TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Alessandro Milici 234171IVGM

Building a cyber-resilient society: a case study of Italy's Public Administration in the face of rising cyberthreats

Master's thesis

Supervisor: Adrian Nicholas Venables

PhD

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Alessandro Milici 234171IVGM

Küberkerksa ühiskonna ehitus: Itaalia avaliku sektori juhtumiuuring tõusvate küberohtude taustal

magistritöö

Juhendaja: Adrian Nicholas Venables

PhD

Tallinn 2025

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Alessandro Milici

09.05.2025

Abstract

As cyber threats against public institutions grow in frequency and sophistication, enhancing national cybersecurity has become a critical priority for public sector governance. This thesis investigates how Italy's Public Administration addresses these evolving risks by evaluating the effectiveness of its cybersecurity strategies, institutional frameworks, and coordination mechanisms.

The study employs a qualitative case study approach, combining semi-structured interviews with Italian and Estonian cybersecurity experts. Empirical findings are structured around five thematic domains: strategy and governance, incident response and coordination, training and awareness, digital transformation, and comparative insights. The Westpole incident, where a third-party provider breach disrupted essential public services, is analysed to expose systemic vulnerabilities, particularly the effects of institutional fragmentation and limited coordination. Estonia's cybersecurity model is used as a benchmark throughout the analysis, offering lessons in centralised leadership, strong public-private partnerships, and a more mature cybersecurity culture.

While Italy has made progress in building institutional capacity, it continues to face major challenges, especially in overcoming fragmentation, integrating operational responsibilities, developing the cybersecurity workforce, and enforcing policy. In contrast, Estonia's cohesive and proactive approach demonstrates how resilience can be embedded across governance layers. The thesis concludes with actionable recommendations to strengthen Italy's cybersecurity posture, informed by empirical findings and comparative analysis.

This thesis is written in English and is 70 pages long, including 6 chapters, 2 figures and 5 tables.

Annotatsioon

Küberkerksa ühiskonna ehitus: Itaalia avaliku sektori juhtumiuuring tõusvate küberohtude taustal

Kuna küberohud avalike asutuste vastu muutuvad üha sagedasemaks ja keerukamaks, on riikliku küberturvalisuse tugevdamine saanud tähelepanuväärseks prioriteediks avaliku sektori juhtimises. Käesolev magistritöö uurib, kuidas Itaalia avalik haldus nendele muutuvatele riskidele reageerib, hinnates kehtivate küberturvalisuse strateegiate, institutsionaalsete raamistikute ja koordineerimismehhanismide tõhusust.

Uuring tugineb kvalitatiivsele juhtumiuuringule, mille aluseks on poolstruktureeritud intervjuud Itaalia ja Eesti küberturvalisuse ekspertidega. Empiirilised tulemused on organiseeritud viie temaatilise valdkonna kaupa: strateegia ja juhtimine, intsidentidele reageerimine ja koordineerimine, koolitus ja teadlikkus, digipööre ning võrdlevad tähelepanekud. Westpole'i intsident—kus kolmanda osapoole turvanõrkus halvas olulised avalikud teenused—on analüüsitud süsteemsete haavatavuste esiletoomiseks, eelkõige institutsionaalset killustatust ja piiratud koordineerimist. Analüüsi käigus kasutatakse Eesti küberturvalisuse mudelit võrdlusraamistikuna, pakkudes õppetunde tsentraliseeritud juhtimisest, tugevast avaliku ja erasektori koostööst ning laialdasest küberturvalisuse kultuurist.

Kuigi Itaalia on saavutanud edusamme institutsionaalse suutlikkuse ülesehitamisel, seisab riik jätkuvalt silmitsi suurte väljakutsetega—eriti killustatuse ületamisel, operatiivsete vastutuste integreerimisel, küberturvalisuse tööjõu arendamisel ning poliitiliste strateegiate jõustamisel. Seevastu näitab Eesti terviklik ja ennetav lähenemine, kuidas vastupanuvõime saab olla juurutatud kõigil valitsemistasanditel. Töö lõpeb rakenduslike soovitustega Itaalia küberturvalisuse olukorra tugevdamiseks, tuginedes empiirilistele leidudele ja võrdlevale analüüsile.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 70 leheküljel, 6 peatükki, 2 joonist, 5 tabelit.

List of abbreviations and terms

ACN	Agenzia per la Cybersicurezza Nazionale (National Cybersecurity Agency)
AGID	Agenzia per l'Italia Digitale (Agency for Digital Italy)
AI	Artificial Intelligence
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
COR	Comando per le Operazioni in Rete
DDoS	Distributed Denial of Service
DIS	Dipartimento delle Informazioni per la Sicurezza (Security Intelligence Department)
DPO	Data Protection Officer
E-ITS	Eesti Infoturbestandard (Estonian Information Security Standard)
ENISA	European Union Agency for Cybersecurity
GAN	Generative Adversarial Network
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
ITU	International Telecommunication Union
MFA	Multifactor Authentication
ML	Machine Learning
NATO	North Atlantic Treaty Organisation
NCSI	National Cyber Security Index
NLP	Natural Language Processing
NSC	Nucleo Sicurezza Cibernetica (National Cybersecurity Management Board)
PA	Public Administration
PNRR	Piano Nazionale di Ripresa e Resilienza (National Recovery and Resilience Plan)
PSN	Polo Nazionale Strategico (Strategic National Centre)
RIA	Riigi Infosüsteemi Amet (Information System Authority)
SME	Small and Medium Enterprises

Table of contents

List of figures

List of tables

1 Introduction

This chapter outlines the research problem and the broader context of cybersecurity in Italy's Public Administration (PA). While digital transformation has improved efficiency and service delivery, it has also exposed critical vulnerabilities, making the PA a growing target for cyberattacks. High-profile incidents have demonstrated the risks to sensitive data and the continuity of essential services, highlighting the need for stronger protective measures. This chapter provides an overview of the current state of cybersecurity in Italy's public sector and introduces the key research questions that this study aims to address.

1.1 The problem

Italy's PA is facing unprecedented challenges in the digital era, with cybersecurity becoming a critical concern. Building a cyber-resilient society is an urgent necessity amid the increasing prevalence and sophistication of cyber threats. Public institutions face mounting challenges as cyberattacks grow in frequency and impact, jeopardising national security, economic stability, and public trust.

The case of Italy illustrates this urgency: as the country undergoes rapid digitalisation within its PA, it has also become a prominent target for cybercriminals. Italy accounted for 12% of global cyber incidents in 2024 [1] , up from 11% in 2023 and 3.5% in 2011 [2] - highlighting a troubling upward trend.

The CLUSIT Report 2025 reveals that the number of significant cyberattacks - those causing substantial economic, technological, legal, and reputational damage [1] - in Italy increased by 9% in 2024 [1], confirming the growing vulnerability of Italy's public sector to increasingly complex and coordinated threats. The increasing digitalisation of public services, supported by the Triennial Plan for Digitalisation 2024-2026 [3] has created new opportunities for efficiency and citizen engagement but has also introduced complex security risks. Italy's PA - which includes central and local government bodies, judicial authorities, law enforcement agencies, and infrastructure services - saw a 12% increase in cyberattacks in 2024 alone [1].

Italy's response to these challenges has included the adoption of the National Cybersecurity Strategy (2022–2026) [4] and the establishment of the National Cybersecurity Agency (ACN) in 2021 to centralise and enhance national defense capabilities. However, despite these measures, the increasing frequency and impact of attacks reveal persistent gaps in Italy's cybersecurity infrastructure, including fragmented defense mechanisms, underfunded programs, and insufficient strategic integration [5].

While the health sector faces distinct challenges and is treated separately from general PA in cybersecurity frameworks, this research focuses exclusively on PA. The health sector, although mostly public in Italy, is therefore not considered within the scope of this study.

1.1.1 State-sponsored and politically motivated attacks

A notable shift in cyber threats has emerged in recent years, with hacktivism - politically motivated attacks and state-sponsored operations - becoming more prevalent. Russian-affiliated hacking groups have been particularly active, targeting key Italian institutions, including the Senate [6] and the Ministry of Defense [7]. The CLUSIT Report 2025 attributes a large proportion of these attacks to Russian-backed operations, reflecting broader geopolitical tensions.

While malware remains the most common attack type, accounting for 38% of incidents in 2024, the use of Distributed Denial of Service (DDoS) attacks underscores the increasing use of cyberattacks as tools of political and ideological pressure [1]. This trend is also confirmed by the European Network and Information Security Agency (ENISA), which highlights the growing prevalence of politically motivated DDoS campaigns targeting public institutions and critical infrastructure across Europe [8].

A DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of Internet traffic. The influx of illegitimate requests exhausts the target's resources, rendering it inaccessible to legitimate users [9].

DDoS attacks represented 21% of attacks in 2024, though the overall number of DDoS attacks in Italy decreased by 36% from 2023 due to improved mitigation strategies [1].

The decline in DDoS attacks suggests that Italy's defensive measures have improved in this area, but the persistent threat of malware and politically motivated data breaches remains significant [1].

1.1.2 Structural weaknesses and strategic gaps

Italy's fragmented and underfunded cybersecurity framework remains one of the key reasons behind its vulnerability to large-scale attacks. Despite the adoption of the National Cybersecurity Strategy and the establishment of the National Cybersecurity Agency (ACN), Italy's cybersecurity infrastructure continues to suffer from insufficient investment, and lack of coordination.

The December 2023 Westpole incident remains a key example of these weaknesses: a supply chain attack on Westpole, a private contractor that hosts the software PA Digitale and URBI, which are used by numerous PA bodies for digital services and administrative management. The attack caused widespread disruption to public services, including citizen registration systems and digital communication networks [10]. Italy's PA relies on private vendors for essential digital infrastructure. While this allows for technological innovation and improved service delivery, it also introduces security risks by creating potential vulnerabilities in the supply chain, especially if adequate checks are not conducted during the procurement process. The case was selected for its representative nature, impact scale, and the insights it offers into systemic vulnerabilities in Italy’s digital public infrastructure.

Supply chain attacks remain a growing concern. The CLUSIT Report notes that 19% of attacks in 2024 targeted infrastructure vulnerabilities linked to third-party service providers [1]. This underscores the need for stronger oversight, more robust contractual safeguards, and enhanced threat monitoring in vendor ecosystems.

At the same time, Italy’s national cybersecurity budget remains critically low. In 2023 Italy invested only 0.12% of its GDP in cybersecurity - approximately half the level of France and Germany, and well below the 0.3% allocated by the United States [2]. This lack of funding limits Italy’s ability to implement advanced threat detection systems, coordinate response efforts, and build resilient infrastructures.

Despite improvements such as the establishment of the Network Operations Command (COR) - responsible for the secure technical and operational management of all ICT systems of the defense - and the ACN, challenges in coordinating civilian and military roles continue to hinder Italy's ability to respond rapidly and effectively to cyber threats.

The European Union's NIS2 Directive aims to address these gaps by introducing stricter cybersecurity standards and reinforcing public-private cooperation. However, Italy's decentralised governance structure complicates the implementation of NIS2 measures at the local and regional levels.

While Estonia has implemented a Whole-of-Society Approach [11], combining civilian and military efforts in a unified defense structure, Italy's more compartmentalised strategy continues to hinder rapid threat mitigation and recovery. The absence of an integrated national threat response mechanism remains a critical gap in Italy's cyber resilience strategy.

1.1.3 Cybersecurity culture

One of the most critical challenges facing Italy is the lack of a cybersecurity culture and strategic awareness within public institutions. The CLUSIT Report identifies human error as a key factor in 40% of successful attacks in 2024, with incidents such as credential theft and phishing remaining common due to insufficient training and awareness [1]. This finding aligns with the views of Italian Chief Information Security Officers who identified the "human factor" as one of the main contributor to cyber risk in 2024 [12].

The NIS2 Directive mandates that Italy adopts a more proactive approach to cybersecurity training and awareness. However, Italy still lags behind other EU countries in implementing structured training programs for public sector employees. While some progress has been made, particularly with the introduction of security awareness programs under the National Cybersecurity Strategy, the overall level of cyber awareness remains low. The ACN highlights that education, training, and awareness are key to improving cyber resilience, especially in the public sector, and stresses the importance of building a strong cybersecurity culture at all levels of government [13].

In contrast, Estonia has embedded cybersecurity training into its national defense strategy. Estonia's Cyber Defense League and structured civilian-military cooperation have established a robust framework for both institutional and individual preparedness.

1.1.4 Emerging threat landscape

The 2024 CLUSIT Report identifies several evolving trends in Italy's cyber threat landscape:

- Malware remains the dominant threat, representing 38% of all incidents [1].
- DDoS attacks declined in absolute terms (from 111 in 2023 to 76 in 2024), but they remain strategically significant due to their use in politically motivated operations [1].
- Phishing and social engineering attacks increased slightly, accounting for 11% of all attacks in 2024 [1].
- Data exfiltration and targeted breaches targeting government networks increased, often linked to state-sponsored hacking groups [1].

These findings are validated by ENISA's Space Threat Landscape 2025, which highlight similar trends across Europe [14].

1.1.5 Estonia as a benchmark for Italy's cybersecurity

Estonia's position as a global leader in cybersecurity was shaped by a defining moment in its history - the 2007 cyberattacks, known as the Estonian Cyberwar or Bronze Night attacks. In April 2007, a wave of coordinated cyberattacks targeted Estonia's government institutions, banks, media outlets, and communication networks [15]. The attacks were triggered by a political conflict surrounding the relocation of the Bronze Soldier in Tallinn, a Soviet-era war memorial, which sparked protests and political tensions with Russia. The attacks were DDoS campaigns, which overwhelmed Estonia's digital infrastructure, taking down government websites, financial services, and communication systems for weeks. The scale and impact of the attacks were unprecedented at the time, as Estonia was already one of the most digitally connected societies in the world, with e-government services and online banking deeply integrated into daily life.

Estonia's cybersecurity model is built on a security-by-design approach [16] , developed after the 2007 cyberattacks exposed critical vulnerabilities in the country's infrastructure.

This event became a turning point for Estonia's national strategy, leading to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn in 2008 [15] . Estonia has since emerged as a global leader in cybersecurity, advising NATO on cyber defense and hosting major exercises like Cyber Coalition and Locked Shields. Estonia's proactive approach integrates public-private collaboration, and workforce training, positioning it as a model for effective national cybersecurity governance in Europe [16].

While Estonia differs significantly from Italy in terms of size, administrative structure, and digital infrastructure maturity, its integrated and proactive approach to cybersecurity might still offer relevant insights and adaptable practices for improving Italy's cyber resilience.

1.2 Research gaps

Although cybersecurity is an increasingly critical issue, significant gaps remain in the existing academic literature. Despite the growing importance of cybersecurity in Italy's PA, research on the topic remains limited. Most existing studies focus on general challenges, with little attention to the specific vulnerabilities and resilience strategies of the public sector. Comparative research, particularly in relation to other countries, is virtually absent. Estonia, as a global leader in e-governance and cybersecurity, offers a valuable benchmark for analysis. While the CLUSIT reports provide useful statistics on cybersecurity in Italy, they lack academic analysis.

1.3 Research questions

Given the context outlined and the challenges identified in Italy's PA cybersecurity framework, this study seeks to address the following research questions:

- How are cyber threats to both public and national security being addressed within the Italian public sector in the context of increasing digitalisation?
  - What factors contribute to the Italian public sector being a particularly attractive target for cyberattacks?

- How effective are Italy's cybersecurity policies and institutional responses in protecting Public Administration infrastructures, given its high-priority status for cyber threats?
    - What lessons can be learned from Italy's response to major cyberattacks, such as the Westpole incident, in terms of improving these strategies?
- How does Italy's approach to cybersecurity in the public sector compare to that of Estonia, a global leader in e-governance?
    - What best practices from Estonia's experience can Italy adopt to enhance its own cybersecurity strategy?

1.4 Research goals

Building on the identified challenges and research questions, this study aims to evaluate how cyber threats to Italy's PA are being addressed, assess the effectiveness of existing cybersecurity policies and institutional responses, and identify actionable improvements based on Estonia's best practices.

The research will focus on the following key areas:

- **Strategy and governance** - analysing the nature and scope of cyber threats targeting Italy's PA, including politically motivated and state-sponsored attacks and evaluating how well Italy's current cybersecurity policies and institutional frameworks protect PA from cyberattacks.
- **Incident response and coordination** - assessing Italy's capacity to detect, respond to, and recover from cyber incidents, including the level of coordination between government agencies.
- **Training and awareness** - examining Italy's efforts to build a cyber-aware workforce and enhance security culture within Public Administration.
- **Digital transformation and emerging technologies** - exploring how digital transformation and emerging technologies are influencing cyber resilience.
- **Comparative insights** – drawing lessons from Estonia's cybersecurity model, including its integrated public-private partnerships and strategic response framework.

By comparing Italy's framework with Estonia's cybersecurity practices, the study aims to identify critical areas where Italy's cybersecurity efforts can be strengthened and provide actionable recommendations for building a more resilient PA. This dual approach - assessing Italy's internal challenges while drawing insights from Estonia - offers a strategic framework for addressing both short-term vulnerabilities and long-term resilience.

