The Architecture of Intimate Power: Seduction, Espionage, and Institutional Compromise Across History

An Independent Historical and Psychological Investigation into Honeypot Operations, Intelligence Acquisition, and the Consequences of Human Vulnerability

Independent Research Thesis

Emmanuelle Di Gallo

November 23, 2026

Independently researched and prepared; not submitted in fulfillment of an institutional degree requirement.

Copyright © 2026 Emmanuelle DiGallo. All rights reserved.

DOI: **10.5281/zenodo.24482572**

Abstract

This independent historical and psychological study traces selected evidence for how intelligence actors have used intimate relationships as routes to information, access, recruitment, leverage, and institutional compromise, and how those practices and their costs changed over time, from early historical records to digital platforms. It asks what conditions made such use possible; how trust, attachment, reciprocity, status, secrecy, stigma, and coercion shaped decisions; how gender and law affected the roles of recruiters, intermediaries, sources, targets, and agents; what information was sought or transferred; what consequences followed; and how digital communication and synthetic intimate material changed these practices.

The thesis uses comparative historical analysis of selected literary narratives, archival records, court proceedings, official inquiries, declassified materials, scholarship, and contemporary reporting. It distinguishes social access from deliberate seduction, recruitment from later exploitation, transfer from intelligence use, and documented fact from allegation or legend. Psychological research informs analysis of general mechanisms but is not used to diagnose historical individuals. Ancient and medieval cases are assessed with period-appropriate standards; modern claims are evaluated against documentary and legal evidence where available.

The evidence supports a qualified conclusion: personal trust and social proximity recur as routes to information and influence, but modern, state-directed sexual entrapment was not an unchanged method across history. Women and men served as agents, sources, intermediaries, targets, and victims, while gender expectations shaped both opportunity and public memory. Courts and inquiries more often establish transfer and punishment than strategic use or policy effect. Digital platforms broaden contact and enable surveillance, sextortion, and synthetic kompromat, yet attribution and state direction still require case-specific evidence. This selective study cannot estimate global prevalence or success rates.

DOI: **10.5281/zenodo.24482572**

Contents

Abstract 2

Contents 3

Chapter 1. Introduction and Research Foundations 8

1.1 Introduction 8

1.2 Research problem and questions 9

1.3 Central argument 10

1.4 Definitions and analytical distinctions 10

1.5 Historiography and related research 11

1.6 Historical scope and case selection 13

1.7 Evidence classifications and source standards 14

1.8 Comparative method and psychological framework 16

1.9 Limitations and ethical commitments 16

1.10 Organization of the thesis 17

1.11 Conclusion 17

Chapter 2. From Story to Record: Intimate Access and Intelligence Before the Modern State 18

2.1 Introduction: continuity without an invented tradition 18

2.2 Method for reading premodern evidence 19

2.3 Antiquity: seduction stories and the political idea of informers 19

2.4 Medieval Europe: mobility, disguise, and paid information 22

2.5 Renaissance Europe: courts, diplomats, and relational intelligence 25

2.6 Seventeenth-century Britain: organized networks and the sexualized afterlife of women's work 28

2.7 The eighteenth century: diplomatic households and political sociability 30

2.8 Comparative analysis: what persists, and what changes 31

2.9 Conclusion 33

Chapter 3. The Psychology of Intimate Influence: Trust, Disclosure, and Coercion 34

3.1 The psychological question 34

DOI: **10.5281/zenodo.24482572**

3.2 What psychological research can establish 35
3.3 Intimacy, disclosure, and perceived responsiveness 35
3.4 Reciprocity, liking, and the limits of social influence 37
3.5 Attachment, belonging, and situational stress 38
3.6 Secrecy, compartmentalization, and the burden of double life 39
3.7 Shame, stigma, and coercive leverage 40
3.8 Motives, agency, and mixed participation 42
3.9 Institutional vulnerability and security culture 42
3.10 The Target Cases Within the Coordinated Operation 43
3.11 Conclusion 44
Chapter 4. Gender, Access, and the Seductress Myth 46
4.1 Gender is a historical condition, not an explanation by itself 46
4.2 Late medieval Europe: women as messengers and intelligence gatherers 47
4.3 Tudor England and Scotland: plausibility, status, and movement 48
4.4 The ambassadress: diplomatic sociability as an information network 49
4.5 Seventeenth-century Britain: the woman agent beyond the courtesan stereotype 49
4.6 Mata Hari and the making of the "spy-courtesan" 50
4.7 Women in the Second World War: access, labor, and operational skill 51
4.8 The Romeo operations: men cultivate women for institutional access 52
4.9 A woman operative targeting a man: the Vanunu capture 53
4.10 Gender inside intelligence institutions 54
4.11 What the history does and does not establish 55
4.12 Comparative questions for the case studies 56
4.13 Conclusion 57
Chapter 5. Europe at War: Intimate Access and Intelligence, 1914-1945 59
5.1 From gendered access to operational evidence 59
5.2 The First World War: intelligence systems and the uses of proximity 59
5.3 Mata Hari: intercepted messages, an execution, and a durable myth 60
5.4 Lizzi Wertheim and Georg Breeckow: a male agent's relationship with a woman 61

DOI: **10.5281/zenodo.24482572**

5.5 Interwar Britain: Olga Gray and the effectiveness of patient social infiltration.... 63

5.6 German intelligence and Hildegard Beetz: a documented effort to win Ciano's confidence 64

5.7 Amy Elizabeth "Betty" Pack and British Security Coordination 66

5.8 Soviet wartime women agents and the limits of the "honey-trap" claim 67

5.9 Comparing operations and outcomes 68

5.10 Institutional consequences and the value of exposure..... 70

5.11 Conclusion: intimacy was one tool within a wider craft 71

Chapter 6. Cold War Recruitment and Compromise: Romance, Blackmail, and State Security 72

6.1 The Cold War as a comparative field 72

6.2 John Vassall: staged exposure, coercion, and years of disclosures 73

6.3 The KGB and same-sex entrapment: operational practice beyond one case 74

6.4 The East German Romeo operations: long-term recruitment through relationships 76

6.5 France: Pierre Chaignot and the penetration of counterintelligence 78

6.6 Maurice Dejean: a reported compromise operation, with recruitment unproven 80

6.7 Clayton Lonetree: romantic recruitment without blackmail 81

6.8 Sharon Scranage and Michael Soussoudis: relationship, threat, and a diplomatic exchange..... 82

6.9 What the cases show about operational design 84

6.10 Institutional responsibility, public exposure, and lasting consequences 85

6.11 Conclusion: intimate access was a method, not an explanation 86

Chapter 7. Capture, Deception, and Kompromat: Israeli, Chinese, Soviet, and Russian Cases 88

7.1 Scope and comparative method..... 88

7.2 Mordechai Vanunu: a romantic lure within a capture operation 89

7.3 Bernard Boursicot and Shi Pei Pu: relationship, recruitment, and uncertain beginnings.....91

7.4 Soviet and Russian *kompromat*: a practice, not a single tactic 94

DOI: **10.5281/zenodo.24482572**

7.5 Yuri Skuratov: intimate material in a political struggle 95
7.6 Comparison: three different uses of intimacy 97
7.7 Findings and limits 98
7.8 Conclusion 99
Chapter 8. Political Access, Corporate Networks, and Contemporary Espionage Claims 100
8.1 Scope and evidence rules 100
8.2 Jonathan Pollard: a documented Israeli espionage benchmark 100
8.3 Christine Fang and Eric Swalwell: access, warning, and limits of the public record 102
8.4 NVIDIA, Alice Huang, and Megaspeed: an unresolved intelligence and corporate-security case 104
8.5 Conclusion 112
Chapter 9. The Digital Honeytrap: Online Intimacy, Sextortion, and Synthetic Kompromat 114
9.1 Scope and definitions 114
9.2 From proximity to platform-mediated intimacy 115
9.3 David Slater: classified disclosure through a dating platform 116
9.4 Saurabh Sharma and the digital false persona 117
9.5 Romance fraud and sextortion: a neighboring threat, not automatically espionage 119
9.6 Synthetic intimacy and the changing meaning of kompromat 120
9.7 Gender, anonymity, and the apparent seductress 122
9.8 What digital operations demonstrably obtain 122
9.9 Institutional and personal consequences 124
9.10 Comparative findings 124
9.11 Conclusion 125
Chapter 10. Comparing Information Gains and Consequences 127
10.1 Purpose of the comparison 127
10.2 A comparative framework for intelligence gain 127

10.3 Cases with documented information transfer 128
10.4 Access, capture, and scandal without demonstrated intelligence gain 132
10.5 Comparison cases outside intimate recruitment 133
10.6 Digital cases and the limits of outcome attribution 134
10.7 What the comparison says about historical change 135
10.8 Personal and institutional consequences are not interchangeable 136
10.9 Why some cases become visible 137
Chapter 11. Findings, Limits, and the Architecture of Intimate Power 138
11.1 The question the thesis can answer 138
11.2 The architecture: from social access to institutional effect 138
11.3 Psychology explains vulnerability without diagnosing the target 140
11.4 Gender shaped the craft and the story told about it 141
11.5 What the cases show about information actually obtained 142
11.6 Consequences were real but unevenly traceable 142
11.7 Limits of this investigation 143
11.8 Final findings 143
Author's Statement 146
References 147

DOI: **10.5281/zenodo.24482572**

Chapter 1.
Introduction and Research Foundations

1.1 Introduction

Intelligence depends on access. Information may be taken from a document, intercepted in transmission, purchased, volunteered, or obtained through a person who can enter a trusted space. Intimate relationships can create such access because they involve attention, confidence, routine, private conversation, and sometimes a willingness to take risks for another person. States and intelligence services have, in particular circumstances, turned those elements into instruments of collection, recruitment, coercion, or influence.

The historical record, however, is not a continuous catalogue of "honey traps." A woman who carried a message was not necessarily a seductress. An affair involving an official did not automatically constitute espionage. A person who passed information to a foreign service may have acted from conviction, money, grievance, affection, coercion, or some combination of motives. A public scandal may have exposed a security risk without proving that an intelligence service designed it. The purpose of this thesis is to identify these distinctions and test the evidence behind each case.

The subject matters because intimate compromise may affect more than the person directly targeted. A relationship can expose identities, documents, routines, access points, vulnerabilities, or institutional relationships. It can also create leverage that changes what a person is willing to disclose or do. Even when no consequential secret is transferred, an operation or accusation may produce professional loss, political instability, public humiliation, diplomatic friction, or lasting damage to an institution's security practices. These outcomes must be demonstrated case by case rather than presumed from the scandalous character of a story.

This independent historical and psychological investigation traces selected evidence for how the use of intimate relationships in espionage changed over time and what costs followed. Its chronology runs from ancient narratives and medieval records through modern institutional operations to contemporary digital manipulation, but it does not attempt a complete history or biography of espionage. The ancient and medieval material provides selected evidence and context for access, information gathering, and political influence; it cannot recover a complete origin story or establish modern intelligence practice unless the

DOI: **10.5281/zenodo.24482572**

sources support that claim. The comparison follows changes in method, institutional conditions, and consequences rather than assuming one continuous technique.

1.2 Research problem and questions

Popular accounts often present the "honey trap" as a timeless and self-evident method. That picture compresses several distinct activities into one dramatic label. It may turn women's ordinary intelligence work into seduction, treat a target's private relationship as proof of recruitment, or equate blackmail with successful intelligence collection. Scholarship on women in espionage has shown that women's actual work included carrying information, maintaining correspondence, gathering military and political intelligence, and operating within formal or informal networks. The eroticized female spy is a recurrent cultural image, but it does not describe the full record (Akkerman 2018; Proctor 2003; Wheelwright 2016).

This thesis asks:

1. Under what historical and institutional conditions have intelligence organizations or political actors used intimate relationships to gain information, access, recruitment, or leverage?
2. What psychological and social mechanisms help explain why people in positions of authority may trust, protect, or cooperate with intimate partners, and how did coercion, stigma, status, secrecy, or emotional attachment shape those decisions?
3. How have women and men operated as recruiters, intermediaries, sources, targets, and agents, and how have laws and gender expectations shaped their opportunities and risks?
4. What information was actually sought, transferred, recovered, or judged useful, and what evidence supports claims that an intimate relationship influenced a political, military, corporate, or institutional decision?
5. What personal, institutional, financial, diplomatic, and geopolitical consequences followed, and why do some cases become public while others remain hidden?
6. How have digital communication, social media, online relationship manipulation, sextortion, surveillance, and synthetic intimate material changed the acquisition and use of compromising information?

The questions are comparative. They do not assume that an intimate operation always succeeds, that intelligence value can be measured in a single unit, or that a relationship necessarily affects policy. In some cases the operation may have been designed to collect secrets. In others, the relationship may have begun without intelligence direction and later been exploited. In still others, the security significance may lie principally in exposure, public response, or later mythmaking.

DOI: **10.5281/zenodo.24482572**

1.3 Central argument

This thesis argues that private intimacy has periodically served as a channel through which information, access, influence, and coercive leverage move between individuals and institutions. The operational forms have varied across time. The historical record does not support an unbroken, universal practice called the "honeypot." It instead reveals recurring opportunities created by personal trust and social proximity, combined with different forms of deliberate recruitment, seduction, blackmail, coercion, or political influence.

The thesis further tests whether public memory has disproportionately sexualized women's intelligence work. Cases such as Mata Hari became powerful cultural symbols, while women's less sensational work as couriers, correspondents, informants, and organized agents has often received less attention. At the same time, male agents have used romantic relationships to recruit women, as in the East German Romeo operations, and men have been targeted through same-sex entrapment and the threat of legal or social exposure. The inquiry therefore treats gender as an operational and historical factor, not as an assumption that women alone used seduction or that men alone were targets (Akkerman 2018; Huneke 2023; Proctor 2003; Roldugina 2025).

The evidence supports this argument only in a qualified form. Several modern operations establish deliberate romantic recruitment, sexual compromise, or coercive use of private material. Earlier cases establish a longer history of information moving through social and intimate access, but do not show that the modern operation existed unchanged across centuries. The thesis therefore separates historical continuity in access from the period-specific design of sexual entrapment.

1.4 Definitions and analytical distinctions

The language of intimate espionage is unstable. Terms such as "honey trap," "sexpionage," "romantic recruitment," and *kompromat* are used differently across agencies, countries, periods, journalism, and popular culture. This thesis uses the following working definitions.

Intimate intelligence refers to information collection or access obtained through an emotional, romantic, sexual, familial, or otherwise private relationship. The term describes a channel of access, not proof that the relationship was deliberately engineered.

Seduction operation refers to a planned effort to create or exploit romantic or sexual attraction for an intelligence, recruitment, influence, or coercive purpose. A relationship qualifies only when evidence supports the intent or subsequent intelligence use.

Honey trap refers to a staged or deliberately cultivated sexual or romantic situation intended to compromise, recruit, manipulate, or obtain information from a target. Because the term can carry sensational or anachronistic meanings, it is not applied automatically to historical cases.

Romantic recruitment describes the use of an actual or constructed romantic relationship to persuade a person to provide information or other assistance. The recruited person's feelings may be genuine even when the operative's identity or purpose is concealed.

Sexual entrapment and blackmail describe the creation or exploitation of compromising sexual material or circumstances to threaten exposure, punishment, professional loss, or legal consequences. The threat may precede cooperation, follow an independently initiated relationship, or operate alongside other forms of pressure.

Kompromat means compromising material collected or used to exert pressure, discredit, or influence. It is not treated as a synonym for every affair, leaked image, or intelligence operation. Each claim requires evidence about who collected the material, for what purpose, and how it was used.

Institutional compromise includes demonstrated exposure of protected information, personnel, facilities, decision processes, or security weaknesses. It may also include a documented attempt to influence decisions or behavior. The term does not imply that the attempt succeeded.

These definitions keep several questions separate: Was there a relationship? Was it intelligence-directed? Was information transmitted? Was the information useful? Did it affect a decision? Each question requires its own evidence.

1.5 Historiography and related research

The scholarship reviewed here addresses essential parts of the subject, including women's intelligence work, early modern information networks, sexuality and state surveillance, intelligence recruitment, and digital coercion. This thesis brings those lines of research into a comparative account across historical periods and operational forms; it does not claim that the subject has never been studied.

Research on women's espionage corrects the tendency to reduce female agents to sexual stereotypes. Nadine Akkerman reconstructs women's political and intelligence work in seventeenth-century Britain, while Tammy M. Proctor examines women's varied contributions to British intelligence during the First World War. Julie Wheelwright's analysis of Mata Hari

traces how wartime and postwar accounts helped produce the “spy-courtesan” image. Together, these studies support a distinction between the work women performed and the meanings later attached to their sexuality (Akkerman 2018; Proctor 2003; Wheelwright 2016).

The literature review also draws on research into early modern intelligence. Ioanna Iordanou’s study of Renaissance Venice examines intelligence as an organized state activity and draws attention to networks of informants, officials, merchants, and intermediaries. Her work also notes the limits of the surviving evidence for women’s intelligence activities. The broader early modern scholarship places information gathering within diplomacy, patronage, travel, commerce, and political competition. These settings are relevant because personal access could matter without constituting a seduction operation (Iordanou 2019; Marshall 2015).

Cold War scholarship helps explain how sexuality could become an instrument of both intelligence and social control. Samuel Clowes Huneke examines gay informants and surveillance in divided Berlin, complicating accounts that treat queer identity only as a vulnerability. Irina Roldugina’s archival study documents Soviet KGB same-sex entrapment operations and the use of criminalization as leverage. Jordyn Bailey’s dissertation examines the Stasi’s surveillance of prostitution and sexual behavior, while Isabel J. Blaylock’s undergraduate thesis studies the federal surveillance and weaponization of sex in Cold War America. These works are related but do not, individually, provide the long comparative history pursued here (Bailey 2024; Blaylock 2025; Huneke 2023; Roldugina 2025).

Research on the early People’s Republic of China is also relevant because it studies both claims of female-agent “honey traps” and the political uses of those narratives. Amanda Zhang’s study examines internal reports and public narratives about female agents, showing why accusations themselves must be investigated as part of state practice and culture (Zhang 2023).

The review also includes Stephanie A. Bloomer’s master’s capstone on susceptibility to honey-trap operations. Its focus on high sensation-seeking and special-operations settings makes it a useful lead for reviewing vulnerability research, not a substitute for historical or clinical evidence about individual cases (Bloomer 2016).

Research directly testing interpersonal mechanisms in intelligence recruitment is comparatively limited. Neequaye and Granhag’s experiment found that a shared experience could increase felt closeness and perceived opportunity for social connection, but found little evidence that these changes increased commitment to an intelligence arrangement. This result cautions against treating attraction or rapport as a sufficient explanation for cooperation. Contemporary scholarship on sextortion likewise describes a broad range of contexts and reports serious harms alongside low rates of disclosure and help-seeking, while emphasizing

that the empirical evidence base remains small (Neequaye and Granhag 2024; Ray and Henry 2025).

Related theses and dissertations also address narrower parts of the field. Arghawan Farsi and Luděk Michálek study contemporary Iranian "swallow" narratives and reported honey-trap practices, while Amanda Zhang's doctoral thesis examines women's clandestine work and spy narratives in China before and after 1949. These projects demonstrate that scholarship already exists on specific national and gendered dimensions. The present thesis asks a broader comparative question across periods, regions, operational forms, and demonstrable institutional outcomes; it does not claim that intimate espionage has never been studied (Farsi and Michálek 2023; Zhang 2021).

The literature review draws on intelligence history, gender history, diplomatic history, social psychology, research on coercion and digital abuse, and the history of sexuality. It is scoped to the thesis questions and case register, rather than presented as an exhaustive review of every national literature.

1.6 Historical scope and case selection

The thesis uses a long chronology to examine historical change, but applies period-appropriate evidentiary standards. Ancient stories such as Delilah and Samson can be examined as cultural narratives about desire, trust, disclosure, and betrayal. They cannot establish that a state organized a sexual intelligence operation. Medieval accounts of female scouts or couriers may demonstrate women's participation in intelligence gathering without demonstrating seduction. The distinction is necessary if the thesis is to make a credible claim about continuity.

The medieval and early modern cases show information gathering through gendered mobility, household and court access, diplomacy, and social networks. Examples include Margoth's reported reconnaissance at Kenilworth in 1265, women's intelligence and courier work around Ypres in 1488–1489, seventeenth-century British women intelligencers, Venetian networks, and Aphra Behn's Restoration mission (English Heritage n.d.-b; Demets and Haemers 2025; Akkerman 2018; Iordanou 2019; Marshall 2015). These cases provide historical context. They are not automatically examples of intimate manipulation.

The nineteenth and twentieth centuries provide a stronger record of intimate political influence, compromise, recruitment, and prosecution. The Countess of Castiglione's role in the court of Napoleon III is relevant to intimacy and political influence, though it is not established as a secret-stealing operation (Metropolitan Museum of Art n.d.). Mata Hari's trial and

execution are central to the study of sexualized espionage narratives, while the intelligence she actually passed remains disputed. Cold War cases such as John Vassall, the East German Romeo operations, Sharon Scranage, Clayton Lonetree, Maurice Dejean, Pierre Chaignot, and the Vanunu capture operation provide a varied record of recruitment, coercion, information transfer, and exposure.

The contemporary cases include Christine Fang and Eric Swalwell, the reported U.S. intelligence assessment concerning Alice Huang and Jensen Huang, and online relationship manipulation, sextortion, and synthetic intimate material. These cases are not treated as interchangeable. U.S. media have reported intelligence indicating that Chinese intelligence recruited Alice Huang, alongside official statements that the U.S. government had not reached a final conclusion. Reuters reported on November 14, 2026 that it could not independently verify the spying allegations. The analysis examines the reported intelligence assessment and related case while separately evaluating the alleged operational objective, claims concerning the woman's husband and sister, any information obtained, and consequences. Reuters reported on November 16 that Singapore's investigations into Megaspeed continued without a public finding that the company had violated export rules (Reuters 2026a; Reuters 2026b).

Case selection is purposive. Cases are included because they illuminate one or more of the following: a documented intimate recruitment method; a notable institutional response; a major cultural or political accusation; a well-documented alternative mechanism; or a contemporary change in the means of compromise. The cases were selected when credible primary or scholarly sources established their relevance to the research questions. Inclusion does not mean that an allegation has been proven. The purpose is not to provide a complete biography of espionage, a comprehensive global catalogue, or an equally detailed record for every period. It is to compare how the intelligence use of personal relationships evolved and what human, institutional, political, financial, diplomatic, and geopolitical costs followed. Ancient and medieval cases offer early evidence and context where surviving records permit, not a fully recoverable account of espionage's origins. Modern cases allow more detailed reconstruction of institutional recruitment and information transfer, while digital cases show how those channels change under networked communication. Conclusions remain limited to this sample and the public record reviewed.

1.7 Evidence classifications and source standards

Each case is classified according to the following evidence categories:

A. Documented intelligence-directed operation. Reliable records establish intelligence direction or recruitment and support the relevant intimate mechanism.

B. Strongly supported but partly disputed operation. The operation is credible, but important details, attribution, or outcomes remain contested.

C. Reported allegation or intelligence assessment. Credible reporting identifies an intelligence claim, but the public evidence does not independently establish all operational details.

D. Security-relevant scandal or influence effort. The case has security, political, or institutional consequences, but no intelligence-directed honeypot is established.

E. Historical legend or contested interpretation. The case matters to the history of espionage narratives, but its operational meaning or evidence is uncertain.

Classification applies to a specific claim, not necessarily to every aspect of a case. A person may have been convicted of espionage while the claim that an intelligence service engineered the relationship remains disputed. Likewise, an operation may be documented even when the amount or value of information transferred is unknown.

The source hierarchy prioritizes archival files, court records, official inquiries, parliamentary records, declassified documents, contemporary correspondence, and intelligence-service records, with attention to the circumstances in which those records were produced. Scholarly books and articles establish context and historiography. Credible journalism provides original reporting, access to records, or documented accounts of current events. Memoirs, popular histories, and later retellings are treated as leads unless corroborated. The organization of the project also follows Umberto Eco's practical guidance to define a research problem, delimit its scope, identify usable sources, and make the method visible. Eco is a guide to thesis construction here, not the authority for the historical findings or a substitute for independent verification (Eco 2015).

For each case, the research record distinguishes four quantities: what an actor sought, what the target transmitted, what investigators later recovered, and what analysts assessed as useful. These quantities are not interchangeable. This thesis does not calculate an overall success rate without a defensible denominator, and it does not infer policy influence from timing alone.

DOI: **10.5281/zenodo.24482572**

1.8 Comparative method and psychological framework

The method is comparative historical analysis. Each dossier follows the same questions about actors, institutions, relationship formation, information sought and transferred, evidence, exposure, consequences, and competing interpretations. The resulting comparison can identify recurring mechanisms without claiming that operations in medieval courts, Cold War embassies, and online platforms are identical.

Where sources permit, the analysis uses process tracing: reconstructing how contact began, what access followed, when intelligence personnel became involved, what requests were made, what information moved, and how the operation was discovered. The purpose is to establish sequence and causal connection, not to infer causality from a relationship alone. Claims that an operation altered a political, military, corporate, or institutional decision require specific evidence of the decision process and the relationship's role in it.

Psychological analysis is cautious and non-diagnostic. It examines documented mechanisms such as trust, emotional attachment, reciprocity, validation, status, loneliness, secrecy, shame, fear of exposure, coercion, and the perceived cost of refusing. These are analytical categories, not retrospective diagnoses. An experimental HUMINT study found that shared experiences can increase felt closeness without necessarily increasing commitment (Neequaye and Granhag 2024). This finding supports a distinction between an emotional response and an operational outcome. Individual behavior may reflect several motives at once, and public accounts may overemphasize personal weakness while minimizing institutional failures, legal vulnerability, or deliberate coercion.

The analysis also distinguishes attraction from deception and deception from coercion. A relationship that begins voluntarily may later become a means of blackmail. A target may provide information without recognizing the intelligence purpose. An operative may develop genuine feelings that complicate the operation. These possibilities should be evaluated from the evidence rather than assumed.

