LUISS

Degree Program in International Relations

Course of Crisis Communication

Crisis and Strategy: How Intelligence Agencies Manage High-Stakes Events

Prof. Donatella Selva

SUPERVISOR

Prof. Carlo Magrassi

CO-SUPERVISOR

Lucio Forlano (ID 657422)

CANDIDATE

Academic Year 2024/2025

Acknowledgements

I would like to start off by thanking my thesis advisor, Professor Donatella Selva, for the excellent assistance provided throughout the course of this research. She has proven to be a patient and insightful professor who has taught me the value and importance of studying communication in today's world, and for this I thank her. I would also like to thank Professor Magrassi for his contribution to my interest in national security policies.

I would also like to thank all of those who have proven to be wonderful friends throughout my university years. Thank you to Federico and Luca, who were always able to make me laugh when I needed it the most. To Jerome and Greg, for being amazing friends since my first day in Rome. To Xiaojie, thank you for being an amazing friend since the day we met. To Francesco, my university years would not have been the same without you: thank you for being always there for me, no matter the distance. To Matteo, for being an amazing friend for all of these years: never change. To Luca, who I know I can always count on. And to the two friends who I know I will always have the best time with: Rebecca and Giulia.

I would also like to thank Paolo, Paola and Isabella Gommellini for helping me feel always at home on our little street. Thanks to Raffaella as well, for always being the woman I remember.

Thank you to Rosemary and Chiara, for being the best internship supervisors I could have ever hoped for. You always made me feel valued and empowered in the workplace, and I will never forget that I would also like to thank Aurélien, Morgan and Valentin for all the good times we had together in Brussels even when times were difficult for all of us. I truly can't wait to see you guys again.

I would also like to thank my family. Thank you to my mom, who is simply the best woman I know. Thanks for always giving me a shot and always believing in me, especially when I need it the most. You make me feel brave and I will always cherish what you taught me throughout my life. Thanks to my father, who has always encouraged me to improve myself and push myself harder when I needed it. Thank you to Luigi, for always being a fun guy and taking such good care of my mom. Thanks to Dario, for being the brother I know I can always count on. Thank you to my cousin Ilaria and my aunt Cristina, for always being there for me and always helping me find

my smile. Thanks to my grandma, for always being one of the best reasons to come and visit in Milan. I truly have the best family a person could ever ask for.

Lastly, I want to thank Cecilia. Since the first day I met you, I knew that you are simply one of a kind. I will never stop thanking you for all the amazing moments and all the fun that we have lived through together. Thank you for being everything that I have always dreamed about and more. You will always be the first person I call when something good happens because all of these years of university have given me something that makes me feel to this day full of life and joy: you.

Lastly, I would like to thank all those who have given me advice and shown interest in the following research. Thank you to everyone.

Abstract

This study analyzes the crisis communication strategies employed by the American Central Intelligence Agency and the Italian Agency for External Information and Security (Agenzia Informazioni e Sicurezza Esterna, or AISE) during high profile events, focusing on the theoretical implications of managing public perception under operational secrecy. By analyzing historical sources and contemporary case studies, this research explores how secretive government organizations can adapt crisis communication to the challenges they face. Delving into key crisis communication theories, including Situational Crisis Communication Theory and Image Repair Theory, this thesis analyzes the interconnection between intelligence work and crisis management, and how intelligence organizations seek to maintain public trust in these contexts. By studying the evolution of the communication practices implemented by the selected organizations, this study aims to broaden the theoretical understanding of how intelligence agencies can improve crisis communication practices during high-stakes events. The findings demonstrate that the crisis communication strategies undertaken by these intelligence agencies not only impact the institutional credibility of the States' intelligence community, but are also a key element of the national security framework of their home country.

Table of Contents

Abstract 3
Introduction 8
CHAPTER 1: LITERATURE REVIEW 10
1.1 Intelligence and Democratic Tensions: Bobbio's Theory of Invisible Power 10
1.2 The Public Image of Intelligence Agencies 11
1.3 Situational Crisis Communication Theory 14
1.4 Image Repair Theory 16
1.5 Perception Management and Intelligence Agencies 20
1.6 Transparency, Intelligence Dissemination and the Press 21
1.7 Conclusion 23
CHAPTER 2: RESEARCH METHODOLOGY 24
2.1 Research Design 24
2.2 Selection of Case Studies 25
2.3 Data Collection 26
2.4 Analytical Framework 27
2.5 Ethical Implications and Limitations of the Study 29
2.6 Conclusion 30
CHAPTER 3: CASE STUDIES 31
3.1 The Formation of the Central Intelligence Agency 31
3.2 The Evolution of AISE in Italy 32
3.3 The Snowden Leaks 34
3.4 Paragon Scandal 39
3.5 Conclusion 43
CHAPTER 4: DISCUSSION 44
4.1 Implications for Crisis Communication Theory 44
4.2 Strategic Responses to Reputational Threats 47
4.2.1 Denial Strategy 47
4.2.2 Corrective Action 49
4.2.3 Mortification 53
4.3 Other Strategic Approaches 56
4.4 Conclusion 66
CHAPTER 5: POLICY PROPOSALS 66
5.1 Proactive Transparency in Intelligence Disclosures 67

5.2 Strengthen Oversight and Civil Society Participation Mechanisms 69
5.3 Internal Reforms 70
5.4 Conclusion 72
Conclusions 72
Bibliography 75

List Of Abbreviations

AISE – Agenzia Informazioni e Sicurezza Esterna

AISI – Agenzia Informazioni e Sicurezza Interna

CIA – Central Intelligence Agency

CISR – Comitato Interministeriale per la Sicurezza della Repubblica

COI – Coordinator of Information

COPASIR – Parliamentary Committee for the Security of the Republic (Italy)

DCAF – Geneva Centre for Security Sector Governance

DIS – Dipartimento delle Informazioni per la Sicurezza

DNI – Director of National Intelligence (U.S.)

ECHR – European Court of Human Rights

EU – European Union

FBI – Federal Bureau of Investigation

FISA – Foreign Intelligence Surveillance Act (U.S.)

FNSI – Federazione Nazionale Stampa Italiana

GCHQ – Government Communications Headquarters (UK)

GDPR – General Data Protection Regulation (EU)

HUMINT – Human Intelligence

ICE – U.S. Immigration and Customs Enforcement

IRT – Image Repair Theory

LIBE – Committee on Civil Liberties, Justice and Home Affairs (European Parliament)

NATO – North Atlantic Treaty Organization

NSA – National Security Agency (U.S.)

NSO – Israeli surveillance company

ODNI – Office of the Director of National Intelligence (U.S.)

OECD – Organisation for Economic Co-operation and Development

OSS – Office of Strategic Services

PCLOB – Privacy and Civil Liberties Oversight Board

PEGA – European Parliament Committee of Inquiry on Pegasus and equivalent spyware

POGO – Project on Government Oversight (U.S., NGO)

PRISM – NSA surveillance program revealed by Snowden

SCCT – Situational Crisis Communication Theory

SID – Servizio Informazioni Difesa (Italy, historical intelligence agency)

SIFAR – Servizio Informazioni Forze Armate (Italy, historical intelligence agency)

SIGINT – Signals Intelligence

SISDE – Servizio per le Informazioni e la Sicurezza Democratica (Italy, domestic intelligence, disbanded 2007)

SISMI – Servizio per le Informazioni e la Sicurezza Militare (Italy, military intelligence, disbanded 2007)

Introduction

The digital age has brought about technological advancements in all fields. National security is no stranger to this. Intelligence services have benefitted from technological advancements that have created "unparalleled capabilities for collection, storage, cataloging, and use of sensitive data about individuals" (Laperruque, 2019). This has allowed for the intelligence agencies of the United States and Italy to establish large data collection and surveillance programs on their citizenry, such as the ones denounced during the 2013 Snowden revelations. The NSA had established a data collection program on millions of Americans and citizens around the world for counterterrorism purposes. This program came under heavy scrutiny during the Obama presidency due to Edward Snowden leaking the details of this program to the press in 2013. President Obama then ordered a full review of the program. In the Italian case, the Italian intelligence apparatus recently came under scrutiny for using an Israeli-grade spyware to monitor human rights activists and critics of Prime Minister Giorgia Meloni. These episodes can be traced back to an analysis conducted by the Geneva Centre for Security Sector Governance, which highlighted how the main difficulty that the selected intelligence agencies have endured alongside these technological advancements is the balancing of national security concerns and democratic accountability (Geneva Centre for Security Sector Governance, 2021).

By using official press releases, academic articles, and credible journalistic sources the objective of this thesis is to examine the communicative strategies set in place by Italian and American officials affiliated with the intelligence services and examine their impact on the general public. The research seeks to address a research gap in crisis communication scholarly literature, focusing on intelligence agencies which represent an unexplored yet highly relevant topic in the study of contemporary crisis communication. By examining the strengths and weaknesses of the strategies of the CIA and AISE, this thesis aims to analyze how intelligence agencies have dealt with reputational crises in recent years during surveillance-related scandals.

The selection of the case studies stems from the author's interest in national security policies and the possibility of conducting a comparative study between a global superpower and a medium-sized European state. The Snowden revelations have had a lasting impact on international affairs, prompting the passage of legislation such as the USA FREEDOM Act in the U.S. and the GDPR in the EU. The Snowden case also ignited a strong debate on civil liberties and the right to

privacy. As the Paragon case in Italy is still ongoing, it is crucial in analyzing the response of AISE and other government officials to a reputational crisis.

This thesis will analyze two case studies: one for the United States and one for Italy. The selected case studies shall be the Snowden revelations and the Paragon scandal. The thesis is divided into five chapters. The first chapter will analyze the theoretical framework set out by important crisis communication scholars, such as Image Repair Theory developed by W. Benoit (1995) and Situational Crisis Communication Theory theorized by W.T. Coombs (2007). The second chapter will explain the research methodology of this thesis by explaining how examining the recurring themes in the communication style of the CIA and AISE enables readers to grasp the shortcomings of the strategies of the U.S. and Italy's intelligence agencies. The third chapter will explain the case studies and their relevance in crisis communication, analyzing how the responses of governmental and intelligence officials influenced both outcomes and the broader national security apparatuses of the selected nations. The fourth chapter will discuss the findings of the research and analyze the communication styles of both agencies and how these strategies impacted public opinion. After having discussed the impact of these strategies, the fifth chapter will provide policy proposals as to how these agencies can improve their responses to crises. These proposals will be grounded in crisis communication theory and the analysis of the selected case studies.

CHAPTER 1: LITERATURE REVIEW

This chapter will examine the theoretical framework on which the study is based. By applying theories such as Situational Crisis Communication Theory and Image Repair Theory, the research will analyze the relationship between intelligence agencies and the principles of democracy and transparency. Drawing from political science texts such as Bobbio's *La Democrazia e il Potere Invisibile* and communication studies, the chapter will highlight how institutional transparency can come under pressure when national security is at stake. The chapter will also focus on declassified documents and scholarly literature, which will allow readers to better comprehend the internal dynamics of intelligence agencies' crisis communication strategy.

1.1 Intelligence and Democratic Tensions: Bobbio's Theory of Invisible Power

One of the most important concepts in understanding the complexities of how intelligence agencies operate within the crisis communication framework is discussed in *La Democrazia e il Potere Invisibile* by Norberto Bobbio. In his analysis, Bobbio articulates fundamental concepts for clarifying the theoretical framework of this work. Bobbio begins his analysis by engaging in the notion of "public power in public", one of the basic notions of democratic governance. By stressing the importance of making legislative acts public and accessible, Bobbio argues that the ideal democracy operates through a visible power, yet the evolution of the modern state has brought to light more secretive forms of power, often used to advance national security interests. Bobbio continues his study by stating that no democratic or authoritarian state has renounced the use of intelligence services due to the fact that there is no better way to gather information on other nations. Bobbio states that modern democracies have formed sub-governments and crypto-governments. The author defines sub-governments as technocratic institutions within the democratic form of governance that operate without sufficient democratic oversight, whereas crypto-governments are defined as "the set of actions carried out by subversive political forces acting in connection with the secret services, or a part of them, or at least unhindered by them (Bobbio, 1980, p.201). Bobbio reinforces these claims by citing historical examples such as the Piazza Fontana terrorist plot, emphasizing how more silent powers within a democracy can evade supervision by claiming national security concerns. Furthermore, the expansion of technocratic governance and the institutionalization of state secrets have created a condition within democratic societies were democratic control no longer functions effectively. Democracies have shown

growing reliance on experts that operate largely independently due to their expertise, particularly in times of crisis where secrecy becomes a necessity (Bobbio, 1980). Bobbio's insights are extremely important for the research of this thesis: for an effective communication strategy on the part of intelligence agencies to take place, an adequate amount of governmental oversight and public confidence-building measures must be undertaken, while also safeguarding the need for secrecy for operational security (Bobbio, 1980).

1.2 The Public Image of Intelligence Agencies

Hayward expands on the concepts outlined by Bobbio and analyzes the communication methods employed by intelligence agencies. Throughout the course of his research, Hayward analyzes how intelligence officials communicate with the public. Especially in recent times, intelligence service chiefs have taken to social media to engage in a more direct approach regarding the communication of intelligence-related information in an attempt to reinforce their commitment to ethics, democracy, and the importance of free speech. But these values remain vague as to their true significance, accentuating their messaging in limited sectors such as diversity and education. Hayward continues his study by expressing skepticism towards the public outreach undertaken by intelligence agencies to express their moral allegiance. Hayward asserts that the availability of higher quality information does not necessarily lead to better decision making. Furthermore, public intelligence disclosures often coincide with a carefully curated narration of the crisis the intelligence agency is facing at that moment, thus creating a paradox: stories put forward by intelligence agencies lack the possibility of creating an effective debate due to the strategically shaped narratives that aim to serve predetermined political objectives, undermining the possibility of the public to critically assess official accounts and undercutting the democratic ideals that these intelligence apparatuses declare to uphold. Another focal point of Hayward's research is the work conducted by intelligence agencies regarding countering disinformation, a high-level strategic goal that has begun to gain traction among Western democracies. Hayward provides a working definition of disinformation given by Hinšt: "Disinformation is much more than just false information. It would be easy to argue that the world's history, as well as social, and especially political, relations have been full of false information and lies. That way, the geopolitical problem of modern-day disinformation could easily be relativized and even ignored. In fact, the goal of actors behind disinformation is to undermine and relativize liberal democratic institutions of the transatlantic world and its democratic allies. The analytical approach toward disinformation

requires a deep understanding of the context, political risks and the motives of actors. While fake news and false information can be relatively easily debunked, disinformation requires stronger and more systematic analytical efforts to detect and reduce the risks of promoting massive false dilemmas, often combined with populist narratives, conspiracy theories, public apathy and hostile intelligence influence from authoritarian powers" (Hayward, 2023, p. 315). Hayward goes on by discussing how the laws regarding the countering of disinformation in the USA and the UK have become harmful to the national security concerns of the nations involved. Even if the supposed targets of these efforts are foreign nations, intelligence agencies have often resorted to tackling legitimate dissenting opinions of their own citizens during episodes such as the Salisbury poisonings and the supposed chemical attack in Douma. During such episodes, covert government institutes such as the Institute for Statecraft monitored private citizens' social media accounts and presented the findings to the public as the users being either bots or "useful idiots" of the Kremlin. The mainstream media accepted this narration, even if the methodological approach to counter-disinformation of the British intelligence apparatus lacked competence. Furthermore, covert operations by intelligence agencies have also partaken in the planting of false stories or political interference, such as the attempts to undermine the candidacy of Jeremy Corbyn for Prime Minister. Hayward then analyzes the question as to who exactly do the intelligence services answer to: appearing as agents of an effective power to define the national interest that neither the electorate nor the parliament have power over, it is not easy to determine as to who they answer to. Intelligence chiefs have shown reluctance to provide complete transparency to oversight committees of legislative bodies. The security services have also exercised significant interference not only with social media users, but with social media companies themselves. A significant episode of this is the Twitter Files, where security agencies blocked the circulation of a New York Times story that demonstrated problematic ties of the Biden family with elements of the Ukrainian State. This blockage was reinforced by a letter from American intelligence officials stating that the story had the earmarks of a Russian disinformation campaign, but this proved to be a mischaracterization of the story to the American public. Similar approaches conflict with other episodes such as Donald Trump's Russiagate scandal, undermining not only the credibility of the American national security agencies but also transparency and democratic accountability. Hayward emphasizes the role of academics in evaluating and revealing the manipulative strategies of the security services, thereby highlighting the significance of scholarly investigation and public

awareness in preserving democratic rights and values (Hayward, 2023). The Italian Intelligence services have also suffered from similar issues: a long list of scandals including the involvement in the extraordinary renditions program of the CIA, unlawful monitoring of the activities of government officials, businessmen, legislators, and, more recently, attorneys, judges, and non-governmental organizations. The Italian intelligence community has also partaken in the dissemination of false information and scare tactics in the media, with journalists acting as paid informants. In November 2006, Nicolò Pollari, the director of SISMI, the military intelligence service at the center of the controversies, was dismissed and prosecuted for the extraordinary rendition of Abu Omar. In addition to violating fundamental rights, these episodes damaged public confidence in the Italian government, due to the fact the political elite allowed the agency to stray from their remit with little responsibility. One of the most important reforms of the Italian intelligence security architecture happened in 2007 (Law 124/2007). The reform aimed to enhance transparency within the Italian intelligence system. Both AISE and AISI (the domestic intelligence agency) were placed under the authority of the Prime Minister and a parliamentary oversight committee (COPASIR) was established. COPASIR's primary role is to ensure accountability and continuously review the operations of Italian intelligence agencies (Statewatch, 2012). Furthermore, Senator Enrico Borghi from Italia Viva has recently introduced a bill to create a national agency against disinformation meant to operate alongside AISE and AISI. The immediate goal outlined by Senator Borghi is safeguarding the country's democratic mechanism from influence operations, such as the varied barrage of Russian disinformation operations (Decode39, 2024). While these reforms intend to create a more transparent environment in the Italian national security architecture, the Republic's security apparatus has recently come under scrutiny for a new surveillance scandal that involved the Paragon software, used to spy sea rescue activists and other members of civil society (Amnesty International, 2025a).

1.3 Situational Crisis Communication Theory

Current literature establishes the groundwork for the theoretical framework to be employed in making a detailed examination of the crisis communication practices employed by the selected intelligence agencies. Guided by Hayward's assessment of intelligence communication plans and their broader ramifications on democratic accountability, the chapter will apply leading theories proposed by crisis communication scholars such as Timothy Coombs and William Benoit. Their work on Situational Crisis Communication Theory (SCCT) and Image Repair Theory, respectively, has provided essential insights for organizational crisis communication. In order to examine further into the crisis communication tactics employed by the CIA and AISE, it is crucial to define key theoretical principles to better address the topic of this study. The first definition that we will explore is that of 'crisis'. The concept of crisis explored by Coombs emphasizes how one of its central themes is the matter of accountability and the ability of organizations to meet certain demands from the stakeholders. In his book, Coombs continues his analysis by stating how a timely response by the organization is key to delivering a successful crisis communication response, such as in the Johnson and Johnson Tylenol "product tampering" case. Recently, Coombs has provided a key definition as to what a crisis is: "A crisis can be viewed as the perception of an event that threatens important expectancies of stakeholders and can impact the organization's performance. Crises are largely perceptual. If stakeholders believe there is a crisis, the organization is in a crisis unless it can successfully persuade stakeholders it is not. A crisis violates expectations; an organization has done something stakeholders feel is inappropriate" (Coombs and Holladay, 2010, p. 6). Coombs states that a crisis can be divided into three stages: pre-crisis, crisis, and post-crisis. The pre-crisis communication phase is oriented towards what can be done in the event that a crisis arises. The crisis stage is the most studied in the field; this interest is commonly sparked by the news coverage of the crisis event. Finally, the post-crisis phase allows the organization that is undergoing the crisis to have the opportunity to employ follow-up communications, and to learn from what went wrong during the crisis in order to diminish the likelihood of its occurrence in the future. It is worth noting that if the organization employs an effective crisis communication strategy and policy changes are made, the event cannot be characterized as a crisis, as in order to experience a crisis the organization must do something wrong (Coombs and Holladay, 2010). Haupt expands this concept by delving deeper into the concept of "emergency management". Experts in the field must comprehend the multifaceted nature of communication by identifying

strategies that encompass information sharing and comprehension, and then adapt those strategies to the needs of the community. Haupt notes that emergency managers and public administrators were able to achieve impressive results when they integrated awareness of cultural differences within their communities into practice. If attention is given to local community needs when communicating during a crisis, negative impacts can be avoided in an effective manner. Haupt continues her analysis by explaining how one of the most employed theories in the domain of crisis communication is SCCT. The main theme of SCCT is an emphasis on recovering from the crisis at hand through balancing proactive and reactive measures. In her study, Haupt analyzes how SCCT is applicable not only to organizational reputation, but also to emergency management. The results of Haupt's study stress the importance of emergency managers in preparing a communication strategy that fits the needs of the organization and the community. The main characteristics that emergency managers have to demonstrate in their communication strategy are trust, transparency, consistency, perseverance, honesty, and competence, along with the importance of networking and fostering relationships with impacted stakeholders. The policy recommendations for community leaders and decision-makers are to exercise regularly the strategies of crisis communication and involve emergency managers in the decision-making and policy-making of crisis communication plans (Haupt, 2021). In his book, Coombs investigates the social scientific approaches to the concept of crisis, in order for it to be enriched by a broader view of the topic. Coombs continues his study by analyzing how the key to effective crisis response lies in understanding when key spokespersons should deliver and adopt the most reassuring tone. Public relations theory that emphasizes media relations may alter the understanding of crises by framing them primarily as media events. Consequently, this perspective extends to evaluating crisis response effectiveness based on its success or failure in managing media relations. The theoretical framework on this topic has focused on the source of the crisis as the main sufferer of this event, but the current discourse on the suffering of crises includes many other voices rather than only focusing on media relations. The construction of the narrative of a particular crisis is developed within a particular community and, in some instances, may be outside the control of the organization. Following this assumption, communication can be intended as more than simple information sharing, as newer theories have shown that modern communications also rely heavily on attribution theory. Scholarly work in the last decade has delved deeper into how risk and crisis are both interdependent and unique matters. Risks tend to occur with various magnitudes and

degrees of predictability. By showcasing various case studies (such as Hurricane Katrina), Coombs investigates how a crisis may occur. Throughout his book, Coombs defines 'risk' as a calculation of the probability of what could go wrong. Certain issues may arise from risks, which may also lead to a crisis. The example illustrated by Coombs is the safety hazards caused by smoking, which caused a crisis for the tobacco industry. The interconnections between risk, issue and crisis can have public policy implications and lead to threats or opportunities for the private sector. This link is fundamental in enriching the understanding of public relations. The parameters of success or failure outlined by Coombs are not limited to reputation management, but include control as well. The organization must control the narrative surrounding the crisis because controlling the discussion around the crisis at hand represents a vital interest for the organization itself, in order to save face or frame the issue in a more favorable way. The interest for control is also shared by communities. An effective crisis response makes it certain that the interested communities have sufficient knowledge to make educated decisions and act in a coherent manner towards the organization. The final result of how the narrative enters communal discussions is a fundamental factor in determining the consequences of the crisis and the success of the organization's response. In essence, crisis outcomes must be analyzed not only through reputation, but also by assessing other factors such as issue evolution, shared control and uncertainty reduction (Coombs and Holladay, 2010).