This study is also designed to serve a range of stakeholders:

- **Institutions and policymakers** by offering a comparative perspective with Estonia to inform policy reforms and identify best practices.
- **PAs** by providing practical, targeted recommendations to improve training, preparedness, and institutional coordination.
- **Citizens and businesses** by contributing to improved service continuity and stronger protection of personal and organizational data.
- **Academia** - by filling a research gap on comparative cybersecurity in the public sector and contributing to broader studies on e-governance and institutional resilience.

Despite the increasing relevance of cybersecurity in Italy's public sector, academic research remains scarce. Most studies focus on general or private sector issues, while PA-specific risks and resilience strategies are often overlooked. Comparative analyses, especially with countries like Estonia, are nearly absent. The annual CLUSIT Report remains the main accessible data source but offers limited strategic analysis tailored to the public sector.

1.5 Thesis structure

This thesis is structured into six chapters. The first chapter introduces the research problem, objectives, and questions, focusing on Italy's cybersecurity challenges and positioning Estonia as a comparative benchmark. Chapter 2 reviews relevant literature and outlines the theoretical foundations, covering five key areas: governance, incident response, training, digital transformation, and Estonia's cybersecurity model. Chapter 3 describes the research design, including the qualitative case study approach, semi-structured interviews, and the methods used for data collection and analysis. Chapter 4 presents the results of the interviews, thematically organised. Chapter 5 offers a critical analysis of the findings in relation to the literature, highlighting systemic weaknesses in Italy's PA, the Westpole incident case-study and transferable insights from Estonia. The final chapter concludes the thesis by summarising key findings, answering the research questions, highlighting limitations and offering policy recommendations and inputs for further research.

2 Frameworks and Existing Research

This chapter outlines the theoretical foundations of this research. It begins with the presentation of a multidimensional theoretical framework that integrates compliance and regulatory theory, risk management theory, and organisational culture and behavioural theories. These perspectives offer a comprehensive lens to examine both the technical and human factors that influence Italy's PA cyber resilience. Following this, the chapter reviews existing literature on five key dimensions: national strategies and governance models, incident response and coordination mechanisms, training and awareness initiatives, the impact of digital transformation and emerging technologies, and comparative insights from Estonia's cybersecurity ecosystem. This review highlights existing knowledge, identifies gaps and situates the present study within a growing body of interdisciplinary research on cybersecurity governance and resilience.

2.1 Theoretical frameworks

2.1.1 Compliance and regulatory theory

Compliance and regulatory frameworks, such as the General Data Protection Regulation (GDPR), ISO27001, and NIS2, establish baseline requirements for data protection and security protocols. Effective regulation involves a combination of voluntary compliance and enforcement, where regulation should be responsive to the behaviour of the regulated entities [17]. This theory helps assess how well Italy’s PA aligns with these standards, the impact of compliance gaps on cyber-resilience, and the interplay between national strategies and European directives.

However, the distinction between formal compliance - adherence to legal and procedural requirements on paper - and operational compliance, meaning the consistent, real-world application of these measures, is critical. A PA may appear compliant in policy documents while lacking the practical capacity, resources, or awareness to implement those measures effectively. By examining the extent of alignment and enforcement at the local level, this framework clarifies whether fragmented governance is contributing to Italy’s cybersecurity weaknesses [5].

2.1.2 Risk management theory

Risk management theory provides a structured approach to identifying, evaluating, and mitigating cyber risks [18]. According to ISO31000, effective risk management involves four key stages: risk identification, risk assessment, risk treatment, and monitoring [19]. This framework will guide the analysis of Italy's incident response capacity, particularly in relation to the Westpole case. It will help assess whether Italy's PA effectively identifies and mitigates emerging threats and how governance gaps affect the country's overall risk posture.

2.1.3 Organisational culture and behavioural theories

The human element plays a critical role in the effectiveness of cybersecurity measures. Even the most advanced technical systems can fail due to human error, poor training, and weak institutional support. Organisational Culture and Behavioural Theories provide a lens to evaluate the state of cybersecurity training and awareness within Italy's PA, the cultural attitudes toward cybersecurity, and the role of PA leadership in fostering a security-conscious environment [20].

Human errors continue to play a significant role in cyber incidents globally. According to IBM, fostering a strong security-aware culture is among the most effective ways to mitigate human-related cyber risks and build resilience across institutions [21].

2.2 Literature review

2.2.1 Strategies and governance

Italy's cybersecurity landscape has faced escalating challenges, underscored by a significant increase in cyberattacks. According to the CLUSIT 2025 Report, Italy accounted for 10% of global cyberattacks in 2024, marking a 15.2% rise compared to the previous year. This surge highlights the growing intensity of cyber threats targeting the nation.

The PA sector has been particularly vulnerable, experiencing a notable rise in cyber incidents. This trend underscores the complexity of emerging threats and suggests gaps in Italy's defensive measures within the public sector.

Beyond individual incidents, these trends have broader implications, potentially undermining national security, public trust, and administrative efficiency. However, there remains a need for comprehensive research to determine whether these trends are driven by structural weaknesses within PA or broader systemic vulnerabilities in the national cybersecurity framework. Addressing this gap is essential for identifying root causes and formulating effective countermeasures.

Evolving institutional and strategic cybersecurity frameworks

Italy's cybersecurity architecture has undergone significant evolution since 2013, driven by the need to centralise responsibilities, improve national coordination, and align more closely with international standards [22] . The transformation began with the 2013 Monti Decree [23], which designated the Security Intelligence Department (DIS) as the principal authority responsible for national cybersecurity. This foundational step was expanded by the 2017 Gentiloni Decree [24], which reinforced DIS's role and established the National Cybersecurity Management Board (NSC) to support inter-institutional cooperation.

Further institutional consolidation occurred with the 2019 Legislative Decree No. 105 [25], which introduced the National Cybersecurity Perimeter, requiring critical infrastructure operators to comply with enhanced security standards and mandatory incident reporting protocols. A pivotal shift followed with the 2021 Legislative Decree No. 82 [26], which created the Agenzia per la Cybersicurezza Nazionale (ACN). This agency now leads Italy's cyber strategy, absorbing and streamlining functions previously scattered across ministries and security bodies. This structural consolidation was followed by the adoption of the National Cybersecurity Strategy 2022-2026, which outlines Italy's strategic vision for strengthening its cyber resilience. The framework sets out 82 concrete objectives structured around five key pillars: protection of national interests, development of cybersecurity capabilities, promotion of a secure digital transition, strengthening of public-private cooperation, and enhancing Italy's role in international cyber governance [4]. The strategy emphasises risk prevention, crisis response readiness, and capacity building across both the public and private sectors, reflecting ACN's central coordinating role.

Complementing the civilian-focused governance reforms, Italy also developed military cyber capabilities through the establishment of the Comando per le Operazioni in Rete (COR) or Network Operations Command in 2020 under the Ministry of Defense [22]. COR is tasked with defending national defense infrastructure and critical assets against cyberattacks, marking a significant step toward the militarisation and centralisation of cyber operations.

Italy's cybersecurity posture is increasingly shaped by its integration with NATO frameworks. As a supporter of NATO's collective defense commitments under Article 5, Italy is expected to contribute to and benefit from joint responses to large-scale cyber incidents. Italy's participation in NATO cyber exercises and policy coordination reflects a growing convergence with allied doctrines and practices [22].

A key development in Italy's cyber governance has been the transposition of the NIS2 Directive (EU 2022/2555) [27] through Legislative Decree No. 138/2024 [28]. The ACN has been appointed as the national authority to enforce the directive across sectors including PA, energy, transport, and health [29]. The directive introduces stricter incident reporting timelines, mandates enhanced supply chain risk management and reinforces obligations on both public and private entities. ACN is responsible for issuing secondary legislation and ensuring national alignment with the directive's strategic goals - particularly relevant in the wake of the 2023 Westpole incident, which exposed Italy's vulnerabilities in managing third-party risks and underlined the importance of rapid coordinated response capacity.

A significant barrier to coherent and long-term cybersecurity policymaking in Italy has been the chronic instability of its political landscape. Over the past decade, Italy has had six different governments, often accompanied by ministerial reshuffles that disrupt policy continuity. Each new administration tended to redefine its priorities, leading to cybersecurity frameworks being underfunded, inconsistently implemented, or deprioritised altogether. However, recent developments suggest that cybersecurity is gradually being taken more seriously at the political level. The ACN has outlined three key pillars - preparedness, capacity building, and autonomy - as the core of Italy's cybersecurity strategy moving forward, signalling increased institutional attention and a stronger commitment to long-term planning [30].

Governance gaps, cultural deficits, and supply chain risk

Italy's cybersecurity posture continues to be undermined by a range of systemic and structural weaknesses that limit its ability to respond effectively to a rapidly evolving threat landscape. Central among these issues are fragmented cybersecurity measures and institutional inconsistencies, which have made the country an increasingly attractive target for malicious actors. The lack of consistent policies and the absence of a cohesive national cybersecurity infrastructure have created critical gaps in defense, leaving key public sector assets vulnerable to attack [5]. This fragmented approach exacerbates risk exposure, as PA entities frequently fail to align with national strategies or implement coordinated cyber defense measures [31].

While the adoption of secure-by-design systems, structures, and software is essential, it is not sufficient to ensure national cyber defence. Effective defence requires a joint approach, given the pervasiveness of cyber threats and the shared vulnerability of both civilian and military infrastructures. Italy's COR was conceived to provide a unified response across the Ministry of Defence's digital ecosystem [22]. However, despite its joint mandate, its integration across institutions remains partial, with room for improvement in consolidating demand, reducing inefficiencies, and enhancing interoperability [22].

This lack of full integration reflects broader structural challenges. Unlike other NATO countries such as France, the UK, or the US, Italy does not currently adopt an "advanced defence" posture - a strategy allowing pre-emptive or offensive cyber operations outside of explicit attack scenarios. While this cautious approach aligns with domestic legal constraints, it limits Italy's cyber deterrence and agility. In contrast, other allies benefit from more flexible rules of engagement that enable the armed forces to anticipate and counter cyber threats more proactively [22].

Furthermore, Italy's cyber defence capacity remains underdeveloped due to insufficient investment in personnel training and intersectoral coordination. The skills developed within the military could be strategically leveraged to support broader national efforts, including the upskilling of civilian officials. This would contribute to a more unified, whole-of-nation approach to cybersecurity and enhance Italy's strategic posture within the evolving digital threat landscape [22].

In addition, Italy faces enduring resource constraints that hinder the operationalisation of its cybersecurity strategy. These include a shortage of skilled cybersecurity professionals, insufficient public investment in digital modernisation, and uneven capacity among regional and local administrations to comply with national standards. Compounding these issues is the limited cybersecurity culture across public institutions, where awareness of cyber risks and adherence to basic security protocols are not yet widespread or systematically reinforced [32].

2.2.2 Incident response and coordination

Incident response and coordination are widely recognised in the literature as foundational pillars of national cybersecurity resilience. In the context of PA, the ability to detect, respond to, and recover from cyber incidents requires not only technical readiness but also clear coordination mechanisms across institutional levels and sectors [8]. A failure to achieve timely coordination can exacerbate the impact of cyberattacks, leading to prolonged service disruption and cascading institutional risks. Literature also stresses the need for simulation exercises and institutional rehearsals to test system resilience and inter-agency collaboration [8]. These elements are often lacking in bureaucracies where cybersecurity responsibilities are dispersed, or where public-private collaboration is limited.

Furthermore, cybersecurity researchers emphasise the importance of role clarity and standardised communication channels during incidents. Without pre-established protocols and authority hierarchies, response efforts may become fragmented, with overlapping or contradictory interventions [33].

Institutional developments

Recent institutional changes in Italy, such as the creation of the ACN and the COR, reflect an attempt to formalize response structures. The ACN coordinates national efforts and has begun to define a clearer perimeter of cybersecurity responsibilities within the Public Administration. COR, within the Ministry of Defence, is designed to ensure readiness in detecting and mitigating national-level cyber threats. However, these initiatives are still maturing, and there remains a gap between strategic planning and operational execution, particularly at the regional and local levels [20].

In April 2025, the Italian Chamber of Deputies' Defense Commission reinforced this direction by calling for the creation of a unified national cyber command under the Ministry of Defence. The proposal aims to centralise coordination across civilian, military, and private actors, addressing persistent fragmentation in Italy's cyber defense structure. Alongside this, the Commission emphasised the urgent need for advanced cybersecurity training and the integration of digital security awareness into national education systems [34]. These recommendations underscore the growing recognition that institutional reform must be matched by long-term cultural and operational capacity-building to ensure effective cyber resilience.

Supply chain risks

Another critical vulnerability lies in supply chain security. Italy's increasing dependence on external service providers and third-party technology vendors has widened its attack surface. The Westpole ransomware attack, which disrupted services for hundreds of PAs, revealed how a single point of failure in the supply chain can cascade across the public sector. This reflects broader international concerns about the need to integrate cybersecurity safeguards into procurement, vendor oversight, and IT service management [35].

The literature also highlights the complexity introduced by third-party service providers and supply chain actors in cybersecurity response [5] . These dynamics are particularly relevant in cases where PA functions rely heavily on outsourced IT infrastructure. Though not deeply analysed in academic sources yet, this case underscores key literature findings on the importance of coordinated response protocols that extend beyond government institutions to include private sector stakeholders.

To enhance state control over sensitive public sector data and services, Italy introduced the Polo Strategico Nazionale (PSN) in 2022, a secure, state-coordinated cloud infrastructure. The PSN is designed to host the most critical digital services of the Public Administration, including justice, health, and finance. It forms a key component of Italy's broader national cloud strategy, aimed at strengthening digital sovereignty and cyber resilience [36]. Operating alongside other ACN-qualified providers, the PSN reflects a shift toward a vertical governance model, in which Public Administrations are required to migrate their data according to official risk classifications and security criteria.

While Italy has made structural progress in establishing national-level cybersecurity institutions, academic and policy sources consistently point to unresolved challenges in operational execution, particularly in complex, multi-actor environments like PA. These issues will be explored further through the empirical and case study components of this thesis.

2.2.3 Training and awareness

Organisational weaknesses and the human factor

The absence of a strong cybersecurity culture and the persistently low levels of digital literacy within Italy's PA significantly exacerbate institutional vulnerabilities to cyber threats. These challenges are deeply embedded in both the organisational structure of the PA and the behavioural conduct of individual officials, creating a dual axis of fragility that cybercriminals readily [20]. The average age of Italian public sector employees - approximately 49.8 years in 2024, according to Agency for the Negotiation Representation of PAs [37], further compounds the issue, as many workers may lack familiarity with digital tools or emerging cyber risks. This generational gap, combined with inconsistent and often insufficient training opportunities, contributes to a workforce that is ill-prepared to recognise, prevent, or respond to cybersecurity incidents effectively. Human error remains one of the most exploited entry points, with phishing and social engineering techniques alone accounting for approximately 11% of attacks in Italy in 2024, following malware and DDoS [2]. This confirms that attackers continue to prioritise the human factor as one of the most accessible and exploitable weaknesses in institutional cybersecurity architectures.

Training gaps

These shortcomings are often a direct result of insufficient training and a lack of sustained institutional emphasis on security protocols. In many cases, the conduct of public servants is shaped by a broader absence of cybersecurity awareness, leading to lapses in judgment, improper use of digital tools, and failure to adhere to basic security hygiene practices. A more structured and continuous educational effort is therefore essential. Training programs specifically tailored to the public sector are necessary not only to improve technical preparedness but also to instil a culture of accountability, vigilance, and shared responsibility. It is essential to work extensively on staff training to reduce risks coming from human error, such as failing to identify a phishing email or knowing how to respond appropriately in the event of an attack. Promoting awareness of the full cost of an attack could help employees understand the real impact of their actions and take cybersecurity precautions more seriously [1].

Despite recent efforts, the depth, consistency, and coverage of training remain highly fragmented across Italy's public sector. This reflects another structural deficiency in Italy's decentralised governance model, where many local and regional entities lack the necessary financial and technical resources to roll out comprehensive training and prevention programs. Moreover, cybersecurity often still remains a peripheral concern rather than an integrated component of institutional risk management, further limiting the potential impact of educational efforts [20].

A key national initiative to address training gaps is the "Syllabus" platform [38], recently reinforced by a 2025 Directive of the Minister for Public Administration Zangrillo, which mandates at least 40 hours of annual training for all public employees. While not limited to cybersecurity, the platform includes dedicated modules on cybersecurity and cyber hygiene [37]. Other certified courses may also be recognised, reflecting a more flexible but structured approach. This marks a notable step forward in institutionalising digital upskilling. However, persistent issues, such as limited IT support and uneven digital maturity, risk turning this obligation into a formality rather than meaningful progress on cyber resilience.

IBM highlights that around 95% of human decision-making is governed by intuitive, fast-thinking processes (System 1), rather than the slower, rational System 2. Most employees operate on autopilot, relying on habits and heuristics. Traditional awareness campaigns, focused on rational instruction, often fail to influence real behaviour unless they are reinforced in everyday routines.

To address this, IBM recommends applying the COM-B Behaviour Change framework, which emphasises:

- Capability: Do individuals have the knowledge and skills?
- Opportunity: Does the environment support secure behaviour?
- Motivation: Are people sufficiently motivated to act securely?

Rather than one-size-fits-all training, organisations should adopt role-specific and interactive approaches such as gamified learning, real-life simulations, and peer engagement through cyber champions. Positive reinforcement and leadership involvement are also key to embedding security into institutional culture [21].