1.9 Limitations and ethical commitments

The record is uneven. Intelligence files may remain classified, be destroyed, or preserve only the service's own interpretation. Court proceedings may reveal the charge and prosecution strategy while omitting sensitive operational details. Memoirs and defector accounts can contain unique information but may also reflect self-interest, memory, or political motive. Historical archives disproportionately preserve the activities of people whose communications and actions were recorded by institutions. The absence of a surviving file

therefore does not prove that an operation did not occur, but neither does archival silence justify inventing one.

The thesis uses “spy,” “agent,” “informant,” and related terms with attention to historical context. It does not assume that a person’s sexuality, gender, occupation, or relationship constitutes evidence of espionage. It avoids presenting intimate details that do not materially explain the operation or its consequences. Where allegations concern living people or recent events, claims are attributed to their sources and separated from established findings.

1.10 Organization of the thesis

The thesis is organized from research foundations and historical evidence to comparative analysis and findings. Chapter 2 examines ancient, medieval, Renaissance, and early modern precedents, distinguishing cultural narratives from documented intelligence. Chapter 3 considers intimacy, trust, coercion, and vulnerability. Chapter 4 examines gender, sexuality, social access, and operational roles. Chapter 5 treats European intelligence before and during the World Wars, including the limits of claims about Soviet wartime operations. Chapter 6 compares Cold War recruitment and compromise, including Vassall, the Romeo operations, KGB entrapment, and selected British, American, French, and East German cases. Chapter 7 examines Israeli, Chinese, Soviet, and Russian cases, including the Vanunu operation, Boursicot and Shi Pei Pu, and uses of *kompromat*. Chapter 8 analyzes contemporary political and corporate access, including the Fang and Swalwell case and the reported Alice Huang intelligence assessment. Chapter 9 studies online relationship manipulation, sextortion, digital surveillance, and synthetic intimate material. Chapter 10 compares information gains and consequences. Chapter 11 presents the findings, limitations, and conclusion.

1.11 Conclusion

Chapter 1 establishes the thesis’s central distinction: social and intimate access recur across history, while deliberate sexual entrapment is a more specific practice whose evidence varies by period. The remaining chapters apply the same questions to different records: who created access, what was sought and transferred, what was used, what changed, and what consequences can be traced.

DOI: **10.5281/zenodo.24482572**

Chapter 2.
From Story to Record: Intimate Access and Intelligence Before the Modern State

2.1 Introduction: continuity without an invented tradition

The earliest material reviewed here comes in two unlike forms: narratives that imagine sexual betrayal as political strategy, and records that document information gathering through people with social or physical access. The first cannot confirm an operation; the second can show specific tasks. This chapter follows that uneven record from antiquity through the eighteenth century, tracing how information moved through households, court service, diplomacy, correspondence, travel, and patronage.

Rather than project modern tradecraft backward, the chapter asks what its period sources reveal: how access was obtained, what made a person useful, how information travelled, what incentives or risks shaped participation, and what can be demonstrated about results.

The evidence falls into different categories. Religious and literary narratives reveal cultural ideas about seduction, betrayal, and secret knowledge, but they do not by themselves establish historical operations. Political treatises can show that writers understood informers and spies as instruments of rule, but they are not operational files. Medieval chronicles and account books offer evidence of specific people and payments, yet the distance between an event and its surviving account must be measured. Early modern correspondence, state papers, and intelligence instructions offer a more direct view of organized activity, though their survival remains selective. These materials cannot be collapsed into a single category of "sex espionage."

The chapter's central finding is therefore qualified but significant: across many centuries, private and social relationships created channels for intelligence, and women repeatedly used, were assigned, or were accused of using those channels. The strongest continuity lies in access and information movement. The evidence for state-directed seduction is narrower, varies by period, and must be demonstrated case by case. The record also complicates the familiar assumption that the woman spy was principally a temptress. In many documented cases, the operative craft consisted of observation, mobility, correspondence, translation, memory, coded communication, local knowledge, and the cultivation of trust.

DOI: **10.5281/zenodo.24482572**

2.2 Method for reading premodern evidence

The evidence classifications introduced in Chapter 1 apply here with one additional caution: an ancient or medieval text can be evidence that a story circulated, while remaining weak evidence that the events occurred exactly as narrated. A classification describes the claim supported by surviving sources, not the truthfulness or moral character of a person.

The chapter distinguishes four questions. Did the relationship or contact occur? Was it deliberately organized for intelligence purposes? Was information actually passed? Can the information or leverage be connected to a decision or measurable consequence? A source that answers one question does not automatically answer the others. For example, a record that a woman carried a sealed letter establishes communication; it does not establish that she seduced its recipient. A text that tells of a lover reporting political speech may preserve an ancient motif, but without corroboration it does not prove a service-directed operation.

The word "spy" is also historically unstable. Latin terms such as *explorator* and *exploratrix* could refer to scouts, agents, or people who investigated conditions. Early modern references to "intelligencers" and "espials" likewise covered different tasks. This chapter uses "intelligence work" broadly for organized or purposeful acquisition and communication of political, military, or institutional information. It reserves "seduction operation" for cases where a deliberate romantic or sexual purpose is evidenced.

Finally, the surviving archive is shaped by power. Officials paid for particular tasks; chroniclers recorded episodes that served their narratives; court correspondence preserved the concerns of elites; and women's routine work often went unrecorded. Archival silence cannot prove that women were absent. It also cannot serve as permission to fill gaps with speculation. The responsible approach is to mark what is visible, what is plausible, and what remains unknown.

2.3 Antiquity: seduction stories and the political idea of informers

2.3.1 Delilah and Judith as cultural narratives

The Hebrew Bible's story of Delilah and Samson is one of the best-known narratives in which an intimate relationship becomes a route to military advantage. In Judges 16, Philistine leaders offer Delilah money to discover the source of Samson's strength. She presses him for the secret, learns it, and tells the Philistine rulers, who seize and blind him. The text presents an explicitly paid betrayal within a sexualized relationship. It is a literary and religious narrative, however, not a case file. The historicity of the episode cannot be independently established

from the biblical account, and the text does not describe a modern intelligence organization or a continuing collection program. Its value for this thesis is evidence of a durable narrative structure: intimacy can be imagined as a vulnerability that exposes a powerful man and transfers advantage to a political opponent (Judges 16:4-21).

The Book of Judith presents a related but different pattern. Judith enters the camp of the Assyrian commander Holofernes, uses her appearance and speech to gain access, and kills him. The narrative combines deception, intimacy, and military action, but its decisive result is assassination, not the transfer of secrets. Its historical setting and composition have long been debated; it should therefore be treated as a religious and political story rather than proof of an actual operation (Judith 10-13; Miller 2014). The distinction matters. In later retellings, seduction, spying, assassination, and intelligence collection can blur into one "honey trap" image even when the underlying narratives describe different ends.

Both stories demonstrate that ancient audiences could understand sexuality and private trust as political instruments. They do not establish that states routinely organized such operations. They belong in the thesis as evidence about cultural imagination and the gendered moral language attached to information, not as verified intelligence cases.

Consequences within the narratives are explicit, but they are not historical case outcomes. In the Book of Judges, Samson is captured, blinded, and imprisoned after Delilah obtains the source of his strength; he later dies when he brings down the Philistine temple. In Judith, Holofernes is killed and his army withdraws, relieving the threat to Bethulia. The texts do not identify real intelligence targets or establish consequences for historical families. These are literary outcomes, not evidence of an actual operation. (Judges 16; Judith 13-16.)

2.3.2 Aristotle's account of surveillance in Syracuse

In Politics, Aristotle discusses methods tyrants used to learn what their subjects said and did. He refers to women at Syracuse whom Rackham translates as "provocatrices" and Jowett as "female detectives," alongside men whom Hiero sent to listen at gatherings (Aristotle, Politics 5.11, 1313b; Aristotle 1885; Aristotle 1944). The translation affects how the women's role is understood: one rendering suggests that they prompted speech, while the other suggests an investigative role. Aristotle describes them as spies but names no women or specific mission. The passage records his account of tyrannical surveillance; it does not independently verify a particular operation.

The passage places women's intelligence work within surveillance and political control. Aristotle emphasizes proximity: a person who can attend conversations, prompt disclosure, or

report what is heard can extend a ruler's knowledge. His account also identifies the effect of surveillance on behavior. Fear of informers makes people speak less freely. This is an early formulation of a problem that recurs in later intelligence systems: collecting information can itself change the conduct of the people being watched.

Frank Santi Russell's study of information gathering in classical Greece places espionage within a broader system that included military observation, scouts, messengers, informants, and the evaluation of reports (Russell 2000). Jennifer Martinez Morales's study of women and war cautions against treating women as one uniform group or assuming their wartime contributions were always exceptional. She documents varied participation, including forms of support, advice, resistance, and betrayal, while also emphasizing the limits and rhetorical purposes of ancient sources (Martinez Morales 2015). Together these works support a restrained conclusion: ancient writers knew that information could be gathered through human access, and at least one political account associated women with surveillance. The sources do not support a claim that ancient states maintained a formal corps of female seduction agents.

Consequences for the people being watched cannot be traced individually. Aristotle names no subjects who were arrested, punished, dismissed, exiled, or harmed because of reports from the women at Syracuse or Hiero's listeners. The consequence he does identify is collective and behavioral: fear of being overheard made people speak less freely and made those who did speak more likely to be noticed. This supports a finding about the chilling effect Aristotle attributed to tyrannical surveillance, not a claim about the known fate of particular targets. The passage gives no information about consequences for their families. It also describes a political method and its intended effect; it does not independently verify how often or how systematically the practice was used.

2.3.3 Antigone and Philotas: a reported relationship turned into surveillance

Plutarch's *Life of Alexander* contains a more specific account. Antigone, a captive woman and the lover of Philotas, reportedly repeated his insulting remarks about Alexander to an acquaintance. The story passed through other people until it reached Craterus. Alexander then ordered Antigone to continue meeting Philotas and report what she learned from him (Plutarch, *Alexander* 48.4-49.1). In Plutarch's account, a private relationship became a channel for information after Alexander formalized the reporting. The material concerned Philotas's speech and loyalties, not a broad cache of military secrets. Plutarch links this episode to the later political crisis surrounding Philotas and a plot against Alexander, but the narrative does

not quantify intelligence gained or isolate the effect of Antigone's reports on the eventual punishment.

This is among the clearest ancient narratives of a ruler exploiting an intimate relationship to monitor a powerful man. It remains a retrospective literary account. Plutarch wrote centuries after Alexander's campaigns, and the episode is not independently corroborated by surviving operational records. The proper classification is E, a contested interpretation, not A, a documented intelligence-directed operation. It preserves an early version of the motif and a plausible account of a mechanism, but it does not prove that the event unfolded precisely as told.

The case also resists a simplistic account of female agency. Antigone first appears as a captive and lover whose words circulate informally. Alexander's order changes her role by directing her to continue the meetings for surveillance. The source does not tell us whether she acted willingly, under pressure, or with mixed motives. It gives no basis for diagnosing her psychology. Its evidentiary value is strongest for how ancient biography could frame intimacy as a tool of royal control.

Consequences in Plutarch's account were severe, but the causal link to Antigone's reports is uncertain. Plutarch says Philotas was later arrested, tortured, and put to death amid accusations connected to a separate conspiracy against Alexander. Alexander also ordered the execution of Philotas's father, Parmenio. The account does not establish that Antigone's reports caused or decided either execution. It gives no further information about Antigone's fate after her reporting role. Her later personal consequences are therefore unknown. (Plutarch, Alexander 49.3-7.)

2.4 Medieval Europe: mobility, disguise, and paid information

2.4.1 Early royal service and Alice of Saintes

Medieval evidence is fragmentary, but it shows that rulers could employ people designated as scouts or informants. English Heritage's survey of medieval espionage cites royal financial records for an early thirteenth-century French woman, Alice of Saintes, who travelled to England around 1209 in King John's service and reported what she learned. The same survey notes that royal accounts used *exploratrix*, a feminine form related to a term for scout or agent (English Heritage n.d.-b). This is evidence of a woman's reported intelligence service, but the public summary does not establish that her work involved seduction or disclose what information she obtained. The available evidence supports a provisional B classification for the reported service because the modern synthesis points to royal accounts, while the underlying

entry still needs direct examination. The intimacy question is not applicable on present evidence.

Alice's significance lies partly in what she is not. She is not a known "honey trap." The surviving description presents travel and reporting. Including her prevents the history from being reduced to sexualized operations and reveals a wider craft built around the ability to cross boundaries and observe conditions. It also raises a recurring archival question: when payment records identify a task but not its content, the service may be documented while its intelligence value remains unmeasurable.

The consequences of Alice's service, and of any information she reported, are unknown. The cited account gives no named targets, report contents, resulting action, or record of Alice being rewarded, exposed, punished, or otherwise affected. It also provides no information about her family. The available evidence therefore supports no claim about personal fallout for Alice or consequences for the people she may have reported on. This is an archival gap, not proof that there were no consequences. (English Heritage, "Margoth.")

2.4.2 Margoth at Kenilworth

The account of Margoth concerns the 1265 conflict at Kenilworth. Walter of Guisborough, writing about fifty years after the events, states that Prince Edward learned of the vulnerability of Simon de Montfort the Younger's position through a spy named Margoth, who was a woman wearing men's clothing, and through Ralph of Ardern, who betrayed his comrades. Henry of Knighton later repeated the account. Other chronicles mention spies or deception surrounding the episode, but only Walter and the derivative account name Margoth (English Heritage n.d.-b).

This source pattern is mixed. The broader presence of espionage or deception receives support from several accounts. Margoth's name and disguise rest on a narrower tradition, and the principal named account is retrospective. The broad episode of intelligence or deception is strongly supported, while the identity and method attributed to Margoth remain contested. This chapter treats the named-agent details as provisional, rather than as a fully corroborated operational record. It is not an intimate operation. It is a report of disguise and tactical intelligence.

Margoth is revealing because the chronicle makes gendered disguise part of the surprise. The Latin shift from *explorator* to *exploratrix* marks the spy's sex as noteworthy to the writer. The story has often been repeated as evidence that a woman's gender allowed her to move undetected. That interpretation is plausible, but the source does not tell us how she gained

access, what she observed, or whether her clothing was decisive. The chapter therefore treats disguise as a reported method, not as an established general rule about medieval women's invisibility.

The immediate consequences are clearer than Margoth's later fate. The surprise attack routed the rebel force at Kenilworth. Simon de Montfort the Younger escaped into the castle, while many of his barons and bannerets were captured. Three days later, Edward defeated and killed Simon the Elder at Evesham, a major blow to the rebellion. The chronicles connect intelligence and deception with Edward's surprise, but they do not establish that Margoth's report alone caused these outcomes; Ralph of Ardern's betrayal and other sources of information are also part of the account. The sources cited here do not record what happened to Margoth afterward, including whether she was rewarded, exposed, or punished, or what happened to her family. (English Heritage n.d.-b; Victoria History of the County of Bedford, "Political History.")

2.4.3 Women's intelligence during the Hundred Years War and the Flemish Revolt

Military records from the Hundred Years War show women in roles that could gather, carry, or transmit information. Anne Curry's research on soldiers' wives describes women moving through military environments, seeking prisoners, and passing information. In one instance from 1435, an English lieutenant at Evreux sent two women to several towns to seek prisoners and information about the army of Jean, Count of Dunois. Another account records a woman travelling with a man to observe enemy activity. These examples belong to the practical work of reconnaissance, communication, and access. They do not establish romantic recruitment (Curry 2009).

City accounts from the late fifteenth-century Flemish Revolt provide stronger collective evidence. Drawing on the city accounts of Ypres and related records, Lisa Demets and Jelle Haemers show women moving between Ghent, Ypres, Bruges, and military camps during the conflict with Maximilian of Austria in 1488-89. The accounts distinguish some letter-delivery tasks from the conveyance of information. Demets identifies 38 named women who performed one or more tasks for Ypres during the period, while noting that others remain anonymous. Some women received repeated assignments, a pattern the article describes as growing professionalization in a more structured intelligence effort by 1489 (Demets and Haemers 2022; Demets 2025, 632-34).

These records make a useful comparison with later intelligence systems. The tasks were paid or institutionally commissioned, but the boundaries between courier work, observation, and intelligence were not always sharp. The city's need for information during war created

demand; women's movement and social position could make them useful intermediaries; and repeat assignments could turn ad hoc activity into a recognizable service. The documents do not indicate that these women were recruited through sexual relationships. Their importance is precisely that a long history of women's intelligence work exists outside the seduction narrative.

Consequences for individual women and the people they reported on cannot be reconstructed from the city accounts**.** The records document assignments, payments, travel, and repeated service, but do not link a named woman's report to a specific punishment, military decision, or family outcome. The archive therefore establishes that the work was commissioned and remunerated, while the personal aftermath for the agents and the downstream consequences for reported subjects remain unknown. (Demets and Haemers 2022; Demets 2025.)

2.5 Renaissance Europe: courts, diplomats, and relational intelligence

2.5.1 Venice and the limits of the "courtesan spy" story

Sixteenth-century Venice developed a comparatively organized state intelligence apparatus. Ioanna Iordanou shows how the Council of Ten used ambassadors, governors, merchants, professional agents, and informants to gather and report information across a wide geography (Iordanou 2019). Women's role in this system is less fully documented, partly because surviving records and social structures made their activity difficult to see. A contemporary review of Iordanou's book notes examples of Chirana, who acted as an intermediary between Venetian authorities and Nurbanu Sultan, and Beatrice Michiel, who supplied intelligence on Ottoman political, diplomatic, and military affairs in hopes of improving her sons' prospects (Iordanou 2019; Rushton 2021, 244-46).

These examples show women acting as intermediaries and informants within trans-imperial networks. They do not establish that Venice maintained a large corps of prostitutes or courtesans deployed to seduce targets. Iordanou has emphasized that firm evidence for such a general claim is limited. The popular image of the Venetian courtesan as a state spy is more familiar than the documentary record warrants. The cases that can be named show that women could provide information because of their social and familial position, incentives, and access, without requiring an erotic operation.

The Venetian evidence helps separate the institutional architecture of intelligence from its sexualized legend. The state could organize reporting, provide incentives, and use intermediaries. Women's documented value came through their relationships and mobility, but

DOI: **10.5281/zenodo.24482572**

the available examples do not make romantic manipulation the method. The operation's gender dimension is therefore not a simple story of seduction. It includes access, patronage, information brokerage, and strategic self-interest.

The consequences are documented unevenly. The Council of Ten sent Chirana payments and gifts, including cash and household goods, for acting as an intermediary between Nurbanu Sultan and Venice. This establishes a material reward for her service. Beatrice Michiel supplied intelligence partly in the hope that Venice would favor her sons, but the cited account does not establish whether they received that favor. It identifies no person punished as a result of the intelligence either woman supplied and does not document legal or personal fallout for either woman. Those outcomes remain unknown in the sources used here. (Iordanou 2019, 177-89; Rushton 2021, 244-46.)

2.5.2 Tudor England and gendered plausibility

Recent research on women's military intelligence under the Tudor regimes examines correspondence and state papers from roughly 1509 to 1603. Samantha Nelson argues that women should not be categorized as automatically "above suspicion." Instead, they could use or negotiate gender and social expectations to create different degrees of plausible deniability. The records show women as intelligence gatherers, transmitters, and nodes in communication networks, while also documenting that some women were suspected or punished (Nelson 2025).

This revises an easy but misleading claim that women were naturally invisible to authorities. Gender could shape how a person was searched, questioned, trusted, or accused, but it did not confer universal immunity. Rank, marital status, legal identity, local reputation, and the nature of the conflict also mattered. A woman's ability to move through an environment could be an operational resource; the same movement could expose her to interrogation and severe consequences. This is a historical mechanism relevant to intimate intelligence because it concerns how social expectations structure access. It is not evidence that Tudor women generally seduced their targets.

The documented personal consequences vary, and the record is incomplete. Nelson identifies a Scottish woman who, with two men, was executed in 1548 after conviction for providing military intelligence to the English. A different Scottish woman, captured and questioned in 1525, is unnamed; the surviving source does not reveal whether she was punished or what later became of her. Nelson also discusses how rank and marital status may have affected women's exposure to punishment, but the evidence does not establish family

consequences for these individuals. The study does not trace specific consequences for the people or forces they reported on. (Nelson 2025.)

2.5.3 Mary Beaton and Thomas Randolph: an intimate channel with two-way interests

The Anglo-Scottish diplomacy of the 1560s provides a more directly intimate example. V. Smith's study of the diplomats Nicholas Throckmorton and Thomas Randolph describes the political networks surrounding Mary, Queen of Scots. Randolph's relationship with Mary Beaton, one of the queen's attendants, has been discussed as a possible channel through which information moved between the English diplomat and the Scottish court. Smith's analysis presents the relationship as potentially two-way: Randolph could gain access and information, while the court could also use the relationship to influence or assess him (Smith 2024).

This case does not prove a centrally directed seduction operation. It shows how intimate relations could exist within a diplomatic environment where personal ties, political counsel, and intelligence overlapped. A relationship might create access without being initiated by a service. It might also provide leverage or influence in both directions. This is a useful contrast with the highly staged "honey trap" model: the practical reality could be reciprocal, ambiguous, and embedded in court politics.

Because the evidence consists of historical correspondence interpreted through a modern diplomatic study, the thesis must distinguish the documented relationship from inferences about operational intent. Until a source documents deliberate recruitment or direction, this remains a relationship with intelligence implications, not a proven seduction operation. Its likely information gains and effect on policy require further case-level examination in the later comparative chapters.

The surviving record establishes little personal fallout from this relationship. Mary Beaton married Alexander Ogilvy of Boyne in 1566, but the marriage record does not show that her relationship with Randolph caused that decision. The sources reviewed here document no prosecution, formal punishment, or loss of office for either person because of the relationship. They identify no specific person punished or political decision changed as a result of information passing between them. Those outcomes remain unknown (Smith 2024; Tayler and Tayler 1933).

DOI: **10.5281/zenodo.24482572**

2.6 Seventeenth-century Britain: organized networks and the sexualized afterlife of women's work

2.6.1 Jane Whorwood and Charles I

Jane Whorwood's career shows how intelligence work, personal loyalty, political finance, and intimacy could coexist without being reducible to any one of them. During the English Civil War she served the Royalist cause as a secret agent, maintained contacts with London merchants, and arranged the transfer of large sums of money to the king's forces. English Heritage reports that in 1644 she arranged the movement of at least £80,000 in gold, concealed in soap barrels and carried through Parliamentary checkpoints. After Charles I was imprisoned on the Isle of Wight, she helped plan escape attempts and managed coded correspondence with other Royalists (English Heritage n.d.-a).

In 1648, the correspondence between Whorwood and Charles also became sexually charged. English Heritage, drawing on the letters and Sarah Poynting's analysis, reports that the king proposed a private sexual meeting, and that Whorwood expressed conflict between duty and personal feeling. Subsequent meetings were in part sexual. This intimacy did not create her intelligence role: she had already served as a Royalist agent and helped move money and messages. It did, however, coexist with her operational work and could have affected the relationship between the king and his agent (Poynting 2006).

Whorwood is therefore not evidence of a female operative seducing a male target for a foreign service. She acted for the Royalist cause and appears to have been personally loyal to Charles. The case involves an agent and a political leader whose working relationship included sexual intimacy, emotional attachment, and operational trust. The records document substantial logistical assistance and several escape attempts. They do not demonstrate that the intimate relationship changed Charles's political decisions or produced a measurable intelligence advantage beyond the access and communications already inherent in Whorwood's role.

The case also clarifies the consequences borne by women agents. Whorwood was not rewarded in the same manner as several male associates after the Restoration. Her later life included poverty and a destructive marriage. This does not prove that her gender alone determined her treatment, but it signals that states and political movements could rely on women's labor while giving them less durable recognition or protection. The personal consequences belong within the analysis of institutional compromise, not as a sensational coda.

Charles I's consequences were immediate and irreversible. He was tried, sentenced to death, and executed on January 30, 1649. That year Parliament abolished the monarchy and declared England a Commonwealth. The record places these events within the Civil War and the political process that led to the King's trial. It does not connect his execution or the abolition of the monarchy to his intimate relationship with Whorwood or to her escape attempts. (UK Parliament, "Engrossment of the Official Record of the Trial of King Charles I"; "Pride's Purge, 'the Rump' and Regicide.")

2.6.2 Aphra Behn and the work behind the legend

Aphra Behn is often remembered as a writer with a secret life, but archival scholarship has reconstructed a specific intelligence mission. In 1666 the English Secretary of State's office sent her to the Low Countries with written instructions known as "Memorialls for Mrs Affora." Alan Marshall's research examines the instructions and Behn's task of contacting William Scot, recruiting or persuading him to return to the English side, and gathering information on English exiles and possible plotting (Marshall 2015). The mission was part of Restoration intelligence practice, not a demonstrated sexual entrapment operation.

Behn's inclusion matters for two reasons. First, she was an identifiable woman operating under official instructions, with a target, a political purpose, and an administrative chain. Second, later retellings can turn a woman agent into an erotic figure even where the surviving evidence centers on correspondence, recruitment, money, and political reporting. Nadine Akkerman's archival study of seventeenth-century Britain similarly shows women operating across political and religious networks as couriers, correspondents, code users, and intelligence gatherers. Rachel Weil's review notes that some agents have been remembered erroneously as sexual temptresses, even though the historical evidence concerns the transmission of information under dangerous conditions (Akkerman 2018; Weil 2020).

The broader seventeenth-century record reveals an intelligence craft that depended on household access, family links, patronage, postal routes, coded letters, invisible inks, and personal trust. These methods could make intimacy relevant, but their existence does not transform every agent into a seducer. The gendered stereotype often substitutes for the more complicated operational record.