1.4 Image Repair Theory

The second theory that will be explored throughout this chapter is Image Repair Theory (IRT), a theoretical framework developed by William Benoit in 1995. Benoit developed this theory in order to analyze how individuals, organizations, and governments respond to crises that threaten their reputation. Credibility is the main factor of Benoit's theory, as it is crucial for persuasion and restoring credibility to the actor's image. The main factor to take into consideration when understanding IRT is the nature of attacks or complaints. Benoit identifies two components to an attack: holding the accused responsible for an action, and considering that action offensive. For example, a business can be accused of acts that it performed, ordered, encouraged, facilitated, or permitted to occur. What is important about an attack is not if the act itself is offensive, but if it is perceived as such. IRT encompasses various strategies for mitigating reputational damage: Denial, Evading Responsibility, Reducing Offensiveness, Corrective Action, and Mortification. Denial presents two possible variants: a simple Denial and shifting the blame, arguing that another actor

is actually responsible for the offensive act. This was the case for the Exxon Valdez oil spill, when Rawl, the chair of Exxon, blamed state officials and the Coast Guard for the delay in authorizing the company to arrive at the scene and apply chemical dispersant.

Evasion of responsibility has four versions that are applicable to crises. The first method of evasion of responsibility can be stated as a response to another actor's action, such as a company moving a plant to another country due to a law being passed reducing its profit. The second method of evasion of responsibility is defeasibility. In this case, the business states that important pieces of information were missing regarding the situation at hand. The third option is to claim the offensive action was an accident. The fourth strategy that can be used is stating that the offensive action being discussed was performed with good intentions.

A company that is accused of having committed an offensive act may try to reduce the offensiveness of the act by either fostering the positive feelings of the public towards the organization, minimizing the negative feelings, differentiating the act from more offensive acts, placing the act in a more favorable context, Attacking the Accuser of the organization, or offering compensation to the individuals who were offended by the act.

Corrective Action represents a promise by the company to correct the problem. This can be undertaken by the company through the restoration of the initial conditions or promising to the audience to implement measures in case of the recurrence of that offensive act.

Mortification is an image restoration strategy that consists in confessing and asking for forgiveness from the public. Benoit applied this approach to a diverse sample of case studies, such as the Valdez oil spill and the advertisements by Coca-Cola and Pepsi-Cola in *Nation's Restaurant News*.

Benoit's suggestions for crisis communication firstly emphasize carefully planning the organization's response to a potential crisis. Contingency plans are a key element in preventing missteps in an organization's initial response. Secondly, it is crucial to understand the nature of the crisis and the targeted audience. Lastly, it is vital for a firm to identify the relevant audience. Prioritizing the most important audience is vital to make sure the process of appeasing the audiences afflicted by the crisis reaches the most satisfying results.

A firm must also decide whether to respond to accusations in the first place. Accusations and apologies are interdependent, but responding to all accusations might not always be the best course of action for organizations. Instead, a firm may choose to redefine the attack, shift attention to other matters, or dismiss less relevant accusations that do not significantly impact the audience. In cases where an accusation gains traction or is repeated frequently, direct engagement might become necessary.

Furthermore, an organization must use a suitable rhetorical strategy. Image repair discourse recommends avoiding making false claims and that any reply must be adequately evidenced. Blame shifting can sometimes succeed, but can also fail if the organization has some fault: Exxon's failed blame deflection of the Valdez oil spill onto Captain Hazelwood demonstrates the danger of this tactic. Conversely, Tylenol effectively deflected the blame for product tampering onto a third party while also taking remedial measures, e.g., embracing tamper-resistant packaging, intended to regain public trust. The effectiveness of an organization’s crisis response depends on the transparency and the corrective action that the firm decides to implement. Admitting fault can be considered a useful tool to restore credibility, which is a key element in crisis management: Exxon’s claims of a swift and competent crisis response were contradicted by independent reports, which led to even greater reputation damage.

Ultimately, a company's response must be precisely calibrated to its audience, the nature of the crisis, and the possible consequences of different approaches. Using several strategies, such as Corrective Action, transparency, and strategic messaging, might be the best course of action to take in a crisis and still preserve trust and credibility (Benoit, 1997).

The implementation of Image Repair Theory has been a fundamental notion in the U.S. national security framework and has been employed by governmental agencies such as the CIA. One of the most notorious examples of the use of Image Repair Theory was when the Agency’s Director Helms and his successor William Colby denied the involvement of the intelligence apparatus in the participation in the Watergate scandal. According to declassified materials, the agency was put in a difficult situation when presidential aides approached the CIA with requests to influence the ongoing investigation. The intelligence community decided to resist the pressures of the Nixon administration and deny any involvement from Langley’s part in the offensive action that Nixon had committed. Aligning itself with the Denial and shifting blame strategies, the CIA

asserted that the agency had no operational connection or knowledge of the Watergate break-in. During the Watergate scandal, Langley also attempted to control the narrative surrounding the scandal by undertaking a proactive approach through a series of public declarations distancing the organization from the political aspects of the crisis that the Nixon administration was undergoing. Even though intelligence agencies generally avoid public declarations and interviews, the CIA made its position publicly known throughout hearings and interviews by its leadership (Claiborne, n.d.; Stern, 1973). The episode of the Watergate scandal set a precedent in the American intelligence community with regard to crisis communication: when faced with public scrutiny, intelligence agencies must intervene with communication restricted to the essential facts of the crisis that the organization is facing, aimed at preserving the institutional integrity of the intelligence apparatus. The Italian intelligence community has had to rely on similar strategies during the Abu Omar case, where Italian military intelligence operatives aided the CIA in the extraordinary rendition mission in Milan. The former director of SISMI Nicolò Pollari stated that during his tenure the CIA did not involve him in the decision to abduct Nasr Osama Mustafa Hassan, in accordance with Benoit's' Denial strategy. Pollari denied the involvement of the Italian intelligence community, despite mounting evidence pointing to the contrary, and the Berlusconi government invoked state secrecy to prevent judicial authorities from examining the case more closely (La Stampa, 2007). The strategy adopted by the Italian government can be traced back to the evasion of responsibility defined by Benoit, as Italian officials shifted blame citing national security concerns. The State also overturned the conviction of Nicolò Pollari, Mancini and other SISMI officials as the Supreme Court of Cassation exonerated them citing secrecy laws (Reuters, 2014). In conclusion, these parallel cases highlight how Denial, evasion of responsibility, and legal containment are crisis communication strategies used by intelligence services in democratic governments, not only to protect individual agents but also to maintain the institutions' legitimacy and ability to continue operations.

1.5 Perception Management and Intelligence Agencies

The last theoretical concept that will be explored throughout this chapter is "Perception Management". Perception Management can be defined as "actions that are designed and carried out by organizational spokespersons to influence audiences' perceptions of the organization" (Elsbach, 2003, p. 298). Elsbach outlines four key components, which can be identified as: (1) perceptions of the organization; (2) actions or "tactics"; (3) organizational spokespersons; and (4) organizational audiences. For example, the organization at hand may implement symbolic actions or select a specific spokesperson to facilitate the conveying of the message that the organization wishes to transmit to the selected audience (Elsbach, 2003).

As Taylor argues, Perception Management is a crucial component of the security architecture of the United States. Taylor provides further insight into how Perception Management plays a decisive role in information warfare and intelligence operations, particularly in the post-9/11 era. Using the War on Terror as a case study, Taylor illustrates how the American media rallied behind the war on Al-Qaeda after a period of declining interest in American foreign policy. After initial mistakes (such as using the word "crusade") the United States had to quickly learn the importance of Perception Management to foster the impression of America as a force of good in the world, especially after the release of photos of Guantanamo Bay prisoners caused ethical concerns also among the allies of the USA. Furthermore, Taylor continues his analysis by focusing on how anti-American narratives were countered by the American establishment framing the 9-11 attacks. The fact that mainland USA was attacked without prior detection by using Cold War-era intelligence techniques proved to be a wake-up call for the American establishment. With the American victory against communism in the Cold War, HUMINT was given less importance. The integration of the United States Information Agency into the State Department in 1999, coupled with the ensuing demoralization of its personnel, can be identified as the beginning of the declining interest in public diplomacy on behalf of the State Department in comparison to the Reagan era, where it represented a more than useful tool to help the United States win the Cold War. During the Afghan campaign, the State Department demonstrated how drastically the lessons of the Cold War had been forgotten. When the Bin Laden tape reached American news outlets, the Voice of America ignored the governmental request to not rebroadcast the tape for fear of hidden messages to sleeper cells within the United States. The situation created a substantial divide with the State Department, which had disregarded a fundamental precept of international public information: to

make an information service credible, it is necessary to encompass divergent points of view, inclusive of negative news. Taylor continues the study by delving deeper into how a majority of independent media complied with the official guideline, but government-controlled media did not. There are a number of lessons in this case that are worth revisiting, not least because the appeal to stop the broadcast of the tape was interpreted in many areas as just another example of the 'hypocrisy' of Western democracies. According to this view, democracies claim to be the champions of freedom of speech, which is displayed as a fundamental value for progress in many Arab countries. In the wars that involved the Western hemisphere, the media has rallied behind its 'boys', but in the modern world, the West no longer perceives the wars it is involved in as truly its own. This factor can be closely linked to the decline of ideology, where we can observe that the number of democracies is in decline and their threats are on the rise. In this scenario, the security architecture of a State should be prepared to face national emergencies in a changing world in which different types of interventions will be needed (Taylor, 2002).

1.6 Transparency, Intelligence Dissemination and the Press

Scholarly literature has examined the implications of the relationship between the Central Intelligence Agency and news outlets. Throughout its history, Langley has committed intelligence errors that brought about catastrophic consequences, such as claiming Saddam Hussein's possession of WMDs to justify the invasion of Iraq. Such errors are gravely detrimental to U.S. credibility and press credibility alike. Such dynamics underscore the crucial role of the press in holding intelligence agencies accountable. The study conducted by Gup showcases how both elements of the intelligence community and the press tended to accept many obscure notions surrounding the Iraq war as if they were common knowledge rather than uncertainties. If CIA Director George Tenet firmly believed that Iraq had WMDs, the same was true for Judith Miller of *The New York Times* and several other journalists. The limited access to knowledgeable sources that the press had to endure during the Iraq War made less credible sources seem more authoritative. But secrecy is not sufficient to explain the failings of the CIA during this period: many other elements, such as political pressures, jealousy between Langley and the FBI, and the loss of experienced intelligence analysts after the Cold War period were just some of the elements that brought about the greatest U.S. intelligence failures of the twenty-first century. The Global War on Terror that ensued after the 9/11 attacks saw an expansion of the activities of the CIA, which started to participate in active warfare (such as with Predator drones). Gup argues that an

effective reporting of the Central Intelligence Agency must entail skepticism of official statements and analyze the patterns that lead to intelligence failures, rather than focusing on isolated cases. Journalists may also play a key role in explaining the internal culture of the CIA, which has often appeared as a distant entity by the general population. By explaining such culture, many stories of the Agency's shortcomings begin to make more sense. Finally, Gup explains how journalists must strive to avoid the distractions that Langley attempts to implement to distance itself from its failures and hold the intelligence community accountable for its actions (Gup, 2004).

Building on these concerns, a report from the Office of Training of the CIA regarding the methods of communicating intelligence information outside the intelligence community strengthens the explanation of Gup regarding the challenges of accountability in the American intelligence community. The report, dated 1964, explains how the Agency has an ineffective policy regarding the declassification of documents. The report outlines how the CIA believes that selectively disseminating pieces of intelligence to the academic community may help researchers improve the quality of their work and, in turn, that their research may help the agency. The response of the academic community has been shown to be enthusiastic regarding the dissemination of unclassified intelligence. The report argues that the existence of a well-informed American public is fundamental to the conduct of good government. Consequently, Intelligence has been disseminated to the public on an *ad hoc* basis. The majority of the intelligence disseminated at the time originated in the Economic Research Area (ERA). The program for the sharing of unclassified ERA research publications to academic institutions was founded on September 11 1959, where some of the members of the Senior Economic Advisor Panel pointed out that the academic community benefited from the publications of the Sino-Soviet bloc that originated within the agency. As a result of this meeting, a memorandum was written by Otto E. Guthe. In the memorandum, Guthe outlined what he perceived to be the benefits of sharing intelligence. Guthe believed the sharing of intelligence with the public to be beneficial due to the fact that these persons and institutions would produce a better quality of product for Langley's interests if the data of the studies undertaken was based on information that only the CIA could provide. He also believed that the sharing of intelligence with the public represented a crucial element in the Perception Management of the Agency. The report also showcased several disadvantages: first of all, the general public can misunderstand the purpose of dissemination of reports and consequently undermine the Agency's efforts in the relative field. The second disadvantage outlined is that the

press and the congressional committee might find issues with the findings of the CIA and some individual researchers who were not on the recipient list might request copies, causing embarrassment to Langley. Dr. Guthe concluded stating that the advantages far outweighed the disadvantages. The report concludes that the dissemination of intelligence by the CIA has contributed to improving the Agency's image (Office of Training, 1964).

Italy's intelligence community has also faced challenges in its relationship with the media and transparency. The SISMI-Telecom scandal is one of the most notorious scandals to have ever hit the Italian security apparatus: unauthorized surveillance activities were carried out on businessmen, politicians and journalists leading to public concern on the oversight on the Italian intelligence agencies. According to the internal investigation carried out by Telecom the procedure used to wiretap phones had numerous flaws and the machines used allowed to spy on telephone conversations without leaving a trace, allowing for SISMI and Telecom Italia to access sensitive data regarding Italian citizens. An investigation was also carried out by the Italian Data Protection Commission to check if the personal data protection obligations were respected by SISMI. The scandal highlighted the potential of intelligence agencies to overstep their legal boundaries and highlighted the extremely important role that investigative journalism has in bringing such cases to light (EDRi, 2020).

In conclusion, by examining how the Italian and American security architectures engage with the media and intelligence dissemination, the reader may grasp a better understanding of how intelligence officials employ strategies to influence public perception.

1.7 Conclusion

To conclude, this chapter has explored how different theories of crisis communication are applicable to the national security apparatus of the United States and Italy. The research has shown how the intelligence community has adapted to crises such as the Watergate or the Global War on Terror. The theoretical frameworks that have been established in this chapter have highlighted key differences in how intelligence agencies communicate their crises compared to more conventional organizations: the CIA's and AISE's crisis responses reflect a more limited transparency and a tendency to shift blame onto external actors, such as during the Watergate scandal. The following chapters will apply the theoretical foundations analyzed to case studies, in order to better

understand how intelligence agencies have employed crisis communication strategies throughout its history. The next chapter will provide an overview of the research methodology of this thesis.

CHAPTER 2: RESEARCH METHODOLOGY

This chapter discusses the research methodology which will be applied throughout the course of this work. By applying the thematic analysis approach and focusing on a limited number of case studies, the research will analyze how the CIA and AISE implement their crisis communication procedures. The selected methodology will allow readers to better comprehend individual cases and will allow the researcher to create a foundation on which to build policy recommendations to optimize the intelligence communities' crisis communication strategy.

2.1 Research Design

This study adopts a qualitative research approach, which is considered the most appropriate when conducting research tied to specific contexts such as the crisis communication of intelligence agencies. Aspers and Corte define qualitative research as "an iterative process in which improved understanding to the scientific community is achieved by making new significant distinctions resulting from getting closer to the phenomenon studied" (Aspers and Corte, 2019, p.155). Aspers and Corte further state that qualitative research allows the researcher to take a more comprehensive method to the topic under examination: qualitative methods allow for a greater nuance in the materials, researchers to familiarize themselves with a great quantity of information, and transmitting the necessary data to readers in order to grasp the complexities of the subjects within the scope of a research's subjects (Aspers and Corte, 2019). In order to conduct effective qualitative research, De Blasio outlines three key characteristics. The first one is reliability: the research must be organized using systematic procedures and defined protocols. The second criteria is validity, meaning that the researcher should abstain from influencing the object of the study by providing untainted data. Lastly, generalization is also very important in conducting a qualitative analysis. Generalization refers to the extent to which findings from a study - which can be based on smaller or non-representative samples - can be applied to broader contexts or inform general

patterns, without necessarily claiming statistical representativeness of the population (De Blasio et al., 2018). Therefore, the qualitative approach is the most appropriate to show the nuances of the crisis communication policies of intelligence agencies.

This study adopts a multiple case study design. As illustrated by Eisenhardt, the case study is a research strategy that "focuses on understanding the dynamics present within single settings" (Eisenhardt, 1989, p. 534). Case studies typically combine data collection methods through both qualitative and quantitative means and can be used to accomplish various objectives: to provide descriptions, to test theory or to generate theory. Another important point of case study research is the rationale behind the selection of cases. Throughout her research, Eisenhardt stresses the importance of population, as it defines the entities on which the research will draw on and help define the boundaries within which the researchers must outline their findings (Eisenhardt, 1989). Gerring reinforces the points raised by Eisenhardt by stating that case studies are a viable source of producing causal and descriptive inferences. The main strength of case studies is their capacity to provide explanatory mechanisms alongside the relevant research, especially when variables are complex to isolate. Gerring also outlines the methodological limitations: case study research explains patterns rather than establishing absolute rules (Gerring, 2004).

2.2 Selection of Case Studies

The case studies that will be presented in this research represent high-stakes crises that involved the American and Italian intelligence communities. After being analyzed through the theoretical framework presented in the first chapter, policy proposals to provide more transparent and effective communication will be presented. The rationale behind the selection of case studies is based on their relevance to the present study, the diversity of scenarios and the availability of information. The criteria will also include the gravity of the crisis itself measured by their impact on public confidence in government among the American and Italian populations.

- Snowden Leaks: an important example of how the Central Intelligence Agency faced one of the most important political scandals in the history of the United States. Even though public approval rating among Americans remained relatively stable more or less the same between 2012 and 2013 (53 percent held a favorable view of CIA in 2012, 50 percent in 2013), the leaks led to a sharp decline in public perception of the accuracy of intelligence work (Zegart, 2013). Furthermore, a poll conducted by Pew Research Center in June, 2013

showed that while the American public thought that Edward Snowden should be prosecuted, a majority of Americans believed that the release of classified information about government data collection programs served public interests (Pew Research Center, 2013).

- Paragon Surveillance Scandal: At the end of January 2025, the Italian government found itself in the middle of controversy due to the surveillance of 90 journalists and members of civil society by a spyware software owned by Paragon solutions. After 2 investigative journalists who expressed criticisms towards Meloni's government came forward, sources from the Italian secret service confirmed the existence of a contract between Paragon Solutions and the Italian government. While the Italian Intelligence Community has shown to increase the public approval rating year after year, reaching 67.2% approval rating in May 2025 (PiazzaBorsa, 2025), the disclosures in the Paragon spyware scandal had a quantifiable impact in diminishing public approval of some of Italy's main political parties, as expressed in later opinion poll ratings (Ipsos, 2025).

2.3 Data Collection

To investigate each case, this study will use document analysis. The use of multiple data sources will enhance the readers' understanding of the crisis communication strategies implemented by the selected intelligence agencies. The document analysis will involve primary and secondary sources. Primary sources are defined as all documentation pertaining to the agency's external communication. This includes materials such as press releases, internal memoranda, and public statements made by intelligence officials.

Secondary sources will refer to materials useful for contextualizing the case studies, such as academic papers and crisis communication handbooks. For each case, an analysis of media coverage will be provided to readers, offering crucial insights into the public perception of the Agency during the crises that have been selected. These insights will be supported by relevant academic papers and textbooks.