Strategic reforms and the NIS2

To address these weaknesses, Italy must pursue an integrated strategy that aligns national practices with international standards, such as ISO 31000. This alignment would enable the systematic identification, evaluation, and mitigation of cyber risks, particularly in dynamic and complex environments where adaptability is paramount [39]. Beyond compliance, adopting a risk-based approach grounded in international frameworks would encourage proactive thinking, continuous monitoring, and the institutionalisation of resilience as a strategic objective.

Furthermore, as cyberattacks against Italian public infrastructures increased in both frequency and severity, the stakes are growing. Fragmented responses and isolated initiatives are no longer sufficient. A holistic policy shift is needed - one that incorporates regulatory reform, robust training programs, long-term investment, and the adoption of advanced technological safeguards. As the ACN has repeatedly emphasised, prevention remains the most viable form of deterrence, and this cannot be achieved without a digitally literate and cyber-aware workforce across all levels of government [33].

The NIS2 Directive along with its Italian transposition (Legislative Decree 138/2024), mandates periodic and comprehensive cybersecurity training across all organisational levels, from top management to general staff.

Article 21 [27] of the NIS2 mandates that entities implement appropriate and proportionate technical, operational, and organisational measures to manage cybersecurity risks. Among these measures, the directive explicitly includes basic cyber hygiene practices and cybersecurity training.

Furthermore, NIS2 places accountability on corporate management, requiring them to oversee and approve cybersecurity measures actively. This includes ensuring that both they and their employees possess the necessary knowledge and skills to address cyber risks effectively. Such stipulations aim to embed cybersecurity considerations into the core of organisational governance, promoting a top-down approach to security awareness.

By mandating these training and awareness initiatives, NIS2 aspires to rectify existing inconsistencies in cybersecurity preparedness across sectors. The directive's proactive stance on education and management involvement is anticipated to promote a more robust and uniformly secure digital environment throughout the EU.

Ultimately, building a cyber-resilient PAs require more than technological fixes. It demands a cultural transformation that embeds cybersecurity into the values, practices, and day-to-day operations of public institutions. Only through this integrated and sustained effort can Italy effectively safeguard its digital sovereignty and ensure the continuity of essential public services in the face of rising cyber threats.

Talent shortage and workforce development

Italy continues to face a significant shortage of cybersecurity professionals, with only 333 graduates from cybersecurity-specific university programs in 2023, just 0.09% of the total graduate population. This figure lags far behind countries like France and Spain, where comparable rates exceed 1% [40].

The PA is particularly vulnerable, struggling to attract and retain experts amid uncompetitive salaries, slow recruitment procedures, and limited career development pathways. Even with promising employment outcomes, such as a 93% employment rate [40] and above-average starting salaries for cybersecurity graduates, public roles remain unattractive compared to private sector opportunities.

Recent efforts, including new university programs, ITS expansion, and national certifications, reflect growing attention to workforce development. The ACN is also advancing doctoral scholarships and innovation networks to boost long-term capacity. Yet these initiatives are still early and unevenly distributed. Without coordinated investment and more attractive public sector conditions, Italy risks continuing to lag in building a robust cybersecurity workforce [41].

2.2.4 Digital transformation and emerging technologies

Emerging technologies such as AI (Table 1), cloud computing, the Internet of Things (IoT), and blockchain (Table 2) are rapidly transforming the cybersecurity landscape, offering both new tools and new vulnerabilities. While AI can significantly enhance PA's defensive capabilities by enabling predictive analytics, anomaly detection, and automated response, it also introduces complex risks. These include adversarial attacks exploiting algorithmic flaws, ethical challenges related to decision-making, and over-reliance on systems not fully understood or audited [42]. Italy's PA has yet to establish a comprehensive AI-specific cybersecurity framework, leaving a gap in both preparedness and regulatory oversight. Although some experimentation is underway, integration remains limited and highly uneven across sectors.

Italy's structural and financial limitations further hinder the effective adoption of emerging technologies in cybersecurity. As of 2023, Italy allocated just 0.12% of its GDP to cybersecurity - approximately half the levels seen in France and Germany [2]. This chronic underinvestment reflects a wider perception of cybersecurity as a cost rather than a strategic enabler of digital sovereignty and economic resilience [33]. Countries like France, which committed €1 billion to cybersecurity between 2014 and 2019, illustrate the transformative effect that sustained investment can have on institutional capacity and public-private innovation [43]. In contrast, Italy's fragmented procurement landscape where each PA often relies on different vendors, platforms, and IT security standards, creates silos that weaken national cyber defense and hinder interoperability [31].

Although Italy's Triennial Plan for Digitalisation [3] aims to improve digital public services, enhance interoperability, and streamline IT governance, cybersecurity is still treated as a peripheral concern in many digital transformation initiatives [18]. The uneven implementation of the plan has left smaller public entities especially vulnerable, with limited resources to upgrade legacy systems or adopt resilient-by-design digital infrastructure. According to recent analysis, Italy's digital attack surface is rapidly expanding, driven by hybrid work models, increased connectivity, and the accelerated adoption of cloud services [44]. At the governance level, a lack of strategic continuity and interinstitutional coordination further limits progress toward a unified, resilient digital ecosystem.

However, recent developments indicate a shift in this narrative. In 2025, the ACN secured a new wave of public and private investments to support national cybersecurity priorities. These include not only operational upgrades, but also targeted support for SMEs, innovation partnerships, and skills development. Such initiatives mark a promising move from reactive fragmentation to proactive ecosystem-building, laying the groundwork for a more secure, sovereign, and future-ready PA [45].

In the context of cybersecurity for PA, AI refers to the use of machine learning and data-driven algorithms to enhance threat detection, automate incident response, and support decision-making processes. However, AI also introduces new risks: it can be leveraged by malicious actors to carry out more sophisticated attacks. This dual-use nature makes AI both a powerful enabler and a potential vulnerability within digital transformation efforts.

Table 1. Use of AI in cybersecurity.

Category	Use case	Description
Defensive	Anomaly detection, threat prediction	ML algorithms identify deviations from baseline patterns to detect threats early [46].
	Automated malware classification and response	AI models classify malware and automate response actions based on behavior [47].
	Phishing detection, email filtering	NLP-based models scan emails and detect suspicious patterns typical of phishing [48].
Offensive	Deepfake-based impersonation attacks	GANs generate synthetic audio/video to impersonate individuals in scams [49].
	Data poisoning	Injection of malicious data into AI training sets to manipulate model behaviour [50].
	Adversarial machine learning (evasion attacks)	Manipulating input data to trick AI models into misclassifying threats [51].

Within cybersecurity for PA, blockchain is a distributed ledger technology used to secure and verify digital transactions, logs, and identities in a tamper-resistant manner. Its decentralised and immutable structure makes it particularly useful for ensuring data integrity, tracing document changes, and establishing trustworthy audit trails. However, blockchain also introduces novel security concerns. Vulnerabilities in smart contract logic can be exploited, while its structure can serve as a hidden, persistent channel for illicit communication or malware payloads.

Table 2. Use of blockchain in cybersecurity.

Category	Use Case	Description
Defensive	Tamper-proof audit trails, logs	Immutable ledger entries ensure that logs cannot be altered retroactively [52].
	Decentralised identity authentication	Blockchain enables secure and user-controlled digital identity verification [52].
	Document validation and timestamping	Hashes and timestamps stored on-chain validate the integrity of digital documents [52].
	Supply chain traceability	Tracks products/software through the supply chain to prevent tampering [52].
Offensive	Smart contract vulnerabilities	Exploitable bugs in smart contract logic can be used for unauthorised actions [52].
	Blockchain-based command & control infrastructure	Malware uses blockchain for hidden, tamper-resistant communication channels [52].

Although Artificial Intelligence and Blockchain appear conceptually opposed, one opaque and adaptive, the other transparent and immutable, their complementary strengths offer unique opportunities for building robust cybersecurity frameworks in the public sector.

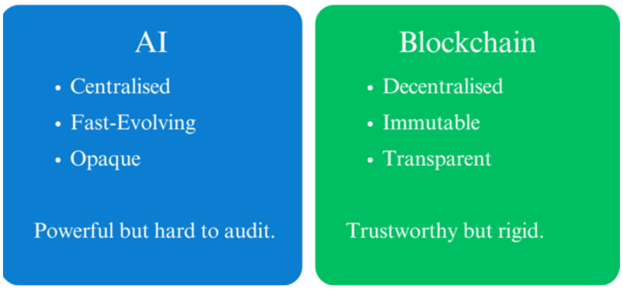


Image 1. Main differences between AI and blockchain [53].

2.2.5 Estonia’s cybersecurity governance

Estonia is widely recognised as a global leader in cybersecurity, due in large part to its early digital transformation, structured policy planning, and integrated public-private governance model, although recent concerns about growing bureaucracy and political interference have raised questions about the long-term agility and efficiency of its digital governance system [54]. Following the 2007 cyberattacks that targeted its critical infrastructure, Estonia developed a strategic, whole-of-society approach to cybersecurity that has since become a model for resilient digital governance [55].

A central feature of Estonia’s cybersecurity ecosystem is its strong coordination between public and private actors. The Estonian Information System Authority (RIA) and its operational arm, CERT-EE, play a crucial role in ensuring 24/7 monitoring, threat detection, and incident response. This centralised structure allows for consistent coordination across sectors and ensures that incidents are addressed promptly through clearly defined protocols. The National Cyber Security Strategy outlines strategic priorities in areas such as critical infrastructure protection, digital continuity, and public awareness, and is revised regularly to respond to geopolitical shifts and evolving threat landscapes [56].

Estonia also emphasises flexibility and scalability in crisis response. During the 2007 cyberattacks, the country activated a network of trained volunteer cybersecurity experts, enabling rapid scaling of defensive capabilities. This model, known as the Cyber Defence Unit within the Estonian Defence League, has become a permanent fixture in the national cyber ecosystem. It illustrates Estonia’s ability to mobilize community-based expertise and create cost-effective response mechanisms in times of crisis [57].

Another cornerstone of Estonia’s cybersecurity resilience is the integration of enforceable security standards across sectors. The 2021 E-ITS (Estonian Information Security Standard) introduced a binding set of security requirements for public and private network operators, ensuring a uniform baseline of cybersecurity measures. This regulatory clarity strengthens compliance and enhances coordination among stakeholders [56].

Estonia’s risk management and threat monitoring capabilities are also notable. With over 6500 cyber incidents with consequences recorded in a single year [58], Estonia demonstrates robust surveillance, logging, and reporting practices supported by its national

CERT. These systems contribute to early detection and containment, minimising the impact of attacks on public services and national infrastructure [59].

Furthermore, Estonia’s cybersecurity policies are closely aligned with its national digital strategy. With more than 99% of public services available online, cybersecurity is treated as a foundational element of service continuity and trust. Public awareness campaigns, high levels of digital literacy, and the integration of cybersecurity education in schools and universities contribute to a strong cybersecurity culture. These efforts help reduce the risk of human error, which is a common vulnerability in digital systems [60].

Estonia’s proactive investments in cybersecurity are reflected in its top-tier performance in international rankings, such as its third-place position in the 2020 ITU Global Cybersecurity Index. These achievements are the result of long-term strategic planning, resource efficiency, and clear policy direction. Rather than relying solely on budget increases, Estonia has demonstrated how targeted investment aligned with operational goals can yield substantial improvements in national cyber resilience [56].

In sum, Estonia’s cybersecurity framework is characterised by centralised coordination, community engagement, enforceable regulation, and continuous strategic adaptation. These elements are supported by strong monitoring systems and a deeply rooted cybersecurity culture, making Estonia a relevant reference point in the literature on effective cyber governance in digital states.

The National Cyber Security Index (NCSI), developed by the e-Governance Academy, is often used to benchmark countries' cybersecurity readiness [61]. As of 2024, Estonia and Italy are ranked 3rd and 4th respectively, suggesting a comparable level of institutional development. However, the NCSI focuses largely on policy presence and structural indicators, rather than real-world performance or resilience during actual incidents. This study considers the NCSI as a useful point of reference but further reflects on its limitations in the final analysis.

In contrast to Italy’s traditionally fragmented approach, Estonia has long adopted a centralised and integrated cybersecurity model, embedding digital resilience into national defence and public governance.

3 Research Methodology

This chapter outlines the research design and methodology used to investigate Italy's cybersecurity framework in the public sector, with a comparative analysis of Estonia’s approach. Given the complex nature of cybersecurity governance, a qualitative research design was selected to provide a deeper understanding of the underlying challenges, policy effectiveness, and potential improvements. The research combines semi-structured interviews, case study analysis, and comparative analysis to generate a comprehensive and context-specific understanding of Italy’s public cybersecurity landscape.

3.1 Research design

A qualitative research design was chosen because it allows for an in-depth exploration of complex issues such as governance fragmentation, institutional responses to cyber threats, and the cultural and organisational factors influencing cybersecurity measures [62].

The choice of a qualitative research design was justified by the need to:

- Explore the complex governance structures and fragmented institutional responses in Italy.
- Capture the context and human factors influencing cybersecurity effectiveness.
- Understand the lessons from Estonia that could be applied to Italy’s context.
- Allow for flexibility in the research process to adapt to emerging findings and new insights.

A qualitative approach enables a deeper understanding of the strategic, operational, and organisational aspects of cybersecurity governance, which would not be possible through quantitative methods alone.

3.2 Research techniques

The study combines a comprehensive literature review and semi-structured interviews to gather both theoretical and practical insights. The literature review establishes the foundation by analysing existing research, policies, and case studies, while the semi-structured interviews provide first-hand perspectives from experts, offering deeper insights into the practical challenges and strategies involved. The case study framework allows for an in-depth exploration of Italy’s cybersecurity framework, ensuring a well-rounded understanding of the research problem.

3.2.1 Literature review

A literature review, presented in Chapter 2, was conducted to establish a foundational understanding of Italy's and Estonia’s cybersecurity landscape, identify research gaps, and support the analysis of governance structures, policy frameworks, and past incidents. Literature analysis serves not only to summarise existing knowledge but also to identify patterns, contradictions, and areas for further investigation [63]. This method is essential for building a theoretical framework and guiding the research focus [64].

Key sources included the CLUSIT Reports on the state of cybersecurity in Italy, the Italian National Cybersecurity Strategy, the Estonian Cybersecurity Strategy, academic papers, and other official reports from various agencies, including the ACN. These documents provided valuable insights into national-level policies, threat landscapes, and strategic responses to cyber threats. This approach ensured a well-rounded understanding of the research problem and provided critical context for interpreting interview responses and comparative insights.

3.2.2 Semi-structured interviews

Semi-structured interviews were conducted with selected experts and stakeholders involved in Italy and Estonia’s cybersecurity governance. This method was chosen because it allows for both structured and flexible questioning, enabling the researcher to explore specific themes while also allowing for the emergence of new insights. The questionnaire used for interviews with Italian experts is provided in Appendix 3, while the questionnaire for Estonian experts is in Appendix 4.

This type of interview is defined as a managed verbal exchange where the interviewer maintains control over the structure while allowing the conversation to flow naturally [65]. This approach ensures that key themes are covered while giving respondents the freedom to provide deeper insights and expand on issues that may not have been anticipated.

Prior to conducting the interviews, informed consent was obtained from all participants, who were provided with details about the study's purpose, data handling, and confidentiality measures. The consent form is included in Appendix 2. To protect privacy, all participants remained anonymous, and their responses were handled in accordance with ethical guidelines explained at the end of this chapter.

The interviews focused on key themes such as:

- Strategies and governance
- Incidents and resilience
- Training and awareness
- Emerging technologies and future perspectives
- Comparison with Estonia

Participants included cybersecurity experts with experience in the public sector, either as consultants, academics, or public sector professionals. The interviews with Italian experts were conducted in Italian to encourage more genuine and natural responses, while the interviews with Estonian experts were conducted in English. The interviews were transcribed automatically and analysed using thematic analysis to identify recurring patterns and insights.

3.2.3 Research participants sampling

For this research, the purposeful sampling method was the most suitable approach as it targeted specific insights from experts in cybersecurity, policy, and Public Administration. Purposeful sampling involves selecting information-rich cases from which the researcher can learn a great deal about issues of central importance to the research question [66].

Participants were selected based on their experience, including academic or industry experts on cybersecurity in both Italy and Estonia. While outreach was made to members of Italy’s National Cybersecurity Agency, they were not available to participate. However, the selected participants still provided a diverse and valuable range of insights.

Respondents were identified through online searches using university websites and LinkedIn to target experts with relevant experience. The interviews were conducted through video calls, allowing for flexibility and direct engagement with the participants.

3.2.4 Sample demographics

The final sample included 11 participants: 7 from Italy and 4 from Estonia.

The final number of participants was determined based on their availability, aiming to gather a sufficient range of perspectives to capture diverse insights into Italy's cybersecurity framework and its comparison with Estonia's approach.

Table 3. Interview respondents.