The mission's consequences were clearer for Behn than its intelligence gains. Although she initially reported that Scot seemed willing to serve, his later replies were evasive, and the English secretariat came to regard him as unreliable. He was in Dutch custody for debt by December 1666; after his arrest by the Dutch, his fate disappears from the record. Behn's requests for money and for the promised pardon went unanswered. She pawned jewelry,

borrowed £150 to return to England, and later faced a warrant for debt, although the surviving evidence does not establish that she was imprisoned. Her warning about a possible Dutch attack on the English fleet in the Thames was dismissed. The sources do not establish that her reports caused anyone to be punished or changed policy. (Marshall 2015; O'Donnell in The Cambridge Companion to Aphra Behn.)

2.7 The eighteenth century: diplomatic households and political sociability

2.7.1 Women of Pera and informal diplomatic networks

In late eighteenth-century Istanbul, women in the diplomatic society of Pera participated in the political life of embassies and households. David Do Paço's archival study draws on private family collections and diplomatic correspondence to reconstruct how women connected Habsburg, British, Ottoman, and other social worlds. Women served as sources of information, managed relationships and patronage, facilitated access, and helped sustain ties between diplomatic communities. The article emphasizes that mothers, wives, sisters, daughters, lovers, servants, and unofficial partners could function as agents and resources of diplomacy, while also pursuing their own agendas (Do Paço 2022, 640-62).

Constance Spencer Smith, born in Istanbul in 1782, illustrates the distinction between influence and proven espionage. She grew up within the Habsburg diplomatic household, married British diplomat John Spencer Smith in 1798, and participated in overlapping diplomatic and social networks. In later roles, her involvement became extensive enough that Napoleon accused her of espionage; she was arrested, and her eventual release created diplomatic tension. Do Paço's account establishes the accusation and her substantial political activity. It does not make Napoleon's charge itself proof that she conducted an intelligence operation. Her case is classified D, a politically consequential accusation with security implications, unless further evidence identifies a specific intelligence task or transfer.

For this thesis, accounts from Pera describe the social networks that made informal intelligence possible. Embassies were not merely offices staffed by credentialed diplomats. They were households and social communities tied to local families, servants, interpreters, protégés, and patrons. Women could circulate information and create connections because they occupied that structure. Sexual or romantic relationships might be part of the social environment, but the source does not support reducing women's agency to erotic access. The relevant mechanism is a network that combined intimacy, kinship, hospitality, information, and political influence.

DOI: **10.5281/zenodo.24482572**

Consequences and personal aftermath: Constance Spencer Smith's arrest and release had consequences beyond the accusation itself. The diplomatic tensions surrounding her release led her to take refuge in Vienna in the 1810s. She continued working in business, diplomatic, and literary circles there, including promoting scholars who had been her father's protégés. This indicates a disruption to her mobility and diplomatic position, followed by continued public activity; the available account does not establish imprisonment conditions, lasting financial or psychological harm, or consequences for her family. Nor does it show that she conducted espionage. Her later life is documented, but the personal cost of the arrest remains unclear (Do Paço 2022, 640-62)

2.7.2 What the Revolutionary era can and cannot add

In the revolutionary and Napoleonic era, clandestine networks crossed political borders, while family, friendship, romance, and political loyalty could overlap. This chapter does not promote individual women in those networks to verified cases without a stronger source chain. A woman's association with a male agent does not establish that she recruited, deceived, or supplied him. Claims about particular missions must be tied to correspondence, official records, or corroborating scholarship. The late eighteenth-century Istanbul evidence already shows the value of studying this informal diplomatic architecture, while the post-1800 accusation against Constance Spencer Smith shows how quickly political influence could be recast as espionage.

2.8 Comparative analysis: what persists, and what changes

Across these periods, the most durable feature is not a single "honeypot" technique. It is the intelligence value of access. People who could enter households, courts, camps, diplomatic circles, prisons, or enemy-controlled territory could observe and communicate information unavailable to outsiders. Intimacy was one possible route into these spaces, alongside kinship, service, patronage, occupation, travel, political loyalty, bribery, and disguise.

The second recurring feature is the importance of trust and reputation. Antigone's relationship with Philotas, Mary Beaton's proximity to an English diplomat, Whorwood's confidence with Charles I, and the social networks in Pera all show how relationships could shape who spoke, who listened, and who was admitted into private settings. Their evidentiary status differs widely. In some cases the relationship is part of a retrospective narrative; in others, correspondence and account records document the connection. The existence of trust does not itself show deception or intelligence direction.

Third, information work was usually practical and mixed. A courier might also observe. A household intermediary might transmit rumors and negotiate access. A paid agent might pursue personal or family interests alongside political objectives. In Ypres, records differentiate some message-carrying from information-gathering while also showing that the same women could receive repeated assignments. In Pera, social and diplomatic functions were intertwined. In Whorwood's case, money movement, coded correspondence, escape planning, and sexual intimacy occupied the same political relationship. Historical roles rarely fit a single modern job description.

Fourth, gender shaped opportunity and interpretation. A woman's presence might be considered ordinary in one setting and suspicious in another. Disguise could facilitate access, but the Margoth account cannot establish a universal advantage. Tudor evidence indicates that women sometimes used gendered expectations to create plausible deniability, yet women were also suspected and punished. Later memory has often made women's intelligence work more sexual than the records warrant. This process has two effects: it dramatizes some women and erases others. It can also obscure male agents' use of romance and the coercion of male targets, subjects considered in later chapters.

Fifth, state organization changes across the chronology. Ancient literature includes accounts of royal surveillance but provides few verifiable operational details. Medieval records show rulers and cities paying for scouts, messengers, and information. Renaissance Venice provides evidence of a relatively organized service with formal reporting and incentives. Tudor and Stuart materials show expanding networks of correspondence, agents, and coded communication. Eighteenth-century diplomacy relied heavily on households and informal networks alongside formal offices. These differences matter because "state service" and "intelligence agency" are not interchangeable across centuries.

Finally, the evidence for consequences is uneven. Ancient texts connect reports to court suspicion but do not quantify intelligence value. Medieval account books record payments and assignments but seldom show downstream decisions. The Flemish records offer a rare count of named participants and recurring tasks, not a measure of military advantage. Whorwood's movement of funds and escape efforts are more traceable, though the king's escapes failed. Pera's networks contributed to diplomatic influence, but not every relationship can be linked to a discrete policy outcome. The thesis therefore measures demonstrated information and consequences where possible, and states explicitly when the archive does not allow measurement.

DOI: **10.5281/zenodo.24482572**

2.9 Conclusion

The evidence from antiquity to 1800 supports a long history of intelligence through human relationships, but not a universal or unchanging history of sexual entrapment. Ancient stories such as Delilah and Judith show how cultures represented intimacy as a means of defeating powerful men. Aristotle's discussion of women informers at Syracuse shows that female participation in political surveillance was part of classical political thought. Plutarch's account of Antigone gives a specific, though retrospective and contested, narrative of a ruler turning a lover into a source.

Medieval evidence broadens the picture. Alice of Saintes, Margoth, women in the Hundred Years War, and the Flemish agents of 1488-89 illustrate travel, disguise, reconnaissance, messaging, and paid reporting. Renaissance and early modern evidence shows women acting in organized networks, diplomatic households, and political correspondence. The relationships of Mary Beaton and Thomas Randolph and Jane Whorwood and Charles I illuminate how intimacy could intersect with political access without fitting a simple model of a planted seductress. Aphra Behn's mission and the wider work recovered by archival scholarship further demonstrate that women's intelligence craft encompassed recruitment, coded communication, and information transmission.

The eighteenth-century diplomatic society of Pera shows how intelligence and influence could emerge from household structures, social ties, family networks, and informal agents. Napoleon's later accusation against Constance Spencer Smith shows why historians must separate allegation from proof. In every period, this distinction protects the historical record from both sensationalism and unjustified certainty.

The chapter therefore establishes a qualified historical continuity: intimate and social access repeatedly created opportunities for information to move. The form, institutional setting, actors, and consequences changed.

DOI: **10.5281/zenodo.24482572**

Chapter 3.
The Psychology of Intimate Influence: Trust, Disclosure, and Coercion

3.1 The psychological question

Intimate intelligence depends on a basic fact of human relationships: people reveal information, grant access, and assume obligations within relationships they experience as meaningful. The intelligence question is not why a person is foolish enough to trust someone. It is how trust develops, what kinds of disclosure it encourages, how deception can hide within apparently reciprocal interaction, and what changes when affection is joined by pressure, secrecy, stigma, or institutional risk.

The psychological analysis in this chapter addresses mechanisms, not diagnoses. It does not presume that a person who passed information was lonely, narcissistic, sexually impulsive, insecurely attached, or otherwise psychologically abnormal. Such claims are often made after a scandal and may reflect a need to explain a complex event through an individual defect. They require evidence that historical records rarely provide. Instead, the chapter examines processes that can affect ordinary people in varying contexts: reciprocal disclosure, perceived understanding, belonging, social influence, motive, secrecy, shame, coercion, and the costs of refusing or ending a relationship.

This distinction is central to the thesis. A relationship may create opportunity without being an intelligence operation. A service-directed relationship may become emotionally genuine for one or both participants. A person may volunteer information for mixed reasons, or may begin to cooperate only after threats. The fact of an affair cannot establish why it began, who directed it, what was exchanged, or what consequences followed. Those are separate historical questions.

The chapter develops a process model for the later case studies. It treats intimate influence as a sequence of possible conditions: contact and access, a developing sense of connection, private disclosure, an intelligence request or opportunity, and then voluntary cooperation, resistance, coercion, or disengagement. This is not a universal script. Some cases begin with deliberate compromise; others begin with a genuine relationship; still others involve a relationship that is exploited after it has formed. The model is a tool for reconstructing cases, not a claim that every operation follows the same stages.

DOI: **10.5281/zenodo.24482572**

3.2 What psychological research can establish

Research on relationships and social influence can explain why some forms of interaction tend to increase closeness, trust, disclosure, or compliance. It cannot determine what a named historical actor felt unless records support that conclusion. Laboratory experiments generally involve bounded tasks, brief encounters, and participants who know they are in a study. Intelligence operations involve stakes, time, secrecy, institutions, and consequences that are difficult to reproduce experimentally. Findings from one setting should not be transferred to another as though the evidence were interchangeable.

The evidence used here is therefore layered. Meta-analyses and systematic reviews help summarize recurring findings. Relationship studies help explain disclosure and perceived responsiveness. Research on intelligence source recruitment provides a closer, though still limited, comparison to agent cultivation. Historical files, court records, official inquiries, and case studies establish what happened in particular operations. The psychological literature explains possible mechanisms; the historical record determines whether those mechanisms are relevant in a case.

This approach also keeps “vulnerability” from becoming a synonym for weakness. Vulnerability may refer to an exposed circumstance, a relationship of dependence, a social or legal constraint, access to protected information, or a temporary period of stress. A person can be competent and responsible while still facing manipulation. A service can exploit a structurally dangerous situation, such as criminalization of a private relationship, without the target possessing a stable psychological defect.

3.3 Intimacy, disclosure, and perceived responsiveness

Intimacy is not created by disclosure alone. In the interpersonal process model developed by Reis and Shaver and later tested in couple research, one person discloses, the other responds, and the first person interprets that response as understanding, validation, and care. Repeated exchanges can build closeness because each response helps shape what the next disclosure feels safe to include (Reis and Shaver 1988; Laurenceau, Barrett, and Pietromonaco 1998).

This process helps explain why a relationship may become an information channel without either participant consciously treating it as such. A person who feels understood may speak about work pressures, conflict, ambitions, daily routines, or private anxieties. The other partner may learn what the person can access, which colleagues are trusted, what subjects are

DOI: **10.5281/zenodo.24482572**

sensitive, and how decisions are made. A single conversation may reveal little. Over time, ordinary exchange can form a detailed picture of a person and the institution around them.

Self-disclosure is also relational. People use their own and their partner's disclosure to infer the quality and direction of a relationship. Collins and Miller's meta-analysis found a relationship among disclosure and liking, but the association varies by the kind of disclosure and the research situation. It does not show that disclosure mechanically produces attraction, nor that people who disclose more are easier to recruit (Collins and Miller 1994). A later review emphasizes that disclosure develops through reciprocal interaction and communicates information about the relationship itself, including trust, support, acceptance, or disapproval (Willems, Finkenauer, and Kerkhof 2020).

For intelligence analysis, reciprocity deserves particular attention. When one person shares a private concern, the other may respond with a disclosure of their own. This exchange can make the interaction feel mutual even when the parties possess unequal knowledge about identity, purpose, and risk. An operative may reveal true personal details, cultivate a partly genuine bond, or appear emotionally open while concealing the operational purpose. The target may therefore receive real care and still be deceived about the relationship's larger meaning.

Researchers distinguish perceived responsiveness from objective accuracy. Feeling understood does not prove that the partner has understood correctly or shares the same intentions. In a deceptive relationship, a target may experience the partner's responsiveness as emotionally real even if the partner is collecting information. That experience may deepen trust, but it cannot by itself establish the operative's sincerity or the target's reason for cooperating.

This mechanism is visible in documented operations where a relationship is intentionally developed over time. East German "Romeo" agents were assigned to build relationships with women whose government employment could provide access to information. The Stasi Records Archive describes the cultivation of women in secretarial positions and the effort to build durable trust, sometimes by feigning love or promising marriage. A historical account of cooperation between the Stasi foreign intelligence service and the KGB places these operations within broader collection practices (Stasi Records Archive, n.d.; Maddrell 2014, 182-83). The operational advantage was not simply that the women were described as lonely. It was the length of the relationship, the continuity of access, and the possibility that ordinary life together would create repeated opportunities for knowledge and disclosure.

DOI: **10.5281/zenodo.24482572**

Clayton Lonetree's case followed a different pattern. A December 1986 National Security Council summary states that he was recruited through the "uncle" of a Soviet employee with whom he had a sexual relationship. A later damage assessment says he was not blackmailed: according to the assessment, the relative asked him for classified information, which Lonetree willingly provided. The same memo records his stated fascination with espionage, his sense of flattery at being approached, a grievance about the treatment of Native Americans, and payment. These records were based substantially on his confession and officials' early assessments, and should be read as such (National Security Council 1986, doc. 10; National Security Council Staff 1987, doc. 28). This case shows why intimacy cannot stand in for coercion: the relationship facilitated contact, while the surviving account identifies other motives for cooperation.

3.4 Reciprocity, liking, and the limits of social influence

Social influence research identifies several conditions that may shape compliance: a desire to maintain relationships, a desire to form accurate beliefs, and a desire to preserve a positive self-concept. These motives can work together. A person may agree because a request seems reasonable, because someone trusted asked, because the relationship feels reciprocal, or because refusal would imply distrust or disloyalty (Cialdini and Goldstein 2004).

Reciprocity can arise from small acts of help, attention, patience, or practical support. In an intimate relationship, such exchanges do not necessarily feel like influence tactics. They may be genuine. A partner's help during a crisis can create gratitude and a sense of mutual obligation. Later, a request for information may seem like an extension of ordinary support rather than a change in the relationship. The psychological mechanism is plausible, but evidence of gifts or assistance in a case does not establish that the service planned them as inducements.

Commitment can also influence later choices. Once a person has made an initial disclosure or helped with a seemingly minor request, a later request may feel less like a new decision and more like continuation. This pattern is often discussed as escalation or consistency pressure. It should not be treated as a law of behavior. People frequently stop, refuse, confess, or reverse course. The historical investigator must locate the actual requests and decisions, rather than infer a "foot in the door" process from the final outcome.

Research on intelligence recruitment tests this boundary directly. Neequaye and Granhag experimentally studied whether shared experiences could increase prospective sources' commitment to a simulated intelligence arrangement. The shared experience influenced reported closeness and the possibility of social connection, but the study found little evidence

DOI: **10.5281/zenodo.24482572**

that handlers could convert those effects into greater commitment. The authors therefore caution against equating felt affiliation with recruitment success (Neequaye and Granhag 2024). The study is especially useful to this thesis because it examines a proposed intelligence mechanism and reports a limited result. Connection may be present without cooperation; a warm interaction is not proof of a dependable source.

The operational consequence is that relationship building can create conditions for elicitation, but it does not guarantee disclosure, recruitment, or control. A person may feel close and still refuse. A recruited person may provide information while limiting its scope. An operative may misread emotional attachment as reliability. A target may exploit the apparent relationship for their own interests. Human relationships are not instruments that produce predictable outputs.

3.5 Attachment, belonging, and situational stress

Attachment theory studies how expectations about availability, responsiveness, and support shape people's behavior in close relationships. Research on adult romantic attachment connects attachment orientations with emotion regulation under stress, but the findings describe tendencies, not fixed categories or individual diagnoses (Mikulincer and Shaver 2016, 2019). They do not justify labeling a historical person "anxiously attached" from an affair, an act of disclosure, or a retrospective account.

The relevance for this thesis is narrower. People often seek dependable connection, especially during change, isolation, bereavement, career frustration, or family conflict. A relationship that provides attention and stability may become important when other sources of support feel unavailable. An operative may exploit an actual stressor or appear at a moment when the target is receptive to companionship. Yet the presence of a crisis does not prove that a person was unusually susceptible. It may explain timing, while the operation's success depends on access, opportunity, judgment, incentives, pressure, and the target's own choices.

Belonging can operate as both an emotional need and a practical incentive. Intelligence recruitment may involve money or protection, as well as recognition, status, purpose, a sense of being understood, or membership in a trusted relationship. A 2026 study based on interviews with 17 handlers from two Australian law enforcement agencies describes motivation as changing over time and requiring reassessment. The sample is small and agency-specific, so it cannot establish a universal typology. Its findings nevertheless underline the inadequacy of reducing source motivation to a short acronym or single trait (McKenzie, Henry, and Rajakaruna 2026).

DOI: **10.5281/zenodo.24482572**

Motives can change during an operation. A person may begin with affection, move toward cooperation out of loyalty, continue because of fear, and later disclose information to investigators from remorse or self-preservation. Another person may act from political conviction and later regret the consequences. The record may reveal only the final explanation offered in court or a memoir. Where motives are mixed or disputed, the analysis states so.

This framework helps distinguish three patterns. First, an operation may deliberately manufacture or cultivate a relationship before requesting information. Second, a genuine relationship may provide access that one partner later uses for intelligence. Third, a relationship may develop independently, then become a means of pressure when information or leverage is discovered. These patterns produce different psychological and ethical questions, and they should not be collapsed under the label "honey trap."

3.6 Secrecy, compartmentalization, and the burden of double life

Espionage often requires concealment. An agent may hide a relationship, an information request, a foreign contact, or the reason for a meeting. A target may also conceal a relationship from a spouse, employer, political party, or service. Secrecy can protect an operation, but it can also constrain the person keeping it. The burden of secrecy may create stress, narrow the circle of confidants, and reduce opportunities to test one's interpretation of events.

Research on secrecy distinguishes the intention to conceal information from the moments when concealment is actively performed. Slepian, Chun, and Mason found that secrecy can intrude on thought beyond the immediate occasions on which a person must hide a fact, and that the burden is connected to the importance and personal significance of the secret (Slepian, Chun, and Mason 2017). This research does not study spies or intimate operations. These findings provide a framework for examining why secrecy may occupy attention, isolate a person, or make a relationship feel like the only place where parts of the self can be acknowledged.

In intimate intelligence, secrecy can be asymmetrical. The operative may know that a relationship is both personal and instrumental, while the target may believe it is private and separate from work. Alternatively, both people may know they are concealing an affair, but only one knows that classified information is being requested. Such asymmetry can create a form of compartmentalization: the person can keep "the relationship" and "the job" mentally separate even as the two interact in practice. Compartmentalization is not proof of psychosis or pathology. It is a descriptive possibility for understanding how people maintain incompatible roles.

DOI: **10.5281/zenodo.24482572**

Double lives may also produce operational friction. The operative's need to report may conflict with affection. The target's occupational obligations may conflict with loyalty to a partner. A handler may demand more information than the source is willing to provide. A relationship that appears to make collection easier may instead expose the operation through behavioral changes, missed communications, unexplained access, or emotional distress. The success of an operation depends on the management of these conflicts, not simply the presence of intimacy.

The psychological effects of secrecy should be analyzed alongside institutional conditions. If an organization makes disclosure of a relationship professionally dangerous, the employee may be less likely to seek advice. If a service punishes contact reporting or fails to provide a credible route for confidential guidance, it can convert an ordinary private relationship into a security problem. An institution's role is therefore not limited to screening for individual weakness. It also determines whether people can raise concerns before a relationship becomes a source of leverage.

3.7 Shame, stigma, and coercive leverage

Blackmail is often described as though a compromising photograph or secret automatically controls its subject. It does not. Its potential force depends on what exposure would mean to the person, the law, their family, profession, political position, and institution. The threat may work because the target anticipates losing a career, being arrested, being rejected by family, or harming people who depend on them. The material's psychological power is social and institutional as much as individual.

The Vassall case illustrates this point, but its blackmail narrative requires careful qualification. John Vassall, a British Admiralty clerk, was convicted of espionage after passing classified information to Soviet intelligence. The Radcliffe Tribunal concluded that he had been identified and compromised by Soviet intelligence, and it examined the security failures surrounding his recruitment. The public account of sexual blackmail was widely repeated, while parliamentary debate also questioned how much of the blackmail claim rested on Vassall's own testimony. The tribunal record and subsequent debate should therefore be examined directly before treating the precise coercive sequence as settled (Radcliffe Tribunal 1963; Hansard 1963b, 1963a; The National Archives, n.d.). Consensual sexual activity between men remained criminalized in England and Wales until the Sexual Offences Act 1967 partially decriminalized private acts between consenting men aged 21 or older (UK Parliament 2017). The analytical point is not that Vassall's sexuality explains his conduct, but that criminal law and stigma could make exposure an especially potent threat.

Coercion can operate through graduated pressure. A person may first be encouraged to keep a secret, then reminded that disclosure would reveal earlier misconduct, and finally threatened with harm to a partner, colleague, or family member. In the case of Sharon Scranage, court reporting and her guilty plea establish that she provided classified information, including covert identities, to Michael Soussoudis. FBI testimony and a later CIA historical analysis describe threats and intimidation after their relationship began. The CIA account also describes isolation from colleagues and efforts to undermine her trust in managers (FBI, n.d.; Wilder 2017). This record supports analysis of an intimate relationship later joined by coercion. It does not justify treating Scranage as a passive object or assuming that an earlier history of abuse explains all of her decisions.

The distinction between coercion and consent is not always resolved by a person's initial participation. A relationship can begin voluntarily and become coercive. An agent may consent to one disclosure but refuse a later one. Threats can change the meaning of continued cooperation. Conversely, a person may describe pressure after arrest in ways shaped by legal strategy or hindsight. The investigator should assess the timing, wording, corroboration, and context of each alleged threat.

Shame may also inhibit help-seeking. Research on sextortion finds that people often do not report or seek help because of shame, fear, and negative expectations about police or platforms. The systematic review found a limited evidence base and emphasizes that the phenomenon spans intimate partners, online dating, cybercrime, and organized abuse rather than one single pattern (Ray and Henry 2025). These findings are directly relevant to contemporary digital cases and only indirectly comparable to historical espionage. They show how exposure threats can keep a person silent, not that a particular intelligence service is usually behind such threats.

Coercion may produce compliance, but it can also generate resistance, escape, counter-disclosure, self-harm, or attempts to confess. A blackmail threat may be unreliable, exaggerated, or impossible to carry out. Targets may decide that exposure is less damaging than continued cooperation. They may test whether the material exists, inform an institution, or seek protection. The psychological leverage depends on the target's estimate of the threat and the available alternatives. A sound case history must therefore record the threatened consequence, the target's response, the actual disclosure, and whether the threat was used again.

DOI: **10.5281/zenodo.24482572**

3.8 Motives, agency, and mixed participation

Historical and intelligence accounts often search for a motive that will make an operation legible: money, ideology, revenge, sex, ego, coercion, or love. These labels can be useful when tied to evidence, but they are not mutually exclusive. A person may need money and enjoy recognition. A genuine political belief may coexist with resentment. A source may continue out of attachment after the original inducement has lost force. The same action can serve different interests for the handler and the source.

Agency is not the opposite of manipulation. A person can make consequential choices under deception, pressure, or unequal information. Recognizing a person's agency does not absolve an intelligence service from coercion. Recognizing coercion does not erase the fact that some people knowingly provide secrets. The historical record may support both propositions at once.

This account matters for gender analysis. Women have often been described as seductresses even when records show courier, political, or administrative work. Men may be portrayed as dupes when their sexuality or private relationships become the story, while organizational lapses receive less attention. Gender expectations affect whose motives are believed, whose disclosure is treated as coerced, and whose professional competence is questioned. Chapter 4 examines those patterns more fully; here, the psychological point is that stereotypes can substitute for evidence about actual motive and choice.

The term "vulnerability" should therefore be assigned to a condition and period, not to a person as a permanent identity. Access to secrets, a pending promotion, a family crisis, a stigmatized relationship, debt, workplace conflict, or isolation can create an exposed situation. These conditions may pass. They may also affect people who otherwise have strong judgment and stable relationships. The analytical task is to identify what was known and exploited at the time.

3.9 Institutional vulnerability and security culture

Intimate influence becomes an institutional concern when private access intersects with protected information, authority, or decision making. Institutions often focus on the individual's behavior: did the person report a contact, secure documents, or obey a rule? They also need to ask what made the contact difficult to disclose, whether employees understood the reporting process, how managers responded to warnings, and whether information access was unnecessarily broad.

DOI: **10.5281/zenodo.24482572**

Institutional betrayal research examines harm that occurs when an organization fails to prevent or respond appropriately to mistreatment of people who depend on it. A 2024 scoping review describes a growing empirical literature across organizational settings, while also identifying the need for broader populations and longitudinal research (Christl et al. 2024). That literature concerns trauma and organizational response, not espionage. Its relevance here is conceptual: institutions can compound personal harm when they protect reputation over people, punish disclosure, or leave an employee isolated after reporting coercion.