By compiling qualitative data gathered through the aforementioned methods, this study aims to offer well-founded policy recommendations for improving the CIA's and AISE's future crisis communication strategies.

2.4 Analytical Framework

To provide an analytical framework, the thematic analysis approach will be implemented in order to structure the findings of this thesis. Nowell et al. define thematic analysis as a "qualitative research method that can be widely used across a range of epistemologies and research questions. It is a method for identifying, analyzing, organizing, describing, and reporting themes found within a data set" (Nowell et al., 2017, p.2). In order to conduct a successful thematic analysis, Nowell outlines a six-phase method for researchers.

- The first phase of the method consists of familiarizing oneself with the data at hand. This phase includes triangulating different data collection modes to increase the likelihood that the findings of the research at hand will be found credible. All sources of qualitative data are useful in conducting a comprehensive analysis. To immerse himself in the data, the researcher must first read the entire dataset before starting to code it, in order to become familiar with all aspects of the data.
- The second phase begins with the generation of the initial codes. Qualitative coding allows the researcher to simplify and focus on specifics of the data. Researchers find significant textual passages during coding and label them to index them in relation to a subject or problem within the information. According to Boyatzis, a "good code" is one that accurately depicts the phenomenon's qualitative richness.
- The third phase consists in searching for themes. After having coded all of the data, this phase entails sorting the extracted data into themes. A theme may be generated from the raw data or in a deductive manner from prior research. Thematic analysis allows for flexibility in determining themes in a number of ways, but the researcher must remain consistent in his approach in developing the themes: data and codes should not be abandoned at this point since, without carefully examining every extract in the fourth step of theme analysis, it is unclear whether the themes may be retained, integrated, improved, divided, or eliminated.
- The fourth phase involves reviewing themes. Once a set of themes has been devised, researchers must review the data to analyze whether it forms a coherent pattern or not. Incoherent data will be replaced with a new code and overlapping themes will be reduced into a more manageable set of information. By the time this phase is over, researchers have a solid understanding of the various themes, their relationships, and the overall narrative

the data conveys. By going back to the original data and contrasting it with the produced themes, one may test the referential adequacy and ensure that all findings are securely based on the data.

- During the fifth phase, researchers determine what aspect of the data they wish to convey to their readers and why. According to Braun and Clarke, theme names should be catchy and convey the topic's main idea to the reader right away. There may be some overlap between themes and sections of data that are part of several themes. In light of the research questions, researchers may take into account how each theme contributes to the broader narrative of the complete data set. Nowell's findings highlight how it is possible to continue redefining themes forever, and one of the main difficulties for researchers lies in knowing when to conclude the development of their themes. The themes cannot be finalized if there are still passages of text that are pertinent to the study question but are not included. After all of the data has been reviewed and the coding has been examined at least twice, themes shouldn't be regarded as final. The likelihood of producing reliable findings will rise if enough time is spent exploring the themes.
- The sixth phase begins with the production of the report. During this phase, the researcher will have fully established the findings of his research and will be able to provide a concise report to his readers. The statements made in regard to the data set are made credible and convincing by clearly communicating the logical processes used to reach the findings. The final report must include verbatim quotes from the participants. To illustrate the themes' ubiquity and help in understanding particular points of interpretation, brief quotes may be used. To give readers a sense of the original texts, longer quotation passages could be added. If researchers merely present the codes and themes identified in the transcripts the findings will result in a superficial analysis that fails to reflect the data's richness. Researchers should also strive to build an effective argument for choosing the themes that they have used to select their themes by using the literature. The credibility of the study will be determined by the coherence of the argument. In this phase, the researcher should discuss all of the findings, including unexpected results. The final report should create an overall narration about what the different themes reveal about the research question. Many authors suggest submitting the findings of the analysis to participants for member checking,

which allows the researcher to establish the correlation between respondents' views and the researcher's representation of them.

This analytical method provides for a highly flexible approach to this topic: Nowell delves deeper into how thematic analysis offers researchers a more accessible research method and can be easily applied to a variety of topics. Nowell also highlights some of the main disadvantages in applying this approach, such as the limited literature on this method may undermine researchers' confidence in its application. Nowell continued the analysis by analyzing how trustworthiness and credibility remain the cornerstones of thematic analysis, as it allows researchers to convey the worthiness of their findings to their readers. Furthermore, Lincoln and Guba developed the concept of trustworthiness by using the criteria of credibility, transferability, dependability, and confirmability to match the conventional numerical measures of validity and reliability. Nowell goes on by discussing the six-phased method proposed by Braun and Clarke, but remarks how the thematic analysis approach is actually a more fluid process that requires researchers to go back and forth between phases (Nowell et al., 2017). Furthermore, process tracing will be included in the analysis to help shed light on the research questions posed by the researcher. Process tracing can be defined as "the deduction of relations of causality through the identification of causal mechanisms" (De Blasio et al., 2018). Process tracing can be considered as a useful tool in the analysis of social and political phenomena. The process of causal relationships happens through two subprocesses, named process verification and process induction. Process verification is used to confirm that the findings of the researcher confirm previous theories on the subject and process tracing is based on the inductive observation of causal mechanisms. Process tracing is useful to describe political and social singularities, compare their findings with previous theoretical results, scrutinize into the knowledge of causal mechanisms and offer new tools to address challenges such as selection bias (De Blasio et al., 2018). In the context of this thesis, thematic analysis and process tracing will be implemented to establish patterns in the crisis communication strategies of the CIA and AISE in moments of crisis in order to provide policy proposals on how to improve these strategies.

2.5 Ethical Implications and Limitations of the Study

This thesis implies a range of ethical considerations. Firstly, it is crucial to be respectful of the

sensitivity of the research subject. In the following sections of the analysis, the researcher will strive to uphold a rigorous academic and ethical standard in order to approach such a delicate topic.

The main limitation to the research methodology relates to the availability of documents and sources. Even though many documents have been declassified by the Central Intelligence Agency, discussing such sensitive topics in research probably implies that the available record is incomplete. Documents that are used in this thesis have redacted sections due to the protection of national security interests. Furthermore, many internal memoranda, communications and other pieces of content contain inherent bias in favor of certain political positions. Following the precepts outlined in the research conducted by Mobley, Marchio and Keeley, the researcher will carefully cross-check facts and provide readers with the most accurate description of details along with the corresponding analysis after consulting reliable sources such as the US National Archives and Records Administration website or NATO online archives (CIA, 2024b). Furthermore, the recent events of the Paragon case present a challenge for research because its developing nature and political sensitivity imply a scarcity of sources, posing a limitation on the depth of the inquiry.

Secondly, the research will present a small number of case studies rather than select a larger number of cases in order to prioritize the qualitative analysis of processes. By conducting such an analysis, the researcher will be able to focus more on the quality of the research rather than the quantity of case studies. Scholars such as Flyvbjerg have demonstrated that undertaking such an approach is crucial in debunking stereotypes of the research subject and enable a more comprehensive understanding of the subject (Flyvbjerg, 2006).

Lastly, a standardized coding scheme will be employed to ensure comparability between the selected case studies. The coding grid will be constructed initially from key concepts in the theoretical framework and refined through inductive modifications in relation to the examined cases, allowing both the identification of recurring patterns in the CIA's and AISE’s crisis communication and the undertaking of a rigorous comparative analysis.

2.6 Conclusion

In conclusion, after having outlined this thesis's research methodology, the following chapters will elaborate on the collected data and provide readers with a transparent analysis of the selected case studies aligned with the research methodology outlined throughout the course of this chapter. The selected case studies will be examined through the lens of the research objectives, highlighting

patterns in the communication practices implemented by the CIA and AISE. The analysis of this research aims to contribute to academic discourse by delving deeper into an underexplored area within the broader field of crisis communication. Future researchers are encouraged to increase the data collected by interviews: by conducting interviews of national security experts, the field could gain greater insight on an extremely interesting policy issue for our time. Secondly, delving deeper into the institutional aspects of intelligence crisis communication could also help readers understand the policy issues behind the communication strategies of national security apparatuses worldwide. In conclusion, future researchers should also conduct a deeper analysis of how the internal processes at Langley and Rome influence crisis communication policy.

CHAPTER 3: CASE STUDIES

The following chapter will provide readers with an overview of the history of the selected case studies. After giving a historical overview of the process that culminated in the formation of the CIA and AISE, the research will also highlight their institutional and public role. As aforementioned, the case studies have been selected on the basis of their relevance to the study at hand by exploring the most notable controversies that saw the CIA involved in both domestic and international affairs.

3.1 The Formation of the Central Intelligence Agency

The Central Intelligence Agency was first conceived during the Second World War. After finding the intelligence apparatus in disarray, President Roosevelt decided to create the Office of the Coordinator of Information (COI). The Office was first led by William Donovan, whose task was to gather intelligence during the war. Throughout the course of the war, the COI evolved into the Office of Strategic Services, which became the first centralized intelligence agency in American history. After the end of the Second World War, President Truman reorganized the American Intelligence Apparatus into the Strategic Services Unit, a temporary solution before the government of the United States could find a more permanent solution to replace the OSS. In fact, in 1946, the Central Intelligence Group (CIG) was formed and represented a step forward in the American national security architecture: the CIG was the first organization of its kind to be able to conduct research and analysis independently. On September 18th 1947, the National Security Act

established the Central Intelligence Agency. The 1947 Act established the main duties of the CIA. This act established the role of Director of Central Intelligence and the United States Intelligence apparatus. Truman nominated Roscoe Hillenkoetter to lead the American intelligence community. The new CIA largely inherited personnel from the OSS. In 1949, President Truman signed an iconic piece of legislation that allowed the Agency to fund intelligence operations and develop personnel procedures outside the U.S. government practices. The widespread recognition of CIA's role in political action and paramilitary warfare led to a significant expansion of the Agency, as three new departments were set up between 1947 and 1953 while its headquarters moved to Langley, Virginia (CIA, 2023). The next structural shift in the U.S. intelligence apparatus happened in 2004 under George W. Bush, with the adoption of the Intelligence Reform and Terrorism Prevention Act as a response to 9/11. The Act put all the US intelligence agencies under the umbrella of the Director of National Intelligence (DNI), who has both the responsibility of advising the president and that of supervising the 17 national agencies. In light of the hybrid nature of threats to national security in the contemporary scenario, the CIA underwent further modernization in 2015, when it was reorganized into regional and thematic 'mission centers' (e.g. the China Mission Center, the Transnational & Technology Mission Center) in order to foster cooperation and integrated action among the directorates (CIA, 2024a). Throughout American history, the Central Intelligence Agency has proven to be one of the most important actors in the national security architecture of the United States and the selection of the case studies will allow readers to comprehend why the crisis communication strategies that the Agency has employed in the past have been fundamental in shaping the outcome of the cases and influenced the public perception of the security apparatus of the United States of America.

3.2 The Evolution of AISE in Italy

The modern Italian Intelligence apparatus finds its roots in the post post-World War II scenario. On March 30th 1949, the intelligence service was reorganized under the Information Service for the Armed Forces (SIFAR) under the command of Giovanni Carlo Re. One of the first outcomes of the stabilization of the political situation in Italy and its entry in NATO was the establishment of a legitimate intelligence agency such as SIFAR, albeit with limited sovereignty and being in close contact with American intelligence. In 1965, the intelligence community of Italy underwent a reform that transformed the SIFAR into the Defense Information Service (SID), which was entrusted with the duty of protecting the national interests of the Italian Republic. The SID

officially began its activities in July 1966 under the leadership of Admiral Eugenio Henke. One of the most important reforms of the 20th century for the Italian secret service was the Law 801/1977 that founded the Servizio per le Informazioni e la Sicurezza Militare (SISMI) and the Servizio per le Informazioni e la Sicurezza Democratica (SISDE). This new reform placed the intelligence services under the direction of the Ministers of Interior and Defense and gave senior management overall political responsibility, with the coordination of intelligence and security policy to the Prime Minister (Sistema di Informazione per la Sicurezza della Repubblica, 2015). The last major reform that the Italian intelligence service has undergone was the 2007 reform that placed the Italian secret service under a stricter surveillance by parliament and the Prime Minister. The reform also aimed to create the Interministerial Committee for the Security of the Republic (CISR) which was already in place under the previous law and is an advisory proposal and deliberation body that focuses on establishing policy guidelines and objectives chaired by the prime minister and comprising the ministers for foreign affairs, home affairs, defense, justice, and economy. The Italian intelligence community demonstrated its adaptability to different scenarios through operations in fields such as the war in Afghanistan, the war in Iraq and conflicts in the Balkans, which highlighted the importance of human intelligence (HUMINT) and Italy's role in peacekeeping operations in the region. These experiences have allowed for the secret services to develop cybersecurity capabilities within Italy's security architecture, led to stronger ties with international organizations that cooperate with Italy on security-related topics. The intelligence architecture of Italy is facing a wider range of contemporary threats that require for flexible and comprehensive solutions. State and non-state actors have been conducting cybersecurity attacks against critical infrastructure, carrying out espionage activities and spreading disinformation. To face these threats, AISE and AISI have started to enhance their cybersecurity capabilities by bolstering national defenses and collaborating with the private sector to secure infrastructure. Training programs are also being carried out in order to allow personnel to have a more comprehensive view of the evolving threats to Italy. The Italian Intelligence Community seeks to maintain its agility and responsiveness in order to safeguard national security interests in a world that is becoming more unpredictable by embracing technical innovation, encouraging international cooperation, and placing a high priority on the development of its human capital (Vernetti, 2024).

3.3 The Snowden Leaks

The Edward Snowden National Security Agency leaks is one of the most important episodes of political communication in history. The episode not only had global implications and impacted national security apparatuses worldwide, but also underlined the importance and growing power of the media in the contemporary context. During 2013 and early 2014, The Guardian, one of the most well-known British newspapers published a series of investigative articles on the use of the surveillance program known as PRISM, an internet surveillance program that the National Security Agency had developed that consisted of a weakly accountable internet and phone surveillance program. The articles published by The Guardian also underlined how the British equivalent of the NSA (the Government Communications Headquarters, or GCHQ) collaborated in these activities. According to the Guardian's story, GCHQ and the PRISM project conspired to allow American surveillance of British nationals. Additionally, it claimed that the NSA had been listening in on the communications of foreign nationals and foreign heads of state who were allies, including—most remarkably—the cell phone of Angela Merkel, the German chancellor. These pieces were published in The Guardian and were based on a purported cache of tens of thousands of confidential papers that were revealed by Edward Snowden, a former NSA insider (Chadwick et al., 2014). Snowden, a former technical assistant of the CIA, had spent his entire career working in the defense sector, by undertaking roles with contractors such as Booz Allen and Dell. After conducting a series of interviews with The Guardian, Snowden requested the newspaper to reveal his identity as he felt that he had done nothing wrong and was ready to face the consequences of going public with the information he gathered during his time at the NSA. Snowden did not initially believe that the security apparatus of the USA posed a threat to his personal political beliefs. In 2003 Snowden enlisted in the US army and began a training program to join the Special Forces and after an accident that caused him to break both of his legs broken, he was discharged. It was then that he got his first job in an NSA facility, working as a security guard for the NSA's covert facility at the University of Maryland. He was then hired at the CIA, where he was sent as a cybersecurity officer at the CIA station in Geneva. The article published by Greenwald, Macaskill and Poitras underline how the CIA engaged in morally questionable actions such as blackmailing local bankers in order to obtain private banking information. After this episode, Snowden was assigned by a private contractor to an NSA facility in Japan where he saw the Obama administration further the very policies that he was hoping would be rolled back. After having

reached the conclusion that the NSA's global surveillance program would soon be irrevocable, Snowden decided to act and to publish the information regarding these programs. (Greenwald, MacAskill and Poitras, 2013).

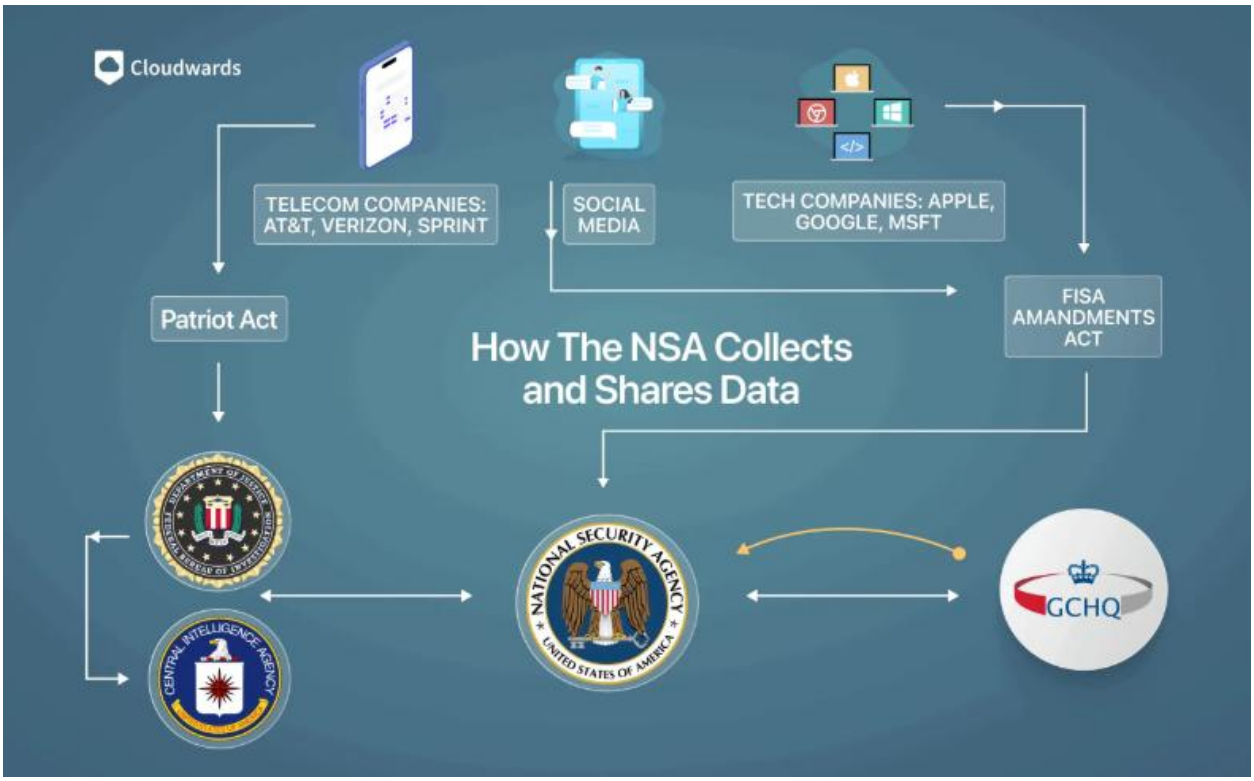

Figure 1: NSA's Data collection system, Hawkins (2025)

The political impact of the Guardian's pieces was almost immediate. Seven weeks after the release of the story, the U.S. House of Representatives voted on a bill that aimed to cut off funding for the NSA's surveillance program and serve as a stepping stone towards greater accountability for the intelligence community (Chadwick et al., 2014). The scandal had almost immediate repercussions for the public relations of the U.S. intelligence community and for the Obama administration. General Keith Alexander, head of the NSA at the time, attempted to embark on a "charm offensive" in order to persuade information security experts that the surveillance programs that the intelligence community had been undertaking were necessary to protect U.S. national security. Alexander's visit to the Black Hat Convention in Las Vegas also had the objective of curbing Washington's efforts to defund the programs and conduct damage control due to the leaks. At the conference, Alexander highlighted the successes of such programs, such as disrupting a 2009 plot to bomb the New York City subway, and emphasized how intelligence operatives worked

under heavy supervision from oversight bodies (Caroll, 2013). Concurrently, the White House and the Office of Director of National Intelligence (ODNI) undertook efforts in publicly attacking Snowden and justifying the surveillance programs. The ODNI notoriously engaged in an active public relations role in an effort to explain, justify, and defend the programs. On June 14th 2013, the United States Government filed a criminal complaint against Edward Snowden, who subsequently departed for Hong Kong and afterwards Russia. Since then, Snowden has made a number of statements from Russia. Since the beginning of the Snowden affair, American authorities revoked Snowden's passport and attempted to persuade the Russian government to return Snowden to the United States. On August 12, 2013, President Barack Obama announced a review of the activities of U.S. signals intelligence (SIGINT) capabilities and communication technologies. Director of National Intelligence James R. Clapper, Jr. announced on the same day that he would be establishing the review group and its final report would be due no later than December 15, 2013. The United States Government also undertook judicial proceedings against Snowden (Richelson, 2013).

The CIA also responded to the Snowden revelations. CIA Director John Brennan stated that his operatives had determined that Al-Qaeda had been using the materials leaked by Snowden for counter-intelligence efforts. Brennan stated that Al-Qaeda members simply had to do a Google search to find classified information that had been leaked to the public (ABC News, 2014). Furthermore, former Deputy Director Michael Morell also intervened on the issue, stating that Snowden was a traitor who had endangered American lives. During his interview with CBS, Morell cited the leak of the "black budget" as an example of the harm to U.S. intelligence activities. The black budget is a document on how the U.S. spends its money on intelligence efforts. Morell goes on to affirm that the leak of this document only strengthened America's adversaries and made them more careful in their communications, preventing the CIA from gathering the intelligence that it would have obtained otherwise (CBS News, 2013b). On an internal level, the CIA launched a campaign aimed at reaffirming the preservation of secrecy within the agency. Director Brennan spearheaded his "Honor the Oath" campaign by informing to CIA personnel that the campaign was intended to reinforce the importance of the CIA's culture of secrecy through education and training. Furthermore, Brennan stated in this memo that the necessity of this campaign derived from a review launched by former Director David Petraeus following several leaks by former senior

officers. Finally, the agency also aimed to strengthen its policy on the publication of articles or books by former employees (CBS News, 2013a).