ID	Role Description	Interview Duration (ca., minutes)
IT1	Head of research and innovation in a cybersecurity focused organisation, involved in public-private sector projects.	55
IT2	Academic specialising in administrative law and cybersecurity, advising public sector bodies on policy alignment.	60
IT3	Former CISO at a large company, now entrepreneur in cybersecurity, working with public sector agencies.	24
IT4	Professor of cybersecurity and penetration testing, advising public sector entities on security assessments.	52
IT5	Entrepreneur and consultant in cybersecurity, supporting public sector institutions with incident response.	38
IT6	Consultant for Public Administration and lecturer in cybersecurity, involved in public sector digital transformation projects.	34

IT7	Former public official and consultant for national cybersecurity agency, advising government on cyber policies.	73
EE1	Former director of a national cybersecurity agency overseeing public sector cyber strategy.	40
EE2	Researcher specialising in cybersecurity, conducting studies on public sector resilience.	55
EE3	Public sector cybersecurity expert, working directly with government agencies.	50
EE4	Cybersecurity Specialist at a national cybersecurity agency, with a focus on coordinating responses to cyber incidents, implementing national security strategies, and supporting critical infrastructure protection.	27

Among the Italian respondents, there is a balanced representation of perspectives: two academics specialising in administrative law and cybersecurity, two entrepreneurs with direct experience in managing cybersecurity companies, two consultants working for Public Administration and private organisations, and a former public official with expertise in national cybersecurity policy. The Estonian respondents include a former director of a national cybersecurity agency, a professor specialising in cybersecurity, and two public sector cybersecurity experts.

This diverse sample provides a comprehensive understanding of national strategies, governance challenges, incident response, and training approaches in both Italy and Estonia, with the contrasting governance models of the two countries serving as a key point of analysis.

3.2.5 Case study

A case study approach was selected to allow for an in-depth examination of Italy's cyberattack response within the PA sector. Case studies are suitable for understanding complex phenomena within real-life contexts, especially when the boundaries between the phenomenon and its context are not clearly defined [67].

The research includes a case study of the December 2023 Westpole cyberattack to examine its impact on Italy's PA and analyse the institutional response to a significant cyber incident. This case study helps explore the governance structure of Italy's cybersecurity framework and the role of public agencies and key stakeholders in managing cyber threats. The case study method involves analysing available sources and documents, including policy reports and official statements to provide a comprehensive understanding of the incident and its broader implications for Italy's cyber resilience.

3.3 Data collection

The study combined primary and secondary data sources.

3.3.1 Primary data

Primary data was collected through semi-structured interviews with cybersecurity experts from both Italy and Estonia. This method provided the flexibility to explore complex issues such as governance fragmentation and policy implementation while encouraging participants to share deeper, context-specific insights. The interviews were audio-recorded, automatically transcribed, and coded for analysis.

3.3.2 Secondary data

Secondary data included existing reports, policy documents, and case studies. A case study, the December 2023 Westpole attack, provided valuable insights into real-world cybersecurity incidents, helping to identify gaps in current measures and propose strategic improvements. By integrating these insights, the research aimed to enhance understanding of how Italy’s PA can strengthen its cyber resilience.

3.4 Data analysis

The data analysis employed three complementary qualitative methods to extract meaningful insights: Thematic Analysis, Case Study Evaluation and Comparative Analysis. The combination of these methods ensured data triangulation by integrating insights from interviews, reports, and case studies. This enhanced the credibility and depth of the analysis, providing a more comprehensive understanding of Italy's cybersecurity landscape.

3.4.1 Thematic analysis

Thematic Analysis was used to identify and interpret recurring themes and patterns across interview responses and secondary data. Thematic analysis involves a systematic process of coding data, identifying patterns, and defining themes to derive meaningful insights [68]. This method allowed for a structured analysis of both qualitative and secondary data, ensuring consistency and depth in the interpretation of findings.

After recording the interviews, a transcript was produced using the AI-based text-to-speech tool Transkriptor. The interviews with Italian experts were conducted in Italian to encourage more genuine and natural responses, while the interviews with Estonian experts were conducted in English.

The researcher read through the transcripts to ensure they were accurate and made sense, but no additional changes were made to the original content. The interviews are available auto-translated in English to allow non-Italian speakers to access them. However, the analysis was conducted on the original transcripts - in Italian for the Italian experts and in English for the Estonian experts - to preserve the authenticity and exact meaning of the responses. Only the findings and quotes used in the research were translated into English to ensure that the analysis remained as genuine and faithful to the original content as possible.

The analysis was guided by a thematic framework aligned with the research objectives, focusing on the following key areas: Strategies and Governance, Incidents and Resilience, Training and Awareness, Emerging Technologies and Future Perspectives, and Comparison with Estonia. In addition to these themes, the interviews with Estonian experts explored the benefits of Estonia's integrated cyber defense approach, offering insights into which aspects could be relevant or transferable to other countries, such as Italy. These categories align with the broader focus areas of the research and ensured coherence between empirical findings and the literature review.

AI tools were used to support the analysis process, including data organisation, thematic coding, and extracting key patterns from the interview transcripts. The use of AI helped to identify recurring themes and quantify consensus among respondents more efficiently. However, all findings, quotes, and conclusions were carefully reviewed and verified manually to ensure accuracy and consistency with the research objectives. This approach ensured that the analysis remains grounded in human interpretation while benefiting from the efficiency and pattern recognition capabilities of AI tools.

3.4.2 Case study evaluation

Case study analysis focuses on identifying patterns, evaluating responses, and extracting lessons from specific cybersecurity incidents, such as the Westpole attack. Case study analysis involves systematically organising data, identifying causal links, and drawing conclusions based on real-life events [67] . The data was analysed using a combination of pattern matching and explanation building to assess the effectiveness of Italy's response and identify gaps in current policies and strategies. This process involved gathering material from online sources, including reports, news articles, and official documents, to provide a comprehensive and up-to-date understanding of the incident and its implications.

Following the analysis, the findings were synthesised to identify lessons learned and potential improvements in Italy's cybersecurity approach.

3.4.3 Comparative analysis

Comparative analysis was used to benchmark Italy's cybersecurity governance against Estonia's digital framework. The analysis involved identifying both similarities and differences in governance structures, policy implementation, and incident response [69]. Thematic patterns emerging from interview data and policy analysis were systematically compared across both countries.

This analysis included a direct comparison of the national cybersecurity strategies, and the organisation of key agencies involved in cybersecurity governance. Differences in strategic priorities, agency coordination, and incident response frameworks were examined to identify practices in Estonia that could be adapted to improve Italy's cybersecurity framework. Insights from the interviews with Estonian experts were particularly valuable in understanding the practical implementation of Estonia's cybersecurity strategy and the operational dynamics between agencies. The interviews provided first-hand perspectives on the strengths and challenges of Estonia’s model, which helped to identify actionable lessons for Italy’s cybersecurity governance. The findings provided concrete recommendations for improving Italy’s cybersecurity governance by adopting some of Estonia’s successful strategies.

3.5 Ethical considerations

All research activities were conducted in accordance with ethical guidelines. Participants were informed about the purpose of the study, and their informed consent was obtained prior to the interviews (see Appendix 2).

To ensure privacy, all data was stored in an encrypted, password-protected environment, accessible only to the researcher. Data will be retained for 12 months and then securely deleted. Data collection and processing complied with GDPR guidelines.

Confidentiality and anonymity were maintained throughout the research process. All quotes and insights used in the analysis were anonymised to protect participants' identities. The data was used solely for the purposes of this study.

A list of the study’s main limitations, including access constraints and the evolving policy context, is provided in Chapter 6.

4 Results

This chapter presents the empirical findings derived from the semi-structured interviews conducted with cybersecurity experts from both Italy and Estonia. The interviews were designed to explore perceptions, experiences, and institutional realities concerning national cybersecurity strategies. In total, 11 participants, 7 from Italy and 4 from Estonia, shared insights on a range of issues, including governance structures, incident response, training and awareness, digital transformation, and international best practices.

To ensure thematic consistency and analytical clarity, the results are organized according to the same five macro-categories established in the literature review: strategy and governance, incident response and coordination, training and awareness, digital transformation and emerging technologies, and comparative insights with Estonia. These categories also guided the structure of the interview questions, allowing for alignment between the research objectives, data collection, analysis and discussion that follow.

4.1 Strategy and governance

4.1.1 Structural constraints

A recurring theme among Italian experts was the persistent gap between the formal cybersecurity strategy and its practical implementation. While the national strategy was generally viewed as well-structured, several respondents emphasised that its real-world execution remains inconsistent:

> *"The strategy looks good on paper, but its execution is lacking."* (IT1)
>
> *"You see the same pattern across the board: strong policies, weak execution."* (IT2)
>
> *"There is a significant gap between strategies and what is actually in place."* (IT4)
>
> *"What we write in strategies is not what happens in real life."* (IT5)
>
> *"There's a long road between what's written in the strategy and what gets implemented."* (IT6)

> *"Everything sounds great in the strategy documents, but we're always improvising when it comes to execution."* (IT7)

This disconnect is especially evident at the local level, where many administrations face severe capacity limitations:

> *"There's a big difference between the strategic document and the ability of small PAs to follow through."* (IT3)
>
> *"The strategic part is there. What's missing is the implementation, especially among small Public Administrations that simply don't have the necessary staff or skills."* (IT4)
>
> *"Many administrations lack both the expertise and the financial resources to implement cybersecurity measures"* (IT6).

These insights reflect a broader perception that strategic documents lack enforceability and are rarely backed by sufficient resources, accountability, or follow-through. This sentiment also casts doubt on international indices like the NCSI, which primarily evaluate the presence of formal strategies and institutions. Despite Italy's strong position "on paper," the real-world implementation remains weak and fragmented.

4.1.2 The role and limitations of ACN

Experts described the ACN as a crucial strategic actor but noted that its role remains limited in operational scope:

> *"ACN probably should play a more operational and less strategic role on certain issues, especially in cases of national interest."* (IT1)
>
> *"They [ACN] say what needs to be done, but then the responsibility falls on the Public Administrations."* (IT2)
>
> *"The implementation is slow because there's no real support for the smaller entities that need to apply it."* (IT3)
>
> *"There is a significant gap between strategies and what is actually in place."* (IT4)

> *"ACN plays a strategic, not an operational role on the ground."* (IT5)

> *"ACN is strategic, but on the ground it's not operational."* (IT6)

> *"There's a lack of support from ACN when it comes to practical implementation."* (IT7)

The agency's coordination efforts were recognised as a step forward, yet interviewees indicated that more hands-on support would be necessary to address the systemic gaps at the local level.

4.1.3 Fragmented Governance and Institutional Silos

Governance fragmentation was seen as a significant barrier to effective cybersecurity implementation. Several experts pointed to the multiplicity of actors and the lack of a coherent system-wide approach:

> *"There are two kinds of fragmentation: a lack of system-wide cooperation and overlapping responsibilities."* (IT6)

This was compounded by competitive behaviours among PAs, which tend to operate in silos:

> *"It's incredibly difficult for institutions to share successful models or even learn from each other."* (IT5)

The issue extends to procurement, where decentralisation further complicates coordination:

> *"Each region developed its own e-health record system. This multiplies the cost of securing them"* (IT4).

> *"Public procurement is not centralised, leading to duplicated efforts and inconsistent protections"* (IT5).

This structural disunity weakens national resilience and contributes to inefficiencies in both spending and protection.

4.2 Incident response and coordination

4.2.1 Inconsistent incident response

The findings align with the literature and highlights that the lack of centralised oversight contributes to slow and disjointed responses to major incidents. This topic appears in all seven interviews with Italian experts, consistently highlighting the systemic issue:

> *"The agency [ACN] has formal authority, but in practice it struggles to enforce decisions across regions and different levels of administration."* (IT1)
>
> *"Every region and municipality has its own approach to handling incidents. There's no unified national response plan."* (IT2)
>
> *"Local administrations often wait for guidance that never arrives. In the meantime, everyone improvises."* (IT3)
>
> *"There is a clear disconnection between central policies and what actually happens on the ground in municipalities."* (IT4)
>
> *"We lack a real chain of command when it comes to cybersecurity incidents. Everyone acts independently."* (IT5)
>
> *"When an incident occurs, the timing of response varies greatly depending on the agency involved. That's a systemic issue."* (IT6)
>
> *"I've seen cases where different institutions duplicate efforts without knowing they're working on the same issue."* (IT7)

4.2.2 Reporting and transparency challenges

The majority of Italian respondents noted that reluctance to report incidents prevents effective post-mortem analysis and weakens Italy's long-term resilience:

> *"There are thousands of incidents that go unreported or unnoticed."* (IT1)
>
> *"There's a cultural issue where agencies are afraid to disclose incidents out of fear of reputational damage."* (IT2)

> *"Incident reporting is not incentivised, and there's no structured feedback loop to analyse what went wrong."* (IT4)
>
> *"Unless the incident becomes public through media, it's often swept under the rug. No lessons are learned."* (IT5)
>
> *"People don't report incidents because they fear being blamed. That mindset needs to change if we want to improve."* (IT6)

This hesitation stems from a lack of incentives to report breaches and from political pressure to minimise public exposure to security failures. As highlighted by multiple interviewees, this culture of underreporting limits institutional learning and slows the development of effective response mechanisms. While not always explicitly addressed in national strategies, underreporting has been recognised as a persistent challenge to building long-term cyber resilience [70].

4.2.3 Need for improved coordination and resources

The lack of technical expertise, especially at the local level prevents an effective response:

> *"We can't expect small towns to defend themselves without external help - they simply don't have the tools or people."* (IT2)
>
> *"In many municipalities, there's only one person handling IT - and cybersecurity is just a small part of their job."* (IT3)
>
> *"Most local administrations lack the personnel and technical knowledge to respond to complex attacks."* (IT4)
>
> *"Even when guidelines exist, local administrations don't have the skills to implement them properly."* (IT5)
>
> *"Managing large-scale incidents requires enormous effort, and given the lack of resources, we just pray they don't happen at the same time."* (IT6)

This disparity reflects broader regional inequalities in Italy's PA and contributes to inconsistent cybersecurity preparedness across the country:

> *"Technical capacity is uneven. Some regions are better equipped, but many are years behind."* (IT6)

Moreover, enhancing public–private partnerships to bridge the expertise gap and create scalable, collaborative response mechanisms:

> *"The private sector has the resources and technical knowledge that the public sector lacks. We need better frameworks for working together."* (IT1)

Although no respondents explicitly commented on the Westpole incident, the broader concern over fragmented governance and reliance on third-party providers was present across interviews:

> *"The problem arises when we apply standards to Public Administrations [...] we should also define how far those standards extend to suppliers."* (IT4)
>
> *"Some administrations have started requiring that suppliers be ISO 27001 certified."* (IT4)
>
> *"The public sector now operates almost entirely via supply chains, lacking the ability to internalize functions or skills. They have many providers who are still not properly managed."* (IT5)
>
> *"Managing the supply chain in cybersecurity is especially challenging in organizations where vendors have full access to systems."* (IT5)

This reflects the broader literature finding that third-party dependencies represent a significant attack vector, particularly when public institutions rely on external vendors without comprehensive security requirements [18].

Respondents also exposed weaknesses in Italy's incident response mechanisms:

> *"There's the will to secure critical infrastructure like Terna, Anas, Poste — but bureaucracy and politics slow down everything."* (IT1)
>
> *"You need clear rules to guarantee resilience, especially when it comes to response mechanisms."* (IT2)

> *“Structures are not prepared in advance. When an incident occurs, they panic, improvise, make a lot of mistakes, and response times are far too slow.”* (IT5)

> *“There’s been improvement in prevention, but not in incident management.”* (IT5)

> *"No one knew who was responsible for coordinating the response. Public and private agencies were operating separately."* (IT6)

The findings highlight a clear need for stronger oversight of third-party providers and enhanced response coordination. Establishing national-level security standards for service providers and strengthening the ACN’s enforcement capacity would reduce these vulnerabilities and improve Italy’s overall resilience to supply chain attacks.

4.3 Training and awareness

The interviews confirmed the literature findings, highlighting both gaps in training coverage and a lack of institutional support for cybersecurity awareness.

4.3.1 Inconsistent training coverage and quality

All Italian respondents acknowledged that cybersecurity training across PA is inconsistent and inadequate. Some agencies conduct regular awareness sessions or distribute occasional materials, while others provide no structured training at all. This fragmented approach leads to highly unequal levels of preparedness across departments, sectors, and regions.

> *“Training is often considered optional. Some agencies invest in it, others don’t even mention it.”* (IT1)

> *"If the leadership doesn’t prioritise training, nothing happens."* (IT2)

> *“There’s no national standard for training. It’s left up to each administration, and the results vary a lot.”* (IT3)

> *“I’ve seen places where no one has ever had cybersecurity training, not even basic awareness.”* (IT5)

> *"It depends on the region or the head of the department. Some prioritise it [training], others see it as a waste of time."* (IT6)

Leadership priorities and institutional culture also influence whether cybersecurity training is valued or sidelined. In some organisations, awareness is embedded into operations, while in others it is seen as a disruption:

> *"If leadership doesn't believe in training, nothing gets done."* (IT2*)*

> *"In some cases, training is seen as intrusive or irrelevant."* (IT3)

> *"There's no culture of security—people do it only when the law forces them."* (IT6)

Some respondents criticised the overreliance on generic e-learning modules, noting that such approaches often fail to drive meaningful behavioural change. Without follow-up or accountability mechanisms, training remains superficial.

> *"People take the training, then go back to doing things the same way. There's no accountability."* (IT6)

> *"We need more than e-learning modules once a year. That's not enough to build real preparedness."* (IT7)

The importance of hands-on, scenario-based training - such as phishing simulations or crisis response exercises - are essential for building operational readiness. However, such initiatives remain rare across local public bodies.

