalities. The state must act as a facilitator, creating frameworks that integrate local and private capacities into national strategies. Without this reorganization, resources risk being dispersed and the effectiveness of protection undermined.

Accountability and legitimacy

The legitimacy of protection policies depends on the ability to demonstrate results. Citizens must perceive concrete improvements in the continuity of services, the reliability of infrastructures, and the transparency of investments. Developing new performance indicators, focused not on spending levels but on outcomes, is essential. Evidence-based accountability would allow Italy to reconcile fiscal constraints with the need for political consensus, transforming protection into a visible and tangible public good. Outcome-based metrics—continuity indices for essential services, time-to-recovery, incident cost avoidance—should replace input-based proxies (GDP shares), thus linking fiscal discipline with political legitimacy.

Cultural change in institutions

Institutional culture represents perhaps the greatest obstacle. Italian bureaucracy is often resistant to innovation, privileging procedures over outcomes. The protection paradigm requires a shift toward flexibility, rapid decision-making, and organizational learning. As Argyris and Schön (1996) remind us, resilience depends on the ability to question underlying assumptions and adapt accordingly. Without cultural change, even the best-designed policies risk being paralyzed by administrative inertia.

6.3 Conclusion

The findings developed throughout this study converge on a fundamental insight: the traditional defensive paradigm, historically grounded in military deterrence and territorial sovereignty, is structurally inadequate to confront the hybrid threats of the twenty-first century. These threats—cyberattacks, pandemics, climate shocks, disinformation, and energy disruptions—are systemic, transnational, and multidimensional. They undermine economic growth, institutional legitimacy, and social cohesion, dimensions that exceed the scope of conventional military logic.

From a theoretical perspective, this paper demonstrates the analytical value of reconceptualizing security through the lenses of management and economics. By integrating public goods theory, risk management, business continuity, and organizational learning, security emerges as a complex and collective public good rather than a purely military function. This interdisciplinary approach bridges a gap in the literature: security studies have traditionally neglected managerial sciences, while management and economics have rarely been applied to national security. The proposed framework therefore enriches both domains, offering a model capable of capturing the complexity of hybrid threats and the need for systemic responses.

From a comparative perspective, the evidence drawn from Germany, Canada, and Japan confirms that protection is not a theoretical aspiration but an operational reality. Germany has institutionalized resilience through massive investments in energy diversification and digital infrastructures, demonstrating the role of redundancy in reducing exposure to geopolitical shocks. Canada has implemented decentralized risk management frameworks, illustrating both the efficiency and the inequalities that can emerge from multi-level governance. Japan has embraced the principle of value for money by investing in dual-use technologies that simultaneously enhance security, innovation, and competitiveness. These cases highlight the feasibility of protection and reveal the managerial and political trade-offs involved in its implementation.

For Italy, the urgency of adopting the protection paradigm is evident. The country's vulnerabilities—high energy dependence, digital fragility, demographic imbalances, and institutional fragmentation—have been repeatedly exposed by recent crises, from the COVID-19 pandemic to the energy shock following the war in Ukraine. Persisting in a defensive paradigm centered on military spending and NATO benchmarks would not only perpetuate inefficiencies but also risk undermining fiscal stability and democratic legitimacy, as recent policy analyses have stressed (Gilli & Rauti, 2025). By contrast, adopting protection would allow Italy to align its security strategy with resilience, sustainability, and modernization.

The practical implications of this transition are threefold. First, financing: Italy should establish a National Resilience Fund capable of mobilizing resources from state budgets, European programs, and public-private partnerships, with allocation criteria based on cost-benefit analyses and evidence-based assessments. Second, governance: protection requires overcoming institutional silos by developing multi-level and networked governance models that integrate local administrations, private actors, and European frameworks. Third, culture: without a cultural transformation toward adaptability, accountability, and organizational learning, financial and institutional reforms will remain ineffective.