The revelations made by Snowden can be interpreted as one of the most important issues in national security of our time. It sparked an international debate and led to limitations on nationwide surveillance programs worldwide, such as through pieces of legislation as the General Data Protection Regulation (GDPR). The connection between the GDPR and Edward Snowden can be traced back to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE). The committee had an expansive mandate and a history of treating intelligence services with hostility. As highlighted by Coyne, LIBE played an important part during the Snowden scandal in Europe by requesting a formal inquiry and conducting studies on the impact of surveillance programs. The study, titled "The US Surveillance Programs and Their Impact on EU Citizens' Fundamental Rights", explored the scope of the surveillance programs carried out by the American intelligence community. On October 21, 2013, LIBE voted to adopt the draft of the GDPR. The importance of data privacy increased significantly after 2013, pushing the LIBE to adopt a careful stance between security and privacy. LIBE adopted legislative provisions such as the 'anti-FISA' clause at article 43, which prevents European companies from sharing European users' data with non-European countries. Despite facing heavy backlash from industrial leaders such as Apple and Google, LIBE maintained a strong position on protecting the data of Europeans. The GDPR was adopted in May 2016 and became applicable in May 2018. The draft adopted by the European Parliament required "Skype, WhatsApp, iMessage, video games with player messaging and other electronic services that allow private interactions to obtain people's explicit permission before placing tracking codes on users' devices or collecting data about their communications" (Coyne, 2019). As stated by Bauman et al., we now know much more on the extent of the surveillance operations that had been undergoing up to the point of the federal investigations into the matter. The Snowden affair allowed the public to better comprehend that the same intelligence agencies that were declaring in public to make the world safer were also engaging in very dangerous practices. From this scandal a greater debate on privacy, human rights and the rule of law arose. The authors continue by affirming that those who attempt to justify intrusive surveillance programs often invoke extreme narratives on the threats that we face. However, it is easy to envision similarly radical narratives about the destruction of the contemporary subjectivity and self-determination that give intelligence agencies much of their

legitimacy. The study continues by analyzing how the documents released by Snowden regarding the NSA's surveillance programs underline how we no longer live in a world of states acting within a system of states, an embryonic hierarchy of the kind envisioned by proponents of globalization, global governance, and so forth, nor a new kind of empire or concert of great powers. The unpredictability of the system that we now live in is closely tied to the practices of intelligence agencies, who have challenged the common understanding of what democracy is. Democracy has always been tied to the knowledge of the population: most democracies rest on the assumption that the people should be able to form opinions for themselves. The author states that: "The cult of secrecy takes us back to far too many historical cases in which claims were made that "the people" cannot afford to know what's good for them while their sovereign needs to know as much as they can about the people whose sovereignty they claim to express" (Bauman et al., 2014, p. 137). The analysis then goes on to note that the phenomenon of the citizen becoming a suspect is not new: the difference between citizens and non-citizens is evident at every border, where non-citizens are subjected to much more scrutiny than ordinary travelers. Bauman emphasizes how the indifference to this practice of border crossing is one of the first symptoms of complicity in the discomforts of the other. An Angus Reid poll conducted after the scandals not only shows that 51% of Americans considered Snowden a hero, but that the percentage of the population that agreed with his actions was even higher abroad, for 67% of Canadians view Snowden's whistle blowing as positive. The study identifies three key factors to help indicate why individuals still accept mass surveillance:

- Familiarity: surveillance has become so pervasive in our daily lives, that we have simply grown to accept. Forms of surveillance such as video cameras and devices that we use on a daily basis have become part of our everyday lives, with many people not realizing their surveillance capabilities
- Fear: government, security companies and other actors use the fear factor in order to influence the population to allow them to be surveilled by using the media to polarize "the good guys" versus "the bad guys", such as against Muslims. The level of fear is much greater than the actual threat of terrorism itself
- Fun: social media has played an extensive role in expanding surveillance activities. The key component to understanding social media is "user-generated content." On the internet, ordinary people participate in providing information. They connect on Facebook by using

their real identities with people who share their opinions and outlook on a vast array of topics.

In conclusion, the research conducted by Bauman et al. emphasizes how difficult it is to hold large surveillance agencies accountable is extremely difficult due to the fact that most internet users feel that everything is normal. This acceptance by the population was faced with the gradual publication of the information released by Snowden in order to keep the media focused on the issue, therefore maintaining high public attention (Bauman et al., 2014).

3.4 Paragon Scandal

Paragon Solutions is an Israeli company in the spyware sector linked to the surveillance of European journalists and several civil society members. The company is registered in Hamburg and has been active since July 24th 2024. Those affected by the data breach were notified by Meta which stated that it had high confidence that the company had targeted these individuals. The first individual to come forward as a target of this spyware is Francesco Cancellato, an Italian investigative journalist known for his articles regarding the young fascists in Giorgia Meloni's Fratelli d'Italia Party. Afterwards, Husam el Gomati, a Libyan activist who spoke out against Italy's actions in Libya, also came forward with similar accusations against the Israeli company. Luca Casarini, the founder of the Italian NGO "Mediterranea Saving Humans" was also made aware of being a possible target of the surveillance activities carried out by the Israeli company (Panagiotopoulos, 2025). Furthermore, another Italian journalist was targeted by Paragon's software: Ciro Pellegrino. Pellegrino is an investigative journalist whose iPhone showed evidence of having been targeted by a targeted mercenary spyware. Pellegrino works at the same newspaper as Cancellato, Fanpage, which is one of the most critical voices against Meloni's government (Satter, 2025). Paragon's establishment in an EU country is nothing new: a European Parliament inquiry indicated that Greece, Spain, Hungary, and Poland have also acquired similar technology to surveil journalists, activists and other members of civil society. The European Commission failed to propose legislation preventing spyware abuse after the PEGA committee called for the adoption of more stringent laws on the matter. Silvia Lorenzo Perez, Director of the Security, Surveillance and Human Rights Program at CDT Europe, a leading civil society coalition against the abuse of spyware technology, stated: "By setting up in the EU, these companies gain unrestricted access to the bloc and benefit from looser export controls, making it easier to sell their

products abroad, clearly undermining global efforts to curb the proliferation of invasive surveillance technology" (Panagiotopoulos, 2025). A report released by the Commission on the implementation of dual use technology highlighted how there has been a 94.78% increase in export licenses for cyber-surveillance equipment between 2021 and 2022 (Panagiotopoulos, 2025). In the Italian context, the undersecretary for Intelligence Alfredo Mantovano confirmed during a hearing at the COPASIR on March 26, 2025 that several members of the NGO Mediterranea were being surveilled with the consent of the government and the Rome Prosecutor General's office. This statement made clear that AISE monitored activists working on human trafficking between Italy and Libya. In February, Justice minister Carlo Nordio denied wiretaps or surveillance operations being carried out in 2024, This statement was made after Mantovano had declared that he could not comment on the matter, as some of the matters were "classified". Afterwards, sources such as Haaretz and The Guardian published articles declaring that Paragon had severed relations with the Italian government due to the misuse of the software. However, these claims were denied by the Minister for Relations with Parliament Luca Ciriani and the office of Prime Minister Giorgia Meloni. Mediterranea cited the "Adversarial Threat Report" published by Meta, where the company identified the operations of paid surveillance spyware targeting individuals around the world. According to the report: "Meta detected spyware operations from eight companies in Italy, Spain, and the United Arab Emirates, which provide their technologies to government authorities. Meta reported various technologies, including malware capable of collecting and accessing device information, location, photos and media, contacts, calendar, email, SMS, Telegram, Skype, Viber, Facebook, Instagram, LinkedIn, Signal, WhatsApp, and activating microphone, camera, and screenshot capabilities" (Biondi, 2025). AISE director Giovanni Caravelli confirmed to the COPASIR that the Italian secret service used the surveillance software by Paragon solutions, but excluded the possibility of the software being used for monitoring journalists and activists (Biondi, 2025). On February 17th 2025, the Italian Data Protection Authority (Garante per la protezione dei dati personali) issued a warning to all of those who were using the spyware "Graphite" from Paragon Solutions: "The Italian Data Protection Authority (Garante per la protezione dei dati personali) issues a warning to anyone who uses the spyware 'Graphite', from the Israeli company Paragon Solutions Ltd, or similar systems, or uses the information collected through this software. Such activities, carried out outside of the uses permitted by law, violate the Privacy Code and may result in the application of an administrative fine of up to 20 million euros or 4% of the turnover"

(Garante Per la Protezione dei Dati, 2025). The Italian Guarantor analyzed how tools like graphite differentiate themselves from spyware software of the past as these programs don't require bold covert operations; the victim's device is penetrated without their knowledge with just one click. To counter this trend, the Guarantor emphasizes the need not only for updates to existing laws, but also for a broader cultural shift. The Paragon case highlights how citizen awareness is crucial and governments should take better care in ensuring that surveillance technologies are used within the scope of the law. The Italian Guarantor further stressed how national security must have appropriate tools to face internal and external threats, but these tools must not impact the freedom of expression and right to privacy of citizens (Garante Per la Protezione dei Dati, 2025).

The COPASIR published the report of its inquiry into the Paragon case on June 5th, 2025. This report has confirmed that the Italian government had used the spyware named Graphite to surveil Luca Casarini and Giuseppe Caccia. The report continued that the investigative bodies were unable to determine who might have targeted Mr. Cancellato. The Italian Department of Security Intelligence (DIS: Dipartimento delle Informazioni per la Sicurezza) also declared that it had rejected an offer from Paragon Solutions to assist Italian Authorities in ongoing investigations, citing national security concerns (Marczak and Scott-Railton, 2025). Afterwards, Paragon released a statement claiming that the Italian government's termination of the contract led the company to shut down all systems for Italian clients. (Peretti, 2025). The DIS went on by stating that the unilateral termination of the contract described by Paragon was not correct, declaring that both parties had agreed to end the collaboration. The COPASIR also specified that the security services had chosen to investigate the Paragon databases rather than accept the company's assistance (Marczak and Scott-Railton, 2025).

Citizenlab conducted an analysis of the Apple devices belonging to a prominent European journalist who requested to remain anonymous. As stated by Marczak and Scott-Railton (2025): "Our forensic analysis concluded that one of the journalist's devices was compromised with Paragon's Graphite spyware in January and early February 2025 while running iOS 18.2.1. We attribute the compromise to Graphite with high confidence because logs on the device indicated that it made a series of requests to a server that, during the same time period, matched our published Fingerprint P1. We linked this fingerprint to Paragon's Graphite spyware with high confidence". Furthermore, Citizenlab also analyzed the devices of Pellegrino and determined that

they were also highly likely to have been targeted by the same software (Marczak and Scott-Railton, 2025).

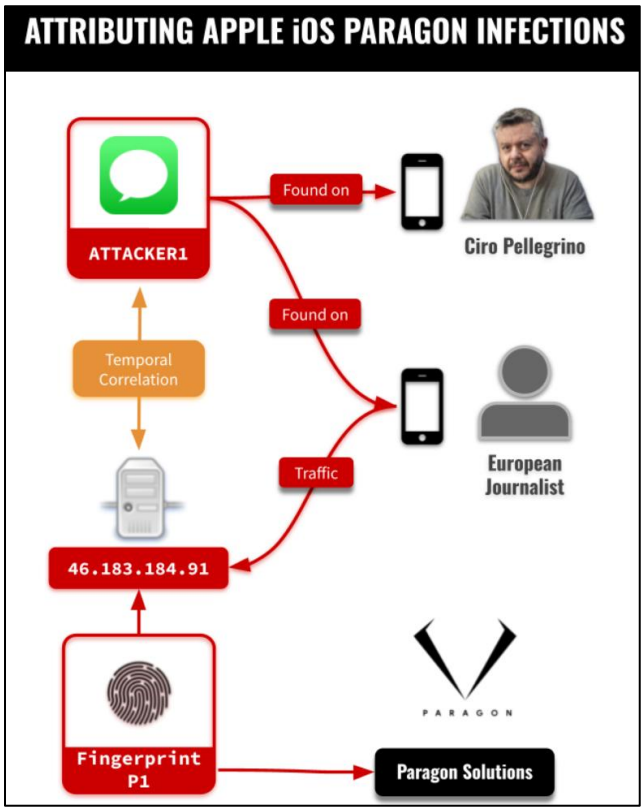

Figure 2: Analysis of a Paragon Spyware Attack, Marczak and Scott-Railton (2025)

The spyware has also been utilized by the security apparatus of the United States. Reports and official sources have confirmed that Paragon Solutions has been awarded a federal contract of $2,000,000 up until September 29, 2025 for the Department of Homeland Security (USAspending.gov, 2025). Paragon Solutions was also employed through other agencies, such as Immigration and Customs Enforcement (ICE) and the US Drug Enforcement Administration. According to Panagiotopoulos (2024): “Paragon’s contract comes amid a comprehensive effort by the US government to reshape the commercial spyware market over the past three years. Measures have included placing spyware vendors like NSO Group and Intellexa on the so-called Entity List to prevent any US companies from doing business with them; enacting a visa restriction policy against multiple individuals “who have been involved in the development and sale of commercial

spyware or who are immediate family members of those involved," and imposing consecutive rounds of sanctions against spyware vendors."

Government espionage and surveillance against political adversaries and activists should not be considered as anything new, but in the digital age it has reached unprecedented proportions. While political police in the past had to undergo careful operations to intercept the correspondence of those targeted, nowadays software can be used to read the private emails of millions of people (Visca, 2025).

The Paragon affair is still ongoing at the time of writing. Nonetheless, this episode is fundamental for readers to better understand how intelligence agencies communicate with the public on crises of this nature.

3.5 Conclusion

In conclusion, the selected case studies emphasize the importance of crisis communication during crises for intelligence agencies. After having presented the process that led to the formation of both the CIA and AISE, the research presented the consequences of the Snowden revelations on the European context and in the security apparatus of the United States. Furthermore, the implications of the ongoing Paragon case are emblematic in understanding the balance between democratic accountability and national security necessities. This chapter has delved into the timeline of events and how various actors influenced the communication strategies of the intelligence agencies concerned. The following chapter will present a rigorous coding scheme to examine further the importance of these case studies in the crisis communication sector and further discuss the implications of the strategies employed by the intelligence agencies under analysis. Afterwards, the research will underline the importance of public trust in the security apparatuses of liberal democracies and provide policy proposals for improving the communication of high-stakes events.

CHAPTER 4: DISCUSSION

This chapter will analyze the impact of the case studies on the realm of crisis communication. After establishing an appropriate coding scheme, the study will conduct a more in-depth analysis of the implications of the Snowden and Paragon affairs by discussing the role of public trust in security apparatuses. Drawing from the theoretical framework of this study, the research will then highlight the strengths and weaknesses of the communication policies of the CIA and AISE in order to suggest policies that will be grounded in the empirical evidence and theory which will lead to a more accountable and effective communication in the future.

4.1 Implications for Crisis Communication Theory

The following coding scheme draws on the main crisis communication theories explained throughout the course of this research, while also taking into account the culture of secrecy of the intelligence agencies under examination. SCCT posits that crisis managers should strive to elaborate a crisis communication strategy that takes into account the reputational threat that a crisis may create to the organization in question. Coombs divides crises into victim, accidental and intentional groupings. Furthermore, SCCT also provides recommendations to crisis managers. Some of the most relevant strategies relevant to the study at hand are:

- Using rebuilding strategies for organizations that have a crisis history or unfavorable prior reputation
- Using diminishment strategies for victim crises for organizations that have a crisis history or unfavorable prior reputation
- Using rebuilding strategies for any preventable crises (Zaremba, 2015, pp.53-54)

IRT also provides a framework with which the crisis managers can provide answers to crises that organizations may face through the categories of Denial, evasion of responsibility, Reducing Offensiveness, Corrective Action and Mortification. An important point raised by Benoit throughout his research on IRT is that apologies through Mortification can be risky, as apologizing publicly can further damage the reputation of the organization: this is due to the fact that the audience plays a key role in granting forgiveness. Having analyzed this point, Benoit goes on to explain how actors seeking forgiveness resort to vague language in their apology towards the public (Benoit, 2015). In the previous chapter the research underlined how both CIA and AISE

officials implemented elements of IRT, such as Michael Morell who criticized Snowden for endangering U.S. Intelligence efforts which can be traced back to the “Attacking the Accuser” subcategory of Reducing Offensiveness. These attempts are aimed at creating new beliefs about the accuser in order to undermine the attack. By applying the theoretical frameworks of this research, coding elements have been identified for themes in crisis communication strategies of intelligence agencies.

Code	Definition	Subthemes	Cases applied	Crisis Type	Communication Strategy	Outcome	Sources
Denial	Denying responsibility for the wrongful act	No involvement, Blame Shifting	Snowden	Victim	Denial strategy	Long term erosion of trust of intelligence agencies	(Benoit, 2015; Fonte and Alvise Armellini, 2025a)
Corrective Action	Actions undertaken to fix the problem at hand	Internal reform, Internal investigations	Snowden, Paragon	Accidental	Announcement of internal reviews and investigations	Mitigation of reputational damage, but did not fully rebuild public trust	(Bauman et al., 2014; Benoit, 2015; Richelson 2013)
Bolstering	Highlighting previous intelligence successes	Loyalty to democratic values, Intelligence succeses, Institutional legacy	Snowden	Accidental	Public appearances held by General Keith Alexander	Public opinion remained deeply divided, with 51% of Americans perceiving Snowden as a hero	(Bauman et al. 2014; Benoit 2015; caroll, 2013)
Attacking the Accuser	Attempt to create new beliefs of the accuser to undermine the attack	Threat framing, Delegitimization of accuser	Snowden	Preventable	Interviews by current and former CIA officials, criminal prosecution of Snowden	Public attacks of Snowden proved to be ineffective	(ABC News, 2014; Bauman et al., 2014; Benoit, 2015; CBS News, 2013b; Eriksson, 2020)
Institutional Shielding	Shifting responsibility to other institutional bodies	Shifting blame	Snowden, Paragon	Preventable	Deflection of responsibility to other institutional bodies	Publick skepticism and concern from civil society arose	(Bauman et al., 2014; Benoit, 2015; Biondi, 2025; Caroll, 2013; Marczak and Scott-Railton, 2025)
National Security Justification	Framing of problematic actions as necessary for safeguarding national security	Institutional duty to protect, Framing surveillance programs as preventive	Snowden, Paragon	Preventable	Testimony delivered in institutional settings	Public skepticism endured	(Bauman et al., 2014; Benoit, 2015; Biondi, 2025; Caroll, 2013; Marczak and Scott-Railton, 2025)
Amplification by Media	Role played by media in applying public pressure on intelligence agencies during crises	Strategic timing of disclosures	Snowden, Paragon	Preventable	Attempt to justify programs and discredit attackers in public forums and interviews with important media outlets	Intensified reputational damage and fueled public scrutiny	(Bauman et al. 2014; Benoit, 2015; Biondi, 2025; Caroll, 2013; CBS News, 2013b)
Security-Democracy Balance	Framing surveillance activities as necessary while emphasizing the respect of democratic norms	Legality as justification, Transcendence	Snowden, Paragon	Preventable	CIA and AISE officials publicly declared that surveillance programs were undertaken with appropriate oversight and were necessary to national security	Concerns from civil society remain deep to this day	(Bauman, 2014; Benoit, 2015; Biondi, 2025; CBS News, 2013b; Garante Per la Protezione dei Dati, 2025; Marczak and Scott-Railton, 2025)
Mortification	Asking for forgiveness for a problematic act	Expression of regret, Delayed accountability	Snowden	Preventable	Public hearings of intelligence officials	Diminishment of public confidence in the U.S. intelligence community	(Ackerman, 2013 Aftergood, 2014; Bauman, 2014; Benoit, 2015)
Surveillance Normalization	Framing surveillance programs as necessary for internet activities, causing mass desensitization	Voluntary data sharing, Social Media, Fear factor	Snowden	Chronic	Public hearings and interviews of intelligence officials, framing surveillance as a necessary practice for national security	Facilitation of intelligence activities but possible democratic erosion	(ABC News, 2014; Bauman, 2014; Benoit, 2015; Caroll, 2013)

Figure 3: Coding Scheme Chart

By assigning to each code a subtheme and linking each one to the most appropriate case, readers will be able to fully assess the importance that the Snowden and Paragon cases represent in analyzing high-stakes events where both the CIA and AISE fell under public scrutiny. The results will show patterns in the communication styles of the selected intelligence agencies and allow readers to gain a better understanding of the communication principles applied by the CIA and AISE.

4.2 Strategic Responses to Reputational Threats

As seen above, both the CIA and AISE had developed similar communication strategies during the Snowden and Paragon cases. While the CIA attempted to convince the public that surveillance operations were not only necessary but beneficial to public security, AISE adopted a more "institutional" approach by limiting public comments and conferring with legislators on the intelligence activities being carried out. The following subsections will examine in greater detail the main communication channels and strategies employed by the Italian and American intelligence communities.