> *"Phishing simulations should be mandatory, but hardly anyone does them."* (IT4)

> *"We run awareness sessions, but very few simulations. When an attack hits, no one knows what to do."* (IT7)

> *"We need practical training, otherwise people forget it or don't take it seriously."* (IT3)

4.3.2 Resource constraints

Budget limitations remain a major barrier to strengthening cybersecurity training. Respondents noted that many public sector organizations - especially small municipalities - lack the financial and human resources to support ongoing training efforts.

> *"Even where there's interest in the topic, there's no capacity to properly address it." (IT4)*
>
> *"Training is always the first thing to be cut when budgets are tight." (IT5)*
>
> *"Small municipalities don't have the resources. If they do any training at all, it's just basic and free materials." (IT6)*

These resource constraints contribute to an overall environment where cybersecurity capacity is fragmented and highly dependent on local context, leadership engagement, and available funding. The upcoming implementation of the NIS2 Directive may help address this gap by requiring regular training and promoting more consistent cyber risk management across the public sector.

Respondents also reported that cybersecurity is rarely prioritised in budget allocations. In some cases, funding is unstable and based on short-term projects, while in others, it is among the first areas to face cuts during financial constraints:

> *"There's no stable line of funding. Every year we start over from zero." (IT4)*
>
> *"The budget for security is always marginal. When cuts are needed, that's the first thing to go." (IT5)*
>
> *"If we had started ten years ago, we'd have spent a little more each year and be in a better place now." (IT6)*

These insights suggest that cybersecurity is still not perceived as a core institutional responsibility. Without consistent investment and long-term planning, it is difficult to adopt modern tools or retain qualified staff, consequently weakening the resilience of the entire system.

4.4 Digital transformation and emerging technologies

4.4.1 AI and automations: a double-edged sword

Respondents recognised the potential of AI but some stressed that misuse, lack of transparency, and excessive reliance on automated decision-making can be dangerous, especially in critical public services:

> *"The integration of AI in cybersecurity will be essential - attackers are already using it to create malware in just a few days." (IT1)*

> *"Artificial intelligence can help, but if we don't understand how it works, we risk creating new problems."* (IT2)

> *"Automating security is useful, but it can't replace human judgment."* (IT7)

The interview findings confirm that while AI is viewed as a valuable asset, its implementation must be carefully regulated and always balanced with human oversight and accountability.

4.4.2 Basic before advanced tech

> *"It's like we've motorised the world without giving anyone a driver's license." (IT6)*

While emerging technologies attract institutional interest and funding, both the literature and interview data suggest that foundational issues remain unresolved. Several respondents stressed that core cyber hygiene, such as secure access control, regular updates, and effective backups, should come before introducing advanced systems like AI, automation, or predictive analytics.

> *"Technology is important, but so is organisation. There's no point introducing advanced solutions if the fundamentals are missing." (IT3)*

> *"Before talking about AI, we should fix the basics: backups, updates, secure access." (IT6)*

This finding aligns with recent critiques which warn against *techno-solutionism* - the idea that all problems can be solved by technology [71] - and argue that resilience is built on basic digital infrastructure, not just innovation. These quotes reflect a pragmatic view from practitioners who see the limits of digital transformation when foundational capacity is lacking.

4.4.3 Beyond AI

In addition to artificial intelligence, interviewees highlighted other technologies shaping cybersecurity frameworks. These included quantum computing, blockchain, IoT and operational technology (OT) convergence, and physical infrastructure risks tied to cloud migration and data centre reliance.

> *"We'll soon see the impact of quantum computing - if it becomes usable." (IT6)*
>
> *"A European public blockchain could help with cross-border admin processes and document trust."* (IT7)
>
> *"We've connected legacy systems like power plants, trains... all vulnerable now."* (IT6)
>
> *"Data centres must be physically protected - not just from hackers, but also floods, blackouts, even terrorism."* (IT7)

These reflections illustrate that cyber-resilience planning cannot be limited to digital threats alone but must also anticipate the physical, systemic, and geopolitical risks linked to emerging infrastructure dependencies.

4.5 Comparison with Estonia

The interviews reinforced the literature findings, highlighting Estonia's centralised governance, effective incident response, and strategic use of public-private partnerships as key differentiators from Italy's approach.

Table 4. Italian and Estonian experts' responses comparison.

Topic	Italy	Estonia
Governance and coordination	Italy follows a fragmented governance model where ACN provides strategic guidance but lacks enforcement power. This leads to inconsistent implementation at the regional and local levels. *"When something goes wrong, the local government says it's the national government's responsibility, and vice versa. No one takes ownership." (IT4)* *"ACN provides the strategy, but the implementation depends on local authorities — and that's where it falls apart."* (IT5)	Estonia operates under a centralised governance model where RIA serves as both the strategic and operational authority. RIA provides direct oversight and enforcement capacity, which ensures consistent implementation of security measures. *"RIA is not a policy-making body, but they execute policy and provide operational support. They ensure that standards are followed and that responses are coordinated."* (EE2) *"Well, they* [RIA] *are the National Cybersecurity Centre. So they have the CERT functionality, supervision functionality, creating the Estonian Information Security Standard. They do the security assessments, reporting, and analysis part."* (EE4)

Incident response and resilience	Italy’s fragmented response structure creates delays and confusion. *"When an attack happens, there’s confusion over who is responsible. A centralised structure would make it easier to track threats and coordinate responses."* (IT3)	Estonia’s centralised governance ensures a coordinated and structured incident response. RIA, working through CERT-EE, provides real-time monitoring and manages national-level threat intelligence. *"CERT-EE provides direct support during incidents — they can isolate threats and coordinate the response immediately."* (EE1) *"RIA provides a single point of contact during incidents. There’s no confusion — everyone knows who is responsible."* (EE4)
Training and awareness	Cybersecurity training among PA employees is inconsistent and insufficient: *"There's no national framework — each agency decides what to do, so it's inconsistent."* (IT3) *"Some agencies have great training programs; others have none."* (IT5) *"Smaller agencies don’t have the budget or the staff for training. It’s not a priority.”* (IT6)	Training in Estonia is mandatory and centrally coordinated. RIA offers training programs across all public sector entities: *"First of all, this training is mandatory for all the agencies. So they need to do something. RIA has their own centralised test."* (EE4) *"Every agency in Estonia is part of the same training framework. That’s why our response time is faster — everyone knows the protocol."* (EE4)

	"People attend training, but there's no real follow-up. No one checks if the knowledge is applied." (IT7)	
Public-private collaboration	Italy's collaboration with the private sector is more fragmented and inconsistent: *"There's some collaboration at the national level, but most local agencies operate independently."* (IT6)	Estonia's cybersecurity framework actively involves private sector support through penetration testing, vulnerability assessments, and shared infrastructure. *"The private sector is a key partner. We rely on their expertise for threat analysis and recovery support." (EE4)*
AI and emerging technologies	Both Italian and Estonian respondents identified AI as a double-edged sword: a potential tool for improving threat detection but also an emerging risk for sophisticated attacks (e.g., deepfakes). *"We already have good systems, but they're not being used properly. Introducing AI without fixing the basics won't help." (IT5)* *"AI is improving threat detection — but if you don't have solid infrastructure, AI won't fix your weaknesses." (EE1)*	
Transparency and information sharing	In Italy, transparency remains an issue: *"Many agencies are afraid to disclose incidents because they see it as a reputational risk."* (IT4)	Estonia's approach to transparency is a key strength: *"Transparency builds trust. If you try to hide an incident, people lose confidence." (EE2)*

4.5.1 Critical perspectives on Estonia's cybersecurity strategy

While Estonia is internationally recognized as a pioneer in cybersecurity and e-governance, expert interviews reveal several critical perspectives and structural challenges that merit attention. These critiques offer a nuanced understanding of the limitations of the Estonian model, particularly when considered for potential adaptation in other national contexts such as Italy"

4.5.1.1 Overemphasis on the public sector

One of the most frequently cited concerns is the Estonian cybersecurity strategy's predominant focus on the public sector. While the public infrastructure is well-developed, the strategy has been criticised for insufficiently addressing the integration of private sector capabilities and responsibilities. As one expert observed:

> *"The Estonian strategy is… leaning more towards the public sector… which has been one of its criticisms." (EE2)*

This delineation risks creating silos and may undermine the holistic resilience of the broader national ecosystem.

4.5.1.2 Over-compliance with external regulations

Estonia's strong alignment with EU policies and directives is generally seen as positive. However, some respondents suggested that Estonia tends to implement supranational regulations too rigidly, sometimes without sufficient critical assessment:

> *"Other more sensible countries… ignore some more stupid regulations, while Estonia tends to fulfil all of them to the prompt." (EE3)*

This rigid compliance may lead to inefficiencies or reduced agility in responding to national priorities.

4.5.1.3 Administrative inflexibility and bureaucracy

Despite Estonia’s reputation for lean governance, some experts highlighted growing bureaucratic inertia, particularly within institutions that were once more agile before structural reforms.

> *“It was much more flexible earlier… with the big university came all the bureaucracy.”* (EE3)

This concern links to a perceived risk that increased institutionalization may reduce the state's responsiveness in rapidly evolving cyber environments.

4.5.1.4 Operational Fragmentation and lack of integration

A more technical critique emerged around the lack of coordination among Security Operation Centers (SOCs) and the use of diverse, incompatible systems across agencies.

> *“Maybe we should have more cooperation between the security operation teams… joint procurement… same tools… same language.”* (EE4)

This fragmentation potentially limits situational awareness and slows down the detection and response cycle during incidents. However, it is important to note that centralised tools are not a cure-all: if they fail to meet the specific operational needs of an agency, they may prove just as ineffective.

4.5.1.5 Technology-centric approaches without sufficient human support

A recurring theme was the perceived imbalance between technological investments and accompanying human or policy development.

> *“It is just giving technology without the training and policy. It’s repeating old mistakes.”* (EE3)

This echoes past national programs, where hardware was provided without adequate support or understanding.

5 Analysis

This chapter interprets the empirical findings from expert interviews by situating them within the broader academic discourse and national policy contexts outlined in the literature review. The analysis is organized into five thematic sections: Strategy and Governance, Incident Response and Coordination, Training and Awareness, Digital Transformation and Emerging Technologies, and Comparative Insights. Together, these areas provide a multidimensional view of how Italy and Estonia approach public sector cybersecurity. Attention is also given to the Westpole case, which exemplifies systemic vulnerabilities in Italy's coordination mechanisms and serves as an applied illustration of the theoretical challenges addressed in this research.

5.1 Interview finding analysis

5.1.1 Strategy and governance

As highlighted in the literature, governance is foundational to cybersecurity resilience, particularly in complex administrative systems like Italy's. Interview data reinforce the notion that Italy's cybersecurity governance remains fragmented despite recent institutional developments. Although the creation of the ACN has been a step toward centralisation, the agency's coordination role is still limited in reach, especially at regional and local levels. The persistence of institutional silos, overlapping mandates, and inconsistently applied strategies undermines the systemic coherence needed for robust cyber governance.

Estonia, by contrast, demonstrates a higher degree of strategic alignment and institutional clarity. Although not without some criticism, respondents described an ecosystem where roles and responsibilities are well defined, strategies are regularly updated, and cyber policies are integrated into broader national planning. This supports the theoretical perspective that mature compliance, and regulatory environments facilitate more effective policy implementation. Estonia's approach reflects a model of embedded governance, where cybersecurity is not only a technical concern but also a public value aligned with national priorities.

5.1.2 Incident response and coordination

The capacity to detect, manage, and recover from cyber incidents is a critical aspect of resilience. In Italy, this domain appears constrained by operational fragmentation and limited interoperability among key actors. While the ACN and COR have introduced national-level coordination mechanisms, the interviews revealed persistent gaps in real-time information sharing, decision-making clarity during crises, and engagement with private sector actors, particularly those providing critical infrastructure.

The Westpole incident serves as a concrete example of these challenges. As a private provider of IT services to multiple PAs, its compromise had ripple effects across the public sector. The lack of a coordinated response mechanism between affected entities, central authorities, and the private sector highlighted systemic weaknesses in Italy's incident management capabilities. This case also reinforces theoretical insights from risk management literature, which stress the importance of distributed yet coordinated response frameworks in complex digital ecosystems.

In contrast, Estonia's CERT-EE and its centralised response model exemplify best practices in national coordination. Incident response is streamlined, well-resourced, and integrated with both private and public actors, allowing for more rapid containment and recovery. The existence of predefined protocols, regular simulation exercises, and continuous threat monitoring ensures operational readiness, aligning with the literature's emphasis on proactive and rehearsed incident response strategies.

5.1.3 Training and awareness

Cybersecurity culture and workforce development emerged as significant themes in the interviews. Italian experts consistently pointed to low levels of digital awareness and cybersecurity literacy within the PA. Despite ongoing efforts and training programs promoted by national agencies, implementation is uneven, and digital security is often seen as a secondary concern in day-to-day operations. This reflects broader organisational culture issues and aligns with behavioural theories that emphasise the role of awareness and habit in shaping security outcomes.

In Estonia, digital literacy and cybersecurity awareness are deeply embedded in the public sector workforce. Cyber hygiene is treated as a collective responsibility, and training is incorporated across educational and professional levels. Interviewees emphasised the benefits of this long-term investment in human capital, which reduces human error and strengthens organizational preparedness. The Estonian model illustrates how cultivating a cybersecurity-aware workforce can enhance resilience without relying solely on technological solutions.

From a theoretical standpoint, the contrast reflects differing levels of maturity in cybersecurity culture. Italy's challenges can be viewed through the lens of organisational behavioural theory, where lack of shared norms and low perceived relevance contribute to gaps in security practice. Estonia's experience, meanwhile, supports the literature on the benefits of sustained investment in awareness as part of a broader cybersecurity strategy.

5.1.4 Digital transformation and emerging technologies

The integration of emerging technologies into PA presents both opportunities and vulnerabilities. In Italy, digital transformation has accelerated, particularly under the national recovery plan (PNRR) [72], but cybersecurity integration remains inconsistent. Interviewees noted that while digital services are expanding, security considerations are often treated as add-ons rather than foundational design elements. This reflects a disjointed transformation trajectory where modernization outpaces secure implementation.

Estonia offers a contrasting model, where cybersecurity is structurally embedded into digital service development. The digital-by-default principle ensures that security is considered from the outset of service design. Secure data exchanges, and the national digital identity infrastructure are examples of how cybersecurity is intertwined with public service delivery. The maturity level of Estonia's digital transformation reflects theoretical frameworks on secure digital architectures and the importance of aligning innovation with resilience.

The findings suggest that while both countries recognise the centrality of digital transformation, the degree to which cybersecurity is internalised varies significantly. Italy's PA faces a risk of expanding its digital footprint without adequate safeguards, a concern that may be further exacerbated by resource constraints and inconsistent implementation of national guidelines.

5.1.5 Comparative insights: Italy and Estonia

The comparative dimension of this study reveals structural, cultural, and strategic differences between Italy and Estonia in their approaches to cybersecurity in the public sector. Estonia's model is characterized by centralized coordination, regulatory clarity, strong public-private partnerships, and a proactive, strategic culture of preparedness. Italy, while demonstrating recent improvements, continues to face challenges related to fragmentation, uneven implementation, and cultural resistance to prioritizing cybersecurity across administrative levels.

The contrast reflects deeper systemic factors. Estonia's small size and digital state model allow for tighter coordination and faster adaptation, whereas Italy's administrative complexity and multilevel governance structure introduce inertia. Nevertheless, the interviews also highlight opportunities for policy transfer. Best practices such as centralized incident management, enforceable regulatory standards (like Estonia's E-ITS), and volunteer-based rapid response mechanisms offer potential pathways for strengthening Italy's national cybersecurity posture.

This section reinforces the relevance of the theoretical framework adopted in this research. Compliance and regulatory theory explains Estonia's institutional success, while risk management theory helps interpret Italy's vulnerabilities and reactive postures. Finally, organisational culture theory offers insight into the differing levels of workforce preparedness and awareness between the two cases.

5.2 The Westpole incident

5.2.1 Overview of the incident

On 8 December 2023, Westpole, a key cloud service provider for Italy's PA owned by Cegeka Company, was hit by a severe ransomware attack. The attack, later attributed to the Lockbit group, made Westpole's data centers in Milan and Rome. The incident had an immediate and cascading impact, particularly on PA Digitale S.p.A., a provider of digital services to over 1300 PAs, including 540 municipalities [73], and on its widely used platform URBI, a critical system enabling public sector digital workflows, from registry and document management to accounting, human resources, and other citizen-facing services.

5.2.2 Immediate Consequences

The attack was considered severe and extensive due to its systemic repercussions on national digital infrastructure. While Westpole confirmed that no personal data was compromised, the availability of data was entirely lost, leaving systems non-functional for over a week.

Municipalities relying on URBI and PA Digitale were unable to process electronic invoices, access digital archives, or issue certificates. Citizens were directed to contact offices by phone or in person, with some local administrations reverting to manual operations, causing long delays [73].

5.2.3 Restoration and institutional response

On 18 December 2023, PA Digitale began restoring essential services, with full recovery depending on a complete system rebuild on a new cloud infrastructure. According to a note issued at 17:00 on 19 December, *"operational functionality was restored for all affected PA clients starting at 08:00 on 18 December 2023" [73]*, with ongoing efforts to improve performance and expand bandwidth capacity. A new data centre in Rome was activated with a different provider accredited by AgID [74], illustrating a strategic shift toward diversification to improve resilience.