At the international level, protection does not undermine Italy's commitments to NATO and the EU but reinterprets them. The new NATO target of 5% of GDP can be transformed from a rigid quantitative constraint into an opportunity to invest in infrastructures, cyber resilience, and energy security that strengthen both national and collective defense. Similarly, alignment with EU instruments such as Horizon Europe and the Recovery and Resilience Facility allows protection to become a lever for fiscal sustainability and political legitimacy.

The broader conclusion is that protection represents not only a security paradigm but a modernization agenda. By reframing security as an investment in resilience, Italy can transform vulnerabilities into opportunities, enhancing competitiveness, attracting international funding, and reinforcing citizens' trust in institutions. Protection thus turns security from a passive cost into collective capital, capable of sustaining long-term prosperity and cohesion.

Ultimately, the transition from defense to protection is not a matter of choice but of necessity. In the twenty-first century, security and modernization are inseparable. States that persist in a defensive paradigm risk marginalization, while those that embrace protection can position themselves as proactive actors in an uncertain global order. For Italy, the adoption of this paradigm is the indispensable path to ensuring resilience, legitimacy, and prosperity in the decades to come.

Bibliography

1. **Anderson, R., & Moore, T.** (2006). The economics of information security. *IEEE Security & Privacy, 4*(2), 68–71. https://doi.org/10.1126/science.1130992
2. **Argyris, C., & Schön, D. A.** (1996). *Organizational learning II: Theory, method, and practice*. Reading, MA: Addison-Wesley.
3. **Bloomberg.** (2025, September 16). *Dutch boost defense spending to €27 billion after NATO pledge*. Bloomberg. https://www.bloomberg.com/news/articles/2025-09-16/dutch-boost-defense-spending-to-27-billion-after-nato-pledge?embedded-checkout=true
4. **Boin, A., & Lodge, M.** (2016). Designing resilient institutions for transboundary crisis management: A time for public administration. *Public Administration, 94*(2), 289–298. https://doi.org/10.1111/padm.12264
5. **Brynjolfsson, E., & McAfee, A.** (2017). *Machine, platform, crowd: Harnessing our digital future*. Cambridge, MA: MIT Press.
6. **Bundesministerium der Verteidigung.** (2016). *Weißbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr*. Berlin: BMVg. https://www.bmvg.de/resource/blob/5261486/015be272f8c0098f1537a491676bfc31/weissbuch-2016-data.pdf
7. **Buzan, B., Wæver, O., & de Wilde, J.** (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner. http://dx.doi.org/10.2307/2586187
8. **Collier, P.** (2007). *The bottom billion: Why the poorest countries are failing and what can be done about it*. Oxford: Oxford University Press. ISBN 978-0-19-531145-7
9. **Dunne, J. P., & Tian, N.** (2013). Military expenditure and economic growth: A survey. *The Economics of Peace and Security Journal*, ISSN 1749-852X – Vol. 8, No. 1 (2013). https://doi.org/10.15355/epsj.8.1.5
10. **European Commission.** (2016). *Joint framework on countering hybrid threats: A European Union response*(JOIN/2016/018). Brussels: European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018
11. **Freedman, L.** (2013). *Strategy: A history*. Oxford: Oxford University Press. ISBN 9780199325153.
12. **Gilli, A., Gilli, M., & Petrelli, N.** (2024). *Before Vegetius: Critical questions for European defense* (Policy Brief No. 31). Institute for European Policymaking @ Bocconi University. https://iep.unibocconi.eu/publications/policy-briefs/policy-brief-n-31-vegetius-critical-questions-european-defense
13. **Gilli, A., & Rauti, A.W.** (2025). *The European defense spending trilemma* (Policy Brief No. 42). Institute for European Policymaking @ Bocconi University. https://iep.unibocconi.eu/publications/policy-briefs/policy-brief-n42-european-defense-spending-trilemma
14. **Herbane, B.** (2010). Small business research: Time for a crisis-based view. *International Small Business Journal, 28*(1), 43-64. https://doi.org/10.1177/0266242609350804
15. **Hoffman, F. G.** (2007). *Conflict in the 21st century: The rise of hybrid wars*. Arlington, VA: Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf
16. **Hooghe, L., & Marks, G.** (2003). Unraveling the central state, but how? Types of multi-level governance. *American Political Science Review, 97*(2), 233–243. https://doi.org/10.1017/S0003055403000649
17. **Hook, G. D., Gilson, J., Hughes, C. W., & Dobson, H.** (2018). *Japan's international relations: Politics, economics and security* (3rd ed.). London: Routledge. ISBN 9780415587433
18. **Hopkin, P.** (2018). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (4th ed.). London: Kogan Page.