4.2.1 Denial Strategy

One of the most notorious communication strategies employed by American intelligence officials is the Denial strategy. The most noteworthy example of this is the exchange that happened between DNI director James Clapper and Senator Ron Wyden during a congressional hearing in March 2013. As DNI, Clapper's statements reflected the position of the American intelligence community as it is the responsibility of the DNI to lead the intelligence community. When asked by Senator Wyden if the NSA was in the process of collecting data on millions or hundreds of millions of Americans, Clapper responded by denying these claims. The revelations made by Snowden proved these statements to be false (Miltimore, 2022). Afterwards, Clapper did not admit wrongdoing and stated that he had not thought about section 215 of the Patriot Act, a legal requirement that intelligence officials have to follow in order to justify the surveillance of the American public. Furthermore, the ODNI acknowledged soon after the hearing that the statement made by Director Clapper was misleading, but refused to correct the public record. Clapper's letter to Senator Feinstein fails to recognize that he previously informed Andrea Mitchell of NBC News that he had given Wyden the "least most untruthful" response he could publicly make. Moreover, Clapper

expressed doubts about open intelligence hearings by stating that "An open hearing on intelligence matters is something of a contradiction in terms" (Ackerman, 2013).

During the Snowden case, the Denial strategy employed by the CIA was mainly focused on blame shifting. CIA Director Brennan commented on the Snowden revelations in an interview with the Guardian in the wake of the Paris attacks. In 2015, Brennan stated that due to the fact that policy changes had been made in the aftermath of the Snowden case, finding terrorists across the globe proved to be much more challenging after legislation such as the USA FREEDOM Act had been passed. Brennan did not comment on any possible privacy breaches from the CIA itself. Other members of the American intelligence community voiced similar concerns to those raised by Director Brennan, but civil liberties activists urged caution. Naureen Shah, director of Amnesty International USA's security and human rights program, acknowledged the need to reinforce security policies but emphasized how the Paris attacks should not have been used by intelligence agencies to reinforce surveillance policies. (Smith and Roberts, 2015). Former CIA officials also engaged in blame shifting. Former NSA and CIA Director Michael Hayden stated in an interview with *The Guardian* that the European stance was hypocritical as European intelligence agencies also engaged in similar surveillance operations as the American intelligence community. Furthermore, Hayden continued his interview by asserting that European governments were informed of the data collection program of the NSA and that European intelligence agencies were surveilling the European population more than most politicians realized (McGreal, 2016). These comments emphasize how the CIA employed a Denial strategy, a strategy that can be traced back to the theoretical framework outlined by Benoit. The statements made through interviews and public appearances by intelligence officials such as the ones made by former Director Hayden can be linked to blame shifting, as the CIA attempted to deflect responsibility for the surveillance activities exposed by Snowden by emphasizing how other allied agencies had carried out comparable operations. Benoit places these kinds of statements in the "blame shifting" subcategory, where an organization attributes the offensive action to other actors involved in the crisis (Benoit, 2015).

Regarding the Paragon case, Italian officials also employed Denial in the ongoing Paragon case. The administration of President of the Council of Ministers Giorgia Meloni denied the use of Paragon's spyware. Officials stated that illegal surveillance against critics of the Meloni

government had not been carried out (Fonte and Alvise Armellini, 2025a). Italian intelligence officials also intervened on the issue. In February 2025, Secretary of the Council of Ministers Alfredo Mantovano denied that Paragon rescinded its contracts with the Italian government in front of journalists at the Chamber of Deputies. He went on by affirming that the Italian intelligence services respected the necessary legal requirements for surveillance activities, in contrast with what had been declared by the articles of The Guardian and Haaretz. Furthermore, Giovanni Caravelli declared to the COPASIR that surveillance activities had been carried out with the Paragon software, but not against journalists and activists. Mantovano then deferred to the Italian judges for investigating any improper use of the spyware (Holgado, 2025). Similarly, Bruno Valensise (Director of AISI) admitted the use of Graphite, but denied its implementation in surveillance activities of journalists and activists. Former President of the Council of Ministers Matteo Renzi attacked the administration by affirming that the Italian intelligence had spied on Pope Francis and that the Graphite spyware was used also by other Italian institutional bodies, such as the penitentiary police. Green Party leader also attacked Mantovano for not allowing the parliament to debate on this topic by discussing it only with the COPASIR. Italian officials from the State Police, Carabinieri, Guardia di Finanza all denied having used the spyware from Paragon Solutions. Justice Minister Carlo Nordio also denied the accusations from Renzi of the use of Graphite from the penitentiary police (Attianese, 2025; L'Espresso, 2025; Vergine, 2025). Throughout the course of the Paragon scandal, the pattern of communication exhibited by Italian intelligence can be placed under Benoit's Denial strategy. The Meloni government and intelligence chiefs employed simple Denial strategies in their communications with the public. Furthermore, in his statements to the press, Mantovano also used a shifting blame strategy by affirming that if there had been an improper use of the spyware, the judiciary would investigate any wrongdoing regarding possible crimes being committed. This declaration allowed the government to distance itself from the scandal and place the responsibility of the actions under judicial competence. In conclusion, Italian authorities employed the Denial strategy and its subcategories in its press hearings and committee hearings, seeking to emphasize the legality of the surveillance activities that had been undertaken (Benoit, 2015; Holgado, 2025).

4.2.2 Corrective Action

The CIA and AISE have both resorted to Corrective Action during the Paragon and the Snowden crises. In IRT, Corrective Action is defined as the communication strategy in which the accused

vows to remedy the offensive action (Benoit, 2015). In June 2014 the CIA launched its first social media accounts. Director Brennan explained that this policy change was intended to increase the public outreach of the Agency by sharing unclassified information with the public while also preserving national security. Social media posts from the Agency included posts such as "the latest news, statements, and career information from CIA, the Agency's social media updates will also feature artifacts and other information from the CIA's Museum - the best museum most people never get to see" (Ferran, 2014). To begin its social media presence, the CIA adopted a sarcastic tone in its posts in an attempt to build a more approachable organization.

Figure 4: First Tweet by the CIA, Ferran (2014)

The Agency's arrival on social media was met with skepticism from civil society members, as Zeke Johnson, Director of Amnesty International USA's Security and Human Rights Program, said in a statement to the media. Johnson condemned the attention given to social media rather than the respect for human rights. The reinforced social media presence from the CIA came in the wake of a public relations campaign to repair the reputational damage caused by the Snowden revelations (Ferran, 2014). In the aftermath of the Snowden scandal, the CIA also applied policy changes to strengthen privacy standards in its surveillance operations. In January 2014, President Obama issued a new directive on U.S. Signals Intelligence. The guidelines cover general policy,

collection, the use of SIGINT collected in bulk (distinguishing between acceptable and unacceptable uses), retention and access, dissemination, compliance, and responsibilities. The new guidelines set by the Obama administration restricted the ability of the American intelligence community to carry out data collection programs on a massive scale by inserting privacy and civil liberties as fundamental considerations into intelligence activities and restricting data collection programs to solely support national security concerns. The document also outlines the role of the Director of the CIA in approving any exception to the new regulation. The document also emphasizes the importance of compliance by CIA personnel, while also highlighting the importance of reporting any issues to the appropriate oversight bodies. This directive set out by the Obama administration marked a concrete policy change regarding the policy directive (CIA, 2014; Richelson, 2015). The disclosures made by Edward Snowden also prompted an overseas trip to Europe to reassure the main allies of the U.S. that appropriate steps were being taken in limiting the intelligence community's surveillance of them. During a summit in the Hague, Obama emphasized how American intelligence agencies should work to rebuild the trust of both the public and governments. The Obama White House and intelligence officials attempted to embark on concrete steps into creating a more transparent intelligence community. In January 2014 President Obama banned the surveillance of foreign allied leaders and began to limit the massive archive the intelligence community had on the phone records of millions of Americans. While criticizing the press by stating that some coverage of the Snowden revelations had been exaggerated, Obama admitted that concerns over privacy in the 21st century were legitimate. Furthermore, General Keith Alexander went on an interview with Fox News and stated that the intelligence apparatus of the United States would start to limit the scope of their surveillance activities and limit themselves to phone numbers linked to terrorist activities. Moreover, Alexander denied that the NSA is capable of listening to all phone calls and reading all emails (Croft, 2014).

The U.S. intelligence community also underwent legislative reform that limited its capabilities of surveillance of the American public. One of the most significant reforms is the USA FREEDOM Act, passed in June 2015. This reform ended the bulk collection of domestic telephone metadata under section 215 of the Patriot Act and replaced it with a more targeted system. The USA FREEDOM Act introduced the necessity of a Foreign Intelligence Surveillance Court (FISA) authorization to collect records tied to a specific selector, such as a phone number. Furthermore, companies are now allowed to publish limited statistics of national security requests. Another

crucial provision introduced by the Act was to increase the transparency measures of entities subject to non-disclosure requirements. The USA FREEDOM Act allowed these entities to publish statistics on the number of national security letters, directives or orders from U.S. intelligence agencies (Congress.gov, 2015). Even though the USA FREEDOM Act limited the NSA surveillance activities, the law failed to address some key concerns. As highlighted by Goitein, recently the CIA came again under fire for similar activities during the Snowden revelations. Goitein highlights how Senators Wyden and Heinrich announced that the CIA had been running a bulk collection program regarding the data about Americans. This is due to the fact that the legislation passed in 2015 applies only to certain types of surveillance that regard American citizens. When these programs regard data collection abroad, they take place under Executive Order 12333, issued by Ronald Reagan in 1981. This executive order allows for much less stringent limits on the surveillance activities of the CIA. The CIA released an official statement stating that the intelligence committees of congress had been kept up to speed on the data collection programs, but Senators Wyden and Heinrich denied these claims. In conclusion, Goitein underlines the importance of public trust for intelligence agencies to operate effectively, and how this trust took an enormous hit after the Snowden revelations. Even as the CIA undertook corrective measures to increase transparency, this recent episode is extremely important in understanding how the Agency did not implement sufficient change to its policies, as it released generally vague and incorrect statements to both the press and the legislative branch (Goitein, 2022).

Regarding the Paragon case, AISE undertook corrective measures with a reactive approach to the issue. In February 2025 the Italian intelligence community severed its relationship to the Israeli spyware company Paragon Solutions. Nonetheless, both these actors gave conflicting accounts as to who ended the commercial relationship. Following these statements, a report from the COPASIR stated that AISE had initially suspended the use of the software then ended the use of the software. The report analyzed how, with the government's approval, members of the Mediterranea charity were surveilled regarding activities tied to illegal immigration. According to the report, on September 5, 2024, Meloni's highest-ranking intelligence official, undersecretary Alfredo Mantovano, approved the use of Paragon spyware on Mediterranea activists Beppe Caccia and Luca Casarini. The report failed to address when the contract had ended, fueling further confusion when government officials addressed parliament mid-February stating the program was still in use. Reuters reports that Mantovano, Paragon Solutions and the Office of Giorgia Meloni

were all unavailable for comment. The National Cybersecurity Agency was tasked in reviewing the matter (Fonte and Alvise Armellini, 2025b). The Corrective Actions undertaken by Italian authorities came under scrutiny for being insufficient. As mentioned above, the Italian Guarantor for Data Protection raised objections. While the COPASIR report confirmed that Italian intelligence agencies had been using the Graphite spyware, it attempted to justify the surveillance activities being undertaken in the interest of national security. Civil society organizations such as Amnesty International expressed worry when Italian authorities failed to respond adequately to credible allegations of surveillance abuse, fearing that such inaction could send a message of impunity. Furthermore, the report denied that reporter Francesco Cancellato had been targeted by the software, but new evidence suggested the contrary. This finding fueled speculation on unaddressed surveillance cases (Amnesty International, 2025b). Other organizations such as AccessNow highlighted how the Italian intelligence apparatus and institutions adopted a largely reactive approach to the issue, emphasizing how contract suspension after having being publicly exposed was not an adequate substitute for transparency and accountability. The absence of a victim notification system, remedy framework or public reporting of abuses of clients indicates a failure to manage the risks associated with surveillance technology on Paragons' part (Greene, Rowe and Sprechman, 2025). In the aftermath of the scandal, Italian authorities claimed they replaced Paragon with Italian offensive cyber firm NEGG, according to the French outlet Intelligence Online. Paragon has repeatedly stated that its software was to be used on terrorists and criminals, but the company has attracted criticism for being too reliant on client assurances (Shahaf, 2025). Similarly to the Snowden case, the replacement of the software provided by Paragon suggests that surveillance activities have continued but with a different tool. In sum, while AISE did take some steps in distancing itself from the scandal, these actions were seen as insufficient from human rights organizations that have highlighted how the Italian authorities failed to address the scandal in a more in-depth manner. The actions undertaken by both the CIA and AISE can be classified under the Corrective Action without formal apology, similarly to the one undertaken by Tylenol when it introduced tamper-resistant bottles after their customers were poisoned. Nonetheless, the concerns raised by the public demonstrate that these strategies did not fully achieve the intended objectives (Benoit, 2015).

4.2.3 Mortification

In the aftermath of the Snowden revelations, DNI James Clapper wrote to the Senate intelligence

committee and expressed how he apologized for giving an erroneous answer regarding the data collection program of the NSA. The letter from Clapper came only after the publications of articles from the press. In his letter sent to Senator Feinstein, Clapper acknowledged that the statement about data collection was given due to the fact that he was thinking about section 702 of FISA, which includes inadvertent data collection even though it is targeted at foreigners. His letter also addresses that he felt he made a mistake as he did not think about section 215 of the Patriot Act (Clapper, 2013). DNI Clapper apologized only after the Snowden revelations had been published by The Guardian. Regarding the issue of transparency, Clapper acknowledged that Snowden had highlighted an issue of transparency in the intelligence community. During an interview with Loch K. Johnson, Director Clapper stated: "… I guess the major take-away from this whole Snowden experience, for me, has been the need for more transparency. Had we been open about this and said, 'This is a gap we need to fill. Here's the program and here is how it is going to run, and here's why, and, importantly, here are the safeguards that are going to be built into it', it would have been easy, I think, to acquire legislative support to close this gap. The oversight of this program has been unparalleled. All three branches are involved. I am convinced that, had it been explained, people would not have been any more disturbed about that program than they are about the fact that the FBI maintains fingerprint files on millions of US persons. These FBI files are a known program, and have been for years People understand the need" (Johnson, 2014, p. 16). The apology for the metadata collection exposed by Snowden did little to restore faith in the American intelligence community. Senator Wyden stated that he was troubled due to the fact that the ODNI staff had informed his staff that Clapper's answer was wrong, but the DNI came out only in June after the Snowden revelations, largely due to public pressure. After the disclosures made by Snowden, Clapper gave an interview to MSNBC where he explained that the answer he gave was a ploy to avoid revealing classified information. Throughout the interview, Clapper also criticized Wyden, as he felt that the question he had been asked was not fair. In June 2013, Senator Rand Paul attacked Clapper by stating that he had lied to congress and questioned if he could continue his position. In June, Clapper sent the abovementioned letter to Senator Feinstein where he walked back his statement to MSNBC, declaring that he misunderstood the question. In his article, Roberts and Ackerman analyze how in the letter Clapper did not address why it took until March to correct the record. These misleading statements led to Wyden leading a group of 26 Senators from both sides of the aisle who sent a letter to Clapper complaining about the collection of massive amounts

of data on US citizens (Roberts and Ackerman, 2013). Even though legislators took concrete steps into investigating the claims of the intelligence community, Aftergood criticizes Congress for permitting the deception made by Clapper to occur, as the Senate Intelligence Committee was already aware to the real answer to Senator Wyden's question as noted by ODNI General Counsel Robert S. Litt. Aftergood goes on by stating that the real target of the deception was not Congress, but rather the American public. Aftergood concludes his analysis by stating that by deciding that national security classification trumped all other obligations regarding an accurate public record, the Senate Intelligence Committee aided DNI Clapper's deception (Aftergood, 2014b).

In the aftermath of the Snowden disclosures, Human Rights Watch delves deeper into how government officials have become less willing to talk to the press, even regarding unclassified materials. The fear of surveillance by officials constituted a difficulty for journalists who covered national security topics, as they usually implement government opinions, documents and materials in their projects. Regarding journalists, journalists adopted elaborate steps to protect sources and information. These actions can be defined as using burner phones, abandoning online communication and meeting sources in person. Human Rights Watch goes on by stating that the situation created a difficult situation for national security reporting, especially regarding intelligence activities. Lawyers faced similar challenges to journalists as the lawyers interviewed for the report published by Human Rights Watch expressed concern about situations when the government might take an intelligence interest in a case. This led to lawyers taking similar steps to journalists by using secure communication technology. Other lawyers interviewed for the report expressed reluctance in accepting cases tied to national security. The situation created by the Snowden revelations highlighted how the apologies made by the American intelligence community through Clapper were not sufficient in re-establishing confidence in the American intelligence apparatus (Human Rights Watch, 2014).

The actions undertaken by DNI Clapper can be categorized under Mortification, as Clapper apologized to Senator Feinstein for giving misleading statements regarding the data collection program that Snowden exposed. Even though Benoit affirms that Corrective Action and Mortification are strategies that work well together, the situation described by the report of Human Rights Watch highlights how Clapper did not produce a convincing apology, as it was perceived more as "damage control" rather than a sincere apology (Benoit, 2015).

4.3 Other Strategic Approaches

A recurring theme in the communication strategies employed by the CIA and AISE is "Attacking the Accuser". Benoit defines Attacking the Accuser as "reducing credibility of the accuser (and, if the accuser is the victim, about how victim deserved what happened)" (Benoit, 2015, p.30). Former CIA Deputy Director Michael Morell stated in an interview with CBS News that Snowden's leak of classified intelligence materials caused more damage to U.S. security than any other leak in history. Morell went on by defining Snowden not as a whistleblower, but as a traitor of the worst kind. As mentioned above, one of the most sensitive documents leaked by Edward Snowden was the so-called "black budget", a playbook revealing where the intelligence community spends its money. In his interview, Morell explains how this document could be used by hostile nations to better understand where the United States spends its money for intelligence activities, hampering the efforts of the United States. Finally, Morell also criticized the partisan politics displayed by the Democratic and Republican parties. He goes on by stating that the political warfare that the two parties had begun engaging in to gain political favor was detrimental to national security (CBS News, 2013b). CIA Director Brennan also reinforced these claims by stating that Al-Qaeda was "going to school" with the documents leaked by Snowden. Brennan went on by stating that the leaks helped Al-Qaeda's counterintelligence efforts as all Al-Qaeda operatives had to do is run a google search or read the newspaper as to see new information that had been leaked (ABC News, 2014). Regardless of these attacks, the American public remained skeptical of the narration of the intelligence community. A Reuters/Ipsos poll carried out in June 2013 showed how 31% of Americans perceived Snowden to be a hero as opposed to 23% believing that he was a traitor. 46% of respondents answered that they did not know. Furthermore, the poll highlighted how 35% of Americans believed that Snowden should face no charge (Sullivan, 2013). Moreover, a similar poll conducted by the Pew Research Center demonstrated how a majority disapprove of the NSA surveillance program, with 53% of Americans disapproving as opposed to 40% approving. The same poll showed how 45% of Americans believed that the Snowden revelations served the public interest while 43% of respondents answered that it harmed it. While presenting different results regarding the willingness of the American public regarding the willingness for the government to pursue a criminal case against Snowden, the Pew Research Center poll highlights how young people offer the least support for Snowden's prosecution, with 42% of those aged less than 30 stating that they would be against Snowden's prosecution (Tyson, 2014). Moreover, a report

published by the Chicago Council on Global Affairs analyzed the long-term effects of the Snowden revelations on public perception of the American intelligence community. The report highlights how while a majority of Americans believe that the intelligence community as effective in their mission, only about half of respondents (51%) answered that they believe that American intelligence agencies safeguard their privacy and civil liberties. Furthermore, the number of Americans that believe U.S. intelligence services should treat foreigners with the same respect as Americans increased by 15% between 2017 (38%) and 2018 (53%). Finally, the report underscores how the number of U.S. citizens who agree that American intelligence could share more information with the public while maintaining its effectiveness increased from 54% to 65% between 2017 and 2018 (Slick, Busby and Burns, 2019). In conclusion, the attacks carried out by the CIA had little effect on the public due to fact that the agency's campaign was undermined by its reputation for little transparency and violation of privacy by the public.

Regarding the Paragon case, AISE officials and members of the Meloni government quickly on the offensive against journalists covering the Paragon case. Mantovano attacked the press covering the issue by stating, in contradiction with news coverage, that Paragon Solutions had not suspended its government contracts and that press accounts of the use of the spyware were "gratuitous defamation" regarding the accusation of the press that AISE Director Caravelli had employed the spyware to spy on Libyan dissidents. Mantovano went on by stating that it was up to the judiciary branch to verify if there had been any wrongdoing by the Italian intelligence community (Holgado, 2025). Government officials also intervened on the issue: Minister for Parliamentary Relations Luca Ciriani stated in an interview to Huffington Post that the Meloni government would pursue legal action against all those who accused intelligence services of using the Graphite spyware in an improper manner (Ucciero, 2025). The COPASIR report reflected the defensive posture displayed by the Meloni government by downplaying journalistic allegations and highlighting how activists Casarini and Caccia were surveilled following legal obligations and in relation to possible ties to illegal immigration. The report goes on by stating that investigations on the surveillance of Cancellato were still ongoing and that other targets defined by the press such as Don Mattia Ferrari had not been subject to the surveillance with the Graphite spyware (COPASIR, 2025).