PA Digitale also confirmed to AgID on 15 December that the qualified digital preservation system remained intact, although it was temporarily suspended pending full system stabilisation and security checks [73].

In a positive step toward transparency, PA Digitale S.p.A. organised a public webinar on 18 December 2023 to clarify the incident's impact, share available evidence, and address concerns from affected partners and clients. The initiative, featuring top company leadership and the DPO, marked a noteworthy example of post-incident communication and accountability in the public-private digital ecosystem [75].

5.2.4 Classification as a supply chain incident

While not a supply chain attack in the traditional sense, where malicious actors compromise upstream software or hardware, the Westpole case exploited supply chain vulnerabilities by targeting a private provider whose services underpinned critical public infrastructure. This type of indirect compromise, affecting downstream users of cloud platforms, highlights structural weaknesses in Italy's cybersecurity posture, especially in the context of public-private digital dependencies. Importantly, this is not just a national issue: ENISA has identified supply chain attacks among the top 10 cyber threats for 2030, underlining their increasing relevance in the global cybersecurity landscape [76].

5.2.5 Strategic and regulatory implications

The incident catalysed several changes and exposed urgent governance issues:

- Cybersecurity governance is shifting from fragmented private oversight to centralized public authority and verticalization. ACN's role has expanded, and new national guidelines for public-sector cloud providers were introduced [77].
- The Piano Triennale per l'Informatica nella PA 2024-2026 [3] now includes enhanced cybersecurity funding and stricter compliance mandates for cloud providers.
- ACN has begun implementing more robust incident response coordination protocols, along with audit and qualification frameworks for cloud service providers. These frameworks assess providers based on criteria such as data security, service continuity, legal compliance, and operational transparency. The new qualification process, live since August 2024, aims to ensure that only providers meeting strict cybersecurity and sovereignty standards can offer services to the PA [78].

5.2.6 Lessons learned

The Westpole incident surfaced a range of critical weaknesses in Italy's digital public infrastructure, offering valuable insights for policy and practice:

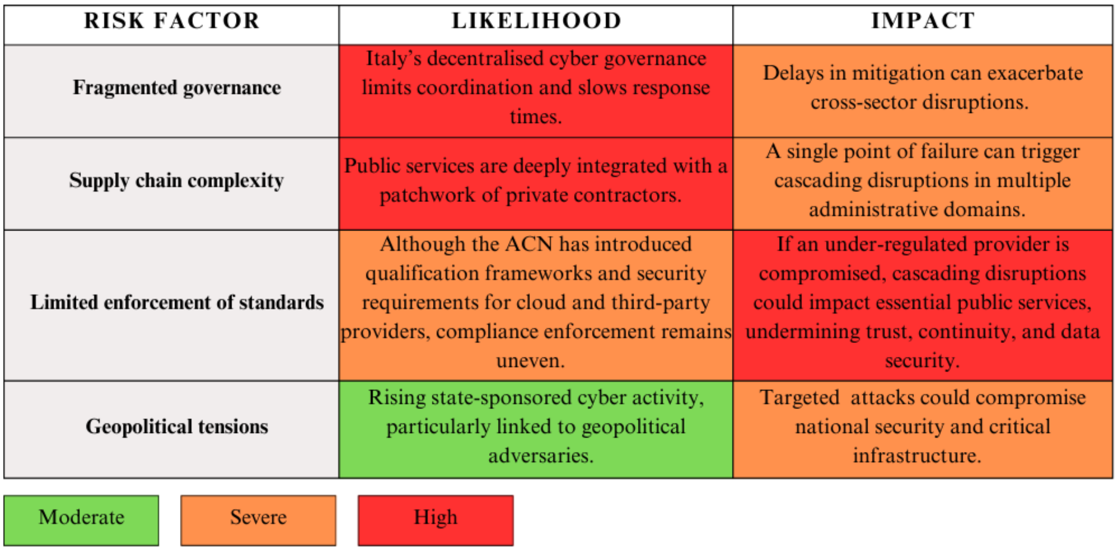
- **Overreliance on private contractors increases exposure**. The disruption highlighted the risks of depending too heavily on private actors for the delivery of essential public services. As highlighted in the literature review, governance models based on horizontal partnerships often lack the coordination and accountability needed during crises. The systemic impact of a single compromised provider emphasised the need to reassess the balance between public and private responsibilities.

- **Cybersecurity as a PA function**. The event reinforced the notion that cybersecurity must be treated not as a technical add-on, but as a core function of PA. This perspective, discussed in the literature review, supports ongoing shifts toward greater public oversight and integration of cybersecurity into the foundational structure of government services.
- **Procurement and risk-based cloud service evaluation**. The attack revealed shortcomings in the way cloud service providers are selected and monitored. As the literature review suggests, risk assessments should extend beyond technical capabilities to include resilience, transparency, and incident response preparedness. The limited communication from Westpole throughout the crisis further underlined the need for clearer standards on provider obligations and crisis communication, which ACN has implemented as of August 2024 [78]. These developments are embedded in the national cloud strategy, including the PSN, which provides a secure and state-supervised infrastructure for critical public sector services [36]. The Westpole case clearly exploited a supply chain vulnerability. This aligns with broader trends identified in the literature review, where indirect attacks on service providers have emerged as a growing threat vector. It illustrates the importance of incorporating supplier risk into cybersecurity planning and governance.
- **Toward resilience and strategic realignment**: the incident underscored the need for faster recovery protocols and better-coordinated responses. The shift toward more centralised governance, already underway, appears not only justified but urgent. As highlighted in the literature review, national resilience depends not only on technology but on institutional clarity, preparedness, and leadership.

The Westpole incident is a cautionary message for modern PA: a technical failure in a third-party private provider can paralyse state functions, revealing the fragile foundations of even the most digitalised systems. As Italy continues its quick digital transformation, this case underscores the need for strategic oversight, robust vendor management, and national-level preparedness to ensure continuity and security of public services in an era of rising cyber threats. However, the general difficulty in accessing timely, detailed information from official sources about the incident highlights an ongoing issue with institutional transparency. This concern, also echoed by several Italian interviewees, suggests that public communication protocols have room for improvement.

5.2.7 Risk Assessment of Future Supply Chain Attacks

If Italy's risk management practices would remain unchanged, similar or even more disruptive incidents are likely to occur in the future. Below is a structured risk assessment of key contributing factors.



RISK FACTOR	LIKELIHOOD	IMPACT
Fragmented governance	🟥 Italy's decentralised cyber governance limits coordination and slows response times.	🟧 Delays in mitigation can exacerbate cross-sector disruptions.
Supply chain complexity	🟥 Public services are deeply integrated with a patchwork of private contractors.	🟧 A single point of failure can trigger cascading disruptions in multiple administrative domains.
Limited enforcement of standards	🟧 Although the ACN has introduced qualification frameworks and security requirements for cloud and third-party providers, compliance enforcement remains uneven.	🟥 If an under-regulated provider is compromised, cascading disruptions could impact essential public services, undermining trust, continuity, and data security.
Geopolitical tensions	🟩 Rising state-sponsored cyber activity, particularly linked to geopolitical adversaries.	🟧 Targeted attacks could compromise national security and critical infrastructure.

🟩 Moderate 🟧 Severe 🟥 High

Image 2. Supply chain attacks risk assessment.

Unless these systemic gaps are addressed, Italy may face:

- **Prolonged recovery timelines**, with essential public services offline for extended periods.
- **Erosion of citizen trust** in digital PA platforms.
- **Economic losses** stemming from service interruptions and crisis management costs.

As highlighted in the literature review, these risks call for a more proactive and integrated approach to cybersecurity governance, one that prioritises resilience, regulatory enforcement, and strategic oversight of both public and private actors within the digital ecosystem.

5.3 Comparative cyber governance: Italy and Estonia

While both Italy and Estonia score similarly on international indices like the NCSI [61], a closer examination reveals fundamental differences in how the two countries govern, implement, and operationalise cybersecurity. This comparison covers not only their strategic frameworks but also the institutional landscape, incident response, supply chain oversight, and real-world resilience.

5.3.1 National cybersecurity frameworks comparison

Table 5. Italian and Estonian cybersecurity frameworks comparison.

Dimension	Italy	Estonia
Strategy name	**Strategia nazionale di cybersicurezza 2022-2026** (National Cybersecurity Strategy 2022–2026) [4].	**Küberturvalisuse Strateegia 2024–2030** (Cybersecurity Strategy 2024–2030) [79].
Strategic goals	▪ Strengthen PA systems ▪ Enhance incident response Align with EU/NATO ▪ Promote cybersecurity culture	▪ Ensure digital service resilience ▪ Adopt zero-trust architecture ▪ Address AI & quantum risks ▪ Maintain public trust
Strategic pillars	▪ Protection ▪ Response ▪ Development	▪ Digital Society ▪ Cyber Industry ▪ Global Leadership ▪ Cyber Literacy
Governance	▪ Led by ACN ▪ Decentralised coordination across Pas ▪ Aligned with NIS2 and EU crisis management	▪ Now led by the Ministry of Justice and Digital. Previously led by the Minister of Economic Affairs and Communication ▪ Centralised, cross-ministerial execution ▪ Strong alignment with EU/NATO
Military role	▪ Separate from core strategy (COR)	▪ Integrated via Cyber Command and Cyber Defence League

Threat models	▪ State-sponsored threats (Russia, China) ▪ Ransomware ▪ Disinformation ▪ Supply chain risk	▪ State-sponsored threats (Russia, China, Iran, North Korea) ▪ Hybrid warfare & ransomware ▪ Cloud & encryption threats
Key initiatives	▪ Public-sector modernisation ▪ National encryption standards ▪ Threat sharing platforms ▪ Public-private collaboration ▪ Workforce training (e.g. Piano Triennale)	▪ Zero-trust implementation ▪ Post-quantum encryption ▪ Secure cloud transition ▪ Public awareness campaigns ▪ Talent pipelines via education
Cyber hygiene & secure environment	▪ Secure-by-design principles ▪ MFA for public systems ▪ Encryption & testing encouraged	▪ IPv6 rollout ▪ Cyber hygiene campaigns ▪ AI/IoT regulation ▪ Public-sector IT modernisation
Public-private partnerships	▪ ACN coordination with critical sectors ▪ Tech sovereignty promoted	▪ Deep academic & private sector integration ▪ Cyber Defence League volunteers in national planning
Resilience & continuity	▪ Crisis simulations ▪ Early warning systems ▪ National ISAC structure	▪ Data embassies in Luxembourg ▪ CERT-EE 24/7 response ▪ Civil-military incident coordination

Funding & resources	▪ €1.2B via PNRR + budget law ▪ Performance reviewed annually	▪ Part of Digital Society 2030 ▪ Uses EU funds for innovation, education, and infrastructure
International cooperation	▪ EU ▪ Cyber Shield, ▪ NATO partnerships	▪ EU/NATO leader, ▪ Home of Tallinn Manual ▪ Active in bilateral/multilateral cyber diplomacy
Training & awareness	▪ Mandatory PA training plans ▪ Courses by AGID ▪ Evaluation of staff awareness	▪ Embedded in national education, University and vocational training ▪ Broad societal engagement
Critical infrastructure protection	▪ Supply chain security framework ▪ Secure cloud migration ▪ National encryption standards	▪ State-audited service providers ▪ Hybrid threat countermeasures

5.3.2 Beyond frameworks: real-world differences in cybersecurity practice

Institutional capacity

Italy's cybersecurity governance is formally centralised under the ACN, but operational responsibilities remain fragmented across various ministries, agencies, and local governments. In contrast, Estonia operates under a more unified model, with RIA playing both a strategic and operational role under the Ministry of Justice and Digital Affairs. RIA not only defines national cybersecurity policies but also acts as a second line of defense, directly supporting public entities in implementation and incident response. This integrated approach allows Estonia to ensure faster response times and stronger enforcement mechanisms compared to Italy's still-evolving framework.

Incident response and operational readiness

Italy conducts regular crisis simulations and has developed a national early warning system. However, its fragmented implementation results in uneven preparedness. Estonia's CERT-EE operates 24/7 with close coordination from defense units, enabling more rapid containment and mitigation during cyber incidents.

Cloud security

Estonia enforces strict cybersecurity standards for cloud services, including mandatory audits under its E-ITS [80] standard. Italy, once reliant on voluntary compliance, has recently taken a stricter turn. Since 2022, and reinforced through updated guidance in 2024, ACN requires cloud providers for the public sector to be certified according to official security criteria and registered [77]. This marks a shift toward stronger enforcement and state oversight, supported by national frameworks like the PSN.

Public sector cyber awareness and culture

Italy and Estonia adopt distinct strategies to develop cybersecurity capacity and culture within their public sectors. While both invest in training, Estonia takes a more holistic and integrated approach. Cybersecurity is embedded throughout society, from early education to national defense volunteering and public awareness campaigns. RIA leads initiatives such as the Cyber Test [81], phishing simulations, and targeted communication efforts. These are reinforced by the E-ITS regulation [80], which mandates ongoing cybersecurity training across all public institutions.

Italy, by contrast, has traditionally emphasised structured training for PA employees. The introduction of the Syllabus [38] offered modular, role-specific training also in digital and cybersecurity skills, but uptake was initially voluntary and uneven. A 2024 directive mandating 40 hours of annual training marked a policy shift. However, given the breadth of topics covered by the Syllabus from digital citizenship to data management, 40 hours yearly is unlikely to be sufficient for developing deep cybersecurity competence.

The Triennial Plan for Digitalisation [3] further outlines broader strategic priorities, but many smaller or less digitally mature entities still face barriers to implementation.

Without institutional commitment and resource support, training risks becoming a formal requirement rather than a catalyst for meaningful change.

Unlike Italy's centralised yet administratively fragmented rollout, Estonia benefits from unified digital governance and a strong culture of cybersecurity as a public duty. Cybersecurity-specific training is not only mandatory but directly tied to institutional resilience and service continuity.

With the implementation of the NIS2 directive, both countries face new obligations. Estonia's mature ecosystem provides a clear advantage, but Italy's recent reforms show commitment to catching up. Closing the gap will depend on Italy's ability to integrate cyber-training into organisational culture and ensure leadership accountability.

Finally, while not the primary focus here, Estonia's cross-sector collaboration helps sustain a dynamic cybersecurity workforce. Italy is advancing through ACN-led initiatives, but long-term progress will require structural investment and greater flexibility.

NIS2 implementation

As of early 2025, Estonia has not yet formally transposed the NIS2 Directive, missing the EU's October 2024 deadline. However, the country has a strong foundation due to its proactive implementation of NIS1 and the adoption of the Estonian Information Security Standard (E-ITS), which positions it well for future compliance. A draft law is under consultation and expected to enter into force by July 2025.

In contrast, Italy has aligned NIS2 implementation with its National Cybersecurity Strategy and PNRR and has formally transposed the directive. Yet, challenges remain in achieving consistent enforcement across Italy's highly decentralised PA.

5.3.3 Key Takeaways

- **Governance:** Estonia's centralised model offers more consistent enforcement and real-time coordination.
- **Resilience:** Estonia's rapid recovery capabilities and infrastructure (e.g., data embassies) enhance national resilience.
- **Execution over policy:** Despite similar strategic documents, Estonia's edge lies in implementation and cultural integration.

- **Public trust:** Estonia’s citizen-centric and transparent model fosters higher trust in digital services.
- **Strategic alignment:** Both countries align with EU and NATO frameworks, but Estonia plays a more proactive role globally.

Estonia demonstrates how centralised governance, even if not without its imperfections, integrated civil-military response, and an embedded cybersecurity culture can significantly enhance national cyber resilience.

Italy has made important strides, but structural fragmentation continues to pose challenges. Strengthening operational integration, particularly at the local PA level, will be critical for Italy to close the resilience gap. However, not all Estonian solutions are directly transferable, given differences in scale, institutional complexity, and strategic culture.

6 Conclusion

This thesis set out to explore how Italy is addressing the growing threat of cyberattacks against its PA, evaluate the effectiveness of its national cybersecurity framework, and draw comparative lessons from Estonia, a global leader in cyber resilience. The integrated methodological approach including literature review, semi-structured expert interviews, a case study on the Westpole incident, and comparative analysis, enabled a critical assessment of Italy's current posture and emerging challenges. In addition to these findings, the chapter also highlights key limitations of the current research and outlines avenues for future research.

6.1 Cybersecurity in the context of digital transformation

Italy's approach to cybersecurity is increasingly integrated into its broader digital transformation agenda. Strategic frameworks such as the 2022–2026 National Cybersecurity Strategy and the Triennial Plan for Digitalisation, alongside institutional milestones like the establishment of the ACN and the COR, demonstrate a growing national commitment to cybersecurity governance. However, challenges persist. Structural decentralisation, capacity shortages, particularly at the local level, and talent gap continue to hinder consistent implementation. While Italy has significantly increased its cybersecurity investment, this financial effort has yet to fully translate into operational resilience. Fragmentation, legacy systems, and limited technical expertise still pose barriers. Addressing these foundational issues will be key to ensuring that cybersecurity becomes not just a strategic vision but a functional pillar of Italy's digital future.