Security cultures can also create perverse incentives. If employees expect humiliation, loss of clearance, or career destruction after reporting a relationship, they may delay reporting. If an institution assumes that a private relationship is automatically a security violation, it may make honest disclosure less likely. A credible process should distinguish relationship formation from suspicious conduct, provide confidential advice, protect a person who reports threats, and investigate actual access or disclosure.

The institutional perspective reframes the question from “Why did this person fall for it?” to “What interactions, policies, and access arrangements allowed a relationship to create risk, and what options did the individual have when that risk became apparent?” This shift does not excuse misconduct. It identifies preventable conditions and helps explain why one compromised individual can affect many colleagues, sources, records, or diplomatic relationships.

The Scranage case is instructive because the intelligence loss extended beyond the employee. The CIA’s retrospective account states that staff officers, agents, and operations were compromised, and that African sources and families had to be moved. It estimates the total cost in the several-million-dollar range (Wilder 2017, 34). Those consequences show how an intimate operation can create institutional costs far beyond the amount of material directly disclosed. This assessment is an institutional retrospective, not an independently audited accounting. The case does not establish that every relationship risk can be predicted through personality screening. Indeed, Wilder’s article presents a provisional typology, not a validated diagnostic method.

3.10 The Target Cases Within the Coordinated Operation

This overview describes the author’s model of a coordinated operation. The target cases that follow identify the personnel and decisions documented in each case.

DOI: **10.5281/zenodo.24482572**

Target designation and tasking

Each target case centers on the person designated for an operation and shows that person within the larger coordinated effort. Target selection is made by one individual in the chain of command: the handler or one person above the handler. The handler directs and supervises the operation; the team carries out its assigned tasking.

The tasking sets the operation's purpose, the target's relevance, and what the honeypot is assigned to do. The target's position or relationships give the operation access to information, people, institutions, or decisions.

Campaign and honeypot deployment

An operation can take a year, two years, or several decades. The relationship with the target is one part of the campaign, which involves preparation, contact, trust-building, tasking, requests, transfers, reporting, and changes in approach over time.

When an operative cannot establish contact in the campaign described here, the handler replaces that operative and decides how the next approach will proceed. The Stasi used replacement operatives in some Romeo operations. The CIA's historical account records that women who had fallen in love with the original operative typically rejected a replacement, while women drawn to espionage itself often accepted one (Central Intelligence Agency n.d.-b).

Handler intent and beneficiary

Public records can identify the service or country behind an operation without naming the individual who selected the target or commanded it, establishing the handler's personal intent, or tracing every beneficiary.

In the author's model, the handler has the power to abandon or expose the honeypot. The distinction between motive and beneficiary matters most when the operative pays the cost. Consider a handler who orders an operative's death to conceal his own conduct or to take revenge. Even if the state benefits afterward, that benefit does not establish why he acted. Within this hierarchy, the handler can treat the honeypot as disposable.

3.11 Conclusion

The psychology of intimate intelligence is not a catalogue of personal flaws. It is a study of how trust and disclosure develop, how people infer care and reciprocity, how a relationship can create repeated access, and how secrecy, stigma, or threat can change a person's choices. Research supports several of these mechanisms, but no single mechanism explains every

operation. Empirical work on recruitment further shows that felt closeness does not necessarily produce commitment.

The central analytical distinction is between relationship, intelligence purpose, disclosure, coercion, and consequence. A relationship may be genuine, staged, or both in different respects. A target may be recruited voluntarily, manipulated without awareness, pressured after disclosure, or exposed by an incidental relationship. People can have agency within coercive circumstances, and institutions can be responsible for the conditions that made reporting difficult.

The case chapters use this framework to test, rather than presume, why people participated and what the relationship accomplished. Psychological concepts identify questions for the record. They do not replace the record. Chapter 4 examines the gendered expectations, social roles, and forms of access that shape who becomes an operative, target, intermediary, or public symbol.

DOI: **10.5281/zenodo.24482572**

Chapter 4.
Gender, Access, and the Seductress Myth

4.1 Gender is a historical condition, not an explanation by itself

Popular accounts of espionage often arrange people into familiar roles: the male officer who pursues, the female seductress who deceives, and the powerful man who loses judgment. The pattern is memorable, but it is a poor historical model. Across the centuries, women and men gathered, carried, interpreted, and transmitted intelligence in many capacities. They also became sources, targets, recruiters, intermediaries, administrators, and subjects of surveillance. The role a person occupied depended on political status, class, occupation, nationality, sexuality, institutional access, and the local rules governing where women and men could move.

This chapter examines how gender expectations shaped access and how intelligence organizations, political authorities, journalists, and later historians described that access. It distinguishes three propositions that are often blurred. First, women and men have performed intelligence work across historical periods. Second, gender norms sometimes created opportunities to move, meet, or communicate with less scrutiny. Third, deliberate romantic or sexual entrapment is a specific operational method that requires evidence of intent, direction, and purpose. The first two propositions do not establish the third.

The difference matters to the thesis. A woman who carried military messages in a war zone was not necessarily a seductress. An ambassador's wife who learned political information through court friendships was not automatically a covert agent. A male officer who entered a genuine relationship with a source was not necessarily conducting a service-directed operation. A service that deliberately assigned an operative to cultivate a romantic relationship presents a distinct case. Evidence of relationship, access, and intelligence activity must be documented separately before they are treated as one operation.

The available scholarship supports a longer history of gendered access than a history of continuous "honeypot" operations. The evidence reaches at least into late medieval Europe for women paid to carry messages and gather military information, and into early modern diplomacy and state espionage for women's use of household, court, and correspondence networks. These are historical antecedents to intimate intelligence in a broad sense. They do not prove that the same formal methods or intelligence institutions existed in every century. The relevant continuity is that private and social relationships could bridge boundaries

DOI: **10.5281/zenodo.24482572**

between people, households, political factions, and institutions. The form, purpose, and scale varied considerably.

4.2 Late medieval Europe: women as messengers and intelligence gatherers

Records from the Flemish conflict of 1488-1489 provide an unusually concrete starting point. During war between Flemish cities and Maximilian of Austria, the government of Ypres paid women to carry letters and collect information in the surrounding countryside. Lisa Demets's study, based on municipal accounts and other contemporary evidence, identifies rural and urban women who performed intelligence and communication tasks. Some were reused for assignments, suggesting that the city developed recurring relationships with trusted workers. The records also show that intelligence gathering and message delivery were not always separate jobs (Demets 2025).

Jelle Haemers's study of women spies and messengers in the late medieval Low Countries places the Ypres case within a wider pattern of women participating in wartime communication. Cities and commanders could employ women to cross front lines, observe enemy forces, and move messages. Women were not the majority of intelligence workers, and their specific roles differed from those of most male participants. The surviving records nevertheless challenge an account of medieval intelligence as exclusively male (Haemers 2024).

The value of this evidence lies partly in its ordinary character. The women in the Ypres records were not presented as erotic agents, aristocratic masterminds, or spectacular lone spies. They performed tasks that depended on mobility, local knowledge, and repeated trust. Some worked in rural areas and did not derive their position from high birth. Their case shows that female intelligence work could operate through labor and communication networks rather than romantic access.

The evidence also has limits. City accounts establish payments and tasks more readily than they reveal the women's motives, personal relationships, or the ultimate value of the information they collected. A payment for "news" does not tell us whether a report changed a military decision. Nor does a woman's ability to cross territory establish that she was overlooked by adversaries. This case therefore supports a claim about women's documented participation and the organization of their work. It does not support a claim about sexual manipulation.

DOI: **10.5281/zenodo.24482572**

4.3 Tudor England and Scotland: plausibility, status, and movement

Sixteenth-century intelligence networks offer a further example of gender expectations being used as operational conditions. Samantha Nelson's study of Tudor-era women and military intelligence examines women who gathered, carried, and transmitted information in conflicts connected to the Tudor regimes. Her analysis draws on correspondence and state papers. Women's status, kinship ties, religious affiliation, and political loyalties shaped what they could do and how their activities could be explained if questioned (Nelson 2025).

Nelson's argument refines the common suggestion that women were simply "above suspicion." Some women could benefit from assumptions that they lacked military knowledge or political agency. Others were watched precisely because their religious and family networks were politically suspect. Their ability to claim plausible deniability therefore varied. A noblewoman with access to court and powerful kin had different resources from a servant or a rural messenger. Social status could increase access while also increasing exposure to scrutiny.

Scottish noblewomen appear in the period's intelligence record as participants in exchanges between factions. Nelson discusses Helen Stewart, Countess of Erroll, and a woman identified in the sources as the wife of Lord Tullibardine, likely Katherine Campbell. The women were connected to Scottish court society and passed information to English-aligned political actors through networks of family and patronage. Their positions mattered because access to elite households and court life could provide information unavailable to an ordinary messenger (Nelson 2025).

This type of work did not require the women to perform sexual attraction. Their influence arose from status, trusted social relations, and the accepted movement of women between households. The relevant intimacy was often social or familial. The distinction helps broaden the thesis beyond a narrow definition of seduction: intelligence could travel through relationships that were close, private, and politically consequential without being romantic or sexual.

Gendered movement was not a simple advantage. Women could pass as dependents, relatives, or household visitors, but their access could be conditional on male patrons and family ties. They could be accused of disloyalty or religious conspiracy, and the consequences of discovery could be severe. Gender did not remove risk. It affected which forms of access were available, which activities seemed plausible, and which accounts could be believed.

DOI: **10.5281/zenodo.24482572**

4.4 The ambassadress: diplomatic sociability as an information network

From the sixteenth through the seventeenth centuries, diplomatic households created another channel for women's access to political information. English ambassadors' wives accompanied diplomatic missions from the 1530s to 1700. Gemma Allen's research shows that these women contributed to diplomatic culture through hospitality, gift exchange, and relationships with women at host courts. Their social networks could provide diplomatic information to which their husbands had limited access, and some women's friendships helped advance the objectives of a diplomatic mission (Allen 2019).

This evidence complicates the boundary between public diplomacy and private sociability. An ambassadress might communicate information through conversation, family correspondence, or a trusted friendship. Her information gathering could serve a state purpose without resembling the clandestine recruitment of a secret agent. Describing every such woman as a spy would erase the social conventions that made her role possible and would import a modern category into a different political setting.

The ambassadress's access shows that private access did not require sexual access. Her influence could depend on shared gendered spaces, household visits, religious activities, correspondence, or friendship. These settings could create a channel for information without any party arranging a romantic deception. The historical record supports a claim that women's sociability could have diplomatic and intelligence value. It does not make every friendship a covert operation.

This distinction guides the analysis throughout the thesis. Intimate power may operate through a range of relationships, from kinship and friendship to courtship and marriage. Only some of these relationships are deliberately constructed or exploited by intelligence services. The evidence must establish which one is present in each case.

4.5 Seventeenth-century Britain: the woman agent beyond the courtesan stereotype

In seventeenth-century Britain, women served as informants and intelligence transmitters during civil conflict, the Interregnum, and the Restoration. Nadine Akkerman's archival study *Invisible Agents* documents women ranging from aristocrats and ladies-in-waiting to postmistresses and laundry workers. These women transmitted political information for varied reasons, including conviction, money, influence, or allegiance to a patron. Their work involved correspondence, ciphers, letter interception, and the movement of messages through social and occupational networks (Akkerman 2018).

DOI: **10.5281/zenodo.24482572**

The women Akkerman documents were not a single operational type. Some used their public position and access to households. Others were able to move letters or observe people because their work took them across social spaces. The methods depended on written communication, local knowledge, and cooperation. Their work also depended on male spymasters and political patrons, who could use women's labor while leaving them absent from official narratives or histories written around male officials.

Behn's case complicates the seductress stereotype because the surviving record describes government-assigned intelligence work, not a sexual operation. The distinction matters here: later literary reputation should not be used to recast the documented mission as seduction (Marshall 2015).

The document supports a government-directed mission and makes Behn relevant to intelligence history. It does not, by itself, establish how much intelligence she collected, whether officials considered her effort successful, or whether the popular description of her as a professional spy accurately captures her full role. The uncertainty is analytically useful. It shows how the label "woman spy" can become more certain in literary biography than the operational record allows.

The seventeenth-century material shows intelligence work relying on people whose social and occupational positions gave them access to information and correspondence. It does not establish that women were used as seductresses. Some women were agents by assignment; others served as intermediaries, sources, or couriers. Their work was consequential even when official institutions did not preserve it in a form that later historians could easily see.

4.6 Mata Hari and the making of the "spy-courtesan"

Mata Hari's importance to this chapter lies in the cultural image built around her, not in a settled finding that sexual seduction produced valuable intelligence. French military authorities arrested Margaretha Zelle in 1917, tried her for espionage, convicted her, and executed her. The French Defence Historical Service preserves records from the case and notes that neither the French nor German side demonstrated after the war that she had supplied information of decisive importance. Her actual intelligence contribution remains contested (Service historique de la Défense, n.d.; Wheelwright 2016).

Julie Wheelwright's analysis traces how press accounts, memoirs, and later popular culture turned Mata Hari into a figure who embodied the "spy-courtesan": a woman whose sexuality was presumed to be a weapon for extracting secrets from men. That image fused the real record of a wartime prosecution with broader anxieties about female independence, sexuality,

and women's changing place in public life. It became a template through which later female intelligence officers and agents were described (Wheelwright 2016).

Tammy Proctor's history of British women's intelligence work during the First World War likewise shows how the Mata Hari image obscured the more varied work women performed. Women served in intelligence offices, gathered and transmitted information, and carried out tasks that did not depend on seduction. Cultural stories often sorted women into narrow categories: the dangerous sexual predator or the self-sacrificing patriot. Both categories flatten the motives and professional skills visible in the historical record (Proctor 2003).

French authorities executed Mata Hari after convicting her of espionage during wartime. The verdict records what the court found, but it does not establish the amount or operational value of information she supplied, or that sexual seduction was her method. Later scholarship disputes those claims. Any assessment must use the trial record, intelligence files, and subsequent historical research.

4.7 Women in the Second World War: access, labor, and operational skill

The Second World War expanded women's work across intelligence and clandestine operations. Women served as analysts, codebreakers, clerks, couriers, radio operators, resistance organizers, interrogators, and field agents. Helen Fry's history of women in British intelligence documents the breadth of these roles across both world wars. The research on women in MI5 during the Second World War also shows that women performed essential work within the service while facing gendered and class-based limits on status and recognition (Fry 2023; Toy and Smith 2018).

The Special Operations Executive record provides a clear field example. The National Portrait Gallery reports that the SOE sent 75 female special agents into occupied Europe and that their duties included intelligence collection, communications, training resistance members, sabotage, escape routes, and arms delivery. Sixteen did not return. Women could sometimes move through enemy-held territory more freely because German authorities and civilians did not expect them to perform military operations. This advantage was situational and carried extreme risks if they were detected (National Portrait Gallery, n.d.).

Krystyna Skarbek, who served as Christine Granville, illustrates the range of these responsibilities. The National Portrait Gallery's account describes her courier work, intelligence movement across borders, resistance contacts, training in radio and weapons, and later field activity in France. Her relationships and personal life mattered to her biography, but the record of her service cannot be reduced to a romantic role. Her tradecraft relied on

mobility, language, local knowledge, nerve, and operational judgment (National Portrait Gallery, n.d.).

Women's ability to use gendered expectations as cover did not mean that they were naturally invisible or always underestimated. Anne-Marie Walters's experience in the SOE, studied by Raphaële Balu, shows how gender assumptions could constrain women's field responsibilities and diminish their credibility within headquarters. Walters's account shows how gender affected institutional responses when she reported misconduct by a senior officer (Balu 2020). Operational opportunity and institutional inequality existed at the same time.

The term "femme fatale" cannot explain this work. Women in the SOE used codes, wireless equipment, false identities, courier routes, sabotage training, and relationships within local resistance networks. Some could exploit assumptions about women's social roles, such as shopping, nursing, or family visits. These were forms of disguise shaped by wartime gender expectations. They were different from a service assigning an operative to create a sexual relationship for recruitment or blackmail.

4.8 The Romeo operations: men cultivate women for institutional access

For gender analysis, the records show an asymmetry of roles: male intelligence officers conducted the cultivation, while women employed in West German government offices became the sources whose access was exploited. The cases also show how the label "Romeo" can center the male operative and obscure the women's participation in intelligence work (Stasi Records Archive, n.d.; Maddrell 2014).

The operative's gender was part of the method. Men were trained to build a relationship over time and present themselves as serious partners. Some promised marriage; some relationships may have become emotionally genuine for the agent. The operation depended on a long period of attention and trust, followed by requests for information or recruitment. It was not simply a sexual encounter staged to obtain one secret. Its intended value was sustained access through a relationship that could continue across career changes and private life.

The women's institutional roles matter as much as the romance. Secretaries could handle correspondence, arrange meetings, prepare documents, and observe the routines of senior personnel. Their professional access was often greater than their formal status suggested. A gendered workplace created an intelligence opportunity: women could be placed near important information but denied equivalent authority and protection. An operation that targeted these women exploited both intimate trust and an institutional division of labor.

The word “Romeo” can make the operation sound like a story of irresistible male charm and foolish female victims. That framing hides differences among the women’s motives and choices, as well as the Stasi’s systematic selection and training. Some women knowingly cooperated, some may have believed their partner was a genuine lover, and some learned the truth only later. Each individual case requires its own evidentiary account. The program establishes a documented operational pattern; it does not tell us that every woman’s experience or intelligence contribution was identical.

This operation reverses the common popular script. Men were the romantic recruiters, and women with government access were the targets. The reversal does not mean gender did not matter. It shows that gender shaped the assumptions both sides could exploit. The operative used conventions of heterosexual courtship; the institution had placed women in work with access but limited authority; the service targeted a role, not merely an individual’s private life.

4.9 A woman operative targeting a man: the Vanunu capture

The 1986 capture of Mordechai Vanunu provides a contrasting case in which a romantic approach reportedly brought a male target within reach of an intelligence service. Vanunu, a former technician at Israel’s Dimona nuclear facility, had disclosed information about the program to the British press. Contemporary reporting described a woman using the name “Cindy,” later identified in press accounts as Cheryl Bentov. She met him in London and persuaded him to travel to Rome, where Mossad operatives seized him and returned him to Israel (The Washington Post 1986b; Jewish Telegraphic Agency 1986).

The operation is significant because a woman’s role was reportedly instrumental in the capture of a male target. It complicates any assumption that women were only targets of romantic recruitment or that men were always the operative pursuers. The reported tactic used attraction and trust to influence movement across borders. The ultimate objective, however, was capture and transfer, not a documented long-term sexual blackmail arrangement or a demonstrated stream of intelligence collected from a continuing relationship.

The account must retain its evidentiary limits. Public descriptions of Bentov’s identity and role emerged through press investigations and later reporting. The Israeli government did not publish a complete operational file. Vanunu’s capture and transfer are established; the private details of the approach and the full internal chain of command are less transparent. This chapter therefore treats the episode as a strongly supported account of romantic deception facilitating capture, while reserving judgment on operational details that cannot be independently established from public primary records.

DOI: **10.5281/zenodo.24482572**

Together, the Romeo and Vanunu cases show why gender should be analyzed as a variable in operational design. A man may be selected to court a woman with access. A woman may be selected to create trust with a male target. In both cases, the operational task is not explained by gender alone. The service must identify an objective, select a person who can reach the target, sustain the cover, manage the relationship, and exploit the access. The historical question is what was asked, what was obtained, and whether the relationship achieved the service's purpose.

4.10 Gender inside intelligence institutions

The history of women agents is only one part of the gender question. Intelligence services also employed women as clerks, analysts, translators, codebreakers, administrators, and officers. Their formal authority, promotion opportunities, and recognition varied by country and period. A woman could be essential to intelligence production without being named in the public story of an operation. Conversely, she could become highly visible after an arrest because a narrative of sexual betrayal made her easier to sensationalize than the institution's organizational failures.

Rosemary Toy and Christopher Smith's research on MI5 during the Second World War examines the relationship between gender, class, and women's work in the service. It shows that women's growing presence did not automatically eliminate assumptions about appropriate roles or status. Women could perform work central to security and counterintelligence while remaining subject to institutional boundaries shaped by class and gender (Toy and Smith 2018).

Andrea Pető's study of Hungarian intelligence records follows women's roles and representations from the interwar period into the 1980s. It examines women as employees and agents, as well as their treatment in training and surveillance materials. Pető argues that women could be deployed in intelligence culture as images through which male subjects were understood or managed. Her analysis shows that gender operated both in field recruitment and within institutions that classified, employed, and observed their own personnel (Pető 2020).

The cases of John Vassall and Clayton Lonetree, addressed in earlier chapters, also show that gender and sexuality shaped the risks faced by men. Vassall's same-sex relationships existed within a legal and social order in which exposure could threaten liberty and reputation. Lonetree's relationship with a Soviet embassy employee was an access route, but a contemporary U.S. assessment states that he was not blackmailed and records his stated motives for cooperating (National Security Council Staff 1987). These cases warn against

DOI: **10.5281/zenodo.24482572**

treating all male targets as heterosexual men vulnerable to a female seductress. Sexuality, stigma, and institutional norms can produce different forms of leverage.

Gender also shapes who is portrayed as a calculating agent and who is described as an unwitting victim. Women accused of espionage have often been represented as seductive, sexually available, manipulative, or psychologically unstable. Men in comparable cases are more often narrated through ideology, greed, grievance, or political judgment. These patterns do not prove that women's motives are always misunderstood or that men's motives are accurately reported. They identify a bias to test in each investigation.

Recent scholarship has begun to map this problem directly. A review of literature on diversity in intelligence finds that gender, sexuality, and race remain underexplored in a field constrained by secrecy and limited public data (Stephenson and Rimmer 2023). A later review focused on women's intelligence work identifies recurring themes in women's roles, networks, movement, representation, and institutional treatment while also emphasizing gaps in the research record (Drumhiller 2025). These works support using a gender-aware framework, but they do not supply a universal explanation for individual cases.

4.11 What the history does and does not establish

The cases in this chapter establish that women's intelligence work is not a modern exception and that women's access often developed through social positions overlooked by accounts centered on male officials. Late medieval records show paid women carrying messages and gathering military information. Tudor sources show women moving information through kinship and court networks. Early modern diplomatic histories identify women's sociability as a channel of political intelligence. Seventeenth-century archives document women transmitting information through correspondence and other practical networks. Modern intelligence services used men and women in professional and clandestine roles.

The record also establishes that gender expectations sometimes created operational advantages. Women might be able to move through a household, court, market, or occupied territory because others did not recognize their potential role. A male operative might use social conventions of heterosexual courtship to cultivate a female source. A female operative might use a romantic appearance to bring a male target into a controlled setting. In each example, gender worked with class, occupation, nationality, and institutional structure.

What the evidence does not establish is an uninterrupted, identical practice of sexual entrapment running from the Middle Ages to the present. The medieval Ypres sources document messengers and intelligence gatherers, not an organized seduction program. The

DOI: **10.5281/zenodo.24482572**

ambassadress's network was a form of diplomatic sociability, not automatically espionage. The Mata Hari case cannot validate a general theory of femme-fatale tradecraft. The East German Romeo operations and the reported Vanunu operation are much more directly connected to deliberate romantic cultivation, but they differ in target, duration, objective, and evidentiary record.

The history therefore supports continuity at the level of opportunity and access, with substantial change in operational form. Governments have repeatedly used personal networks, social trust, and role-based access to move information. The modern intelligence service adds formal recruitment systems, handlers, training, surveillance, and institutional objectives that cannot be assumed in medieval or early modern cases. The thesis distinguishes these continuities from claims of identical methods.

4.12 Comparative questions for the case studies

The gender analysis in later chapters is guided by these questions:

Operational role

Was the person an agent, source, target, recruiter, courier, intermediary, official, or public symbol? Did their role change over time? What evidence supports each label?

Access and social position

What access came from occupation, class, family, marriage, diplomatic placement, sexuality, nationality, language, or gender expectations? Which elements were deliberately selected by a service, and which arose from the target's ordinary circumstances?

Relationship type

Was the relationship romantic, sexual, familial, professional, diplomatic, religious, or based on political allegiance? Was it genuine, staged, coerced, instrumental, or mixed? What records establish the relationship's purpose?

Information and influence

What information was requested and obtained? Was it personal observation, policy, technical data, classified material, or access to another person? Can an institutional or political decision be linked to it?

DOI: **10.5281/zenodo.24482572**

Gendered narrative

How did contemporaries describe the person? Did accounts focus on sexuality, marital status, appearance, loyalty, ideology, money, class, or professional ability? Did later retellings reproduce or challenge those descriptions?

Evidence and consequence

What primary records, testimony, official reports, court findings, or archival materials support the story? What remains based on a single account or later journalism? Did discovery cause punishment, institutional reform, diplomatic cost, reputational damage, or harm to other people?

These questions keep gender analytically useful without allowing it to replace case evidence. They also allow comparison across periods while preserving differences in law, social organization, and intelligence structures.

4.13 Conclusion

The history of intimate intelligence cannot be written as a succession of female seductresses and male victims. Women served as couriers, informants, agents, diplomatic intermediaries, clerks, analysts, codebreakers, and field operatives. Men also used romantic relationships to cultivate women with access to government information. In some documented cases, women operatives used intimacy to approach male targets. These patterns varied with period, profession, class, political status, and institutional structure.

Medieval and early modern records document instances of gendered access to information. It does not demonstrate that every close relationship was a honeypot, or that all periods practiced the same form of sexual entrapment. The strongest historical conclusion is narrower and more useful: gender expectations repeatedly shaped who could travel, meet, work, be trusted, or pass information, and intelligence actors sometimes made deliberate use of those conditions.

Mata Hari's afterlife shows how quickly a woman's intelligence work could be rewritten as sexual danger. The Romeo operations show the opposite operational direction, men cultivating women for access to government institutions. The Vanunu operation illustrates a reported female operative using romantic deception against a male target. Taken together, these cases prevent the thesis from assigning operational agency to one sex and vulnerability to the other.