The attacks of the Italian intelligence and the Meloni government have proven to be largely ineffective. The unclear messaging on the issue prompted criticism from the opposition. Lawmakers demanded clarity over the episode and voiced concerns over being surveilled, as members of the Green/Left Alliance met with Casarini (Pagella Politica, 2025). Italy's journalistic and human rights community was also alarmed. The president of the Italian journalist's union FNSI Vittorio di Trapani stated to the Associated Press: "It is unacceptable in a democratic country that journalists are spied on without knowing the reason. We do not know how many there are and if there are others. The EU should intervene. The democracy of a founding country of the union and therefore of the whole of Europe is at stake". An EU commission spokesperson also commented on the issue, by declaring that the illegal access of the private data of citizens is unacceptable and that the commission "will use all the tools at its disposal to ensure the effective application of EU law." (Kinetz and Santalucia, 2025). In March 2025, Amnesty International also intervened on the issue. Responding to the Citizen Lab report, Amnesty expressed concern in the surveillance of human rights activists and journalists across Italy, indicating it as a symptom of the worsening digital surveillance across Europe. The Amnesty report also criticizes the European Union, as the European Commission has neglected to implement the recommendations of the European Parliament Committee of Inquiry concerning Pegasus and analogous surveillance spyware (PEGA), thereby endangering activists, journalists, and other susceptible individuals to these perilous surveillance instruments. In the report, Amnesty also states that the security lab of the organization has unearthed more victims of the surveillance of the Italian intelligence (Amnesty International, 2025a).

Regarding public opinion, data from May 2025 suggests that public perception remains high, recording 67.2% of approval of the Italian intelligence agencies (PiazzaBorsa, 2025). However, as the Paragon scandal is still ongoing, media coverage and concern from human rights organizations highlight how important parts of civil society remain concerned with the surveillance activities carried out by AISE. A lawyer from Access now questioned the adequacy of the parliamentary investigation into Paragon when the spyware was discovered on one of Cancellato's colleagues. Furthermore, Sandro Ruotolo, the spokesman for the Democratic Party, stated that parliament should reopen its inquiry into the matter (Satter, 2025).

In conclusion, the attacks carried out by intelligence officials and members of the Meloni government responsible for the security services were ineffective, as they intensified scrutiny from civil society and created parliamentary protests against the government's actions the statements made by Mantovano and Ciriani regarding legal action and "gratuitous defamation" only fueled criticism from journalists, human rights organizations, and political opposition rather than deflecting it. As mentioned above, the COPASIR report was largely perceived as insufficient to reassure civil society. While the Eurispes poll highlights how public perception of the intelligence community remains high, the persistence of international, political and civil scrutiny highlights how these attacks were ineffective in containing reputational damage. Historical examples and academic literature further confirm the findings of the research. As highlighted in the research carried out by Benoit, during the fraud case of Sears in 1992, Sears used Denial and Attacking the Accuser strategies, but when the California Department of Consumer Affairs were corroborated by New Jersey, Sears began to implement Corrective Action. This case highlights how Attacking the Accuser is largely ineffective when selected as the main strategy adopted by organizations, and underlines how timely and effective Corrective Action is better for achieving the desired results (Benoit, 2018).

The following code that shall be analyzed is 'bolstering'. In the IRT framework, Benoit defines bolstering as a subcategory of Reducing Offensiveness. Benoit continues his assessment of bolstering by delving deeper into what it represents: "bolstering may be used to mitigate the negative effects of the act on the actor by strengthening the audience's positive affect for the actor. Here those accused of wrongdoing might relate positive attributes they possess or positive actions they have performed in the past; the persuader attempts to add new beliefs (or remind the audience of forgotten beliefs) that are associated with positive values. Although the amount of guilt or negative affect from the accusation remains the same, increasing positive feeling toward the actor may help offset the negative feelings toward the act, yielding a relative improvement in the actor's reputation" (Benoit, 2015, p. 24). In the wake of the Snowden revelations, the intelligence community undertook a transparency initiative that attempted to make the public understand the activities of the intelligence services and gain public trust by engaging with it and conducting intelligence work more openly than in the past. The main findings of the initial report from the Chicago Council on Global Affairs found that 79% of American responded that the U.S. intelligence services play a significant role in warning against foreign threats. Furthermore, the

report outlines how 59% of respondents regarded how the intelligence community is effective in assisting the president in preparing sound foreign policy, but only 43% believe that security apparatus of the United States was adequate in ensuring the protection of privacy and civil liberties of Americans. Another important point raised by the report is that 87% of Americans agreed with the assumption that the intelligence community should employ all reasonable and lawful means to safeguard national security, but 48% of respondents answered that they believe that the intelligence community should extend the same privacy protection to foreigners as with American citizens. Furthermore, the Global Affairs report also analyzes the partisan views of Americans: 67% of Democrats believed that the intelligence community could share more information with the public without compromising its effectiveness, as opposed to 50% of Republicans (Busby, Slick and Nguyen, 2023).

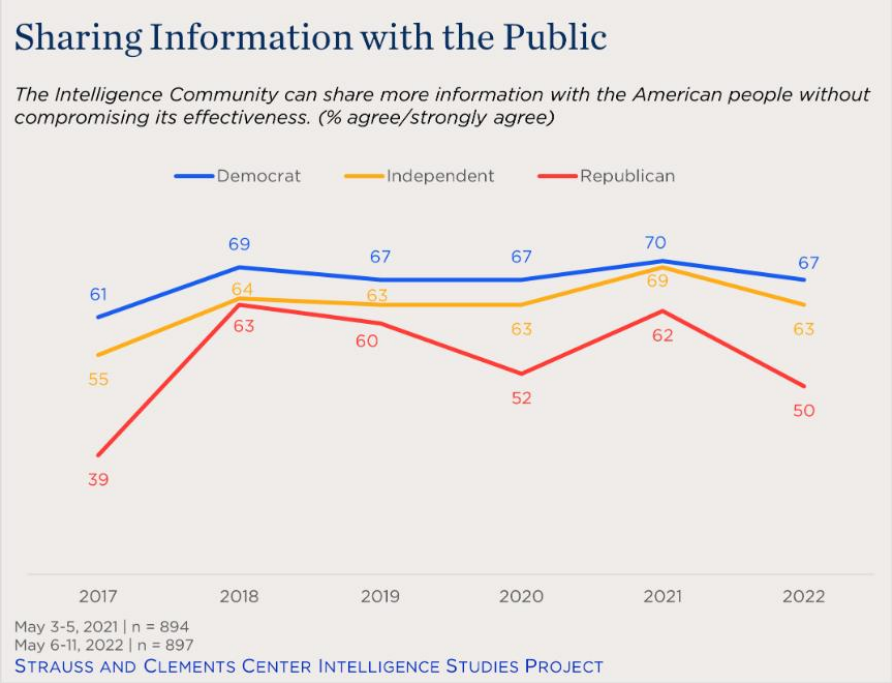

Figure 5: Polling data on Intelligence information sharing. Busby, Slick and Nguyen (2023)

In conclusion, the bolstering efforts from the CIA and the intelligence community can be considered as ineffective. Recent scandals, similar to the Snowden revelations highlighted in the analysis authored by Goitein underline how intelligence leaders have started once again to withhold key information from the public on surveillance activities. As noted above, Goitein stresses the importance of public trust in rendering intelligence activities as efficient as possible

and emphasizes how intelligence leaders should not withhold information about current surveillance programs if they wish to maintain the ground that they have gained with the transparency initiatives of the years since Snowden (Goitein, 2022). Furthermore, as public opinion polling data suggests, the public does acknowledge the important role played by the intelligence community in curbing terrorist and foreign threats, but the need for more transparency and respect of privacy was largely reflected in the data presented by the Chicago Council on Global Affairs (Busby, Slick and Nguyen, 2023). Bolstering efforts appear to be largely absent from the Paragon scandal, as Italian authorities focused more on a defensive posture rather than highlighting the positive characteristics of AISE's past.

Another crucial point in the communicative strategies of the CIA and AISE is the attempt to frame their operations within a security-democracy balance. Throughout their development, the Snowden and Paragon cases have been characterized by responses aiming to balance national security and democratic values. Such a narrative can be inserted in the theoretical framework of Perception Management. As highlighted by Derman, Perception Management is one of the main propaganda methods that is mostly used to influence the opinions and emotions of the target audience. Perception Management has three main purposes:

- Influencing public opinion both at home and abroad in order to gain and preserve legitimacy.
- Convincing the enemies what will happen to them as a result of their actions.
- Influencing the behavior and attitudes of the target audience in the desired direction (Derman, 2021, p. 65-66).

As noted above, American and Italian intelligence officials also implemented elements of IRT. In particular, the research has delved deeper into the aspects of Denial, Corrective Action and Mortification. Intelligence officials also attempted to reduce the offensiveness of the surveillance operations by framing such operations as lawful and necessary to public order, contrary to what the press or whistleblowers such as Snowden were declaring. Such a narrative strategy can be traced back to elements of the Reducing Offensiveness category of IRT, such as Attacking the Accuser and Transcendence. In the IRT framework, Transcendence can be defined as the attempt to place the offensive act that has been undertaken in a more favorable context (Benoit, 1997). Such attempts can be traced back to both the Snowden and Paragon cases. For instance, in the

wake of the Snowden revelations, President Obama stated during a speech at the National Defense University prior to the leaks that a more robust discussion on the balance between security and liberty was necessary. The press release from the Obama White House goes on by criticizing the actions made by Snowden, highlighting how such leaks put in a more advantageous position America's adversaries. In his statement, President Obama also highlighted some of the main steps that his administration would have taken to ensure that national security and democracy would achieve a more sustainable balance: the release cites the creation of an outside Review Group on Intelligence and Communications Technologies to make recommendations for reform, the consultation with the Privacy and Civil Liberties Oversight Board, created by Congress, and the conferral with foreign partners, privacy advocates, and industry leaders. After highlighting the main reforms that the Obama administration was about to undertake, the framing adopted by the Obama White House emphasized the need for balancing national security concerns and democratic values. While denying that the United States collected intelligence to suppress criticism, to disadvantage certain categories of the population or to provide advantages to U.S. companies, President Obama issued a new presidential directive that made clear that the United States would use signals intelligence for legitimate national security purposes. The Obama White House went on by stating that the collection of signals intelligence would be used for "counterintelligence, counterterrorism, counter-proliferation, cybersecurity, force protection for our troops and our allies, and combating transnational crime, including sanctions evasion". In conclusion, the press release from the Obama White concluded by reaffirming the strong necessity for intelligence reform by including the necessity of transparency and national security concerns: "… Those values make us who we are. And because of the strength of our own democracy, we should not shy away from high expectations. For more than two centuries, our Constitution has weathered every type of change because we have been willing to defend it, and because we have been willing to question the actions that have been taken in its defense. Today is no different. I believe we can meet high expectations. Together, let us chart a way forward that secures the life of our nation while preserving the liberties that make our nation worth fighting for" (The White House, 2014).

This choice of messaging found traction with the American public. In the wake of the Snowden revelations, polling data from the Pew Research Center shows that after a series of terrorist events the American public felt that anti-terror operations had not gone far enough, with a 49% to 33% margin. Furthermore, the findings of the Pew Research Center confirm the sentiment found by the

Chicago Council on Global Affairs that the surveillance of the American public is unacceptable; while believing it would be more acceptable to monitor foreign citizens, foreign leaders and American leaders. Moreover, majorities endorsed tracking those specific people who visit anti-American websites (67%) and use terms like "explosives" and "automatic weapons" in their search engine inquiries (65%) (Pew Research Center, 2016). Furthermore, more polling data suggests that the CIA also gained more popularity in 2015, going from 54% in January 2015 to 57% in September 2015 (Pew Research Center, 2015a; Pew Research Center, 2015b). These findings confirm that after being initially shaken by the Snowden revelations, the attention of the American public shifted back to security once the CIA and the intelligence community engaged in transparency reforms and terrorism threats re-emerged, allowing for intelligence officials to frame surveillance as a necessary tool for counterterrorism efforts, which resonated strongly with public opinion in the long term. However, Goitein observes how the CIA has failed to address critical lessons from the Snowden scandal and has once again failed to provide legislators and key sections of civil society with a clear account of the data collection programs (Goitein, 2022). The analysis by Goitein is crucial for understanding how intelligence officials should accompany perception management with proper corrective action.

Regarding the Paragon case, Italian officials used similar strategies to their American counterparts. As noted above, once the Paragon scandal came to light, Minister for Parliamentary Relations Luca Ciriani admitted that the Italian intelligence services were using the Graphite software, but that the authorities were implementing such technology only for national security purposes. Ciriani went on to state that the authorities had respected the law and threatened legal action to all those who stated the contrary (Naughtie, 2025). Furthermore, the COPASIR report reaffirmed the claims of Ciriani and Mantovano by stating that the intelligence services used the Graphite software on a very limited number of people, with permission from a prosecutor. In particular, the report emphasized how AISE had used the spyware to search for fugitives, counter illegal immigration, alleged terrorism, organized crime, fuel smuggling and counter-espionage and internal security activities. These claims were reinforced by AISE Director Caravelli who admitted that the agency used Graphite, but not to spy on activists and journalists. In May 2025 a Sicilian judge ordered six members of Mediterranea to stand trial for activities tied to illegal immigration, including Casarini and Caccia. All of them have denied wrongdoing (Fonte and Alvise Armellini, 2025b; Holgado, 2025). These strategies can be traced back to Transcendence, as Meloni and AISE

officials framed the surveillance operations with Graphite as necessary for national security reasons. The Perception Management undertaken by Italian officials contained the crisis: at the time of writing, no intelligence leaders or government officials tied to the scandal have tendered their resignation. Moreover, when the Italian government faced mounting pressure from the press and opposition parties, Meloni officials announced that the contract with Paragon Solutions had been terminated after an initial suspension (La Stampa, 2025). Other reasons can be identified as to why Meloni's strategy managed to contain reputational damage to the Italian intelligence. Even though opposition parties opposed the use of Graphite, the Italian opposition is largely fractured which has allowed for the Meloni government to enjoy stability throughout the term (Mingardi, 2025). Such a crisis can be classified within the framework defined by Coombs and Holladay as a Paracrisis. The authors define these types of crises as a "publicly visible crisis threat that charges an organization with irresponsible or unethical behavior" (Coombs and Holladay, 2012, p. 409). The authors go on by examining how Paracrises start at the beginning of the crisis management process. These crises are mainly a reputational threat to the organization, where negative information about that organization can harm its reputation. Coombs and Holladay state that crisis managers have three options involving a Paracrisis: refuse, refute, reform. The authors classify refutation as when management defends the positions of the organization against stakeholder accusations. It is perceived as an escalation of the conflict with the concerned stakeholders. In this situation, crisis managers build their defense around shared values with important stakeholders with the objective of gathering support that no change is necessary or that reforming the organization could harm its stakeholders or the organization itself (Coombs and Holladay, 2012). As noted above, this approach mirrors the strategy undertaken by intelligence and governmental officials. The Transcendence strategy put in place by the Meloni government and the fractured opposition allowed for the Paragon scandal to remain at the reputational threat stage and not develop into a more severe crisis for Italy's intelligence apparatus. In comparing the Paragon and Snowden cases, the Snowden affair had a much deeper impact on an institutional level. The revelations prompted the passage of the USA FREEDOM Act and investigations into the matter being undertaken (Congress.gov, 2015; The White House, 2014). However, the only high-ranking intelligence official to resign in the aftermath of the revelations was General Keith Alexander, but his retirement was characterized more as a dignified exit and not directly linked to the revelations. No CIA officials resigned (Ackerman, 2014).

The Perception Management and narrative strategy chosen by Italian officials partially worked, as the strategy found success with the public but failed with civil society, opposition parties and journalists. In the immediate aftermath of the Paragon case the Meloni government and Meloni's personal approval rating saw a contraction in the polls, reaching the lowest level of public approval (41%) in February 2025 since the beginning of the government's mandate. However, polling data also suggests that Meloni's government garnered long-term public support, reaching 30.2% in September 2025 (Ipsos, 2025; SWG, 2025). This can be explained by the fact that the strategy put in place by Meloni officials allowed for the Paragon scandal to remain a reputational threat rather than escalating into an institutional crisis, as can be noted in the Eurispes report which highlights an increase in the public support for the intelligence services by 4.4% (Piazzaborsa, 2025). Nonetheless, polling data from the OECD and Eurispes highlight how public trust in the executive branch has dropped from 36% in 2024 to 30% in 2025. The OECD attributes such a decline after having analyzed different drivers of trust towards public institutions. The report highlights how the cause of such a decline can be attributed to different factors: only slightly above one fifth of Italians believe that the political system allows for the people to have a say in governmental decisions. Another key indicator of the report shows how 26% of people in Italy believe that the government would refuse a harmful practice to society demanded by a corporation and 42% of Italians believe that the government can regulate new technologies appropriately. Italy is also shown to perform slightly worse in terms of appropriate data usage in comparison to other OECD member countries (OECD, 2024). Moreover, the communication strategy adopted by Meloni officials failed to address concerns from key sections of the public: opposition leaders as Matteo Renzi criticized the handling of the scandal by the government by highlighting the lack of regard for democratic norms. The Meloni government was also criticized by other opposition figures such as Federico Fornaro, MP for the Democratic Party who defined the avoidance of questions as "a slap in the face to parliament" (Giuffrida, Tondo and Kirchgaessner, 2025). Furthermore, polling data from Bocconi University underlines how the Italian public has a very low confidence in the government's ability to defend itself against cyberattacks, measured at 4.3%. In order for citizens to have trust, the analysis published by Bocconi emphasizes how greater transparency regarding the state's strategic approach and a consistent communication strategy is crucial for fostering greater trust in the ability of the intelligence community to protect critical infrastructure (Nasi, 2025). In conclusion, even though the Paragon case is still ongoing, these findings confirm that

the framing of the surveillance operations undertaken by AISE and Meloni government officials as necessary to preserve national security while also following the rule of law seems to have resonated with the Italian public. However, this strategy has not silenced critics from civil society and opposition parties. The Paragon case demonstrates that Perception Management without appropriate Corrective Action will achieve only partial success, as lawmakers and human rights organizations continue to criticize the surveillance operations of the government.

4.4 Conclusion

To sum up, while the data has shown that the selected intelligence agencies record positive public approval ratings, polling data and numerous reports have highlighted how many parts of society have concerns regarding the respect of privacy laws of intelligence agencies. Moreover, the selected polls also emphasize how a majority of the public feels that the intelligence sectors of the U.S. and Italy could share more information without compromising operational security. After having discussed how the communication strategies of the CIA and AISE have proven to be inefficient in key areas, the following chapter will provide policy proposals regarding the weaknesses of these strategies by fostering a clearer, more transparent, and more democratic form of communication with the public.

CHAPTER 5: POLICY PROPOSALS

The communication strategies adopted by the CIA and AISE have shown shortcomings regarding transparency, weaknesses that undermine public trust both in the United States and in Italy. As noted above, crisis communication scholars consider transparency and balancing reactive and proactive crisis measures as one the most important elements to successful crisis management (Haupt, 2021). SCCT has also explored the perceptions of organizational transparency, highlighting how higher perceptions of organizational transparency have been shown to have a positive effect on the levels of trust. Holland, Seltzer and Kochigina have grouped organizational transparency into three main areas: information accuracy, clarity, and disclosure. Their research goes on by emphasizing how Seeger highlighted how honest, open, and candid communication was fundamental in the best practices of crisis communication (Holland, Seltzer and Kochigina, 2021). In order to address the deficiencies of the selected intelligence agencies outlined throughout

this study, the following sections will discuss policy proposals aimed at strengthening the crisis communication strategies of the CIA and AISE. It is clear from the harm done to their reputations by the Snowden and Paragon scandals that both CIA and AISE need to implement systematic changes to the way they communicate in times of crisis, not only to preserve operational secrecy but also to uphold democratic legitimacy and public confidence.

5.1 Proactive Transparency in Intelligence Disclosures

As noted in the research conducted by Ruijer, transparency is an intrinsic value of democratic societies. The research goes on by stating that proactive disclosure ensures that the public is informed about the laws and decisions that affect them (Ruijer, 2017). This study has highlighted the inefficiencies of the crisis communication strategies of the Italian and American intelligence apparatuses, and, as highlighted by the study conducted by Holland, Seltzer and Kochigina, transparency makes a valuable contribution to crisis response strategies of organizations. Increased transparency regularly led to elevated perceptions of organizational trustworthiness compared to when the same method was employed alongside a low transparency message. The study by Holland, Seltzer and Kochigina confirms that employing message transparency in crisis responses is in the strategic interest of the organization (Holland, Seltzer and Kochigina, 2021).