19. **M Security.** (2022). *Cost of a data breach report 2022*. Armonk, NY: IBM Corporation. https://www.ibm.com/reports/data-breach
20. **IEA – International Energy Agency.** (2022). *Energy policy review of Italy 2022*. Paris: OECD/IEA. ISBN 9780749479619
21. **Ignazi, P.** (2017). *Party and democracy: The uneasy relationship*. Oxford: Oxford University Press. ISBN 9780198735854
22. **Kaplan, R. S., & Mikes, A.** (2012). Managing risks: A new framework. *Harvard Business Review, 90*(6), 48–60. https://hbr.org/2012/06/managing-risks-a-new-framework
23. **Kaul, I., Grunberg, I., & Stern, M. A.** (Eds.). (1999). *Global public goods: International cooperation in the 21st century*. New York: Oxford University Press. https://doi.org/10.1093/0195130529.001.0001
24. **Ministry of Defense Japan.** (2020). *Defense of Japan 2020 White Paper*. Tokyo: Government of Japan. https://www.mod.go.jp/en/publ/w_paper/wp2020/pdf/index.html
25. **Mumford, A. Carlucci P.** (2023). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*. 2023;8(2):192-206. doi:10.1017/eis.2022.19
26. **NATO.** (2025, June 14). *Defence ministers agree new capability targets to strengthen the Alliance*. https://www.nato.int/cps/en/natohq/news_235900.htm?selectedLocale=en
27. **Nye, J. S.** (2017). *Is the American century over?*, *Political Science Quarterly*, Volume 130, Issue 3, Fall 2015, Pages 393–400, https://doi.org/10.1002/polq.12394
28. **Nye, J. S.** (2023). *Soft power and American foreign policy*. In: Soft Power and Great-Power Competition. China and Globalization. Springer, Singapore. https://doi.org/10.1007/978-981-99-0714-4_7
29. **OECD – Organisation for Economic Co-operation and Development.** (2019). *Strategic crisis management*. Paris: OECD Publishing. https://dac.unb.br/images/DASU/PANDEMIA/Leituras/OCDE_Strategic-Crisis-Management.pdf
30. **Olson, M.** (1965). *The logic of collective action: Public goods and the theory of groups*. Cambridge, MA: Harvard University Press. ISBN 9780674537514
31. **Pisano, G. P., Sadun, R., & Zanini, M.** (2020). Lessons from Italy's response to coronavirus. *Harvard Business Review*. https://hbr.org/2020/03/lessons-from-italys-response-to-coronavirus
32. **Public Safety Canada.** (2018). *Emergency management strategy for Canada: Toward a resilient 2030*. Ottawa: Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgncy-mngmnt-strtgy/index-en.aspx
33. **Reuters.** (2025, September 15). *Swedish government to hike military spending to 2.8% of GDP in 2026*. Reuters. https://www.reuters.com/world/swedish-government-hike-military-spending-28-gdp-2026-2025-09-15/
34. **Rhodes, R. A. W.** (2012). *Network governance and the differentiated polity: Selected essays*. Volume I. Oxford: Oxford University Press. ISBN 9780198786108
35. **Rid, T.** (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux. ISBN 9780374287269
36. **Sandler, T., & Enders, W.** (2004). An economic perspective on transnational terrorism. *European Journal of Political Economy, Elsevier, vol. 20*(2), 301–316. https://www.diw.de/sixcms/detail.php?id=39116
37. **SIPRI.** (2025). *NATO's new spending target: Challenges and risks associated with a political signal*. Stockholm International Peace Research Institute. https://www.sipri.org/commentary/essay/2025/natos-new-spending-target-challenges-and-risks-associated-political-signal