DOI: **10.5281/zenodo.24482572**

The case chapters therefore treat gender as part of each operation's design and historical reception. They ask who had access, who was assigned to build trust, what information moved, and what the record can actually establish. Intimate influence is a human capability used by institutions, not a trait belonging to one gender.

DOI: **10.5281/zenodo.24482572**

Chapter 5.
Europe at War: Intimate Access and Intelligence, 1914-1945

5.1 From gendered access to operational evidence

Chapter 4 traced the history of gendered access and challenged the familiar image of the female seductress as the default figure in espionage. This chapter narrows the inquiry to Europe during the First and Second World Wars and the interwar years. It asks when personal relationships became part of a documented intelligence operation, what information moved through them, and what can be said about the operational result. The period is useful for comparison because states expanded intelligence services, communications interception, security investigations, and clandestine operations while social roles and wartime movement created both new access and new suspicion.

The evidence does not support a single, continuous European "honey-trap system" operating unchanged from 1914 to 1945. It supports a more differentiated history. In some cases, services deliberately used an intimate relationship to build confidence or obtain documents. In others, women or men gathered intelligence through professional, political, or social access without seduction. Still others became scandals in which an affair and a security concern were real, but an intelligence-directed romantic operation was not demonstrated. These distinctions matter because the existence of a relationship, even one involving an intelligence officer, does not establish that it was engineered for espionage.

The cases below are assessed on four separate questions: Was there an intelligence objective? Was an intimate relationship deliberately used? Was information actually transferred or access obtained? Can the result be measured or connected to a decision? Evidence of one does not answer the others. A service report may show what an interrogator was told, not necessarily what happened in full. Official institutional histories can preserve valuable records while also emphasizing an agency's success. Later memoirs may supply details absent from files but can magnify personal exploits. The chapter therefore gives priority to contemporary records, archival material, court records, and scholarship that compares those sources.

5.2 The First World War: intelligence systems and the uses of proximity

By 1914, European states had established military, diplomatic, and police intelligence functions, but the war enlarged their responsibilities. Neutral countries became sites for

DOI: **10.5281/zenodo.24482572**

observation, liaison, recruitment, sabotage, propaganda, and the movement of people and documents. Censorship and communications interception expanded alongside human intelligence. These methods worked together: an agent might provide context for an intercepted message, while interception could expose an agent or guide surveillance. The archive is uneven, in part because wartime services did not preserve or release every record, and later accounts often relied on sensational newspaper reporting (Debruyne 2014; Grawe 2025).

The period also encouraged "spy mania." A suspicious friendship, a foreign accent, a visit to a port, or a relationship with an enemy national could be interpreted as evidence of espionage. Such suspicion sometimes accompanied genuine counterintelligence work, but it also produced rumor, surveillance, and punitive attention to private life. The history of German women's relationships with prisoners of war, for example, documents official anxieties about fraternization and possible betrayal. It does not make those relationships evidence of spying. Lisa Todd shows how authorities and the public read sexual relationships as possible political disloyalty during wartime, demonstrating that anxieties about intimate contact could exceed proof of intelligence activity (Todd 2011).

For this chapter, the First World War cases illustrate three different patterns. Mata Hari became the archetype of the sexual spy, although the intelligence record remains disputed. Lizzi Wertheim was convicted alongside a male German operative after a relationship and shared travels helped form the circumstances of an espionage case, but the evidence of intelligence actually reaching Germany is uncertain. Women also served in intelligence and counterintelligence roles that relied on ordinary social access, professional skill, or infiltration rather than sexual entrapment. The difference between operational practice and public mythology is part of the historical record, not a side issue.

5.3 Mata Hari: intercepted messages, an execution, and a durable myth

Margaretha Zelle, known professionally as Mata Hari, was arrested in Paris in February 1917, tried by a French military court, convicted of espionage, and executed in October of that year. Those facts are not in dispute. The harder question is what she actually did for German intelligence and how much value her activity produced. Her contacts with German officers, her receipt of money, her dealings with French intelligence, and the French prosecution have all been interpreted through evidence created under conditions of war and secrecy. The available record does not warrant treating later claims about her as a complete account of her intelligence contribution.

DOI: **10.5281/zenodo.24482572**

Recent scholarship on German military attachés places the case within the broader intelligence activity of Arnold Kalle, Germany's military attaché in Madrid. French counterintelligence intercepted and decoded German radio transmissions. One message from Kalle contained details that helped French authorities identify Zelle. The intercept forms part of the evidentiary chain. It does not, on its own, establish that Kalle intentionally sacrificed her, that her relationship with him was a planned seduction operation, or that she had delivered substantial secrets. Historians have offered competing explanations for how the message was sent and what Kalle intended. The French Defence Historical Service also preserves the contested character of the case (Grawe 2025; Service historique de la Défense, n.d.).

The case's demonstrated result is therefore clearer on the counterintelligence side than on the collection side. A decoded message assisted French authorities in building a case and identifying a suspected agent. The extent and importance of intelligence Zelle passed to Germany remain uncertain. Her conviction and execution were consequential personal outcomes, but they do not measure intelligence value. Nor does the state's decision to execute her prove that she was a master agent whose actions changed the course of the war.

Julie Wheelwright's analysis of the "spy-courtesan" shows how the prosecution and later retellings fused female sexuality with espionage. Public accounts turned contested evidence into a persistent character type: the attractive woman who gains secrets through access to powerful men. That cultural afterlife obscured a wider intelligence landscape that included professional women, couriers, translators, informants, and analysts. It also invited later authors to treat sexual reputation as proof of operational method. The case matters here because its mythology became more definite than the public evidence about its intelligence yield (Wheelwright 2025).

Consequences for Mata Hari's alleged male targets remain unknown. The cited record does not establish that she passed important secrets to Germany, identify a target punished because of information she supplied, or trace a professional or family consequence to one of her relationships. Her own arrest, conviction, and execution are documented; the fate of any person she may have targeted cannot be attributed to her on the evidence available. (Service historique de la Défense n.d.; Wheelwright 2016, 2025.)

5.4 Lizzi Wertheim and Georg Breeckow: a male agent's relationship with a woman

A less familiar case complicates the assumption that the intimate intelligence story of the First World War was always a woman targeting a man. In 1915, Louise "Lizzi" Wertheim, a

German woman living in Britain, was tried with Georg Traugott Breeckow, who used the names George T. Parker and Reginald Rowland. The two were connected to German naval intelligence networks. Wertheim had met Johannes Wilhelm Brandt, a German agent and former lover, in Amsterdam in 1914. In 1915, Breeckow and Wertheim traveled together in Britain, presenting themselves as a couple while he sought information relevant to naval activity. The Old Bailey trial was held in camera, and the archival record includes the file "1915 Espionage charges: R Rowland and Mrs L E Wertheim" (The National Archives 1915, WO 141/3/1; Wheelwright 2025).

Wertheim's role cannot be reduced to a simple story of seduction. The relationship history, financial pressures, the male agent's movements, and the couple's travel formed a mixed operational context. Contemporary and later narratives disagree about how much naval information Wertheim collected and whether it reached German intelligence. Scholarship notes Breeckow's own later claims that he had manipulated Wertheim for his purposes and had not transmitted the intelligence attributed to her. An account of a woman observing or reporting on ships is not proof that the information was delivered, accepted, or used. The evidence supports a serious espionage case and a relationship-based channel of movement and access; it does not establish a measurable operational success.

Breeckow was convicted and executed in October 1915. Wertheim received a ten-year sentence. She remained in custody until 1920 and died at Broadmoor before completing her sentence. The prosecution established that officials regarded the case as a serious wartime threat, while later researchers have had limited evidence about the actual intelligence flow. Wertheim's sexuality and relationship became central to public accounts even though the operational record remains fragmentary. The case does not establish that German female agents generally used seduction.

This case is especially useful comparatively. A male operative's relationship with a woman appears to have been part of the circumstances through which they traveled and interacted with the environment. That fact should not be converted into a categorical claim that Breeckow recruited Wertheim through a deliberate "Romeo" plan, as the evidence presented in the trial and later scholarship does not establish the full design. Instead, the case asks whether a relationship created shared mobility and whether that mobility produced intelligence. The answer to the first question is better supported than the answer to the second.

The record establishes severe consequences for Wertheim and Breeckow but does not trace effects on their relatives. Breeckow was executed, and Wertheim remained imprisoned until 1920, when she died at Broadmoor before completing her sentence. The

sources cited here do not identify a family member prosecuted or establish how either family was affected. Nor do they identify a specific person harmed by intelligence that reached Germany; the actual transfer and use of information remain uncertain. (The National Archives 1915, WO 141/3/1; Wheelwright 2025.)

5.5 Interwar Britain: Olga Gray and the effectiveness of patient social infiltration

Olga Gray's work inside British communist organizations in the 1930s documents a woman agent using social trust and sustained participation without a romantic or sexual operation. MI5's Maxwell Knight recruited Gray to enter political groups, undertake secretarial work, and develop relationships with Communist Party leaders. Over several years, she gained trust, carried messages, and eventually helped expose a Soviet-linked network attempting to obtain classified plans from the Woolwich Arsenal. The National Archives publishes extracts from Knight's 1945 report and MI5 files concerning Gray and the spy ring (The National Archives n.d.).

Gray's access came through professional competence, political presentation, and patient social integration. She first attended meetings as a sympathetic enquirer, accepted volunteer typing work, and later held secretarial positions. In 1937, Percy Glading asked her to lease a flat that could be used for secret meetings. Gray recontacted MI5 and agreed to cooperate under its instructions. She learned that the flat was used to photograph confidential documents. In January 1938 she alerted authorities to Glading's planned receipt of material at Charing Cross. Police arrested Glading while he was receiving classified documents from Royal Arsenal engineer Albert Williams. The documents included defence-related plans. Glading and Williams were convicted and imprisoned; another suspect was acquitted (The National Archives n.d.).

Unlike some romantic entrapment cases, Gray's role can be connected to a concrete counterintelligence outcome: her reporting enabled authorities to intervene at the point of transfer and prosecute members of the ring. The case does not permit a full measure of what Soviet intelligence had already received through other routes or what additional intelligence the network might have acquired. It does show that sustained access, careful reporting, and institutional coordination can produce a verifiable security result without seduction.

The public framing of Gray also reveals the gender politics of counterintelligence. A contemporary magazine described her appearance as "bait," sexualizing an operation that the archival record presents as long-term infiltration through secretarial work and political participation. MI5's Maxwell Knight praised women's value to agent work but did so using

gender stereotypes. His report simultaneously rejects “Mata-Hari methods” as a model and argues that women’s secretarial skills offered access to organizational information. The record thus contains both an operational history and a male institution’s assumptions about women. Gray’s success should not be explained by a supposed feminine instinct; it is better explained by training, persistence, cover, and the information advantages produced by her role.

Gray’s case also provides a necessary control case for the thesis. The subject is intimate power, but not every operation of trust or personal access is sexual or romantic. Treating Gray as a “honeypot” would be inaccurate and would diminish the skill involved in social infiltration. Her case belongs in the comparative account because it shows what long-term access can achieve and helps identify which elements of a genuinely intimate operation are distinctive.

The operation ended in arrests and convictions for Percy Glading and Royal Arsenal engineer Albert Williams, while another suspect was acquitted. Gray’s reporting helped authorities interrupt a document transfer, but the sources used here do not describe a criminal penalty or public exposure imposed on Gray. They also do not trace consequences for her family or establish the later personal circumstances of the convicted men’s families. The documented outcome is the disruption and prosecution of the network, not a complete account of its private aftermath. (The National Archives n.d., “Olga Gray and the Woolwich Arsenal Spy Ring.”)

5.6 German intelligence and Hildegard Beetz: a documented effort to win Ciano’s confidence

The strongest documented intimate operation in this chapter concerns Hildegard Beetz and Galeazzo Ciano, Italy’s foreign minister under Mussolini. In late 1943, after Ciano was imprisoned following Mussolini’s fall, Beetz was assigned by the German security service’s foreign intelligence branch to serve as an interpreter and gain Ciano’s confidence. A declassified American interrogation report dated June 14, 1945 records Beetz’s account of her assignment, contact with Ciano, intelligence reporting, and efforts to obtain his papers. Because this is an interrogation document prepared after the war, it must be treated as a primary source whose claims require comparison, not as a neutral transcript of every operational fact (U.S. Army, 1945).

The report states that Beetz was sent to assist with interpretation and that her superior, Dr. Horst Hottl, directed her to gain Ciano’s confidence and report his political views. It describes her frequent meetings, efforts to secure documents, and communications with German officials. Beetz said she liked Ciano and wanted to save him, while denying that she had

been his mistress. This record supports an intelligence-directed relationship; it does not establish a sexual affair. The relationship may have included emotional attachment, strategic performance, or both, but those dimensions cannot be collapsed into a claim of a sexual liaison.

The operation pursued several forms of intelligence. German officials wanted insight into Ciano's political views and plans. They also sought his diaries and supporting Foreign Office materials. Beetz's interrogation describes her access to documents and her role in preserving a set of Italian Foreign Office records. The National Archives' account of the "Ciano Rose Garden Papers" explains that Ciano's diaries and supporting papers followed separate paths. His wife, Edda Ciano, carried the diaries out of Italy; Allen Dulles later arranged for them to be microfilmed. Beetz helped preserve and locate supporting records, including translated documents buried in a garden. These should not be conflated as though Beetz alone recovered the diaries themselves (National Archives and Records Administration 2013, 2016; U.S. Army 1945).

The immediate political context was lethal. Ciano and other officials were tried by the Italian Social Republic in Verona and executed in January 1944. Beetz's efforts to obtain or protect records intersected with plans to preserve Ciano's diaries and potentially secure his freedom, but the rescue did not succeed. The operation's intelligence outcome is therefore mixed. German intelligence obtained reports on Ciano's views and sought his papers; Beetz's account and the archival record support recovery or preservation of supporting documents. The attempt to secure Ciano's survival failed. After the war, the diaries and associated papers became part of the record used to reconstruct Axis decision-making.

The Nuremberg relevance must be stated precisely. Extracts from Ciano's diaries were used to challenge aspects of Joachim von Ribbentrop's defense. Scholarship reviewing trial records and prosecutors' files argues that the diaries had a positive effect in the proceedings. That evidentiary use cannot be credited solely to Beetz, because the diaries reached the Allies through Edda and Dulles. Beetz's contribution concerned the supporting records and the larger effort surrounding Ciano's papers. The case is still a strong example of intelligence work built on personal confidence because the operational assignment and reporting are documented, and because it connects individual intimacy to the preservation of politically valuable documents. It is not evidence that one relationship alone changed a verdict (Salter and Charlesworth 2006; National Archives and Records Administration 2016).

This case also complicates the gendered stereotype in two directions. Beetz was a woman serving a German intelligence service, but the record emphasizes her assignment, reporting, political assessment, translation, and document handling rather than reducing her to sexual

DOI: **10.5281/zenodo.24482572**

allure. Ciano was a powerful male official, but vulnerability in the case arose from imprisonment, political isolation, and his dependence on those who could reach him. The relationship was shaped by coercive state circumstances as much as by attraction. Here, intimacy operated within a prison setting where the target's freedom and future were already controlled by competing political authorities.

Ciano was tried and executed in January 1944; the effort to secure his survival failed. His wife, Edda, escaped with his diaries, while Beetz later preserved and directed American interrogators to supporting papers. The sources cited here establish Beetz's postwar interrogation and document work, but do not establish that she was prosecuted or punished for the operation, or document lasting personal or family consequences for her. The record also does not support attributing Ciano's execution to Beetz's reporting or to the intimate relationship. (National Archives and Records Administration 1945, 2016.)

5.7 Amy Elizabeth "Betty" Pack and British Security Coordination

Amy Elizabeth Pack, commonly known by the codename Cynthia, was an American agent for British Security Coordination (BSC), the wartime organization coordinating British intelligence activity in the United States. Her case is frequently presented through a dramatic popular story in which a sexual relationship with a Vichy French official enabled the acquisition of diplomatic codes. The record supports a narrower conclusion: Pack operated for BSC, cultivated contacts including Vichy press attaché Charles Brousse, and provided information from diplomatic circles. The precise scale and operational effect of the material attributed to her require caution.

BSC's official history identifies Pack's participation and codename. The 1998 publication describes her work and claims that access to a Vichy official yielded information, including material relating to diplomatic communications. However, Pack's case officer and later biographer, H. Montgomery Hyde, acknowledged exaggerating parts of her exploits. The CIA's 2022 review of a later biography identifies Mary Lovell's research as a more reliable corrective and cautions readers against unsupported, romanticized accounts (British Security Coordination 1998; Peake 2022; Lovell 1992).

The romantic relationship was not simply an invented cover, but neither should it be assumed to have been emotionally false in every respect. Pack's relationship with Brousse provided a personal route into information and contacts. That route was operationally useful to BSC. Yet claims that a single code acquisition changed the course of the war are much stronger than the public evidence supports. A memoir or official history may report a dramatic success;

a defensible account asks what document was copied, when it was used, what other intelligence was available, and whether an identifiable decision followed. On those measures, the precise value of Pack's contribution remains difficult to quantify.

Pack's case therefore falls between a documented intelligence relationship and a later heroic narrative. The service connection is established, as is her involvement in BSC activity. Public sources attribute information gathering to her relationships, but the detailed operational record remains incomplete and parts of the story are contested by biographical research. Pack's case shows how a relationship could be genuine and operationally useful while later accounts exaggerated parts of her story. It also warns against equating an agent's personal life with a verifiable intelligence result.

The sources establish Pack's service for British Security Coordination and her information work, but they do not document a prosecution or official penalty for her or Charles Brousse arising from the relationship. They also do not establish a specific diplomatic decision or punishment of a person based on the information attributed to Pack. The public accounts reviewed for this case do not trace the private or family aftermath for either person. These outcomes remain unknown rather than evidence that the relationship carried no cost. (British Security Coordination 1998; Lovell 1992; Peake 2022.)

5.8 Soviet wartime women agents and the limits of the "honey-trap" claim

The Soviet Union deployed women in intelligence activity during the Second World War, including on German-occupied territory. Regina Kazyulina's research, drawing on Soviet intelligence reports, memoirs, and autobiographical accounts, documents women working under covers such as cleaners, waitresses, and secretaries. Some used social proximity and relationships with German personnel to collect information. German racial and gender assumptions could lead occupiers to underestimate Soviet women, creating operational opportunity. The evidence establishes women's participation and the diversity of their methods; it does not establish that every relationship was a deliberately engineered sexual entrapment operation (Kazyulina 2024).

The distinction matters because the phrase "Soviet honeypot" is often used without a named target, handler, dated order, transmission, or archival reference. Popular accounts sometimes describe centralized wartime sex schools or a systematic program of seduction as fact, but such claims require stronger evidence than repetition in later books or internet articles. The publicly accessible scholarship and records reviewed for this chapter do not provide adequate case-level evidence to verify an organized Soviet wartime European

campaign of romantic entrapment comparable to the documented East German Romeo program of the Cold War. This is a limit of the accessible record, not proof that no Soviet service ever used an intimate approach during the war.

What can be demonstrated is that Soviet women conducted espionage and resistance work through multiple methods, some of which depended on social relationships. These included maintaining cover, observing military activity, establishing trust, carrying reports, and placing themselves in domestic or service positions near German personnel. In occupied territory, such work took place under extraordinary danger. The operational objective might be to observe troop movements, identify collaborators, assess local officials, or transmit information to partisan and intelligence structures. To establish that a particular relationship constituted a honeypot, a case study would still need to show intentional romantic cultivation and an intelligence purpose.

This conclusion places Soviet operations within the thesis without repeating an unverified legend. It also preserves the importance of women's wartime intelligence work. A woman's employment as a maid or waitress could itself create proximity to an officer or installation. A flirtation might be part of a source's own initiative, a cover tactic, a genuine relationship, or later recollection shaped by the risks of occupation. Each possibility requires its own evidence. The historical record should not be made more certain merely because a sensational explanation seems plausible.

The public evidence reviewed here does not identify a specific wartime romantic operation with a named target and a complete record of personal fallout. It therefore cannot establish what happened to an individual target, an agent's family, or a person reported on through such a relationship. Soviet women faced substantial danger in occupied territory, but the general record of risk cannot substitute for case-specific evidence. For this section, individual target and family consequences remain untraceable. (Kazyulina 2024.)

5.9 Comparing operations and outcomes

The cases in this chapter vary in the strength of evidence and the kind of result they produced. The table separates the relationship mechanism from the intelligence outcome. "Known" means the public record supports that limited claim; it does not imply that all underlying service files are available.

Mata Hari, 1916-1917. Relationships with German and French intelligence figures are documented, but a deliberate seduction operation and the intelligence she delivered remain

disputed. French interception of Kalle's message contributed to her identification. Her arrest, conviction, and execution are established; the value of information she passed is not.

Lizzi Wertheim and Georg Breeckow, 1915. Their couple presentation, travel, and Wertheim's earlier relationship with German agent Brandt are documented in the case record. Naval information was sought or attributed to Wertheim, but delivery and use are uncertain. Breeckow was executed and Wertheim imprisoned. The operation was serious, but measurable collection is not established.

Olga Gray, 1930s. Gray used long-term political and professional infiltration, not romance. Her reporting helped expose classified Woolwich Arsenal documents being transferred. Authorities arrested members of the network and convictions followed. This is a strongly documented counterintelligence result, but not a honeypot.

Hildegard Beetz and Galeazzo Ciano, 1943-1944. German intelligence assigned Beetz to gain Ciano's confidence. Reports on his political views and her access to supporting papers are documented in interrogation and archival records. Ciano was executed; papers survived and later supported historical and legal reconstruction. The diaries' Nuremberg use cannot be attributed to Beetz alone.

Amy Elizabeth Pack, 1940s. BSC agent Pack used diplomatic and personal contacts, including a relationship with Charles Brousse. BSC records and later reviews support access to information, but the exact material and its utility are contested. Her intelligence work is established; its scale and strategic effect remain unmeasured.

Soviet women agents, 1941-1945. Women's espionage and social access roles are documented, although individual relationship-based operations are unevenly recorded. This chapter verifies women's intelligence activity, but not a centrally organized romantic-entrapment campaign in wartime Europe.

Intimacy did not invariably produce secrets. Access arose through different combinations of professional role, political trust, emotional attachment, social convention, and official direction. Beetz is the clearest case of an assigned effort to build confidence with a named target. The record on Pack confirms her service but leaves operational details incomplete, while later accounts exaggerated parts of her story. Wertheim's relationship is documented, but the information transfer remains uncertain. Gray's case shows that sustained trust could produce a security result without romance. Mata Hari's public image became more settled than the evidence about her intelligence value.

DOI: **10.5281/zenodo.24482572**

None of these cases allows a defensible overall success rate. The denominator is unknown: intelligence services conceal unsuccessful operations, successful recruitment may remain undiscovered, and public cases are selected because they ended in arrest, prosecution, or scandal. Even where records identify a document, it may be impossible to measure its influence against other sources. The responsible unit of comparison is therefore the individual claim: what was sought, what was transmitted, what survives, and what consequence can be traced.

5.10 Institutional consequences and the value of exposure

A failed or exposed operation can still have substantial consequences. Wertheim's sentence and Breeckow's execution show the personal stakes of wartime espionage prosecution. Mata Hari was executed after an intelligence accusation made during wartime; later scholarship disputes the certainty of the popular account. In the Beetz and Ciano case, the political execution of the target determined the limits of what the operation could achieve in the short term, while the survival of records later had historical and judicial value. Gray's penetration helped British authorities uncover an attempt to acquire defense documents and prosecute participants. Pack's case, by contrast, shows how secrecy and incomplete records can make claims of strategic success hard to evaluate long after the operation.

These consequences are not interchangeable. Prosecution can disrupt a network, deter other actors, or produce intelligence during interrogation. It can also punish a source or agent without revealing the full chain of command. A security breach may lead to revised procedures, but the historical file must demonstrate that reform. The public embarrassment of a scandal can create political costs without proving that an opponent obtained useful intelligence. This chapter therefore avoids treating publicity, arrest, or execution as a direct measure of operational success.

The institution is also part of the causal story. Services choose targets, define collection priorities, protect or fail to protect their personnel, and interpret evidence after exposure. Wartime governments may magnify danger to sustain public confidence or justify punishment. Interrogators can record self-serving accounts from captured agents. Biographers can turn partial records into a coherent adventure. The same archive can preserve evidence of a real operation and leave its most consequential claims unresolved. A history of intimate intelligence must examine both the relationship and the organization that directed, recorded, exploited, or later narrated it.

DOI: **10.5281/zenodo.24482572**

5.11 Conclusion: intimacy was one tool within a wider craft

European intelligence between 1914 and 1945 did not depend on one gendered technique. It drew on communications interception, political infiltration, couriers, professional access, local networks, document photography, false identities, diplomatic contacts, and personal relationships. In documented cases, women and men used intimate or social trust to approach people and places otherwise difficult to reach. Some operations deliberately sought confidence through a relationship. Other cases involved social access without romance, genuine attachment later used for intelligence, or accusations whose sensational framing exceeded the available proof.

The strongest case-level evidence in this chapter comes from Beetz's assigned effort to gain Ciano's confidence, Gray's prolonged infiltration of political networks, and the formal prosecutions of Wertheim and Breeckow. These cases involved different mechanisms and produced different levels of intelligence yield. The Mata Hari case remains a warning against treating accusation and sexual reputation as proof of successful espionage. Pack's service affiliation is documented, but the scale of her information work remains uncertain. Research on Soviet women agents confirms their substantial wartime intelligence activity while leaving the existence of a centrally organized European romantic-entrapment campaign unverified in the evidence reviewed here.

The historical continuity is therefore best stated as a continuity of opportunity: personal and social relationships could create access, trust, mobility, or proximity that institutions found useful. Operational forms changed with the state, technology, occupation, and workplace. Intimacy could contribute to collection, but it could also fail, expose an agent, yield little information, or become an exaggerated public story.