For intelligence agencies, proactive transparency must coincide with operational security. Nonetheless, intelligence officials themselves have stated that a more proactive approach regarding these crises could have contained the reputational damage done during the Snowden years. For example, the general counsel at the Office of the DNI Robert S. Litt stated: "One lesson that I have drawn from the recent events… is that we would likely have suffered less damage from the leaks had we been more forthcoming about some of our activities, and particularly about the policies and decisions behind those activities" (Aftergood, 2014a). Litt went on by stating that going forward the intelligence community should be taking a closer look into what needs to be classified and evolve from the mindset of merely reacting to formal requests of making information public. In his messaging, Litt clearly stated that one of the main concerns of what the intelligence community should focus on is continuing efforts in proactive transparency. According to a count by cryptome.org, news organizations have disseminated around 1,300 pages of confidential documents revealed by Edward Snowden. The U.S. intelligence agencies have disclosed twice that many in response (Aftergood, 2014a). The approach outlined by Litt resonates with Durmaz

regarding the democratic oversight of intelligence. In his analysis, Durmaz highlights how the bureau of intelligence upholds democratic values and the rule of law by operating within the established boundaries. Furthermore, Durmaz highlights how a bureau of intelligence maintains a clear balance between transparency and effectiveness. The author cites accountability as one of the most important characteristics in classifying an effective intelligence service in a democratic state. Such accountability requires an effective bureaucratic system that prevents unlawful practices through effective oversight mechanisms. These institutions are designed to allow the intelligence services to carry out their operations according to the laws (Durmaz, 2013). A study conducted by the OECD also highlights how proactive transparency is crucial in communicating with the public. Research indicates that withholding information, even if tentative, on lesser-known subjects fosters the emergence of rumors and speculations, as extensively recorded during the COVID-19 epidemic and other crises (OECD, 2023)

With this premise, the following proposal aims to create a framework for the CIA and AISE to increase the activities of proactive transparency. The aim of the proposal is to maximize transparency while maintaining operational effectiveness. In the case of the United States, the ODNI could simplify the language used in the Annual Statistical Transparency Reports. As of now, the language used in this report is quite technical and can prove to be difficult for the general public. Publishing a clear summary of the report that also includes the reasons for which certain tools have been used would embrace the concept outlined by the research conducted by Holland, Seltzer and Kochigina that organizations should embrace honest, open, and candid communication with the public. This reform would allow the broader U.S. intelligence community and the CIA to embrace the concept highlighted in Kumalasari et al. that strong digital communication fosters greater public trust. The findings of the research also showcase how transparency must be accompanied by clarity, honesty, and timely response from national security actors . (Holland, Seltzer and Kochigina, 2021; Kumalasari et al., 2024; Obi, Odilibe and Arowoogun, 2024; ODNI, 2024).

Regarding AISE, the annual Italian report on security information policy published by the Italian intelligence services highlights various topics, such as the Ukraine war and the cyberthreats that Italy is facing. Adopting an approach similar to the reforms undertaken in the United States, such as including sufficient information in the annual report in order to allow the public to

understand the extent of the surveillance operations that are being carried out or allowing companies to publish a redacted report on the national security requests received could prove to be a concrete first step to provide the Italian public with a more transparent communication of the intelligence services (Sistema di Informazione per la Sicurezza della Repubblica, 2025). Moreover, adopting a more proactive approach in its transparency would also align Italy to European jurisprudence and best practices. Cases such as Szabó and Vissy v. Hungary (application no. 37138/14) have highlighted how surveillance operations must be accompanied with appropriate safeguards against potential abuse (European Court of Human Rights, 2016). By adopting such an approach, AISE would align itself with wider European standards on democratic accountability.

In conclusion, both the CIA and AISE could benefit from more proactive transparency with the public. By adding more selected details to their annual report in a clear and comprehensive language could be a concrete first step in remedying the shortcomings of the communication strategies of the intelligence apparatuses under examination.

5.2 Strengthen Oversight and Civil Society Participation Mechanisms

Recent scholarly work has outlined how a secondary oversight mechanism from civil society regarding the intelligence services could help foster trust towards the intelligence services of the United States and Italy. The authors note that: "practicing oversight can take agonistic, contentious, transnational, and public forms than most of literature on oversight suggests, or that applicable policy frameworks acknowledge" (Kniep et al., 2023, p. 212). Civil society actors are expected to contribute to official oversight, limit the power of intelligence agencies, and provide a parallel accountability mechanism to examine the operations of overseers. The findings in Kniep et al. indicate that numerous authors have criticized the emphasis on representative institutions as excessively narrow and bureaucratic, in contrast to broader contexts of democratic accountability. The authors go on by delving deeper into how civil society actors could contribute to the oversight of the intelligence services as a democratic practice (Kniep et al., 2023).

The following proposal aims to build on the model developed by the DCAF and reimagine the interaction between civil society and intelligence services. In the report published by the Geneva Centre for Security Sector Governance, the authors highlight how dialogue between the intelligence community and civil society can increase legitimacy and trust in intelligence services.

The research goes by stating that specialized civil society organizations can produce a valuable contribution to the communication of the activities of the intelligence sector to the public. In the case of the CIA, the Privacy and Civil Liberties Oversight Board (PCLOB) has recently undergone significant changes. President Trump has fired three Democratic members of the Board, leaving only one member affiliated with the Republican Party. Within this context, the PCLOB cannot regularly function, as a quorum is missing. Restoring the PCLOB to full functionality and then creating a structured, proactive roundtable session with accredited specialized civil society organizations would represent concrete steps towards a more efficient CIA crisis communication practice (Geneva Centre for Security Sector Governance, 2021; Nojeim and Lorenzo Perez, 2025).

Following the example outlined by this analysis, AISE could institutionalize a civil oversight body similar to the ones created in Northern Macedonia and Croatia. These bodies are not fully independent and are accountable to parliament, but such a body would be free of political party affiliations, which would entail providing more objective analyses of the intelligence sector. An alternative approach outlined in the work of the Geneva Centre for Security Sector Governance is the inclusion of civil society representatives in expert oversight bodies. This would allow for civil society engagement without the need for legislative amendments (Geneva Centre for Security Sector Governance, 2021). Within this framework, AISE and COPASIR could create a civil society oversight body similar to the ones created in Northern Macedonia and Croatia in order to reestablish trust with civil society organizations after the Paragon Scandal. Regarding AISE, these changes could entail COPASIR directing the efforts towards regular meetings with civil society experts and the release of redacted summaries of what they find during their oversight work. These steps would be in line with the analysis conducted by DCAF and allow Italy to reaffirm democratic accountability and trust in the respect of privacy laws.

5.3 Internal Reforms

In order to achieve maximum effectiveness in their crisis communication efforts, both the CIA and AISE should implement internal reform in order to address crises in a more efficient manner. As highlighted throughout the course of this study, Corrective Action is one of the most effective crisis communication strategies. As noted throughout the course of this study, taking Corrective Action consists in the creation of a new belief about the accused in fixing or preventing the recurrence of the problem. Intelligence agencies have attempted to embark on internal reforms aimed at

rebuilding trust with the public, but have failed to address concerns from key sections of society (Benoit, 2015).

In the case of the CIA, a conference hosted by the Harvard Kennedy School Belfer Center's Intelligence Project is a key element in understanding observations regarding the improvement of crisis communication from within the CIA. During the conference, Rolf Mowatt-Larsson stated that while secrecy is key in intelligence work, the agency should not engage in a "cult of secrecy". Mowatt-Larsson goes on by emphasizing how Langley should improve transparency to strengthen trust with the American public. As noted throughout the conference, Policymakers should be provided with a more in-depth background on the mistakes of intelligence of the past. Clearly written products and tailored oral briefings could help prevent more mistakes being committed by decision makers (Walton et al., 2022). Furthermore, reforming the CIA Public Affairs Office would also facilitate more regular press interaction with Langley. As noted by Coombs, intelligence agencies such as the CIA should not be evading questions by stating "no comment", as this is detrimental to the credibility of the organization. Another communication principle from Coombs that the Public Affairs Office should implement is timely, accurate and consistent messaging on scandals such as the Snowden revelations (Coombs and Holladay, 2010). This could be achieved by improving inter-agency coordination on the messaging of such crises to the public. Moreover, the CIA could also benefit from increasing information disclosure campaigns. The most recent example of this is the declassification of intelligence regarding the 2022 Russian invasion of Ukraine. Former CIA Director Burns described these campaigns as successful in pushing back against the narrative from the Russian Federation (Pomerleau, 2023). The results obtained by the CIA during this episode show that expanding the declassification of intelligence can also be within the strategic interest of the United States (Pomerleau, 2023).

In the Italian case, the Italian intelligence community is currently operating under the 2007 reform that has designated the DIS as the main office for institutional communication. The DIS has undertaken significant steps toward increasing public engagement (such as creating and keeping the agency's website up to date), but the Italian security apparatus still lacks a more robust communication framework. As noted in the report by Montagnese and Neri, the intelligence services are still missing social media platforms, which would be beneficial in expanding AISE's outreach, increasing its efficiency (Montagnese and Neri, 2016). Furthermore, the Italian

intelligence does not have a designated spokesperson, relying on the DIS for institutional communication. Nominating a spokesperson for the intelligence services would be beneficial in creating a more productive and direct relationship with the press (Coombs and Holladay, 2010). After having opened social media accounts and designating a spokesperson, AISE should concentrate its efforts in establishing a clear, transparent communication with the public. Italian intelligence and governmental officials should focus on inter-institutional coordination in preparing communication strategies for crises. As noted in crisis communication literature, organizations should not engage with the public adopting different positions during a crisis, but rather implement consistent messaging with the interested stakeholders in order to build organizational credibility (Coombs and Holladay, 2010). This factor could be resolved by increasing crisis communication training to AISE employees and other national security agencies and developing clear crisis communication protocols would help AISE address possible crises that it faces rather than issuing blanket and vague Denials.

5.4 Conclusion

In conclusion, the policy proposals that have been formulated throughout the course of this chapter have stemmed from the findings of the research. The proposals aim to address critical areas of the crisis communication protocols of the CIA and AISE that have been found to be lacking in effectiveness throughout the course of this research. By focusing on proactive transparency, internal policy reforms, and civil society participation, the recommendations aim to change the reactive tone of intelligence agencies and address concerns raised from society while maintaining operational security.

Conclusions

Throughout the course of this thesis, the research has analyzed how the CIA and AISE operate in the domain of crisis communication. Having focused on scandals related to mass surveillance, the research has highlighted how the intelligence networks of the United States and Italy are capable of garnering a substantial amount of public support, but polling data from various reputable sources has shown that the public perceives that the agencies could provide more information to the general public and involve more stakeholders in the decision-making process.

The first chapter of this thesis explained the main theoretical models that were going to be applied in examining the communication strategies of the selected intelligence agencies, such as

IRT and SCCT. The following section delved deeper into how these models would be applied by explaining the research methodology. The selected research methodology is thematic analysis, a qualitative research method that allows for the examination of the patterns in the communication strategies of the CIA and AISE. In conclusion, after having analyzed the selected case studies (the Snowden revelations and the Paragon Scandal) and their implications for the intelligence sectors of Italy and the U.S., the research was crucial in building policy proposals for improving the areas in which the crisis communication of the intelligence services proved to be lacking.

The aim of this thesis is to contribute to crisis communication literature by examining more thoroughly the strategies of intelligence organizations the strategies of intelligence organizations. By analyzing the recurring themes in their narrative policies, the research aims to apply the principles outlined by crisis communication scholars such as Benoit and Coombs and apply them to the intelligence apparatuses of the selected countries: by expanding proactive transparency policies, engaging elements of civil society and restructuring their public affairs offices to provide clearer information in their interactions with the press, these intelligence agencies would foster public trust. Increasing democratic accountability could prove to be beneficial not only for strengthening democracy in these countries, but also for the broader strategic objectives of the intelligence community.

This thesis has demonstrated how the effectiveness of intelligence agencies cannot be separated from their democratic accountability and communication strategies. The theoretical framework that has been employed highlights how both the CIA and AISE rely on reactive strategies. The findings of the research underscore how corrective action and mortification are important in the long term.

As noted in chapter 2, future researchers are encouraged to increase the data collected by interviews and analyze how the internal processes of intelligence agencies influence crisis communication during national security crises. Furthermore, another interesting topic for future research is to study the crisis communication practices of intelligence agencies in relation to external contractors, such as Palantir Technologies. The reliance that national security institutions place on external contractors may harm the public perception of said institutions. Future studies could focus on the communication of intelligence agencies in relation to the surveillance practices of their external contractors.

In conclusion, this thesis contributes to scholarly work on crisis communication by analyzing how intelligence agencies can become the subject of public scrutiny regardless of their secretive nature. This factor is crucial in understanding how transparency, corrective action and internal reforms are essential for building and maintaining public trust while also offering a framework for more efficient democratic accountability.

Bibliography

ABC News (2014). *Intel Heads: Edward Snowden Did 'Profound Damage' to U.S. Security*. [online] ABC News. Available at: https://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388.

Ackerman, S. (2013). *Clapper: I gave 'erroneous' answer because I forgot about Patriot Act*. [online] the Guardian. Available at: https://www.theguardian.com/world/2013/jul/02/james-clapper-senate-erroneous.

Ackerman, S. (2014). *NSA chief Keith Alexander avoids Snowden in retirement speech*. [online] the Guardian. Available at: https://www.theguardian.com/world/2014/mar/28/nsa-chief-keith-alexander-snowden-retirement-speech [Accessed 2 Sep. 2025].

Aftergood, S. (2014a). *ODNI Rethinks Secrecy and Openness in Intelligence - Federation of American Scientists*. [online] Federation of American Scientists. Available at: https://fas.org/publication/litt-transparency/ [Accessed 24 Aug. 2025].

Aftergood, S. (2014b). *The Clapper 'Lie,' and the Senate Intelligence Committee*. [online] Federation of American Scientists. Available at: https://fas.org/publication/clapper-ssci/.

Amnesty International (2025a). *Europe: Paragon attacks highlight Europe's growing spyware crisis*. [online] Amnesty International. Available at: https://www.amnesty.org/en/latest/news/2025/03/europe-paragon-attacks-highlight-europes-growing-spyware-crisis/ [Accessed 29 May 2025].

Amnesty International (2025b). *New spyware case in Italy confirms worrying trend*. [online] Amnesty International. Available at: https://www.amnesty.org/en/latest/news/2025/06/italy-new-case-of-journalist-targeted-with-graphite-spyware-confirms-widespread-use-of-unlawful-surveillance/ [Accessed 14 Aug. 2025].

Aspers, P. and Corte, U. (2019). What Is Qualitative in Qualitative Research. *Qualitative Sociology*, 42(2), pp.139–160. doi:https://doi.org/10.1007/s11133-019-9413-7.

Attianese, L. (2025). *Nordio: 'Né la Penitenziaria né il ministero usano Paragon' - Notizie - Ansa.it*. [online] Agenzia ANSA. Available at: https://www.ansa.it/sito/notizie/politica/2025/02/19/nordio-ne-la-penitenziaria-ne-il-ministero-usano-paragon_fa51165b-d0e4-4288-b925-ec99523ecc1a.html [Accessed 18 Aug. 2025].

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. and Walker, R.B.J. (2014). After Snowden: Rethinking the Impact of Surveillance. *Interrnational Political Sociology*, 8(2), pp.121–144. doi:https://doi.org/10.1111/ips.12048.

Benoit, W.L. (1995). *Accounts, excuses, and apologies : a theory of image restoration discourse*. Albany: State University Of New York Press, Cop.

Benoit, W. (1997). *Image Repair Discourse and Crisis Communication*. [online] *Science Direct*, pp.177–186. Available at: https://www.sciencedirect.com/science/article/pii/S0363811197900230 [Accessed 14 Feb. 2025].

Benoit, W. (2015). *Accounts, Excuses, and Apologies SECOND EDITION*. State University of New York Press, Albany.

Benoit, W. (2018). Crisis and Image Repair at United Airlines: Fly the Unfriendly Skies. *Journal of International Crisis and Risk Communication Research*, 1(1), pp.11–26. doi:https://doi.org/10.30658/jicrcr.1.1.2.

Biondi, M. (2025). *Spyware di Stato: Paragon e la sorveglianza politica contro Mediterranea - cild.eu*. [online] cild.eu. Available at: https://cild.eu/blog/2025/03/28/spyware-di-stato-paragon-e-la-sorveglianza-politica-contro-mediterranea/ [Accessed 19 Jul. 2025].

Bobbio, N. (1980) 'LA DEMOCRAZIA E IL POTERE INVISIBILE', *Italian Political Science Review/Rivista Italiana di Scienza Politica*, 10(2), pp. 181–203. doi:10.1017/S0048840200007930.

Busby, J., Slick, S. and Nguyen, K. (2023). *2022 Public Attitudes on US Intelligence*. [online] globalaffairs.org. Available at: https://globalaffairs.org/research/public-opinion-survey/2022-public-attitudes-us-intelligence.

Caroll, R. (2013). *NSA director Keith Alexander defends surveillance tactics in speech to hackers*. [online] the Guardian. Available at: https://www.theguardian.com/world/2013/jul/31/nsa-keith-alexander-black-hat-surveillance.

CBS News (2013a). *CIA 'Honor the Oath' program hopes to crack down on leaks*. [online] Cbsnews.com. Available at: https://www.cbsnews.com/news/cia-honor-the-oath-program-hopes-to-crack-down-on-leaks/ [Accessed 22 Jul. 2025].

CBS News (2013b). *Snowden damage the worst, says ex-CIA No. 2*. [online] www.cbsnews.com. Available at: https://www.cbsnews.com/news/snowden-damage-the-worst-says-ex-cia-no-2/.

Chadwick, A., Collister, S., Holloway, R., Bennett, M., Carlson, M., Delli Carpini, M., Jensen, S., Lewis, B. and O'loughlin (2014). Boundary-Drawing Power and the Renewal of Professional News Organizations: The Case of The Guardian and the Edward Snowden National Security Agency Leak. *International Journal of Communication*, 8, pp.2420–2441.

CIA (2014). *Signals Intelligence Activities*. [online] Available at: https://www.cia.gov/static/f812ca58dfcbc4d92e6f791cbe4bb39f/CIA_EO_14086_Procedures.pdf [Accessed 8 Aug. 2025].

CIA (2023). *History of CIA*. [online] www.cia.gov. Available at: https://www.cia.gov/legacy/cia-history/.

CIA (2024a). *Ask Molly: CIA's Mission Centers*. [online] Cia.gov. Available at: https://www.cia.gov/stories/story/ask-molly-cias-mission-centers/.

CIA (2024b). *The Thrill of the Hunt: Lessons from Archival Research into Cold–War Era Intelligence Decision-making*. [online] Cia.gov. Available at: https://www.cia.gov/resources/csi/books-monographs/the-thrill-of-the-hunt-lessons-from-archival-research-into-cold-war-era-intelligence-decision-making/ [Accessed 16 Apr. 2025].

Claiborne, W. (n.d.). *Nixon Name Used to Pressure CIA* . [online] CIA (.gov). Available at: https://www.cia.gov/readingroom/docs/CIA-RDP84-00161R000400210010-6.pdf [Accessed 14 Feb. 2025].

Clapper, J. (2013). *Letter to The Honorable Dianne Feinstein*. [Letter] Available at: https://www.cia.gov/readingroom/docs/LETTER%20TO%20DIANNE%20FEINSTEI%5B16307803%5D.pdf [Accessed 16 Aug. 2025].

Congress.gov (2015). *Text - H.R.2048 - 114th Congress (2015-2016): USA FREEDOM Act of 2015*. [online] Congress.gov. Available at: https://www.congress.gov/bill/114th-congress/house-bill/2048/text.

Coombs, W.T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, 10(3), pp.163–176. doi:https://doi.org/10.1057/palgrave.crr.1550049.

Coombs, W.T. and Holladay, J.S. (2012). The Paracrisis: The challenges created by publicly managing crisis prevention. *Public Relations Review*, 38(3), pp.408–415. doi:https://doi.org/10.1016/j.pubrev.2012.04.004.

Coombs, W.T. and Holladay, S.J. (2010). *The Handbook of Crisis Communication*. Chichester, U.K. ; Malden, Ma: Wiley-Blackwell.

COPASIR (2025). *XIX LEGISLATURA COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA RELAZIONE SULL'UTILIZZO DELLO SPYWARE 'GRAPHITE' DA PARTE DEI SERVIZI DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA CAMERA DEI DEPUTATI SENATO DELLA REPUBBLICA STABILIMENTI TIPOGRAFICI CARLO COLOMBO*. pp.1–24.

Coyne, H. (2019). The Untold Story of Edward Snowden's Impact on the GDPR. *The Cyber Defense Review*, 4(2), pp.65–80.

Croft, A. (2014). Obama says U.S. needs to win back trust after NSA spying. *Reuters*. [online] 26 Mar. Available at: https://www.reuters.com/article/technology/obama-says-us-needs-to-win-back-trust-after-nsa-spying-idUSDEEA2O02A/.

De Blasio, E., Quaranta, M., Santaniello, M. and Sorice, M. (2018). *Media, Politica e Società: Le Tecniche di Ricerca*. Carocci Editore.

Decode39 (2024). *Italy opens debate on setting up anti-disinfo agency - Decode39*. [online] Decode39. Available at: https://decode39.com/8940/italy-debate-anti-disinfo-agency/ [Accessed 29 May 2025].

Derman, G. (2021). PERCEPTION MANAGEMENT IN THE MEDIA. *International Journal of Social and Economic Sciences*, 11(1), pp.64–78.

Durmaz, M. (2013). Balancing Effectiveness and Transparency in Intelligence Community: A Challenge for Consolidating Democracies. *Journal of Defense Management* . doi:https://doi.org/10.4172/2167-0374.1000114.

EDRi (2020). *Telecom Italia wiretapping scandal - European Digital Rights (EDRi)*. [online] European Digital Rights (EDRi). Available at: https://edri.org/our-work/edrigramnumber4-15italy/ [Accessed 29 May 2025].

Eisenhardt, K. (1989). Building Theories from Case Study Research. *Source: The Academy of Management Review*, 14(4), pp.532–550.

Elizabeth Goitein (2022). *How the CIA Is Acting Outside the Law to Spy on Americans | Brennan Center for Justice*. [online] www.brennancenter.org. Available at: https://www.brennancenter.org/our-work/analysis-opinion/how-cia-acting-outside-law-spy-americans.