6.1.1 Why Is Italy a prime target?

Multiple interrelated factors contribute to the Italian public sector being an especially attractive target for cyberattacks. Italy's expanding digital footprint and reliance on third-party service providers, often with unclear risk profiles, create systemic vulnerabilities. Furthermore, legacy underinvestment in both technological infrastructure and human capital exacerbates these risks. Italy's geopolitical alignment, particularly its integration within the EU and NATO frameworks, further heightens its visibility as a target for politically motivated actors, including Russian-backed hacktivist groups.

6.2 Evaluating the effectiveness of Italy’s cybersecurity posture

Although Italy has made significant institutional progress, particularly through the creation of the ACN, the operational effectiveness of its cybersecurity policies remains inconsistent. Expert interviews consistently highlighted a reactive rather than preventive approach to cyber threats. Slow information-sharing practices and the absence of a coherent cyber-risk culture were frequently cited as key issues. Moreover, the system continues to suffer from sectoral fragmentation and insufficient public-private collaboration. Compliance-driven efforts often prioritise regulatory checklists over practical resilience and capacity-building measures, further limiting the effectiveness of national cybersecurity initiatives.

6.2.1 Lessons from the Westpole case

The Westpole cyberattack offers a stark illustration of these systemic weaknesses. As a supply chain incident that impacted critical PA services, it exposed significant gaps in third-party risk management and continuity planning. A lack of incident transparency, limited communication, and the absence of a national-level crisis coordination framework exacerbated the impact. Key lessons drawn from the incident include the need for stricter vendor vetting protocols, the development of standardised crisis response playbooks, and the establishment of robust coordination mechanisms linking local administrations, national authorities such as ACN, and private service providers.

6.3 What can Italy learn from Estonia?

Estonia offers a compelling contrast to Italy's approach. It treats cybersecurity as a core element of national defense and public policy, supported by a centralised administrative system and modern digital infrastructure. Estonia's success lies in its systemic integration of cybersecurity into all levels of governance, from real-time information sharing to the strategic alignment of civil and military cyber initiatives. Centralised platforms, secure digital identity systems, and a robust cyber hygiene culture allow for consistent and resilient service delivery even under pressure.

6.3.1 Adapting best practices to the Italian context

Several best practices from Estonia's experience could significantly enhance Italy’s cybersecurity framework:

- Centralised monitoring and real-time threat detection
- Institutionalised mandatory cyber hygiene education and public awareness campaigns
- Clear legal frameworks delineating roles and responsibilities
- Stronger public-private trust-building measures and joint cyber exercises
- Streamlined hiring pathways, intersectoral partnerships, and competitive incentives to attract and retain skilled professionals in the Public Administration
- Holistic integration of cybersecurity with defense, civil protection, and digital transformation strategies

Nonetheless, these practices must be adapted to Italy’s unique administrative and political context. Italy’s size, decentralised governance model, older legacy systems, and regional disparities introduce significant implementation challenges. While Estonia benefits from its small size, modern IT infrastructure, and unitary administrative structure, Italy must navigate a more complex landscape. Therefore, adopting Estonian practices will require significant adaptation and time. Coordination across multiple levels of government and agencies is more difficult, and policy implementation often faces bureaucratic and technical delays. Therefore, while Estonia's experience offers valuable guidance, its application in Italy must be nuanced, gradual, and sensitive to local conditions.

6.4 Reflections on the NCSI

Although Italy and Estonia are ranked similarly in the NCSI, this metric emphasises institutional presence rather than operational performance. Estonia’s advantage lies in its tested response mechanisms, NATO integration, and cyber crisis experience. Italy’s comparable rank masks its struggle with fragmented implementation and limited testing under real attack conditions. Hence, indexes like NCSI should be supplemented with resilience metrics that reflect readiness and adaptability under pressure.

6.5 Empirical insights and policy implications

In light of the findings presented in this thesis, it becomes evident that many of the challenges, needs, and strategic shifts observed in the Italian public sector echo the broader principles identified in recent European policy discussions on government resilience. Reports such as Government Resilience in the Digital Age emphasize that building a cyber-resilient society requires more than isolated technical fixes: it demands a coordinated transformation that integrates secure digital infrastructure, institutional capacity, remote-enabled governance, and proactive risk management across third-party ecosystems.

The Italian case confirms the urgency of this multidimensional approach. As Italy continues to enhance its cyber posture through centralised agencies, regulatory updates, and investment in skills and infrastructure, these efforts align with a growing consensus that cybersecurity is not just a matter of defense, but a foundation for national continuity, democratic stability, and strategic autonomy in the digital era.

6.6 Limitations of the Study

Several limitations must be acknowledged:

- The interview sample was limited due to the specialized and sensitive nature of the topic.
- Access to ACN personnel was restricted, narrowing the scope of insider institutional perspectives.
- Certain policy documents and attack details were unavailable due to confidentiality or lack of disclosure.
- Clusit Reports, though valuable, are based on reported data, potentially underrepresenting the full scale of incidents.
- Findings are shaped by participant perspectives and may not fully generalise across all PA contexts.
- Cybersecurity remains a fast-evolving domain. New policies, threats, and technologies continue to emerge, which may influence the applicability of findings over time.

6.7 Directions for future research

This research can be extended in several directions:

- Conduct a more technical analysis focused on sector-specific cybersecurity, such as healthcare, a domain mostly public in Italy and highly targeted by cyberattacks.
- Explore how decentralized municipalities and small agencies implement national cybersecurity directives.
- Investigate the cybersecurity implications of AI adoption and blockchain in the PA context.
- Develop metrics and models to assess the operational maturity and resilience of PA cybersecurity frameworks beyond policy compliance.

References

[1] A. Aceti *et al.*, 'Rapporto Clusit 2025 sulla Cybersecurity in Italia e nel mondo', CLUSIT – Associazione Italiana per la Sicurezza Informatica, 2025. [Online]. Available: https://clusit.it/rapporto-clusit/#

[2] C. Bazzucchi *et al.*, 'Rapporto Clusit 2024 sulla sicurezza ICT in Italia', CLUSIT – Associazione Italiana per la Sicurezza Informatica, 2024.

[3] 'Piano triennale per l'informatica nella Pubblica Amministrazione - Edizione 2024-2026', AGID, 2025. [Online]. Available: https://www.agid.gov.it/it/agenzia/piano-triennale

[4] 'Piano di Implementazione - Strategia Nazionale Di Cybersicurezza 2022-2026', ACN, 2022. [Online]. Available: https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza

[5] C. Monteleone and R. R. and, 'Cybersecurity and Italian critical infrastructures: the return of the state?', *Contemp. Ital. Polit.*, vol. 0, no. 0, pp. 1–17, 2024, doi: 10.1080/23248823.2024.2399465.

[6] A. Tieti, 'Attacco all'Italia da hacker russi: colpiti Senato e Difesa. Crescono i segnali di cyberwar globale', *Il Sole 24 Ore*, 2022. Accessed: Jan. 01, 2024. [Online]. Available: https://www.ilsole24ore.com/art/attacco-all-italia-hacker-russi-colpiti-senato-e-difesa-crescono-segnali-cyberwar-globale-AEjkx7VB

[7] I. Doda, 'Ministero della Difesa, in corso un attacco informatico', *Wired Italia*, Wired Italia, 2022. Accessed: Jan. 01, 2024. [Online]. Available: https://www.wired.it/article/attacco-informatico-ministero-difesa/

[8] I. Lella *et al.*, 'ENISA THREAT LANDSCAPE 2024', EUROPEAN UNION AGENCY FOR CYBERSECURITY, Sep. 2024.

[9] 'Attacco DDoS: cos'è e cosa comporta', Cloudflare.com. Accessed: Jan. 01, 2024. [Online]. Available: https://www.cloudflare.com/it-it/learning/ddos/what-is-a-ddos-attack/

[10] 'L'Importanza della Cybersecurity nella Pubblica Amministrazione: Lezioni dal Caso Westpole', SCP. Accessed: Mar. 26, 2025. [Online]. Available: https://www.scponline.it/blog/limportanza-della-cybersecurity-nella-pubblica-amministrazione-lezioni-dal-caso-westpole

[11] H. Pevkur, 'Lessons from Estonia's Whole-of-Society Approach to Cyber Defense – Digital Front Lines'. Accessed: Mar. 25, 2025. [Online]. Available: https://digitalfrontlines.io/2023/08/31/lessons-from-estonias-whole-of-society-approach-to-cyber-defense/

[12] D. Giorgia, 'Vulnerabilità informatica, esempi e linee guida per le aziende', Osservatori Digital Innovation. Accessed: Apr. 19, 2025. [Online]. Available: https://blog.osservatori.net/it_it/vulnerabilita-informatica-fattore-umano

[13] ‘Formazione e consapevolezza - ACN’, Agenzia per la cybersicurezza nazionale. Accessed: Apr. 19, 2025. [Online]. Available: https://www.acn.gov.it/portale/formazione-consapevolezza

[14] E. Rekleitis and M. Adamczyk, ‘SPACE THREAT LANDSCAPE’, EUROPEAN UNION AGENCY FOR CYBERSECURITY, Mar. 2025. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2025-03/Space_Threat_Landscape_Report_fin.pdf

[15] ‘How Estonia became a global heavyweight in cyber security - e-Estonia’. Accessed: Mar. 25, 2025. [Online]. Available: https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

[16] ‘Estonia’s bold approach to cyber security: a holistic model for Europe - e-Estonia’. Accessed: Mar. 25, 2025. [Online]. Available: https://e-estonia.com/estonias-bold-approach-to-cyber-security-a-holistic-model-for-europe/

[17] I. Ayres and J. Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate*. in Oxford Socio-Legal Studies. Oxford University Press, 1992. [Online]. Available: https://books.google.ee/books?id=2043-vvL7HIC

[18] S. Busetti and F. M. Scanni, ‘Evaluating incident reporting in cybersecurity. From threat detection to policy learning’, *Gov. Inf. Q.*, vol. 42, no. 1, p. 102000, Mar. 2025, doi: 10.1016/j.giq.2024.102000.

[19] ‘ISO 31000:2018(en) Risk management — Guidelines’. Accessed: Mar. 26, 2025. [Online]. Available: https://www.iso.org/obp/ui/

[20] S. Rossa, ‘Cyber attacchi e incidenti nella Pubblica Amministrazione, fra organizzazione amministrativa e condotta del funzionario’, *Vergentis Rev. Investig. Cátedra Int. Conjunta Inocencio III*, no. 17, pp. 161–175, Mar. 2024, doi: 10.12800/vg.17.8.

[21] ‘Building the human firewall: Navigating behavioral change in security awareness and culture | IBM’, IBM. Accessed: Apr. 19, 2025. [Online]. Available: https://www.ibm.com/think/insights/security-awareness-culture

[22] A. Marrone, E. Sabatino, and O. Credi, ‘Italy and Cyber Defence’. Istituto Affari Internazionali, Sep. 2021. [Online]. Available: https://www.iai.it/sites/default/files/iai2112_en.pdf

[23] ‘Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale’, Gazzetta Ufficiale. Accessed: Mar. 26, 2025. [Online]. Available: https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg

[24] ‘Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali’, Gazzetta Ufficiale. Accessed: Mar. 26, 2025. [Online]. Available: https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg

[25] ‘Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica’, Gazzetta Ufficiale. Accessed: Mar. 26, 2025. [Online]. Available: https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/s

[26] ‘Disposizioni urgenti in materia di cybersicurezza, definizione dell’architettura nazionale di cybersicurezza e istituzione dell’Agenzia per la cybersicurezza nazionale’, Gazzetta Ufficiale. Accessed: Mar. 26, 2025. [Online]. Available: https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/SG

[27] ‘Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)’, EUR-Lex. Accessed: Mar. 26, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[28] ‘Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell’Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148’. Accessed: Mar. 26, 2025. [Online]. Available: https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG

[29] ‘NIS - Network Information Security - ACN’, Agenzia per la cybersicurezza nazionale. Accessed: Mar. 26, 2025. [Online]. Available: https://www.acn.gov.it/portale/nis

[30] S. Antonello, ‘Cybersecurity, tre priorità per la strategia italiana’, Corriere Comunicazioni. Accessed: Apr. 19, 2025. [Online]. Available: https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-tre-priorita-per-la-strategia-italiana/

[31] P. Gallarati *et al.*, ‘Cybersecurity in Italy’, ADVANT Nctm, 2024. [Online]. Available: https://www.advantlaw.com/fileadmin/nctm/PDF/Guida_Cybersecurity_ENG.pdf

[32] ‘Italian cybersecurity challenges between culture and technology market - About Resilience’, About Resilience. Accessed: Mar. 26, 2025. [Online]. Available: https://www.aboutresilience.com/italian-cybersecurity-challenges-between-culture-and-technology-market/?utm_source=chatgpt.com

[33] R. Baldoni, ‘The Italian cybersecurity recipe: Technological Development and National Strategic Autonomy’, presented at the Event ACN-Luiss, Feb. 2023.

[34] ‘BOLLETTINO DELLE GIUNTE E DELLE COMMISSIONI PARLAMENTARI - Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità.’ Camera dei Deputati, Apr. 02, 2025. [Online]. Available: https://www.camera.it/leg19/824?anno=2025&commissione=04&giorno=02&mese=04&tipo=A&view=&utm_source=chatgpt.com

[35] ‘NIST Updates Cybersecurity Guidance for Supply Chain Risk Management’, NIST. Accessed: Mar. 26, 2025. [Online]. Available: https://www.nist.gov/news-

events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management?utm_source=chatgpt.com

[36] ‘Discover Polo Strategico Nazionale, the secure cloud for the PA’. Accessed: Apr. 25, 2025. [Online]. Available: https://www.polostrategiconazionale.it/en/about-us/polo-strategico-nazionale/

[37] ‘Sale l’età media dei dipendenti pubblici’, lentepubblica.it. Accessed: Apr. 12, 2025. [Online]. Available: https://lentepubblica.it/personale-e-previdenza/sale-eta-media-dipendenti-pubblici/

[38] ‘Nuove competenze per le Pubbliche Amministrazioni’, Syllabus. Accessed: Apr. 23, 2025. [Online]. Available: https://www.syllabus.gov.it/portale/web/syllabus

[39] A. Ajupov, A. Sherstobitova, S. Syrotiuk, and A. Karataev, ‘The riskmanagement theory in modern economic conditions’, *E3S Web Conf.*, vol. 110, p. 02040, 2019, doi: 10.1051/e3sconf/201911002040.

[40] ‘Chi proteggerà i nostri confini digitali?’ Talents Venture, Mar. 2025. [Online]. Available: https://www.talentsventure.com/wp-content/uploads/2025/03/Nota-Osservatorio-3-Chi-protegge-i-nostri-confini-digitali.pdf

[41] P. Atzeni and M. Scannapieco, ‘La Cybersicurezza nelle Università e negli EPR’, Nov. 29, 2023. [Online]. Available: https://www.mur.gov.it/sites/default/files/2024-03/ACN_AtzeniScannapieco.pdf

[42] Babajide Tolulope Familoni, ‘CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS’, *Comput. Sci. IT Res. J.*, vol. 5, no. 3, pp. 703–724, Mar. 2024, doi: 10.51594/csitrj.v5i3.930.

[43] A. Calcara and R. Marchetti, ‘State-industry relations and cybersecurity governance in Europe’, *Rev. Int. Polit. Econ.*, vol. 29, no. 4, pp. 1237–1262, Jul. 2022, doi: 10.1080/09692290.2021.1913438.

[44] A. Bertolino, ‘Governance della cybersecurity: la sfida strategica per l’Italia 2025 - Agenda Digitale’, Agenda Digitale. Accessed: Mar. 27, 2025. [Online]. Available: https://www.agendadigitale.eu/sicurezza/governance-della-cybersecurity-la-sfida-strategica-per-litalia-2025/

[45] ‘ACN intercetta nuovi investimenti in cybersecurity a favore dell’ecosistema cibernetico nazionale - ACN’, Agenzia per la cybersicurezza nazionale. Accessed: Mar. 27, 2025. [Online]. Available: https://www.acn.gov.it/portale/w/acn-intercetta-nuovi-investimenti-in-cybersecurity-a-favore-dell-ecosistema-cibernetico-nazionale

[46] V. Shah, ‘Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats’, Dec. 2022, [Online]. Available: https://www.researchgate.net/publication/378396020_Machine_Learning_Algorithms_for_Cybersecurity_Detecting_and_Preventing_Threats

[47] S. Kumar, Shersingh, S. Kumar, and K. Verma, ‘Malware Classification Using Machine Learning Models’, *Procedia Comput. Sci.*, vol. 235, pp. 1419–1428, 2024, doi: 10.1016/j.procs.2024.04.133.

[48] Z. Amos, ‘How NLP Improves Phishing Detection’, CyberExperts. Accessed: Apr. 23, 2025. [Online]. Available: https://cyberexperts.com/how-nlp-improves-phishing-detection/

[49] P. Sharma, M. Kumar, and H. Sharma, ‘A GAN-Based Model of Deepfake Detection in Social Media’, *Procedia Comput. Sci.*, vol. 218, pp. 2153–2162, Jan. 2023, doi: 10.1016/j.procs.2023.01.191.

[50] T. Krantz, ‘What Is Data Poisoning?’, IBM. Accessed: Apr. 23, 2025. [Online]. Available: https://www.ibm.com/think/topics/data-poisoning

[51] A. Vassilev, ‘Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations’, National Institute of Standards and Technology, Gaithersburg, MD, NIST AI NIST AI 100-2e2025, 2025. doi: 10.6028/NIST.AI.100-2e2025.