DOI: **10.5281/zenodo.24482572**

Chapter 6.
Cold War Recruitment and Compromise: Romance, Blackmail, and State Security

6.1 The Cold War as a comparative field

The Cold War made intimate access part of a wider and increasingly professional contest between intelligence services. Across divided Europe, diplomatic missions and government offices operated amid intense surveillance, restricted movement, and routine security suspicion. Intelligence organizations sought more than a single secret. They sought continuing access to offices, people, communications, and organizational routines. Romantic recruitment could serve that purpose, but it was one method among many. It could coexist with money, ideology, grievance, coercion, or ordinary human attachment.

This chapter compares several Cold War patterns. These include Soviet blackmail of British Admiralty clerk John Vassall; East German "Romeo" recruitment of West German women with government access; KGB same-sex entrapment of foreign men; and the recruitment of French counterintelligence officer Pierre Chaignot. It also examines Marine guard Clayton Lonetree and CIA support employee Sharon Scranage. The KGB effort to compromise French ambassador Maurice Dejean is strongly supported, but successful recruitment and information transfer remain unproven. Evidence quality differs across these cases. Some have parliamentary, court, or declassified records. Others depend on intelligence files accessed indirectly through a defector or on later accounts that cannot be independently confirmed.

The central comparison is not between "successful" and "failed" seduction. Each case is examined through distinct questions: What did the service seek? Was intimacy deliberately arranged or later exploited? What did the person actually disclose? How was the activity discovered? What effects can be traced beyond the individual? The answer to one question does not establish the others. A compromising encounter might be used to recruit, to silence, to punish, to shape conduct, or simply to create pressure. A romantic relationship can also result in voluntary cooperation without an explicit threat. These categories should not be collapsed.

The period further requires attention to law and institutional culture. In Britain and the Soviet Union, criminal law and social stigma attached to same-sex relations made private conduct unusually vulnerable to exposure. The security danger did not arise from a person's sexual orientation. It arose from a political and legal environment in which disclosure could threaten liberty, family, career, and reputation. The same principle applies to heterosexual

DOI: **10.5281/zenodo.24482572**

relationships: the threat's force depends on the target's circumstances and the institution's response, not on a presumed psychological defect.

6.2 John Vassall: staged exposure, coercion, and years of disclosures

John Vassall was a British Admiralty clerk assigned to the office of the Naval Attaché in Moscow from 1954 to 1956. Evidence status: A, documented recruitment and classified disclosures. During that posting, Soviet officials cultivated him through his relationship with a locally employed embassy worker, Sigmund Mikhailski, and drew him into a compromising same-sex encounter. British records and Vassall's later testimony describe a staged exposure followed by pressure from Soviet intelligence officers. In the early 1960s, Vassall passed classified information from his work in the Admiralty to the Soviet Union. He was arrested in September 1962, pleaded guilty to espionage, and received an eighteen-year prison sentence (The National Archives n.d., 1962-1963; Radcliffe Tribunal 1963).

The recruitment did not consist of one encounter followed by a simple demand. Recent archival analysis by Irina Roldugina, using Vassall's British security files and declassified American records about KGB officer Yurii Nosenko, reconstructs a multi-stage process. Mikhailski offered practical assistance and companionship in Moscow. Vassall believed the relationship to be private and friendly. A compromising situation was then created and photographed. Soviet officers used the images and the threat of exposure to exert pressure. Later contacts maintained the relationship and drew disclosures from Vassall after he returned to Britain. The case joined an apparent personal friendship to surveillance, staged sexual exposure, and organized coercion (Roldugina 2025).

Vassall's sexuality should not be written as a diagnosis or as an inherent security weakness. The 1963 tribunal examined the system that made his exposure dangerous: criminalization, prejudice, official discretion, and the fear of public disgrace. Parliament debated whether the scandal revealed weaknesses in personnel selection and security reporting. The Radcliffe inquiry found significant failures in the handling of warnings about Mikhailski and in the treatment of Vassall's posting and later vetting. Officials had received signs that the local employee might be under Soviet control, yet the information was not effectively acted upon (Radcliffe Tribunal 1963; Hansard 1963b).

The intelligence gain is certain in kind but not fully quantifiable in the surviving public record. Vassall photographed and disclosed classified documents that passed through several Admiralty departments, including Naval Intelligence and later offices dealing with defense matters. The government and tribunal described the breach as serious. NATO subsequently

DOI: **10.5281/zenodo.24482572**

reviewed the security implications for alliance information. Public accounts do not establish a reliable total of the documents actually received by Soviet intelligence, or show that a named British or NATO policy decision changed because of one specific document. The defensible finding is sustained access to classified material over a period of years and a breach broad enough to provoke a major inquiry and alliance-level review (The National Archives 1962-1963; NATO Archives 1963, 1964; Hansard 1962).

The case also entered public life through political controversy. The scandal exposed Vassall's espionage and the institutional failure to respond to warnings and protect staff from a known recruitment technique. Public debate often framed the issue through Vassall's sexuality and character, which risked relocating institutional responsibility onto the target. The historical record supports a different emphasis: Soviet officers exploited the legal and social consequences of exposure, while British officials failed to connect warnings and acted too slowly. The relationship was the opening through which coercion operated; institutional complacency allowed the resulting compromise to persist.

Vassall's case should not be treated as a representative account of all Soviet recruitment. It is an unusually well-documented instance of same-sex entrapment, but even it remains mediated by interrogation records, testimony, public inquiries, and the target's retrospective account. It does establish that the tactic was not merely a later rumor. The blackmail continued after Vassall left the location of the compromising incident. It became a long-term system of contact, payment, document photography, and control.

The personal consequences for Vassall included arrest, conviction, an eighteen-year sentence, imprisonment, loss of his civil-service career, and public exposure of the compromising material used against him. He was released on parole in October 1972. The records cited here document prison and institutional consequences but do not establish a spouse, children, or a specific family aftermath. His sexuality was treated publicly as part of the scandal, a cost intensified by the legal and social stigma of the period. (Radcliffe Tribunal 1963; National Archives n.d.; National Portrait Gallery n.d.)

6.3 The KGB and same-sex entrapment: operational practice beyond one case

The KGB's use of same-sex entrapment against foreign men was broader than the Vassall case. Evidence status: A for specific documented operations and B for the claimed scale of the wider program. Roldugina's study draws on newly declassified United States and British files concerning Nosenko, a KGB officer who defected to the United States in 1964 and described his work targeting American, British, and Canadian visitors to the Soviet Union. Nosenko's

DOI: **10.5281/zenodo.24482572**

authenticity was examined intensively by American intelligence. His claims about same-sex entrapment are supported in part by victim accounts and by other intelligence information, although his testimony was not a complete or unproblematic operational record. The value of the study is that it compares what Nosenko said with records created by the services that questioned him and the people who reported being targeted (Roldugina 2025).

Nosenko described selecting targets during surveillance, using recruited Soviet men to create compromising situations, arranging a controlled location, and presenting the encounter as a criminal or reputational threat. The tactic exploited Soviet criminalization of male same-sex activity and the anticipated consequences of exposure to foreign governments, employers, families, or the press. Roldugina reports that Nosenko stated he took part in fourteen operations in the 1955-1959 period, eight of which used same-sex entrapment. He also claimed that the KGB had arranged "hundreds" of such entrapments by 1959. The first figure concerns his own account and should be attributed to him. The larger figure is an estimate by a defector, not a verified service-wide count. It should not be converted into an established total.

The targets were not necessarily recruited because they were gay, and the available research does not warrant speculation about the private identities of individuals. The operational concern was that a person had been caught or could be shown engaging in prohibited conduct. That distinction prevents the thesis from turning state persecution into a claim of inherent vulnerability. The service exploited a legal vulnerability it helped create and maintain.

American journalist Joseph Alsop was the target of an attempted compromise that did not produce a demonstrated recruitment. In Moscow in 1957, Soviet intelligence obtained compromising material through a staged sexual encounter. Alsop promptly informed American officials, depriving the KGB of the secrecy on which blackmail depended. His case shows why an attempted operation cannot be equated with a successful one. Disclosure to one's own service can reduce the leverage of compromising material, though it may entail personal and professional costs. The incident is documented through the declassified records reviewed by Roldugina, who compares victim accounts and intelligence reporting rather than treating the KGB's account alone as conclusive (Roldugina 2025).

Roldugina also identifies operations in which same-sex entrapment overlapped with threats, detention, or physical coercion. These accounts show that "seduction" is sometimes a misleading shorthand. The operative could exploit a target's attraction, but the operation might turn on surveillance, a controlled room, police powers, and the threat of prosecution. Some targets may have been recruited; others resisted, reported the attempt, or left the country. The

DOI: **10.5281/zenodo.24482572**

publicly accessible record does not support a single success rate. Failed approaches are less likely than prosecutions or defections to leave a clear public narrative, and operational files remain incomplete.

This practice also shows why the thesis cannot define intimate intelligence only as a heterosexual woman's approach to an influential man. The KGB used male intermediaries to compromise male targets. Legal discrimination and homophobia provided the leverage. The method therefore belonged to a wider architecture of state power in which intimate conduct could be transformed into a threat by surveillance and law.

Joseph Alsop resisted the Moscow blackmail attempt by promptly disclosing it to American officials and the CIA; the public record does not establish that he supplied intelligence to the KGB or faced a legal penalty. Later reporting says photographs resurfaced among Washington contacts more than a decade later, creating a renewed reputational threat, while Alsop continued his journalism career. The available accounts do not establish family consequences. For other people described in the broader KGB practice, individual outcomes cannot be generalized from Alsop or traced without a named case record. (Roldugina 2025.)

6.4 The East German Romeo operations: long-term recruitment through relationships

The East German Ministry for State Security, or Stasi, developed a well-documented program in which male officers of its foreign intelligence directorate, the Hauptverwaltung Aufklärung (HVA), cultivated women employed in West German government offices. These operations became known as "Romeo" cases. Evidence status: A for an organized HVA approach, with individual recruitment histories varying in completeness. The HVA selected women whose work brought them near political or diplomatic information, including secretaries and administrative staff. Operatives presented themselves as suitable partners and built relationships over time. Some women were asked to pass documents after they had developed strong emotional attachments; in other cases, a woman knew her partner's intelligence role and chose to cooperate (Bundesarchiv, Stasi Records Archive n.d.; Maddrell 2014).

The Stasi's own records reveal that the target selection was organizational. A training document from 1987 reviewed the occupational characteristics of secretaries in West German ministries, the Federal Chancellery, the Foreign Office, and other sensitive institutions. It discussed their work routines, access, and potential vulnerabilities. The document records the service's study of an employment category and its vulnerabilities. It does not provide a count of

Romeo operations or prove that every woman in a named office was approached. The Federal Archives' accompanying material reports that West German counterintelligence identified 58 secretaries as espionage suspects between 1949 and 1987. That figure is not a count of Romeo operations, nor does it establish that all 58 were recruited through romance (Bundesarchiv, Stasi Records Archive n.d.).

Individual cases show how the method could produce significant information. A secretary working in the West German Chancellery passed internal documents to her East German partner over a long period. Another woman working in the Bonn Foreign Office removed decoded diplomatic telegrams from her office and handed them to her Romeo. A later case involved a woman who worked as an interpreter at the United States Embassy. CIA historical accounts, based on declassified files and interviews, describe the quantities of material in some cases as extensive, including thousands of documents. These examples establish that at least some relationships yielded sustained document access. They do not establish the total value of the program or show that every document altered policy (Central Intelligence Agency n.d.-b).

The operation's central technique was continuity. An agent did not need to break into an office if a partner could obtain documents through ordinary work. A relationship could outlast a posting, a transfer, or a change in political personnel. In some cases, the operative encouraged the woman to seek a job that increased access. The emotional relationship created a private channel through which documents could be requested and transferred. This was a combination of romantic trust and workplace access, not merely sexual compromise.

The women's agency varied. Some reportedly understood that their partners were East German agents and regarded cooperation as part of a relationship they had accepted. Others were deceived about the operative's identity or the truth of the relationship. Some described love as genuine even after learning the deception. The service's files and the prosecutions typically prioritized evidence of espionage, not the women's emotional experience. Later accounts risk flattening them into either naive victims or willing traitors. Neither category adequately represents every case.

The operation also depended on inequality within West German institutions. Women could have access to documents and routines while possessing limited rank, recognition, or influence. The HVA exploited both the emotional relationship and this division of labor. The intelligence service did not need to seduce a minister if a secretary could remove a document from a ministry. That insight complicates a focus on powerful men: intimate operations could target employees whose institutional access was substantial even when their formal status was modest.

DOI: **10.5281/zenodo.24482572**

The Romeo cases were exposed through several routes, including defections, counterintelligence investigation, and arrest after document transfers were detected. Some operations remained undiscovered for years. Public cases are therefore a selected sample. The archival program evidence is stronger than any claim of a complete count or a single success rate. The defensible conclusion is that the HVA used romantic relationships as a deliberate recruitment method and that certain individual agents obtained large volumes of sensitive information. The consequences varied with the content of the material, the length of the operation, and whether a source was identified before or after the service had collected what it wanted.

The personal consequences varied. CIA's historical account describes roughly forty West German women prosecuted over four decades; examples include a secretary sentenced to three years and another woman sentenced to four years and three months after learning that the staged marriage was false. Some relationships ended in prosecution and betrayal; other couples continued together and married after the operation. The same account says the Romeo operatives were not convicted after reunification, and Markus Wolf's six-year treason conviction was overturned. These uneven outcomes show that legal exposure fell more visibly on recruited women than on many of the men who had deceived them. The sources do not provide a consistent record of consequences for children or other relatives in each case. (Central Intelligence Agency n.d.-b; Stasi Records Archive n.d.)

6.5 France: Pierre Chaignot and the penetration of counterintelligence

Pierre Chaignot was a French police officer who worked in the postwar Allied sector of Berlin and later served in France's Direction de la Surveillance du Territoire (DST), the domestic security and counterintelligence service. Evidence status: B, strongly supported by KGB archive notes, with the full operational record not publicly available. A Soviet intelligence officer, Valentina Yukum, operated under the identity "Lydia" and the name Lydia Tows. The KGB recruited Chaignot in 1949, and the relationship became both intimate and operational. He supplied information to Soviet intelligence during the 1950s. The account of his case comes largely from the Mitrokhin archive, the notes copied by former KGB archivist Vasili Mitrokhin and later transferred to Britain, as examined in recent reporting by Jacques Follorou for *Le Monde* (Follorou 2025).

The relationship appears to have begun in the postwar environment of Berlin, where occupation forces, intelligence services, police personnel, and displaced people lived in close proximity. Yukum's cover and personal approach were part of a longer recruitment. Chaignot discussed marriage with her, and their relationship was known to some French colleagues.

That visibility paradoxically helped normalize it. The available account describes how the couple's relationship was treated as private and how the DST failed to identify the woman's fabricated identity in a timely way. The marriage request later prompted further scrutiny, but the security response remained ineffective for years.

According to the Mitrokhin material described by Follorou, Chaignot provided the KGB with substantial counterintelligence information, including information about French officers and agents in Germany. The KGB notes, as reported by Follorou, attribute to information he supplied the identification of fifteen French intelligence agents who were arrested and convicted in 1952. This is a specific result claimed in an internal Soviet record, not an independently audited total. A separate KGB summary cited in the same investigation lists 11 American, 3 British, 76 French, and 1 Swedish agents uncovered from February to October 1956 through information from French agents; the archive does not allow those larger totals to be assigned to Chaignot alone. These figures indicate the scale of the reported intelligence consequences while leaving their attribution bounded by the surviving, mediated record (Follorou 2025).

The relationship's operational value was not limited to the initial recruitment. Chaignot remained in police service in France, and Soviet intelligence sought to preserve the channel as his assignments changed. Recent reporting says he was eventually considered for a transfer closer to DST headquarters, but he did not take a position that would have placed him at the center of the service. The episode illustrates both long-term penetration and the limits of a handler's control. An agent could be valuable without following every career path the service preferred.

The case was not resolved through a public trial at the time. It came to broader attention through research into the Mitrokhin archive decades later. As a result, the evidence has a different character from Vassall's tribunal and court record. It is a strong case of Soviet romantic recruitment as represented in the KGB's own archival notes, but access to the original operational files is limited and the public record is mediated through the archive and subsequent reporting. The chapter classifies it as strongly supported, while distinguishing the documented recruitment claim from the exact measure of its consequences.

The consequences recorded in the Mitrokhin material are grave for the French agents whose identities were reportedly exposed: the KGB notes, as relayed by Follorou, attribute the arrest and conviction of fifteen French agents in 1952 to information from Chaignot. This number remains an internal Soviet claim rather than an independently audited total. Chaignot himself was not publicly tried in the period described, and the sources cited here do not

DOI: **10.5281/zenodo.24482572**

establish a later prosecution, family consequence, or documented personal aftermath for him or Yukum. The outcomes for the arrested agents' relatives are also not available in this record. (Follorou 2025.)

6.6 Maurice Dejean: a reported compromise operation, with recruitment unproven

Maurice Dejean, France's ambassador to the Soviet Union from 1955 until 1964, was the target of a KGB operation described by Soviet defector Yuriy Krotkov. A U.S. government counterintelligence reference identifies the operation against Dejean as Krotkov's most important provocation, and Krotkov testified publicly about Soviet operations after defecting in 1963. Historical scholarship also records that the story became public in January 1964 and that Dejean left his post the following month (U.S. Office of the Director of National Intelligence 2009; U.S. Senate 1970; Harris 2021; Le Monde 1964).

The account describes a long operation, reportedly involving a Soviet dancer, surveillance of Dejean and his wife, a staged affair, and material intended to compromise him. The operation was intended to give the KGB leverage over a diplomat with political connections to Charles de Gaulle. A limit remains: Krotkov's testimony and later accounts support a deliberate effort to compromise Dejean, but do not establish that he became a recruited Soviet agent or transferred classified information. The public record supports a compromise attempt and professional consequence, not a proven flow of intelligence or successful recruitment (U.S. Senate 1970; Harris 2021).

This case therefore fits classification B: a strongly supported compromise operation with important details based on a defector's account. The operation's outcome was not equivalent to successful recruitment. In January 1964 the story became public; Dejean departed Moscow in February and was replaced as ambassador. The chronology and reported fallout are documented, while any assertion that the KGB controlled his diplomatic conduct or influenced French policy remains unproven. These findings distinguish being caught in an operation from being blackmailed, recruited, or shown to have transferred secrets. Dejean's departure from Moscow after exposure also carried a diplomatic career cost, even though recruitment is not established.

Dejean's documented professional consequence was departure from the Moscow ambassadorship in February 1964 after the compromise story became public. The record supports neither a criminal prosecution nor proof that he became a Soviet source. Although his wife was reportedly drawn into the staged circumstances and surveillance, the sources cited

here do not establish what happened to their marriage or family, or any lasting personal consequence for her. Those private outcomes remain unknown. (U.S. Senate 1970; Harris 2021; Le Monde 1964.)

6.7 Clayton Lonetree: romantic recruitment without blackmail

Clayton Lonetree, a United States Marine guard assigned to the American Embassy in Moscow, became involved with a Soviet woman who worked in the embassy's customs section. She introduced him to a man presented as her uncle, known to Lonetree as "Sasha," whom U.S. officials identified as a KGB officer. Lonetree then provided information and received money. The relationship began in 1985, and the disclosures continued after he was transferred to Vienna. He surrendered himself to a CIA station chief in Vienna in December 1986 and confessed to having contact with Soviet intelligence. He was court-martialed and sentenced to thirty years, later reduced by five years in exchange for cooperation (National Security Council 1986; National Security Council Staff 1987; The Washington Post 1987, 1988; United States v. Lonetree 1992).

The official 1987 damage assessment is unusually useful because it separates confession from worst-case speculation. It records that Lonetree provided personality-assessment information about embassy personnel and admitted stealing three Top Secret documents from a communications room in Vienna. He said he had been tasked to plant listening devices in ambassadorial offices but denied doing so. The document lists other opportunities he might have had, but explicitly describes those as worst-case damage scenarios, not established acts. U.S. officials stated that he was not blackmailed. He willingly provided information after entering the relationship and meeting the KGB officer (National Security Council 1986; National Security Council Staff 1987).

That distinction changes the interpretation. Lonetree's case is evidence of relationship-based recruitment and access to embassy information, not evidence of sexual blackmail. His partner helped establish contact, but the service then used a handler, meetings, tasking, and payments. The relationship functioned as an entry point into a conventional human intelligence recruitment. The official file does not establish that affection alone explains his cooperation. In later statements, Lonetree described resentment and sympathy toward the Soviet system among his reasons. Motive must be described from the record, not reduced to romance.

The prosecution also illustrates the risks of early public reporting. Initial accounts alleged that Lonetree had arranged for Soviet agents to enter the embassy. A later government memorandum repeated additional claims made by another Marine, Arnold Bracy, about access

to secure areas. Those assertions must be attributed to Bracy and distinguished from Lonetree's own admissions and the material established at trial. The damage assessment separates the information Lonetree confessed to providing from what investigators feared he might have been able to do. The known disclosure was serious, but some reported details remained allegations rather than adjudicated findings (Levitsky 1987; National Security Council Staff 1987; United States v. Lonetree 1992).

The institutional consequences included a formal investigation of the security breach, review of access and guard practices, and a reassessment of other personnel who had contact with Soviet nationals. The case also exposed how routine social events inside an embassy could create contact opportunities. It does not follow that all personal relationships with host-country employees are suspicious. The security issue was whether contact was disclosed, whether personnel could seek confidential advice, and whether access to sensitive spaces and documents was adequately controlled.

Lonetree was convicted, sentenced to thirty years, had the sentence reduced to twenty-five years, and released in 1996 after serving about eight years. His conviction and imprisonment are documented. The public record reviewed here does not establish later family consequences or a specific effect on relatives. The operational response also included a security investigation and review of embassy access. (United States v. Lonetree 1990, 1992; The Washington Post 1987, 1988; The Virginian-Pilot 1996.)

6.8 Sharon Scranage and Michael Soussoudis: relationship, threat, and a diplomatic exchange

Sharon Scranage worked as an operations support assistant at the CIA station in Accra, Ghana. She began a relationship with Michael Soussoudis, a Ghanaian national and relative of head of state Jerry Rawlings, in 1983. The relationship was not initially established as an intelligence-directed seduction operation. The public court reporting and later CIA analysis indicate that Soussoudis learned about Scranage's employment and pressed her for information. Scranage later told investigators that he threatened harm to embassy personnel and family members if she did not cooperate. Her disclosures included the identities of CIA officers and Ghanaian informants, classified cable information, and material concerning political and military matters (Central Intelligence Agency 1990; The Washington Post 1985a, 1985d, 1985f).

The case shows how a relationship can shift from personal contact to coercive exploitation. Contemporary court reporting and the CIA's later analysis document Scranage's disclosure of

CIA source identities and classified information. She pleaded guilty to charges involving those disclosures. Prosecutors also described notes she had taken from classified reports and cables, including information about military equipment Ghana sought from Libya. The public record identifies categories of material but does not provide a complete inventory of everything transferred. The established consequence was a serious breach of source security and a diplomatic crisis; the exact intelligence loss remains unquantified (Central Intelligence Agency 1990; The Washington Post 1985a, 1985b).

The personal and institutional pressures were complex. Scranage's lawyer argued that the CIA had ordered her to end the relationship without explaining the threat, leaving her vulnerable to coercion. The CIA's later internal analysis examines the roles and decisions of both Scranage and Soussoudis, as well as the counterintelligence response. Such claims should not erase Scranage's guilty pleas or the information she disclosed. They do, however, raise a legitimate institutional question: whether an employee given a security instruction was provided enough context and support to follow it safely. The source record describes alleged threats; it does not justify a clinical diagnosis or an assumption that her emotions alone caused the breach.

The case produced consequences beyond the criminal proceedings. Scranage was sentenced to five years, later reduced to two. Soussoudis received a twenty-year sentence that was suspended on condition that he leave the United States within a day. The United States and Ghana then conducted an exchange involving Soussoudis and Ghanaian citizens held in connection with intelligence activity. The United States also worked to protect or remove people whose identities may have been compromised. American officials described the diplomatic work as an urgent effort to safeguard their personnel and Ghanaian contacts. These outcomes show a measurable political and security consequence: a romantic relationship that became a source channel contributed to the exposure of intelligence identities, evacuations, prosecutions, and a state-to-state exchange (The Washington Post 1985f, 1985c, 1986a; Fritts 2004).

This case does not fit a simple model of seduction. Scranage and Soussoudis had a relationship; he had ties to Ghanaian intelligence and political circles; he allegedly used threats; she transmitted classified material; and the governments negotiated after the exposure. Each element is documented at a different evidentiary level. The relationship explains access and opportunity. The threat helps explain the later coercion. Neither fact eliminates the question of agency or the need to identify specific institutional failures.

DOI: **10.5281/zenodo.24482572**

Scranage's sentence was reduced, and she became eligible for release after serving eighteen months; Soussoudis was released to Ghana as part of a state exchange rather than serving the twenty-year sentence imposed on him. The exposed CIA identities prompted efforts to protect or move affected personnel and Ghanaian contacts, but the public record does not identify every person relocated or establish the later circumstances of their families. Scranage's own family aftermath is likewise not documented in the sources cited here. The asymmetry between her imprisonment and Soussoudis's diplomatic release is part of the case's consequential record. (The Washington Post 1985c, 1985d, 1986a; UPI 1986.)

6.9 What the cases show about operational design

The Cold War cases reveal several operational forms rather than one universal "honey trap." Vassall was compromised through same-sex entrapment and then pressured over time. KGB officers also used staged same-sex encounters against foreign visitors, sometimes attempting recruitment and sometimes using exposure as leverage. HVA officers built long-term romances with women in administrative positions and sought sustained access to documents. Chaignot's intimate relationship with a Soviet operative became part of a longer penetration of French counterintelligence. Lonetree's relationship introduced him to a handler, and the official assessment states that blackmail did not occur. Scranage's relationship began outside a proven intelligence operation and was later exploited through an alleged threat and requests for classified information. Dejean is a strongly supported compromise attempt, but recruitment and information transfer remain unproven.