Elsbach, K.D. (2003). ORGANIZATIONAL PERCEPTION MANAGEMENT. *Research in Organizational Behavior*, 25, pp.297–332. doi:https://doi.org/10.1016/s0191-3085(03)25007-3.

Erika Kinetz and Paola Santalucia (2025). *Spyware from US-backed Israeli firm targets European journalists*. [online] AP News. Available at: https://apnews.com/article/spyware-italy-paragon-meloni-pegasus-f36dd32106f44398ee24001317ccf2bb.

European Court of Human Rights (2016). *Hungarian legislation on secret anti-terrorist surveillance does not have sufficient safeguards against abuse*. [online] Available at: https://hudoc.echr.coe.int/eng-press?i=003-5268616-6546444 [Accessed 28 Aug. 2025].

Ferran, L. (2014). *Spy Tweets: CIA Joins Twitter, Facebook*. [online] ABC News. Available at: https://abcnews.go.com/blogs/headlines/2014/06/spy-tweets-cia-joins-twitter-facebook [Accessed 8 Aug. 2025].

Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. *Qualitative Inquiry*, 12(2), pp.219–245. doi:https://doi.org/10.1177/1077800405284363.

Fonte, G. and Alvise Armellini (2025a). Italian lawmakers seek answers from government on spyware scandal. *Reuters*. [online] 4 Jul. Available at: https://www.reuters.com/business/media-telecom/italian-lawmakers-seek-answers-government-spyware-scandal-2025-07-04/.

Fonte, G. and Alvise Armellini (2025b). Italy and Israeli Paragon part ways after spyware affair. *Reuters*. [online] 9 Jun. Available at: https://www.reuters.com/sustainability/society-equity/italy-has-ended-spyware-contract-with-paragon-parliamentary-document-shows-2025-06-09/.

Garante Per la Protezione dei Dati Personali (2025). *Paragon, Garante: 'La sorveglianza è senza limiti: ecco il problema'*. [online] Garanteprivacy.it. Available at: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10105147.

Geneva Centre for Security Sector Governance (2021). *Rethinking Engagement Between Intelligence Services and Civil Society*. [online] *DCAF*, pp.1–12. Available at: https://www.dcaf.ch/rethinking-engagement-between-intelligence-services-and-civil-society [Accessed 28 Aug. 2025].

Gerring, J. (2004). What Is a Case Study and What Is It Good for? *American Political Science Review*, 98(2), pp.341–354. doi:https://doi.org/10.1017/s0003055404001182.

Giglio, F. (2025). *The Paragon case: Walking the fine line between press freedom and national security in Italy and the EU - CiTiP blog*. [online] CiTiP blog. Available at: https://www.law.kuleuven.be/citip/blog/the-paragon-case-walking-the-fine-line-between-press-freedom-and-national-security-in-italy-and-the-eu/ [Accessed 5 Jun. 2025].

Giuffrida, A., Tondo, L. and Kirchgaessner, S. (2025). *Journalists launch legal action against Italian government over spyware claims*. [online] the Guardian. Available at:

https://www.theguardian.com/world/2025/feb/19/journalists-launch-legal-action-against-italian-government-over-spyware-claims.

Greene, M., Rowe, D. and Sprechman, T. (2025). *Access Now - Paragon must answer for spyware use against civil society and journalists*. [online] Access Now. Available at: https://www.accessnow.org/press-release/paragon-must-answer-for-spyware-use-against-civil-society/ [Accessed 14 Aug. 2025].

Greenwald, G., MacAskill, E. and Poitras, L. (2013). *Edward Snowden: the Whistleblower behind the NSA Surveillance Revelations*. [online] The Guardian. Available at: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Gup, T. (2004). Covering the CIA in Times of Crisis. *Harvard International Journal of Press/Politics*, 9(3), pp.28–39. doi:https://doi.org/10.1177/1081180x04266682.

Gustafson, K., Lomas, D., Wagner, S., Abdalla, N.S. and Davies, P.H.J. (2024). Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022. *Intelligence and National Security*, 39(3), pp.400–419. doi:https://doi.org/10.1080/02684527.2024.2322214.

Hansen, W. (2024). *Most Federal Agencies Poll Favorably in Pew Survey*. [online] Meritalk.com. Available at: https://www.meritalk.com/articles/most-federal-agencies-poll-favorably-in-pew-survey/ [Accessed 4 May 2025].

Haupt, B. (2021). The Use of Crisis Communication Strategies in Emergency Management. *Journal of Homeland Security and Emergency Management*, 18(2), pp.125–150. doi:https://doi.org/10.1515/jhsem-2020-0039.

Hawkins, K. (2025). *What Is the PRISM Program? NSA, Edward Snowden and Government Surveillance in 2025*. [online] Cloudwards. Available at: https://www.cloudwards.net/prism-snowden-and-government-surveillance/.

Hayward, T. (2023). Intelligence Agencies' Communications with the Public. *Critical Society Studies*, (2), pp.1–26. doi:https://cdoi.org/1.2/065/000027.

Holgado, Y.H. (2025). *Servizi segreti e caso Paragon, Mantovano attacca i giornali. Il 25 febbraio in aula la sfiducia a Nordio*. [online] Editorialedomani.it. Available at: https://www.editorialedomani.it/fatti/servizi-segreti-e-caso-paragon-mantovano-attacca-i-giornali-ifvvzjmz [Accessed 18 Aug. 2025].

Holland, D., Seltzer, T. and Kochigina, A. (2021). Practicing transparency in a crisis: Examining the combined effects of crisis type, response, and message transparency on organizational perceptions. *Public Relations Review*, 47(2). doi:https://doi.org/10.1016/j.pubrev.2021.102017.

Human Rights Watch (2014). *With Liberty to Monitor All*. [online] Human Rights Watch. Available at: https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and [Accessed 16 Aug. 2025].

Ipsos (2025). *I sondaggi politici di Pagnoncelli: in crescita l'area dell'incertezza e dell'astensione*. [online] Ipsos. Available at: https://www.ipsos.com/it-it/sondaggi-politici-pagnoncelli-crescita-area-incertezza-astensione [Accessed 9 Jun. 2025].

Johnson, L.K. (2014). A Conversation with James R. Clapper, Jr., The Director Of National Intelligence in the United States. *Intelligence and National Security*, 30(1), pp.1–25. doi:https://doi.org/10.1080/02684527.2014.972613.

Kniep, R., Ewert, L., Reyes, B.L., Tréguer, F., Cluskey, E.M. and Aradau, C. (2023). Towards democratic intelligence oversight: Limits, practices, struggles. *Review of International Studies*, 50(1), pp.209–229. doi:https://doi.org/10.1017/s0260210523000013.

Kumalasari, A., Musa, H.G., Garad, A., Emovwodo, S.O. and Aditasari, K. (2024). How Digital Communication Transparency and Public Trust Shape Crisis Communication through Public Engagement. *Komunikator*, 16(2), pp.182–195. doi:https://doi.org/10.18196/jkm.24485.

L'Espresso (2025). *Caso Paragon, Mantovano: 'Tutto quello che si poteva dire è stato detto'. Renzi: 'Se il Papa fosse stato intercettato sarebbe uno scandalo mondiale'*. [online] Lespresso.it. Available at: https://lespresso.it/c/politica/2025/3/4/caso-paragon-mantovano-spionaggio-renzi/53063 [Accessed 18 Aug. 2025].

La Stampa (2007). *'La Cia sapeva che avrei detto no'*. [online] La Stampa. Available at: https://www.lastampa.it/cronaca/2007/01/31/news/la-cia-sapeva-che-avrei-detto-no-1.37136111/ [Accessed 10 Sep. 2025].

La Stampa (2025). *Paragon-governo, contratto rescisso. L'azienda: 'Non hanno voluto cercare la verità'*. [online] La Stampa. Available at: https://www.lastampa.it/politica/2025/06/09/news/caso_paragon_rescisso_contratto_governo_italiano-15183355/ [Accessed 23 Aug. 2025].

Laperruque, J. (2019). *Facing the Future of Surveillance*. [online] POGO. Available at: https://www.pogo.org/reports/facing-the-future-of-surveillance.

Marczak, B. and Scott-Railton, J. (2025). *Graphite Caught: First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted - The Citizen Lab*. [online] The Citizen Lab. Available at: https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/ [Accessed 20 Jul. 2025].

McGreal, C. (2016). *America's former CIA chief: 'If we don't handle China well, it will be catastrophic'*. [online] the Guardian. Available at: https://www.theguardian.com/us-news/2016/mar/09/america-cia-nsa-chief-general-michael-hayden-china-catastrophic-for-world.

Miltimore, J. (2022). *6 Things We Know about the CIA's Secret Mass Surveillance Program | Jon Miltimore*. [online] fee.org. Available at: https://fee.org/articles/6-things-we-know-about-the-cia-s-secret-mass-surveillance-program/.

Mingardi, A. (2025). *Risks and challenges for Italy's Meloni – GIS Reports*. [online] GIS Reports. Available at: https://www.gisreportsonline.com/r/meloni-coalition-risks/.

Montagnese, A. and Neri, C. (2016). *L'evoluzione della sicurezza nazionale italiana*. [online] *Sistema di Informazione per la Sicurezza della Repubblica*, pp.1–59. Available at: https://www.sicurezzanazionale.gov.it/contenuti/levoluzione-della-sicurezza-nazionale-italiana [Accessed 31 Aug. 2025].

Nasi, G. (2025). *Cyber Defense: What Is Missing Is Trust - Bocconi University*. [online] Bocconi University. Available at: https://www.unibocconi.it/en/news/cyber-defense-what-missing-trust.

Naughtie, A. (2025). *Il governo nega di aver spiato illegalmente giornalisti e attivisti*. [online] euronews. Available at: https://it.euronews.com/my-europe/2025/02/13/il-governo-italiano-nega-di-aver-usato-lo-spyware-paragon-per-spiare-giornalisti-e-attivis [Accessed 23 Aug. 2025].

Nojeim, G. and Lorenzo Perez, S. (2025). *Trump's Sacking of PCLOB Members Threatens Data Privacy*. [online] Lawfare. Available at: https://www.lawfaremedia.org/article/trump-s-sacking-of-pclob-members-threatens-data-privacy [Accessed 28 Aug. 2025].

Nowell, L.S., Norris, J.M., White, D.E. and Moules, N.J. (2017). Thematic analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, [online] 16(1), pp.1–13. Available at: https://journals.sagepub.com/doi/full/10.1177/1609406917733847.

Obi, O.C., Odilibe, I.P. and Arowoogun, J.O. (2024). CRISIS COMMUNICATION AND U.S. NATIONAL SECURITY: A COMPREHENSIVE REVIEW: UNDERSTANDING THE IMPORTANCE OF TIMELY AND ACCURATE INFORMATION DISSEMINATION. *International Journal of Applied Research in Social Sciences*, 6(2), pp.116–139. doi:https://doi.org/10.51594/ijarss.v6i2.779.

ODNI (2024). *Annual Statistical Transparency Report Regarding the Intelligence Community'sUse of National Security Surveillance Authorities*. Office of Director of National Intelligence , pp.1–44.

OECD (2023). *Good Practice Principles for Public Communication Responses to Mis-and Disinformation OECD Public Governance Policy Papers N.30*.

OECD (2024). *OECD Survey on Drivers of Trust in Public Institutions 2024 Results - Country Notes: Italy*. [online] OECD. Available at: https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results-country-notes_a8004759-en/italy_ec745ba3-en.html.

Office of Training (1964). *Methods of communicating Intelligence Outside the Intelligence Community*. [online] *CIA (.gov)*, pp.1–19. Available at: https://www.cia.gov/readingroom/docs/CIA-RDP71T00730R000100070072-6.pdf.

Pagella Politica (2025). *Tutti i dubbi che rimangono sul caso Paragon*. [online] Pagella Politica. Available at: https://pagellapolitica.it/articoli/nordio-interrogazione-caso-paragon [Accessed 21 Aug. 2025].

Panagiotopoulos, V. (2024). *ICE Signs $2 Million Contract With Spyware Maker Paragon Solutions*. [online] WIRED. Available at: https://www.wired.com/story/ice-paragon-solutions-contract/.

Panagiotopoulos, V. (2025). *EXCLUSIVE: Spyware firm behind new surveillance of journalists, civil society operates from the EU*. [online] Euractiv. Available at: https://www.euractiv.com/section/tech/news/exclusive-spyware-firm-behind-new-surveillance-of-journalists-civil-society-operates-from-the-eu/ [Accessed 18 Jul. 2025].

Peretti, A. (2025). *Rome and Paragon at odds over spyware termination amid surveillance scandal*. [online] Euractiv. Available at: https://www.euractiv.com/section/politics/news/rome-and-paragon-at-odds-over-spyware-termination-amid-surveillance-scandal/ [Accessed 20 Jul. 2025].

Pew Research Center (2013). *Public Split over Impact of NSA Leak, But Most Want Snowden Prosecuted*. [online] Pew Research Center - U.S. Politics & Policy. Available at: https://www.pewresearch.org/politics/2013/06/17/public-split-over-impact-of-nsa-leak-but-most-want-snowden-prosecuted/.

Pew Research Center (2015a). *Most View the CDC Favorably; VA's Image Slips*. [online] Pew Research Center . Available at: https://www.pewresearch.org/politics/2015/01/22/most-view-the-cdc-favorably-vas-image-slips/.

Pew Research Center (2015b). *Ratings of federal agencies, Congress and the Supreme Court*. [online] Pew Research Center - U.S. Politics & Policy. Available at: https://www.pewresearch.org/politics/2015/11/23/4-ratings-of-federal-agencies-congress-and-the-supreme-court/ [Accessed 23 Aug. 2025].

Pew Research Center (2016). *The state of privacy in post-Snowden America*. [online] Pew Research Center . Available at: https://www.pewresearch.org/short-reads/2016/09/21/the-state-of-privacy-in-america/ [Accessed 23 Aug. 2025].

PiazzaBorsa (2025). *Rapporto Eurispes 2025: cala la fiducia nelle istituzioni, cresce nel Capo dello Stato - PiazzaBorsa*. [online] PiazzaBorsa. Available at: https://PiazzaBorsa.eu/rapporto-eurispes-italiani/ [Accessed 5 Jun. 2025].

Pomerleau, M. (2023). *Authorized strategic intelligence disclosures are likely here to stay, US officials say*. [online] DefenseScoop. Available at: https://defensescoop.com/2023/04/28/authorized-strategic-intelligence-disclosures-are-likely-here-to-stay-us-officials-say/.

Reuters (2014). Italian former spy chief cleared in CIA rendition case. *Reuters*. [online] 24 Feb. Available at: https://www.reuters.com/article/world/italian-former-spy-chief-cleared-in-cia-rendition-case-idUSBREA1N1HZ/.

Richelson, J. (2013). *The Snowden Affair*. [online] nsarchive2.gwu.edu. Available at: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/.

Richelson, J. (2015). *The CIA and Signals Intelligence | National Security Archive*. [online] nsarchive.gwu.edu. Available at: https://nsarchive.gwu.edu/briefing-book/cyber-vault-intelligence/2015-03-20/cia-and-signals-intelligence.

Roberts, D. and Ackerman, S. (2013). *Clapper under pressure despite apology for 'erroneous' statements to Congress*. [online] the Guardian. Available at: https://www.theguardian.com/world/2013/jul/01/james-clapper-apology-congress-erroneous-response [Accessed 16 Aug. 2025].

Ruijer, E. (2017). Proactive Transparency in the United States and the Netherlands: The Role of Government Communication Officials. *American Review of Public Administration*, 47(3), pp.354–375.

Satter, R. (2025). Second Italian journalist targeted with Paragon spyware, watchdog group says. *Reuters*. [online] 12 Jun. Available at: https://www.reuters.com/business/media-telecom/second-italian-journalist-targeted-with-paragon-spyware-watchdog-group-says-2025-06-12/.

Sistema di Informazione per la Sicurezza della Repubblica (2025). *Relazione Annuale sulla Politica della Sicurezza 2025*. [online] *Sicurezzanazionale.gov*, pp.1–76. Available at: https://www.sicurezzanazionale.gov.it/contenuti/relazione-al-parlamento-2025 [Accessed 28 Aug. 2025].

Sistema di informazione per la sicurezza della Repubblica (2015). *Secondo dopoguerra (1948-2007)*. [online] Sicurezzanazionale.gov.it. Available at: https://www.sicurezzanazionale.gov.it/chi-siamo/storia/secondo-dopoguerra-1948-2007 [Accessed 9 Jun. 2025].

Slick, S., Busby, J. and Burns, K. (2019). *Public Attitudes on US Intelligence: Annual Poll Reflects Bipartisan Confidence Despite Presidential Antagonism*. Chicago Council on Global Affairs .

Smith, D. and Roberts, D. (2015). *CIA chief criticises recent surveillance rollbacks in wake of Paris attacks*. [online] the Guardian. Available at: https://www.theguardian.com/world/2015/nov/16/cia-director-john-brennan-criticises-surveillance-reform-paris-attacks [Accessed 7 Aug. 2025].

Statewatch (2012). *Italy: Law reforms intelligence services*. [online] Statewatch.org. Available at: https://www.statewatch.org/news/2007/september/italy-law-reforms-intelligence-services/ [Accessed 29 May 2025].

Stern, L. (1973). *Colby, Helms Deny CIA Foreknowledge of Watergate Entry* . [online] CIA (.gov). Available at: https://www.cia.gov/readingroom/docs/CIA-RDP84-00161R000400210004-3.pdf [Accessed 14 Spring 2025].

Sullivan, A. (2013). More Americans see man who leaked NSA secrets as ‘patriot’ than traitor: Poll. *Reuters*. [online] 12 Jun. Available at: https://www.reuters.com/article/world/more-americans-see-man-who-leaked-nsa-secrets-as-patriot-than-traitor-poll-idUSBRE95B1AF/.

SWG (2025). *Sondaggio politico dell'1 settembre: come andrebbe se si votasse oggi*. [online] TGLA7. Available at: https://tg.la7.it/sondaggi/sondaggio-politico-1-settembre-voto-italiani-01-09-2025-243447?refresh_ce [Accessed 3 Sep. 2025].

Shahaf, T. (2025). *Paragon spyware scandal deepens as Italy faces cover-up allegations*. [online] ynetnews. Available at: https://www.ynetnews.com/article/hj7zeypqlg [Accessed 14 Aug. 2025].

Taylor, P. (2002). Perception Management and the 'War' Against Terrorism. *Source: Journal of Information Warfare*, 1(3), pp.16–29.

The White House (2014). *Remarks by the President on Review of Signals Intelligence*. [online] whitehouse.gov. Available at: https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [Accessed 22 Aug. 2025].

Tyson, A. (2014). *Obama's NSA Speech Has Little Impact on Skeptical Public*. [online] Pew Research Center - U.S. Politics & Policy. Available at: https://www.pewresearch.org/politics/2014/01/20/obamas-nsa-speech-has-little-impact-on-skeptical-public/.

Ucciero, G. (2025). *Caravelli-Mantovano-Ciriani: governo e Servizi attaccano i giornalisti, con querele e minacce di querele*. [online] HuffPost Italia. Available at: https://www.huffingtonpost.it/politica/2025/02/12/news/caravelli-mantovano-ciriani_governo_e_servizi_attaccano_i_giornalisti_con_querele_e_minacce_di_querele-18414277/ [Accessed 20 Aug. 2025].

USAspending.gov (2025). *Paragon Solutions Contract Summary*. [online] Usaspending.gov. Available at: https://www.usaspending.gov/award/CONT_AWD_70CTD024P00000012_7012_-NONE-_-NONE- [Accessed 21 Jul. 2025].

Vergine, S. (2025). *Paragon, fonti ufficiali smentiscono Renzi: 'La penitenziaria non usa lo spyware'. E il governo oppone il segreto*. [online] Editorialedomani.it. Available at: https://www.editorialedomani.it/fatti/paragon-graphite-trojan-polizia-penitenziaria-renzi-smentita-segreto-stato-interrogazioni-parlamentari-akfjlaup [Accessed 18 Aug. 2025].

Vernetti, L.E. (2024). *Italian Intelligence Community: A Deep Dive*. [online] Grey Dynamics. Available at: https://greydynamics.com/italian-intelligence-community-a-deep-dive/#h-7-0-challenges-and-future-directions-for-the-iic [Accessed 21 Jun. 2025].

Visca, A. (2025). Il potere segreto. Wikileaks e la digitalizzazione dell'informazione. Intervista a Stefania Maurizi. *La Rivista di Engramma*, [online] 2025(222). doi:https://doi.org/10.25432/1826-901X/2025.222.0017.

Walton, C., Morrison, N., Miner , M. and Kolbe, P. (2022). *Report: Marking the CIA's 75th Anniversary: Reflections on the Past, Visions of the Future*. [online] Belfer Center for Science and International Affairs. Available at: https://www.belfercenter.org/publication/report-marking-cias-75th-anniversary-reflections-past-visions-future.

Zaremba, A.J. (2015). *Crisis communication : theory and practice*. New York, Ny: Routledge, An Imprint Of The Taylor.

Zegart, A. (2013). *Real Spies, Fake Spies, NSA, and More: What My 2012 and 2013 National Polls Reveal*. [online] Lawfare. Available at: https://www.lawfaremedia.org/article/real-spies-fake-spies-nsa-and-more-what-my-2012-and-2013-national-polls-reveal [Accessed 5 Apr. 2025].