[52] S. Lee and S. Kim, ‘Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges’, *IEEE Access*, vol. 10, pp. 2602–2618, 2022, doi: 10.1109/ACCESS.2021.3136328.

[53] ‘Blockchain + AI in Finance: How Opposites Attract’, Fact Set. Accessed: Apr. 23, 2025. [Online]. Available: https://insight.factset.com/blockchain-ai-in-finance-how-opposites-attract

[54] ‘Kristen Michal: There is too much bureaucracy in Estonia’, ERR. Accessed: Apr. 19, 2025. [Online]. Available: https://news.err.ee/1609629872/kristen-michal-there-is-too-much-bureaucracy-in-estonia

[55] C. Czosseck, R. Ottis, and A.-M. Talihärm, ‘Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security’, *Int. J. Cyber Warf. Terror.*, vol. 1, no. 1, pp. 24–34, Jan. 2011, doi: 10.4018/ijcwt.2011010103.

[56] P. Pernik, *Cyber deterrence : a case study on Estonia’s policies and practice*. in Hybrid CoE paper. The European Centre of Excellence for Countering Hybrid Threats, 2021. [Online]. Available: https://www.finna.fi/Record/fikka.5686023

[57] Y. Yamaguchi, ‘Strengthening public-private partnership in cyber defense: A comparison with the Republic of Estonia’, *NIDS J. Def. Secur.*, vol. 20, pp. 67–111, 2019.

[58] ‘The Cyber Security Yearbook: the number of incidents doubled in a year’, RIA. Accessed: Apr. 23, 2025. [Online]. Available: https://www.ria.ee/en/news/cyber-security-yearbook-number-incidents-doubled-year

[59] ‘Küberturvalisuse aastaraamat 2025’. Riigi Infosüsteemi Amet, 2025. [Online]. Available: https://www.ria.ee/kuberturvalisuse-aastaraamat-2025

[60] A. Hardy, ‘Securing e-Estonia: Challenges, Insecurities, Opportunities’, University of London, 2019. [Online]. Available: https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=4155377

[61] ‘NCSI Ranking’, NCSI. Accessed: Apr. 19, 2025. [Online]. Available: https://ncsi.ega.ee/ncsi-index/

[62] S. Lewis, ‘Qualitative Inquiry and Research Design: Choosing Among Five Approaches’, *Health Promot. Pract.*, vol. 16, no. 4, pp. 473–475, Jul. 2015, doi: 10.1177/1524839915580941.

[63] A. Fink, *Conducting research literature reviews: from the Internet to paper*, 3rd ed. Thousand Oaks, Calif.: Sage, 2010.

[64] J. Webster and R. Watson, ‘Analyzing the Past to Prepare for the Future: Writing a Literature Review’, *MIS Q.*, vol. 26, Jun. 2002, doi: 10.2307/4132319.

[65] J. Ritchie, Ed., *Qualitative research practice: a guide for social science students and researchers*, Reprinted. Los Angeles, Calif.: SAGE Publ, 2010.

[66] M. Q. Patton, *Qualitative research & evaluation methods*, 3. ed., [Nachdr.]. Thousand Oaks: Sage, 2010.

[67] T. Hollweck, ‘Robert K. Yin. (2014). Case Study Research Design and Methods (5th ed.).’, *Can. J. Program Eval.*, vol. 30, no. 1, pp. 108–110, Mar. 2015, doi: 10.3138/cjpe.30.1.108.

[68] V. Braun and V. Clarke, ‘Using thematic analysis in psychology’, *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, Jan. 2006, doi: 10.1191/1478088706qp063oa.

[69] A. Lijphart, ‘Comparative Politics and the Comparative Method’, *Am. Polit. Sci. Rev.*, vol. 65, no. 3, pp. 682–693, Sep. 1971, doi: 10.2307/1955513.

[70] S. Sangari, E. Dallal, and M. Whitman, ‘Modeling Under-Reporting in Cyber Incidents’, *Risks*, vol. 10, p. 200, Oct. 2022, doi: 10.3390/risks10110200.

[71] ‘Techno-solutionism’, *Cambridge*. Accessed: Mar. 27, 2025. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/techno-solutionism

[72] ‘PNRR - Piano Nazionale di Ripresa e Resilienza - ACN’, Agenzia per la cybersicurezza nazionale. Accessed: Apr. 13, 2025. [Online]. Available: https://www.acn.gov.it/portale/pnrr

[73] L. Alessandro, ‘Westpole-PA Digitale, il vero conto del disastro: enorme’, Cyber Security 360. Accessed: Apr. 21, 2025. [Online]. Available: https://www.cybersecurity360.it/nuove-minacce/westpole-pa-digitale-il-vero-conto-del-disastro-enorme/?utm_source=chatgpt.com

[74] Z. Luca, ‘Westpole e PA Digitale, come è andata a finire dopo il grosso attacco informatico’, Wired Italia. Accessed: Apr. 21, 2025. [Online]. Available: https://www.wired.it/article/westpole-pa-digitale-urbi-attacco-informatico-enti-pubblici/

[75] '“L'incidente Westpole S.p.A. Riflessi per i Clienti PA Digitale S.p.A. Fatti, evidenze, trasparenza.', Dec. 17, 2023. [Online]. Available: https://www.padigitale.it/wp-content/uploads/2024/02/InvitoClienti_Webinar181223_webtec.pdf

[76] R. Mattioli, A. Malatras, E. N. Hunter, M. G. Biasibetti Penso, D. Bertram, and I. Neubert, 'IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030', EUROPEAN UNION AGENCY FOR CYBERSECURITY, Mar. 2023.

[77] 'Regolamento Cloud per la PA', Agenzia per la cybersicurezza nazionale. Accessed: Apr. 21, 2025. [Online]. Available: https://www.acn.gov.it/portale/cloud/regolamento-cloud-per-la-pa

[78] 'Qualificazione e adeguamento', Agenzia per la cybersicurezza nazionale. Accessed: Apr. 21, 2025. [Online]. Available: https://www.acn.gov.it/portale/cloud/qualificazione-e-adeguamento

[79] 'KÜBERTURVALISUSE STRATEEGIA 2024–2030'. Majandus- ja Kommunikatsiooniministeerium, 2024. [Online]. Available: https://www.mkm.ee/sites/default/files/documents/2024-07/Kyberturvalisuse%20strateegia%202024-2030_labivalt_IT_vaatlik_Eesti.pdf

[80] 'Eesti infoturbestandard'. Accessed: Apr. 23, 2025. [Online]. Available: https://www.riigiteataja.ee/akt/130012024007

[81] 'Kübertest', RIA. Accessed: Apr. 23, 2025. [Online]. Available: https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/kubertest

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis1

I Alessandro Milici

1.1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Building a cyber-resilient society: a case study of Italy’s Public Administration in the face of rising cyberthreats”, supervised by Adrian Nicholas Venables

1.2. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.3. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

09.05.2025

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Interview consent form

Master's thesis title: Building a cyber-resilient society: a case study of Italy's Public Administration in the face of rising cyberthreats

Tallinn University of Technology (Taltech), School of Information Technologies

Researcher: Alessandro Milici

Supervisor: Dr. Adrian Venables

Thank you for agreeing to be interviewed as part of the above-mentioned research project. The interview will last 60-75 minutes. You have the right to stop the interview or withdraw from the research at any time.

Ethical academic research requires interviewees to explicitly consent to the interview and the use of their information. This consent form is necessary to ensure that you agree to participate in the interview and by signing this form you approve the following:

- The interview will be recorded and transcript will be produced.
- The transcript of the interview will be analysed by Alessandro Milici as researcher.
- Access to the interview transcript will be restricted to Alessandro Milici and her supervisor for the purposes of the research process. Additionally, during the thesis defence process, the transcript may be made available to the members of the thesis defence committee upon request.
- Any summary interview content, or direct quotations from the interview, that are made available through academic publication or other academic outlets will be anonymised so that you cannot be identified.
- All or part of the content of your interview may be used in academic papers that are based on the current research project.

- The actual recording will be kept until the master’s thesis is defended (presumably taking place in May 2025).

MODULO DI CONSENSO PER L’INTERVISTA

Tesi di laurea magistrale: Building a cyber-resilient society: a case study of Italy's Public Administration in the face of rising cyberthreats

Tallinn University of Technology (TalTech), School of Information Technologies

Ricercatore: Alessandro Milici

Relatore: Dr. Adrian Venables

Grazie per aver accettato di partecipare all’intervista per il progetto di ricerca sopra indicato. L’intervista avrà una durata di 60-75 minuti. Ha il diritto di interrompere l’intervista o ritirarsi dalla ricerca in qualsiasi momento.

La ricerca accademica etica richiede che i partecipanti esprimano esplicitamente il proprio consenso all’intervista e all’utilizzo delle informazioni fornite. Questo modulo di consenso è necessario per garantire che Lei accetti di partecipare all’intervista e, firmandolo, approvi quanto segue:

- L’intervista sarà registrata e ne sarà prodotta una trascrizione.

- La trascrizione dell’intervista sarà analizzata da Alessandro Milici in qualità di ricercatore.

- L’accesso alla trascrizione dell’intervista sarà limitato ad Alessandro Milici e al suo supervisore per le finalità del processo di ricerca. Inoltre, durante la difesa della tesi, la trascrizione potrà essere messa a disposizione dei membri della commissione di difesa tesi, se richiesto.

- Qualsiasi contenuto riassuntivo dell’intervista o citazione diretta resa disponibile tramite pubblicazioni accademiche o altri canali accademici sarà anonimizzato per garantire che Lei non possa essere identificato/a.

- Tutto o parte del contenuto della tua intervista potrebbe essere utilizzato in articoli accademici basati sul progetto di ricerca attuale.

- La registrazione originale sarà conservata fino alla difesa della tesi di laurea magistrale (presumibilmente entro maggio 2025)

Date/Data:

Signature/Firma:

Appendix 3 – Semi-Structured Interview Questions for Italian experts

Semi-Structured Interview Questions (English)

Research: Building a cyber-resilient society: a case study of Italy's Public Administration in the face of rising cyberthreats

This research explores the cybersecurity challenges faced by Italy’s Public Administration (PA), focusing on governance, policy implementation, and resilience against cyber threats. By examining Italy’s current strategies and comparing them with Estonia’s integrated cybersecurity approach, the study aims to identify gaps and propose actionable recommendations to strengthen Italy’s public sector cybersecurity framework.

This interview will be audio recorded for research purposes to ensure the accuracy of the analysis. All details regarding the processing of your information are explained in the consent form provided before the interview.

Introduction and Context

1. Could you describe your role and your involvement with cybersecurity in Italy’s Public Administrations?

2. What are, in your opinion, the most pressing cybersecurity threats facing Italy today?

Strategies and Governance

3. How effective do you consider the "National Cybersecurity Strategy" in addressing these threats?

4. What role does the National Cybersecurity Agency (ACN) play in coordinating cybersecurity efforts within the PA?

5. How does governance fragmentation impact the implementation of cybersecurity measures in Italy’s Public Administration?

Incidents and Resilience

6. How would you evaluate Italy's response to significant incidents, such as the Westpole case?

7. What lessons have been learned from past incidents to improve Italy's cybersecurity resilience?

8. In recent years, have you noticed an improvement or a decline in cybersecurity within Public Administrations? What factors do you think have influenced this trend?

9. What improvements would you recommend to strengthen cyber resilience in Italy's Public Administrations?

Training and Awareness

10. What is the current state of cybersecurity training and awareness among public sector employees?

11. What are the main challenges in implementing effective cybersecurity training programs?

Digital Transformation

12. How has the digital transformation process, such as initiatives under the Triennial Plan for Digitalisation, influenced cybersecurity preparedness?

Emerging Technologies, Estonia, and Future Perspectives

13. Estonia adopted an integrated approach where cyber defense is part of its broader national defense strategy. Does this happen in Italy? Do you think it could be beneficial?

14. Are there any emerging technologies or international best practices that you think Italy should adopt to strengthen its cybersecurity defenses?

15. What do you consider the main priorities for improving Italy's cybersecurity framework?

16. How do you foresee the evolution of cyber threats and the related countermeasures in the next 5-10 years?

Domande per Intervista Semi-Strutturata (Italiano)

Ricerca: Building a Cyber-Resilient Society: A Case Study of Italy's Public Administration in the Face of Rising Cyber Threats

Questa ricerca esplora le sfide della cybersecurity affrontate dalla Pubblica Amministrazione (PA) italiana, con un focus sulla governance, sull'implementazione delle politiche e sulla resilienza contro le minacce informatiche. Esaminando le strategie attuali dell'Italia e confrontandole con l'approccio integrato alla cybersecurity adottato dall'Estonia, lo studio mira a identificare le lacune e a proporre raccomandazioni concrete per rafforzare il quadro di sicurezza informatica del settore pubblico italiano.

L'intervista sarà registrata per finalità di ricerca al fine di garantire l'accuratezza dell'analisi. Tutti i dettagli relativi al trattamento delle informazioni sono spiegati nel modulo di consenso fornito prima dell'intervista.

Introduzione e Contesto

1. Può descrivere il suo ruolo e il suo coinvolgimento con la cybersecurity nelle pubbliche amministrazioni italiane?

2. Quali sono, secondo lei, le minacce di cybersecurity più urgenti che l'Italia affronta oggi?

Strategie e Governance

3. Quanto ritiene efficace la "Strategia Nazionale di Cybersicurezza" nel mitigare queste minacce?

4. Che ruolo svolge l'Agenzia Nazionale per la Cybersicurezza (ACN) nel coordinamento degli sforzi di cybersecurity all'interno della PA?

5. In che modo la frammentazione della governance influisce sull'implementazione delle misure di sicurezza informatica nella PA?

Incidenti e Resilienza

6. Come valuta la risposta dell'Italia a incidenti significativi, come il caso Westpole?

7. Quali lezioni sono state apprese da eventi passati per migliorare la resilienza della cybersecurity in Italia?

8. Negli ultimi anni, ha notato un miglioramento o un peggioramento della sicurezza cyber nelle pubbliche amministrazioni? Quali fattori ritiene abbiano influenzato questo cambiamento?

9. Quali miglioramenti consiglierebbe per rafforzare la resilienza cyber nelle PA italiane?

Formazione e Consapevolezza

10. Qual è lo stato attuale della formazione e consapevolezza sulla cybersecurity tra i dipendenti del settore pubblico?

11. Quali sono le principali difficoltà nell'implementare programmi di formazione efficaci?

Trasformazione Digitale

12. Come ha influenzato il processo di trasformazione digitale, ad esempio attraverso il Piano Triennale per la Digitalizzazione, la preparazione alla cybersecurity?

Tecnologie Emergenti, Estonia e Prospettive Future

13. L'Estonia potrebbe essere considerata un punto di riferimento grazie al suo approccio integrato, dove la difesa informatica è parte della strategia di difesa nazionale. Questo succede in Italia? Ritiene che potrebbe essere un approccio benefico?

14. Ci sono tecnologie emergenti o best practice internazionali che, secondo lei, l'Italia dovrebbe adottare per rafforzare la propria difesa cibernetica?

15. Quali sono, secondo lei, le priorità principali per migliorare il quadro della cybersecurity in Italia?

16. Come immagina l’evoluzione delle minacce cyber e delle relative contromisure nei prossimi 5-10 anni?

Appendix 4 – Semi-Structured Interview Questions for Estonian experts

Semi-Structured Interview Questions (English)

Research: Building a cyber-resilient society: a case study of Italy's Public Administration in the face of rising cyberthreats

This research explores the cybersecurity challenges faced by Italy’s Public Administration (PA), focusing on governance, policy implementation, and resilience against cyber threats. By examining Italy’s current strategies and comparing them with Estonia’s integrated cybersecurity approach, the study aims to identify gaps and propose actionable recommendations to strengthen Italy’s public sector cybersecurity framework.

This interview will be audio recorded for research purposes to ensure the accuracy of the analysis. All details regarding the processing of your information are explained in the consent form provided before the interview.

Introduction and Context

1. Could you describe your role and your involvement with cybersecurity in Estonia’s Public Administrations?
2. What are, in your opinion, the most pressing cybersecurity threats facing Estonia today?

Strategies and Governance

3. What are the key factors behind Estonia’s cybersecurity strategy and e-governance?
4. How does Estonia integrate cybersecurity into Public Administration through its "broad-based national defense" strategy?
5. What role does the Information System Authority (RIA) play in coordinating Estonia’s cybersecurity efforts?

Incidents and Resilience

6. How does Estonia ensure resilience against evolving cyber threats?

7. What lessons have been learned from past incidents to improve Estonia's cyber-security resilience?

8. In recent years, have you noticed an improvement or a decline in cybersecurity within Public Administrations? What factors do you think have influenced this trend?

Training and Awareness

9. What is the current state of cybersecurity training and awareness among public sector employees?

Digital Transformation

10. What lessons from Estonia’s cybersecurity practices could be relevant or adaptable for other countries like Italy?

11. How does public-private collaboration enhance Estonia’s cybersecurity strategy?

Emerging Technologies and Future Perspectives

12. What emerging technologies or approaches is Estonia focusing on to maintain its cybersecurity leadership?

13. How do you foresee the evolution of cyber threats and the related countermeasures in the next 5-10 years?