The target's institutional role affected the type of information available. A clerk or secretary might copy documents, names, itineraries, and internal communications. A guard might expose access routines, personnel identities, or facilities. A police officer inside counterintelligence could provide information about agents and investigations. A journalist or academic might be targeted for influence, access, or reporting, but the output would differ from classified documents obtained by an employee. The intelligence value is thus tied to occupational access as well as to personal relationships.

The cases also demonstrate that relationships can have different timelines. A staged encounter may create immediate leverage. A romantic recruitment may take months or years to establish trust. A preexisting relationship may be exploited only after one partner discovers the other's official role. A relationship may remain emotionally genuine for one participant even while the other is operating under service direction. These variations affect whether the operation can be sustained and what risks the service faces if the relationship ends or becomes visible.

Operational intent should not be confused with operational outcome. The HVA selected particular categories of women and some Romeos obtained substantial documents, but not every approach produced recruitment. Nosenko described numerous KGB operations, but his reported totals cannot serve as a complete service-wide count. Vassall's disclosures were real, but the precise volume and policy effect remain difficult to measure. Lonetree admitted to specific disclosures and thefts; other alleged acts remained unproven. Scranage's guilty pleas and court filings establish particular disclosures, while the full intelligence damage remains classified or otherwise unavailable. The Mitrokhin notes describe deep penetration in Chaignot's case, but they do not establish a causal link between every reported arrest and information he supplied.

These records make a general success rate impossible to calculate. We do not know the denominator of attempted operations, failed approaches, unreported disclosures, or cases that remain classified. Public cases are biased toward discovery and scandal. A more defensible comparison records the degree of evidence for intent, relationship, information transfer, exposure, and consequence separately. The same standard prevents sensational claims from making an operation appear more successful than the documents show.

6.10 Institutional responsibility, public exposure, and lasting consequences

Intimate recruitment is often narrated as a test of individual character. The Cold War files show that the organization can shape whether private contact becomes a security breach. The British Admiralty and Foreign Office failed to act on warnings that an embassy employee was under Soviet influence. The U.S. Marine Corps and embassy community did not ensure that Lonetree's contact with a Soviet national was reported, and the initial damage assessment had to separate admitted acts from feared possibilities. The CIA's handling of the Scranage case raises questions about how clearly employees were warned and supported when ordered to break off contact. The West German government's dependence on secretarial labor created access that the HVA deliberately targeted. The DST's handling of Chaignot and his partner shows how a visible relationship could be normalized while the partner's identity went insufficiently checked.

The security response after exposure varied. Vassall's arrest was followed by a public tribunal and NATO review. Romeo prosecutions revealed methods and sometimes induced operational changes, but years of successful collection had already occurred in certain cases. Lonetree's confession allowed a damage assessment, though key parts remained redacted. The Scranage disclosure triggered protection and evacuation efforts, diplomatic negotiations, and an exchange. Chaignot's case became public through later archive research rather than a

DOI: **10.5281/zenodo.24482572**

contemporary courtroom process. The Dejean story remains in the public domain without sufficient evidence to establish the alleged operational outcome. The route by which a case becomes visible influences what can later be known about it.

Exposure can injure the people caught in an operation, but it can also reveal the inequalities and assumptions within the institution. In Vassall's case, authorities had treated his homosexuality as a stigma and had failed to protect him from a known technique. The Romeo files show that West German institutions benefited from women's clerical work while underestimating the intelligence value of that work. The Scranage case reveals the consequences of disclosing informant identities to a government that could detain or harm them. The Lonetree file warns against publishing worst-case threat scenarios as if they were proven facts. Across cases, institutional responsibility includes both prevention and fair assessment after a breach.

The consequences also extend beyond direct document losses. A compromised source may expose other people, disrupt intelligence operations, reduce local willingness to cooperate, damage diplomatic relations, or shape security policy. The Scranage case produced an immediate risk to Ghanaian informants and a bilateral exchange. The Vassall case prompted parliamentary criticism and alliance review. The Romeo cases brought espionage prosecutions and personal trauma for women whose partners had deceived them. Such effects are documented in some cases and more difficult to measure in others. They should be traced individually rather than added together as a presumed geopolitical impact.

6.11 Conclusion: intimate access was a method, not an explanation

The Cold War record confirms that intelligence services used intimate relationships in different ways. The KGB staged same-sex entrapment and exploited criminalization and stigma. The HVA assigned men to cultivate women whose jobs offered access to West German government information. A Soviet officer used an intimate relationship to recruit Pierre Chaignot into French counterintelligence. Other relationships were not shown to have begun as service-directed operations but were later exploited, as in the Scranage case. Lonetree's relationship opened a channel to a handler, although U.S. officials concluded that he was not blackmailed. The effort to compromise Dejean is strongly supported, but recruitment and transfer of intelligence are not established.

The strongest evidence establishes more than the existence of romance. Vassall passed classified documents over several years under KGB pressure. HVA Romeo agents obtained documents from some West German government employees. According to KGB records,

Chaignot provided counterintelligence information. Lonetree admitted to specific transfers and theft. Scranage pleaded guilty to disclosing covert identities and classified information. The measurable gain differs by case. Some records quantify categories or specific items, but none supports a defensible overall success rate.

The comparison also shows why sexuality cannot be treated as the cause of espionage. Services exploited legal penalties, stigma, emotional attachment, workplace access, career opportunity, money, threat, and institutional neglect. These mechanisms could operate together. A relationship might be genuine for one party and operational for another. It might begin privately and become coercive only later. It might lead to extensive disclosure, a failed approach, or no proven information transfer at all.

Cold War intimate operations were therefore neither timeless nor uniform. They were built from the political conditions of divided Europe and the intelligence services that sought to exploit them. The operations acquired secrets and exposed people, penetrated offices, placed informants at risk, and forced organizations to confront security failures.

DOI: **10.5281/zenodo.24482572**

Chapter 7.
Capture, Deception, and Kompromat: Israeli, Chinese, Soviet, and Russian Cases

7.1 Scope and comparative method

This chapter compares three operations in which intimacy or compromising material served different purposes. The first is the Israeli operation that brought Mordechai Vanunu from London to Rome before his capture and return to Israel. The second is the relationship between French embassy employee Bernard Boursicot and Chinese opera performer Shi Pei Pu, which became an espionage case. The third is the 1999 public exposure of a sexual video involving Russian Prosecutor General Yuri Skuratov. These cases are not interchangeable. In the Vanunu case, deception facilitated capture after he had already disclosed information to the press. In the Boursicot case, trial testimony described a relationship later made conditional on access to embassy information. In the Skuratov case, intimate material circulated during a political conflict, but the identity and intent of those who obtained the recording remain unresolved.

The chapter also examines *kompromat* as a broader Soviet and Russian political-intelligence practice. The term refers to compromising material that may be collected, held, threatened, or publicized to influence or discredit a person. It can include sexual material, but it is not a synonym for a sexual entrapment operation. An embarrassing recording can be politically useful without having been produced by an intelligence service. A genuine relationship can be exploited without having been initiated by a service. A capture operation can use a romantic lure without seeking information from the person lured. Keeping these distinctions visible is necessary to answer the thesis question: what did intimacy actually enable, and what evidence establishes the outcome?

The evidence categories developed in Chapter 2 are applied here at the case level. Convictions, official inquiries, contemporary journalism, later recollections, and disputed attribution do not carry the same weight. For the Vanunu operation, his capture and prosecution are established, while the widely reported role of “Cindy” and the precise operational chain rest substantially on contemporary reporting and accounts attributed to Vanunu and his family. For Boursicot and Shi, a French court conviction establishes espionage, while trial testimony provides the principal public account of how the relationship became an information channel. It does not prove that the romance was designed as an operation from its

DOI: **10.5281/zenodo.24482572**

beginning. For Skuratov, the video's broadcast and its political context are established, but the claim that a state service staged the encounter or produced the recording remains contested.

This chapter does not use the cases to claim a uniform national method. Israeli, Chinese, Soviet, and Russian institutions had different aims, political settings, and operational traditions. Nor does it infer intelligence value from sexual scandal. Each case is assessed by separating the relationship, the service's documented role, the information sought, the information shown to have moved, and the consequences that can be traced.

7.2 Mordechai Vanunu: a romantic lure within a capture operation

7.2.1 What the record establishes

Mordechai Vanunu worked as a technician at Israel's Negev Nuclear Research Center. In 1986, after leaving Israel, he gave the British *Sunday Times* photographs and information about the facility. The newspaper published its investigation in October of that year. Before publication, Vanunu traveled from London to Rome. He disappeared there in late September and was subsequently returned to Israel, where he was tried and convicted for offenses connected with disclosure of state secrets. The broad fact that Israeli intelligence arranged his capture and return is strongly supported by contemporaneous reporting, his prosecution, and the later public record, although Israel did not publicly confirm every operational detail.

Accounts of the operation describe a woman using the name "Cindy" who met Vanunu in London and encouraged him to travel with her to Rome. The *Sunday Times* identified her as Cheryl Bentov, an American-born Israeli. Contemporary reports and later accounts attributed to Vanunu and his family likewise describe a woman's role in drawing him to Italy. The identity and role have been widely reported, but the precise operational record remains incomplete. The thesis therefore treats the romantic lure as strongly supported, while identifying its source base and the limits of official confirmation rather than presenting every published detail as an admitted Israeli account (JTA 1986; Los Angeles Times 1986, 2004; Times of Israel 2015).

Italian authorities investigated the alleged abduction. In response to a parliamentary question in 1997, the Italian government stated that the investigation had been archived in 1988 and that it had found no evidence of a violation of Italian sovereignty or international law. That statement is narrower than a finding that no abduction occurred. It records the result and status of the Italian inquiry; it does not erase Vanunu's disappearance, his later appearance in Israeli custody, or the substantial public reporting about the operation (Senato della Repubblica 1997).

DOI: **10.5281/zenodo.24482572**

7.2.2 What intimacy did, and did not, accomplish

The reported relationship with "Cindy" should be understood as an access and movement mechanism in a capture operation. By the time Vanunu met her, he had already supplied the *Sunday Times* with the material that prompted the investigation. The publicly available evidence does not show that the relationship recruited him, induced him to reveal the nuclear information, or secured additional secrets for Israel. It reportedly helped bring him to a location where Israeli agents could seize him. That distinction matters: the romantic approach facilitated physical capture, not a demonstrated intelligence acquisition from Vanunu.

The likely objective was to return Vanunu to Israel, prevent further uncontrolled disclosures, and place him within Israeli jurisdiction. These objectives are consistent with the sequence of events, but the operation's detailed orders and internal assessment are not fully available in the public record. It would be premature to state that the lure recovered documents, stopped all further disclosure, or materially changed Israel's nuclear posture. The *Sunday Times* had already published the core revelations, and the public record does not provide a defensible counterfactual measure of what the capture prevented.

Vanunu was prosecuted and sentenced to eighteen years' imprisonment, much of it spent in isolation. His confinement and later restrictions on travel and contact became subjects of international criticism. His case also intensified public scrutiny of Israel's nuclear ambiguity and the treatment of a person who disclosed information about a highly secretive program. The consequences are demonstrable at the personal and diplomatic level. They are harder to quantify at the strategic level: the operation silenced Vanunu as a freely accessible source, but it did not restore secrecy around information already published.

7.2.3 Evidence classification and interpretation

The case is classified **B: strongly supported, with operational details partly dependent on published accounts**. The capture, return, trial, and imprisonment are well documented. The romantic lure is supported by multiple published accounts, including contemporaneous reporting, but the most specific claims about Bentov's identity and the operational chain are not established through a publicly available Israeli after-action record. It is therefore appropriate to describe a reported romantic deception facilitating capture, while naming the attribution and limits.

The case contributes to the thesis in a specific way. Intimacy can be used to shape a target's movements and reduce resistance without being the source of intelligence itself. The operation's effectiveness should be assessed against its immediate purpose, capture, and its

limited capacity to reverse disclosures already made. This prevents the common narrative shortcut in which "honeypot" is used to imply that the target was seduced into giving secrets. The public record supports a more precise claim: a romantic approach reportedly helped arrange Vanunu's movement into the reach of an operation that returned him to Israel.

Vanunu's arrest, trial, eighteen-year imprisonment, long periods of isolation, and continuing restrictions after release are documented. The record used here does not establish a family consequence caused by the capture operation, and it does not show that the reported romantic contact produced the nuclear information at issue. The known fallout therefore attaches to his capture and prosecution, while consequences for any person who may have served as the lure remain uncertain. (Senato della Repubblica 1997; The Times of Israel 2015.)

7.3 Bernard Boursicot and Shi Pei Pu: relationship, recruitment, and uncertain beginnings

7.3.1 A relationship becomes an information channel

Bernard Boursicot was a young French embassy employee in Beijing when he met Shi Pei Pu in 1964. Shi was a male opera performer and librettist. Boursicot testified that he believed Shi to be a woman and that they maintained a relationship over many years. The story later attracted sensational attention because it challenged Boursicot's account of what he believed and because the court case involved espionage, sexuality, and gender presentation. For historical analysis, the sensational frame is less useful than the question the trial record can answer: when and how did the relationship become connected to the transfer of information?

According to Boursicot's testimony at the 1986 trial in France, after returning to Beijing in 1969, he was approached by a Chinese official or intelligence contact known as Kang. Boursicot said Kang offered to allow him to continue seeing Shi if he provided information from the French embassy. He testified that he feared Shi would be persecuted if he refused. French prosecutors argued that Boursicot had transmitted documents to Chinese intelligence. Contemporary trial reporting stated that approximately 150 documents were involved. Boursicot and his defense disputed the value and sensitivity of the material. The court convicted both men of intelligence activity with a foreign power and sentenced each to six years in prison (Le Monde 1986a, 1986b).

The conviction is strong evidence that the relationship was linked to espionage, but the public trial account does not establish that the relationship was initially created by an intelligence service. Boursicot's testimony portrays the recruitment as a later intervention into

an existing relationship. This remains an account given by a defendant at trial, reported by contemporary journalists; the full Chinese intelligence file and the full French case record are not openly available for independent reconstruction. The safest conclusion is that the relationship became an intelligence channel and that the court found espionage had occurred. Whether Shi was an intelligence-directed seducer from the first meeting is not established by the accessible record.

7.3.2 Access, coercion, and the measure of intelligence gain

The case illustrates a form of recruitment in which an existing attachment may be converted into leverage. The reported offer was not simply money for documents. It framed access to Shi and the continuation of a relationship as conditional on Boursicot's cooperation. His testimony also described fear for Shi's safety. Such a mechanism blends attachment, perceived obligation, and coercion. It is not possible to determine from the trial reporting how much Boursicot's choices arose from emotional commitment, fear, self-deception, or other motives. The chapter therefore avoids a psychological diagnosis and treats the motivations as matters testified to, not independently measured facts.

Contemporary accounts do not even give a uniform count. A *Le Monde* report from the trial described approximately 150 reports and notes delivered during the relevant period. A UPI report on the verdict described 30 French documents handed to Chinese officials between 1977 and 1979. These figures may reflect different definitions, periods, or categories of documents, but the public record cited here does not reconcile them. They are prosecution-era counts, not verified measures of the classification, sensitivity, or operational value of each item. Boursicot's account that many were public or insignificant conflicts with the prosecution's characterization. Without a publicly accessible itemized inventory and independent intelligence assessment, the thesis cannot calculate the value of the material or assert that a specific French policy decision was influenced. The case proves an espionage conviction and an information channel more clearly than it proves the strategic effect of each disclosure (Le Monde 1986a; UPI 1986).

The institutional consequences included criminal convictions, imprisonment, and scrutiny of French diplomatic security. The prosecution also exposed the difficulty of assessing access risks when an employee's private life is intertwined with a foreign environment and when an intelligence service can exploit the relationship. Yet this case should not be used to claim that sexual deception is uniquely effective. The mechanism documented in the trial was access to embassy information combined with a conditional relationship and fear of consequences for

DOI: **10.5281/zenodo.24482572**

the partner. The same structural vulnerability could arise through a nonsexual intimate bond, family tie, friendship, or other dependency.

7.3.3 Gender, performance, and retrospective storytelling

Popular accounts often reduce the affair to a story about a man being "fooled" by a woman. That description obscures both the evidentiary record and the analytical question. Shi was a man whose performance and presentation were read by Boursicot through the expectations and conventions of their context. The court case addressed espionage, not a universal explanation of identity or sexuality. The thesis uses the names and descriptions appropriate to the historical record and does not impose present-day categories where the evidence does not warrant them.

The relationship also unsettles a simple gender model in which an attractive woman seduces a powerful man for an intelligence service. Boursicot was neither a senior decision-maker nor a high-ranking official. His role gave him access to embassy documents, and the relationship reportedly became a means of recruitment. The operational value came from his position and his ability to obtain information, not from his political authority. Shi's sex and gender presentation do not, by themselves, prove the original intent behind the relationship. The case is therefore best treated as a documented espionage relationship with unresolved origins, not as proof of a deliberately planned female honeypot.

Classification: **A for espionage and conviction; B for recruitment through the relationship; unresolved for an intelligence-directed romantic operation from its inception.** This layered classification keeps each element of the case distinct.

The court imposed six-year sentences on both men. French President François Mitterrand pardoned Shi after about eleven months in prison; Boursicot remained imprisoned and later spoke publicly about the relationship and his sense of betrayal. A later profile reported that he attempted suicide while incarcerated. The sources cited here do not establish a lasting family consequence for either man, and they do not identify a separate person punished because of the information. These personal outcomes should be distinguished from the uncertain intelligence value of the documents. (Le Monde 1986a, 1986b; UPI 1986; The Washington Post 2017; Los Angeles Times 2009.)

DOI: **10.5281/zenodo.24482572**

7.4 Soviet and Russian *kompromat*: a practice, not a single tactic

7.4.1 Defining the term carefully

Kompromat is a Russian abbreviation for compromising material. In political and intelligence settings it may refer to information gathered to pressure a person, threaten exposure, undermine credibility, or shape public debate. The material may concern corruption, private conduct, professional misconduct, financial dependence, or other vulnerability. Sexual material can be part of it, but is neither necessary nor sufficient. The term describes the potential use of compromising information; it does not establish who gathered it, whether a service directed the collection, or whether the target was recruited.

Soviet and Russian political systems have generated a large body of claims about surveillance, blackmail, disinformation, and personal compromise. The historical record is uneven. Some accounts are based on official files, court proceedings, or multiple contemporaneous records. Others depend on defectors, memoirs, anonymous sources, or later political accusations. Even archival materials require attention to provenance. The Mitrokhin papers, for example, are notes selected and copied by a former KGB archivist and later deposited in an archive. The Churchill Archives Centre describes the collection and its provenance; it does not certify every statement in those notes as independently verified fact (Churchill Archives Centre n.d.).

This evidentiary caution does not imply that Soviet or Russian services never used compromising material. It means that claims must be made at the level supported by evidence. A source may establish that a recording existed, that it was broadcast, or that a person was threatened. It may not establish who arranged the encounter, who operated the camera, or whether intelligence officers controlled the distribution. The distinction between collection, possession, threat, publication, and recruitment is central to the chapter's analysis.

7.4.2 Continuity and change

The broad institutional logic of compromising material is to convert private or professional vulnerability into an instrument of power. That logic can continue across political systems even as the technologies and audiences change. Earlier operations could depend on physical surveillance, a staged encounter, a controlled photograph, or a threat delivered privately. Later operations could use broadcast television, leaked documents, digital files, or online publication. Continuity in the function of leverage does not prove that every episode descended from a single doctrine or that each was directed by a security service.

DOI: **10.5281/zenodo.24482572**

The difference between a private threat and public release is consequential. A confidential threat seeks compliance while preserving the target's utility and the secret's value. Public exposure can permanently damage reputation and discredit an office, but it may make the target less useful as a source. Public release can also redirect attention from the underlying allegation that the target was investigating. In such cases, the compromising material may work as a political weapon even when it produces no classified information at all.

There is also a difference between evidence collection and evidence manufacture. A service may record conduct that actually occurred, selectively edit it, or fabricate material. The existence of a recording does not establish authenticity, completeness, or the circumstances in which it was made. In the digital era, this problem becomes more acute because synthetic or manipulated media can imitate compromising evidence. The historical cases in this chapter concern older forms of recording and publicity, but they point toward the evidentiary challenges taken up in Chapter 9.

7.5 Yuri Skuratov: intimate material in a political struggle

7.5.1 The public sequence

In 1999, Russian Prosecutor General Yuri Skuratov was involved in investigations into allegations of corruption connected to senior figures around President Boris Yeltsin. A video showing a man resembling Skuratov in a sexual encounter with two women was broadcast on state television. Skuratov said the man was not him and characterized the recording as fabricated or as an effort to discredit him. Accounts differ in how they describe his precise response over time. The recording became part of an intense political dispute over his office and investigations. Yeltsin's administration sought his removal; the Federation Council initially declined to approve his resignation, and the political conflict continued (UPI 1999; The Washington Post 1999; U.S. Senate Committee on Foreign Relations 2018).

The timing gave the recording an obvious political effect. It shifted attention from the substance of investigations toward the prosecutor's private conduct and credibility. Contemporary reporting described the source of the tape as unclear and recorded Kremlin denials of official involvement. Later accounts attributed the operation to the FSB or to political actors close to Vladimir Putin. A former KGB general was quoted as describing it as an FSB operation. These attributions are significant evidence of what observers and participants alleged, but they are not the same as an official finding, a court judgment, or a proven chain of custody.

DOI: **10.5281/zenodo.24482572**

The case is especially useful because it shows a mechanism of institutional compromise without a proven romantic recruitment. The publicly visible product was the tape. The record does not establish that the women were intelligence operatives, that the encounter was staged, that Skuratov was secretly filmed by an intelligence service, or that he was offered a private bargain in exchange for stopping an investigation. The service attribution remains contested. Claims that Putin personally delivered or arranged the tape should be attributed to their sources rather than stated as established fact.

7.5.2 Did the tape change decisions?

The case had measurable political consequences: the tape was broadcast; Skuratov's fitness and credibility became a subject of public debate; and the institutional contest over his position continued. The recording did not, however, immediately secure his removal. The Federation Council rejected his departure at an early stage, and reporting later described his return to investigative activity. A Senate committee report published years afterward summarized multiple competing accounts, including Skuratov's claim that the tape was fabricated and the views of former intelligence officials. That report is a useful secondary synthesis, but it does not resolve the tape's provenance (U.S. Senate Committee on Foreign Relations 2018).

The underlying corruption investigation and Skuratov's treatment must not be collapsed into one causal story. The tape could have been intended to weaken him, whether or not a security agency made it. His eventual loss of office may have resulted from several political and institutional forces. The available evidence does not support a precise claim that the recording alone caused a particular government decision, terminated a specific investigation, or transferred classified information to a foreign power. The strongest conclusion is narrower: a sexual recording was weaponized in a high-level political conflict, with effects on public credibility and institutional legitimacy, while authorship and operational direction remain unresolved.

Classification: **C for reported state-directed kompromat; D for a documented political scandal with security and institutional implications but no established intelligence-directed seduction operation.** This distinction preserves the case's significance while preventing an uncertain attribution from becoming fact.

Skuratov's career and public standing were affected by the scandal, but the tape did not immediately remove him from office and its role in his eventual departure remains disputed. The two women shown in the recording were not established in the sources as intelligence operatives, and their later personal or family outcomes are not documented. The public record does not establish a prosecution or other penalty for them, nor does it prove that the tape alone

ended a particular investigation. (UPI 1999; The Washington Post 1999; U.S. Senate Committee on Foreign Relations 2018.)

7.6 Comparison: three different uses of intimacy

The cases can be compared by the function intimacy served. Vanunu's reported romantic encounter helped move a person into the reach of a capture operation. Boursicot's relationship with Shi became, according to trial testimony and the court's judgment, a channel through which embassy information was obtained. The Skuratov video was used publicly to undermine a prosecutor during a political struggle, but recruitment, service authorship, and the staging of the encounter are not established. These are three different operational or political outcomes: capture, information acquisition, and reputational attack.

7. **Vanunu and "Cindy."** The capture is strongly supported, while details of the romantic lure rely partly on published accounts. The lure reportedly induced travel from London to Rome. There is no public evidence that the relationship yielded nuclear secrets, which Vanunu had already given to the *Sunday Times*. Established consequences include his capture, prosecution, imprisonment, and continuing diplomatic controversy.
8. **Boursicot and Shi Pei Pu.** The espionage conviction is established, while the recruitment account comes principally from trial testimony. The existing relationship was reportedly made conditional on embassy information. Prosecution-era document counts conflict, and the material's sensitivity and value remain disputed. Established consequences include convictions, six-year sentences, and exposure of a diplomatic security breach.
9. **The Skuratov video.** Its broadcast is established, while authorship and service direction are disputed. Sexual material was publicized in a way that damaged the prosecutor's credibility. No classified transfer or recruitment is demonstrated. Public controversy and pressure on a senior prosecutor are established, but the recording's causal role in later decisions remains uncertain.

The table makes a broader point about measuring success. A service or political actor may achieve an immediate tactical purpose without obtaining intelligence. A captured source can be silenced, but capture does not undo disclosures already published. A long relationship can create access, but a document count does not tell us how useful the information was. A scandal can damage an official's legitimacy without proving that a service created the compromising material or gained control over the official.

The cases also show why gender cannot be reduced to the image of a woman seducing a powerful man. In the Vanunu account, the reported lure was a woman and the target was a male source, but the purpose was reportedly capture after the disclosures. In the Boursicot

DOI: **10.5281/zenodo.24482572**

case, a male performer's identity and presentation complicated the target's understanding, while the court found a relationship connected to espionage. In the Skuratov case, the women in the video became part of a public narrative, but the evidence does not establish their operational role. Across the cases, institutional access, political aims, and control of information explain more than gender stereotypes alone.

7.7 Findings and limits

Four findings emerge. First, intimate deception does not have one operational purpose. It can facilitate access, recruitment, movement, capture, coercion, or public discrediting. The analyst must identify the specific function rather than label every scandal a honeypot.

Second, intelligence gained must be measured independently from material discovered or publicized. In the Boursicot case, approximately 150 documents were reported in the prosecution, but the available record does not establish the value of each. In the Vanunu case, the relationship reportedly assisted capture, but the nuclear information was already in the hands of journalists. In the Skuratov case, compromising material affected public debate, but no intelligence transfer is demonstrated. The evidence therefore permits case-specific conclusions, not an aggregate success rate.

Third, the conversion of intimacy into leverage is not always present at the beginning of a relationship. Boursicot's trial testimony described a later offer tied to continued contact. Vanunu's reported romantic encounter appears to have served an immediate logistical purpose. The Skuratov case may involve deliberate recording, but the source and circumstances remain unresolved. The chronology of each relationship is therefore not a side detail; it determines what can reasonably be called recruitment, entrapment, or exploitation.

Fourth, institutional consequences can be real even when the alleged operation is not fully proven. A service may remain unidentified, while a target is captured, prosecuted, exposed, or politically weakened. Yet the thesis must distinguish consequence from attribution. Evidence that a person's reputation suffered does not independently prove who created the material or why.

The limitations are substantial. Israeli operational records concerning Vanunu are not publicly available in a form that would settle every detail. The accessible record of the Boursicot prosecution is mediated through court reporting, and Chinese service records are not open. The Skuratov tape's provenance and authenticity remain disputed. The analysis therefore avoids claims about secret orders, exact intelligence value, or causal impact on policy where

DOI: **10.5281/zenodo.24482572**

the public evidence is insufficient. These gaps are not invitations to fill the record with speculation; they define what the chapter can and cannot establish.

7.8 Conclusion

The cases examined here reveal an architecture of intimate power with several distinct components. A relationship can influence where a target goes. An attachment can be converted into a condition for cooperation. Private material can be used to redirect attention and weaken an institution. But these mechanisms must not be collapsed into a single story of seduction followed by secrets. The Vanunu operation concerns a reported romantic lure and capture. The Boursicot case concerns a relationship that became an information channel and resulted in convictions. The Skuratov affair concerns public kompromat whose authorship remains unproven.

The central thesis is supported in a qualified way: private intimacy can become a route through which information, leverage, and institutional power move. Whether that route produces useful intelligence, successful recruitment, or a political decision depends on the target's access, the operation's design, the timing of exposure, and the reliability of the evidence. The cases do not demonstrate a timeless or uniform method shared by all intelligence services. They show recurring opportunities to use trust and private vulnerability for state or political ends, with materially different results.

Chapter 8 examines contemporary political and corporate cases, including the reported cultivation and access allegations concerning Christine Fang and Eric Swalwell, and the reports concerning Alice Huang, Jensen Huang, and Megaspeed. It keeps official findings, press reporting, and unverified allegations separate. The same standards applied here govern that analysis: identify what is documented, measure what information was actually obtained, and do not infer guilt or intelligence transfer from a relationship alone.

DOI: **10.5281/zenodo.24482572**

Chapter 8.
Political Access, Corporate Networks, and Contemporary Espionage Claims

8.1 Scope and evidence rules

This chapter examines the reported cultivation of American political figures by Christine Fang, the allegations concerning Alice Huang and NVIDIA, and the corporate and export-control questions surrounding Singapore-based Megaspeed International. It also places the Jonathan Pollard espionage case beside these newer episodes as a documented benchmark for what an established foreign intelligence operation can look like in the public record. Pollard's case occurred in the 1980s and did not involve intimate recruitment. It is included here as a comparison, not as a contemporary case or a honeypot.

The distinction is essential. A relationship may provide political or corporate access without producing intelligence. A company can be investigated for export-control or false-declaration concerns without having been directed by an intelligence service. A government may assess that a person is an intelligence asset, while the public record remains too incomplete to demonstrate the basis, exact tasking, or information transferred. Allegations about intimate relationships can also become entangled with political conflict, corporate governance, export policy, and sensational media narratives. These are separate lines of inquiry and are treated separately below.

The evidence categories from Chapter 2 apply to individual claims, not to an entire case. A reported intelligence assessment can support analysis of a serious concern without publicly establishing its basis, tasking, or information transfer.

8.2 Jonathan Pollard: a documented Israeli espionage benchmark

8.2.1 Recruitment and collection

Jonathan Jay Pollard was a U.S. Navy intelligence analyst who delivered classified information to Israeli intelligence between June 1984 and November 1985. The FBI's historical account identifies Israel as the foreign government for which he worked and records his arrest outside the Israeli Embassy on November 21, 1985, his guilty plea, and his life sentence. The U.S. Court of Appeals described an approximately eighteen-month operation in which Pollard removed large quantities of classified information, copied it, and delivered it to Israeli

DOI: **10.5281/zenodo.24482572**

government agents. In the later phase, he received regular tasking and monthly payments from his handlers (Federal Bureau of Investigation n.d.-b; United States v. Pollard 1992).

The declassified 1987 intelligence-community damage assessment says Pollard's operation focused on U.S. intelligence about Arab and Islamic states, including military forces and equipment, as well as Soviet military capabilities and technology. The report's public version redacts the exact number of compromised documents. It concludes that the material created serious risks to U.S. intelligence interests and sources and methods. The court record separately describes the government's position that the damage was substantial and irrevocable. These records make Pollard a documented example of intelligence acquisition, rather than a case inferred from a private relationship or a political accusation (Director of Central Intelligence 1987; United States v. Pollard 1992).

8.2.2 Why Pollard is a comparator, not an intimate operation

Pollard's known recruitment does not fit the thesis's central category of intimate manipulation. The court record describes ideological motivation, Israeli handlers, tasking, classified document removal, payments, and assistance from his wife after he came under investigation. It does not describe a romantic relationship created or exploited by Israeli intelligence to recruit him. Anne Pollard's assistance in removing documents was part of the concealment response, not evidence of a sexual or romantic entrapment plan.

The case remains valuable to this study because it supplies a comparison standard. It shows the kinds of evidence that can substantiate foreign-directed espionage: a guilty plea, a judicial record, an intelligence-community damage assessment, identified handlers, tasking, and documented transfers. Those elements are absent from the publicly available evidence concerning the newer Alice Huang allegations. The contrast does not determine whether those allegations are true. It explains why a thesis should not treat a reported intelligence assessment as equivalent to a conviction and a partially declassified operation record.

Pollard also shows why actual information transferred must be distinguished from information investigators recovered or reviewed after arrest. The U.S. government's damage assessment was based on post-arrest debriefings and document receipt records. Its public release still redacts key figures. Even in a case with a conviction and extensive records, the public cannot quantify every item's intelligence value. That limitation is directly relevant to the contemporary cases, where the public record is less complete.

Pollard received a life sentence and served thirty years before his 2015 release on parole. The parole restrictions initially kept him in the United States; after they ended in 2020, he

moved to Israel and reunited with his wife, whom he had married while he was imprisoned. The record documents long separation and eventual reunification, but the sources cited here do not establish the broader effect on his family or children. These are consequences of his prosecution and sentence, not evidence of intimate recruitment. (United States v. Pollard 1992; The Washington Post 2020; The Times of Israel 2020.)

8.3 Christine Fang and Eric Swalwell: access, warning, and limits of the public record

8.3.1 Reported cultivation

In December 2020, Axios reported that Christine Fang, also known as Fang Fang, had developed relationships with local politicians in California and elsewhere, including Representative Eric Swalwell. The reporting described her as a suspected Chinese intelligence operative and said that she participated in fundraising activity for Swalwell's 2014 campaign, attended political events, and helped place an intern in his congressional office. The same account said federal investigators gave Swalwell a defensive briefing around 2015, after which he cut off contact with Fang and cooperated with the FBI. Axios reported that U.S. officials did not believe Fang had obtained classified information from Swalwell and that he was not accused of wrongdoing (Axios 2020b).

The public reporting supports the conclusion that counterintelligence officials were concerned about Fang's political cultivation and that she had social and campaign access to several politicians. It does not establish that Swalwell knowingly acted for China, that he passed classified information, or that the fundraising involved illegal contributions. The distinction between access and exploitation matters. A foreign operative may seek familiarity, introductions, or a map of emerging political networks even if no classified information is obtained. Yet that general operational possibility does not prove what Fang acquired in this particular case.

8.3.2 Institutional review and consequences

The House Committee on Ethics reviewed allegations that Swalwell may have violated House rules, laws, or other standards through his interactions with Fang. In May 2023, the committee said it would take no further action. It advised members to remain alert to improper foreign influence attempts and recommended that Swalwell contact the House Office of Security for guidance. The committee's closure neither established Fang's intelligence role nor

found that Swalwell committed misconduct. It documents the outcome of the committee's review (House Committee on Ethics 2023a; House Committee on Ethics 2023b).

The public record changed in August 2026 when the White House released declassified FBI interview summaries from interviews with Swalwell in 2015 and 2016. The summaries state that he told FBI agents he had physical relations with Fang on a handful of occasions, while saying they did not date or have a romantic relationship. They also record his account of an encounter at his apartment that he said he barely remembered after taking Ambien. This release materially changes what can be said about the nature of their contact. It does not, by itself, prove Fang used the relationship under Chinese intelligence direction or that Swalwell knowingly cooperated. Because the records were released through a White House transparency initiative amid a highly partisan political environment, the FBI interview summaries must be distinguished from the administration's framing of them (White House Government Transparency Task Force 2026a; ABC News 2026).

ABC News' review of the declassified FBI materials reported that the bureau's investigation also examined campaign donations and internships. It reported that investigators did not find federal corruption violations by Swalwell or evidence of a quid pro quo between Fang and the congressman or his office. This is a more detailed public account than was available when the case first entered this thesis register. It reinforces the distinction between documented sexual contact and proof of knowing espionage, illegal campaign finance, or transfer of protected information (ABC News 2026).

Swalwell's political position became part of the dispute. In January 2023, House Speaker Kevin McCarthy cited the Fang allegations in blocking him from serving on the House Intelligence Committee. This was a political consequence of the public controversy, not proof of espionage or misconduct. The case illustrates how a counterintelligence warning can be transformed into a partisan argument after details become public. The record now establishes that Swalwell admitted to FBI investigators that he had physical relations with Fang. It does not establish that he knowingly participated in an intelligence operation, supplied classified information, or engaged in a quid pro quo. He ended contact after the FBI briefing, cooperated with investigators, and the Ethics Committee took no further action.

8.3.3 Evidence classification

The case is classified **C for the reported intelligence-directed cultivation of Fang** and **D for a political security controversy without established wrongdoing by Swalwell**. The later FBI interview summaries document sexual contact but do not prove that the relationship was intelligence-directed. Its demonstrated information gain is not publicly quantified. The

record does not establish that Fang obtained protected government information from Swalwell. The demonstrated institutional outcome is a defensive briefing, an FBI inquiry, an Ethics Committee inquiry that closed without further action, and the political consequences of the public controversy.

This case helps distinguish two different forms of success. A foreign service might value political access and relationship mapping even without classified disclosures. But access alone cannot be counted as intelligence obtained unless records show what was learned, how it was passed, and how the service used it. For Fang, public evidence supports a cultivation effort, but the exact intelligence product and its effect remain unknown.

The public record reviewed here establishes no criminal charge or formal employment penalty against Swalwell in connection with Fang. The House Ethics Committee closed its inquiry without further action. The sources do not document personal or family consequences for either person or establish what became of Fang after she left the United States. These documented institutional responses must be distinguished from unproven claims about espionage, classified disclosures, or private family fallout (Axios 2020b; House Committee on Ethics 2023b).

8.4 NVIDIA, Alice Huang, and Megaspeed: an unresolved intelligence and corporate-security case

8.4.1 The people and organizations

Alice Huang is also known as Huang Le. Reuters reporting described her earlier work in Chinese finance and investment, followed by senior positions at a Shanghai investment firm and leadership roles at Megaspeed International, a Singapore-based cloud-computing and data-center company. Jensen Huang, NVIDIA's co-founder and former chief executive, and Alice Huang share a surname but are not related. Megaspeed has been described as an NVIDIA customer and cloud partner in the Asia-Pacific region. Corporate records reviewed by Reuters and research group C4ADS indicated that Alice Huang became a controlling shareholder in Megaspeed in 2023. Later ownership changes make the company's control structure and her continuing influence matters for careful source verification (Reuters 2026a, 2026h).

These roles created several possible channels of access. As an executive at a customer and partner, Alice Huang could have had ordinary commercial contact with NVIDIA leadership. As a cloud operator, Megaspeed could acquire hardware and rent computing capacity to customers. As the former chief executive and chair of a company under inquiry, she was also positioned

within a corporate structure that Singapore authorities examined in connection with server purchases and declarations. None of these facts, standing alone, proves intelligence tasking or prohibited chip diversion.

8.4.2 The reported intelligence allegation

The New York Times reported in October and November 2026 that U.S. officials believed Alice Huang had been recruited by China's Ministry of State Security and had cultivated a close relationship with Jensen Huang. It reported that U.S. intelligence had developed an assessment and that a classified memo concerning the matter was prepared for senior officials. Subsequent reporting said intelligence officials believed the relationship could have been used to obtain information about the company or U.S. policy. The New York Times' reporting is significant evidence that a U.S. intelligence assessment existed, but the underlying classified materials and the specific evidence supporting the assessment have not been made public.

Reuters reported on November 16, citing two people familiar with the matter, that U.S. intelligence agencies were still assessing the extent of Alice Huang's relationship with China's Ministry of State Security and what information she may have passed. Those sources said evidence gathered so far indicated she was likely an intelligence asset who shared information, rather than a fully trained spy. This is a reported intelligence assessment; its underlying evidence remains classified and has not been independently examined by the public.

On November 12, U.S. Attorney General Todd Blanche said the Department of Justice had not reached a conclusion on whether she was a Chinese spy. These statements address different thresholds: a reported intelligence assessment about likely asset activity and a public law-enforcement conclusion about espionage. China rejected the allegation. Singapore's Ministry of Home Affairs said Huang was not investigated for espionage and that its inquiry concerned possible domestic business offenses (Reuters 2026g, 2026f; Singapore Ministry of Home Affairs 2026b, 2026a).

For this thesis, the most accurate formulation is that U.S. intelligence officials reportedly assessed Alice Huang as a likely Chinese intelligence asset. The assessment is strongly reported, but its underlying evidence, tasking, and the extent of information transferred remain undisclosed. The word "spy" can accurately describe how named outlets and officials have characterized the intelligence concern, while the chapter still distinguishes that reported intelligence judgment from a publicly disclosed criminal finding.

DOI: **10.5281/zenodo.24482572**

8.4.3 The relationship and NVIDIA's response

Multiple outlets reported a romantic relationship between Jensen Huang and Alice Huang. Jensen Huang acknowledged in November 2026 that he had been unfaithful to his wife, but did not identify Alice Huang in his public statement. Reuters reported that photographs it verified showed the two together at public and business events dating to December 2023. Reuters later reported, citing people familiar with internal correspondence, that Jensen Huang had characterized his interactions with Alice Huang and Megaspeed to NVIDIA leaders as routine business dealings. The same reporting said he later apologized for misleading company leaders about the nature of the relationship. The public record does not establish exactly when the relationship became intimate or what information, if any, was exchanged privately (Reuters 2026b).

NVIDIA's independent directors retained outside counsel to investigate reports that Jensen Huang had been targeted by a foreign intelligence operation and to examine the company's conduct. The board said it had no reason to believe national security information or NVIDIA trade secrets had been compromised and that Jensen Huang would cooperate. These are the board's stated preliminary conclusions, not a complete public report of its investigation. The company's internal findings should be treated as relevant institutional evidence while recognizing that the public has not received the underlying documents or a full account of its scope (The Information 2026c; Reuters 2026b).

On November 12, Jensen Huang resigned as chief executive. Reuters reported that the board's investigation followed reporting about his relationship with Alice Huang, separate reported relationships, and the intelligence concerns. The sequence establishes a serious corporate governance consequence, but it does not show that a foreign service caused the resignation or obtained NVIDIA secrets. The resignation followed a combination of personal conduct, credibility concerns with company leadership, external reporting, and an active board investigation. The specific weight of each factor is not fully public.

8.4.4 Husband, sister, and the company network

Published accounts place Alice Huang's husband and sister in the family-network discussion. The Information reported, citing two people familiar with Alice Huang and corporate registration records, that she, her husband Kang Wei, and her sister Huang Yu were connected to companies across China and Singapore involved in Nvidia chip acquisition and cloud computing. Its reporting described Shanghai Century Litong as a Chinese company founded in June 2023, with a company linked to Huang Yu among its early shareholders.

The Information said Century Litong obtained preferred NVIDIA cloud-partner status within months, a designation associated with priority access to chips. It also reported that Kang Wei had earlier business ties in gaming and investment, and that entities linked to Huang's family had roles in the corporate network. These are reported corporate connections. They do not independently prove that family members knowingly supported intelligence collection or that proprietary information was transferred (The Information 2026b, 2026a).

The same report alleged that Alice Huang's relationship with Jensen Huang and her connections with NVIDIA and distributors helped facilitate at least $7.5 billion in chip shipments to Chinese companies since 2023, including roughly 240,000 H100, H200, and some A100 processors. Reuters summarized The Information's findings but said it could not independently verify the reporting. The figure is a sourced allegation, not a confirmed audit result, official government finding, or proven amount of unlawful exports. The chip count also combines models and periods with different export-control status. Some A100 models were initially eligible for sale to China before later restrictions; H100 and H200 chips were subject to restrictions during relevant periods. A total quantity must not be treated as a total quantity of illegally exported chips without shipment-level evidence (Reuters 2026d; The Information 2026b).

Megaspeed and Century Litong must also be distinguished. Megaspeed is the Singapore-based company associated with Alice Huang's management role and cloud business. Shanghai Century Litong is a separate Chinese company described in The Information's reporting as a preferred cloud partner and a large purchaser or supplier of chips. Reuters reported that some Megaspeed-associated shipments moved through a Malaysian subsidiary, Speedmatrix, and that corporate ownership and control changed over time. A complicated corporate network may obscure the beneficial owner or the final user, but complexity alone does not establish criminal evasion or intelligence direction.

The reports also differ on what happened to the chips. Some describe physical shipments into China; others discuss data centers located in Southeast Asia that rent compute capacity remotely to Chinese customers. Those are distinct export-control pathways. A physical export may be governed by controls on the hardware and its destination. A cloud-service arrangement may raise questions about remote access, end users, beneficial ownership, and the reach of rules designed around physical shipment. This chapter does not merge them into one allegation. It identifies what the shipment and company records support, what a news report attributes to unnamed sources, and what remains under investigation.

DOI: **10.5281/zenodo.24482572**

8.4.5 What Singapore's inquiry did and did not establish

Singapore's Ministry of Home Affairs stated that the Singapore Police Force and Singapore Customs began an independent investigation in February 2025 into several companies, including Megaspeed, and their key officers. The suspected domestic offenses involved possible false declarations in server purchases and related matters. Singapore said the investigation was not initiated at the request of another government. Alice Huang was investigated because of her positions as Megaspeed's chief executive, chairperson, and a key controller. Singapore expressly stated that she was not investigated for espionage.

According to the ministry, on June 24, 2025, the U.S. Bureau of Industry and Security conducted a voluntary post-shipment verification at Megaspeed while Alice Huang was present. Singapore said that was the first time it learned of U.S. interest in the company and Huang. Singapore police interviewed her the same day and impounded her passport to secure her attendance while she was outside the country. In February 2026, after consulting its Attorney-General's Chambers, Singapore concluded there was insufficient evidence to establish that Alice Huang had committed the suspected offenses involving declarations. The police nevertheless assessed that she knowingly gave inaccurate information to downplay her role in Megaspeed, issued a stern warning, and barred her from re-entering Singapore. Investigations involving Megaspeed and six other individuals remained open as of the ministry's November 12, 2026 statement (Singapore Ministry of Home Affairs 2026b).

This is a mixed official outcome. It is inaccurate to say Singapore cleared every company or every person, because its broader investigations continued. It is also inaccurate to say Singapore found Alice Huang guilty of espionage or export-control violations. The ministry explicitly said the inquiry was not about espionage and that evidence was insufficient to establish her involvement in the suspected server-declaration offenses. The warning related to inaccurate information about her role, not a criminal conviction. These distinctions should be preserved in any description of the case.

8.4.6 The intelligence question and actual gains

The central intelligence question is not simply whether Jensen and Alice Huang had a relationship. It is whether a foreign service directed or exploited the relationship, what information was sought, what information was actually obtained, and whether the information altered a U.S. government, NVIDIA, or export-control decision. The public record available in November 2026 does not identify a classified document, source identity, trade secret, policy

discussion, or corporate plan that Alice Huang transmitted to China. The intelligence allegation is serious, but the evidence of specific transfer has not been disclosed publicly.

The commercial allegations are analytically separate. If restricted chips or cloud compute were routed to prohibited end users, that could represent a significant technology-control problem even without a spy operation. Conversely, proof of a romantic relationship and a company's purchase of Nvidia hardware would not establish intelligence collection. Evidence of a family business network does not establish that the network served the Chinese state. The thesis therefore records two open questions: whether any export-control violations occurred, and whether an intelligence service tasked or exploited Alice Huang. These questions may overlap, but neither proves the other.

8.4.7 Institutional, financial, and geopolitical consequences

The case produced clear corporate consequences. NVIDIA's board began an external investigation; Jensen Huang resigned on November 12; the company faced congressional demands for testimony; and reporting described substantial stock-price losses during the controversy (Reuters 2026d, 2026i). These consequences reflect governance, disclosure, and confidence concerns as well as the espionage allegations. Stock-price changes during a volatile period cannot be attributed solely to the story without a defensible causal analysis, so the chapter does not use market-capitalization changes as a direct measure of intelligence damage.

The case also raised questions about the distribution of advanced AI hardware through international customers and cloud partners. Singapore and the United States agreed to continue discussions on Megaspeed, and Singapore said its independent inquiry was ongoing. On November 17, U.S. officials publicly disclosed the 2024 start of the Commerce investigation, the June 2025 end-use check, and DOJ's later assumption of the lead role in the criminal investigation. The House committees' November 12 second request sought closed-door, transcribed interviews from Jensen Huang, NVIDIA General Counsel Tim Teter, and Commerce official Jeffrey Kessler. No completed interview or public hearing is established in the record reviewed here (Department of Justice and Department of Commerce 2026; U.S. House Committees 2026b; Singapore Ministry of Home Affairs 2026b).

For the United States, restricted AI chips have strategic and commercial importance because computing capacity supports model training, cloud infrastructure, and military and industrial research. A case involving alleged diversion therefore carries geopolitical significance beyond one company's conduct. But a large volume of chips moving through a corporate network is not automatically an intelligence gain. Establishing downstream access,

user identity, actual compute use, and any effect on Chinese capabilities requires evidence beyond the headline figure.

8.4.8 Evidence classification

The reported U.S. intelligence assessment of Alice Huang as a likely intelligence asset is classified **B: strongly reported but partly undisclosed and disputed**. Specific tasking, information transferred, and any export-control violations remain **C: allegations under investigation**. The underlying Megaspeed server and declaration questions are separate inquiries, not resolved in the public record. The reported $7.5 billion and 240,000-chip figures are attributed claims requiring shipment-level corroboration. Jensen Huang's acknowledged infidelity and resignation are documented. No public source cited here establishes that Alice Huang obtained NVIDIA trade secrets, classified information, or policy intelligence from him.

This classification marks the boundary between credible reporting about a serious intelligence concern and proof of what the alleged operation accomplished. The unresolved case raises questions about counterintelligence, corporate governance, export controls, and private relationships around strategically sensitive technology. The November 17 U.S. disclosure clarifies that the export-control investigation predated public reporting about the relationship by more than a year; this establishes chronology, not a causal link between the relationship and the investigation.

As of November 17, 2026, Jensen Huang's resignation and public apology to his wife and children are documented. His statement acknowledged that his conduct hurt his family and said he hoped to earn back their trust; no public source establishes his family's private response or later decisions. Reuters reported on November 16 that NVIDIA's board was not considering reinstating him, despite public calls for his return. On November 17, CBS News reported that Huang had agreed to answer questions from House lawmakers on December 1 and NVIDIA General Counsel Tim Teter had agreed to appear on December 2. As of November 23, 2026, the December 1 and 2 interviews were still scheduled. Singapore's stern warning and re-entry bar for Alice Huang are documented. No public criminal finding establishes espionage, and the sources do not establish her private or family aftermath (Reuters 2026b, 2026f; CBS News 2026; Department of Justice and Department of Commerce 2026; U.S. House Committees 2026b; Singapore Ministry of Home Affairs 2026b).

8.4.9 The NVIDIA board's reversal and the campaign to reinstate Jensen Huang

On November 17, 2026, NVIDIA board chair Harvey Jones told investors that the board did not intend to reinstate Jensen Huang as chief executive. Six days later, on November 23, the

board voted unanimously to restore Huang to all three positions he had held: president, chief executive officer, and director. Huang publicly acknowledged infidelity. Reporting identified Alice Huang, an executive at Megaspeed, a Singapore-based NVIDIA customer, as a woman with whom he had a relationship. U.S. officials suspected the executive of spying for China. The Commerce Department had been investigating whether Megaspeed violated U.S. export restrictions (Reuters 2026j; NVIDIA 2026; Kornfield 2026).

President Donald Trump spoke directly with NVIDIA's board before it reinstated Huang. In a November 23 interview with CNBC, Trump said he had spoken to the board "directly and indirectly." He took personal credit for the outcome: "I spoke to them, let me put it that way. And I convinced them." In a separate social media post, he called the reinstatement the "correct and proper decision." NVIDIA gave its own account of the vote. The directors met with Huang, discussed his candor and ability to lead the company, and sought input from senior U.S. government officials. The board said that input gave it confidence that his return posed no national security risk (The Wall Street Journal 2026a; The Guardian 2026; Financial Times 2026; NVIDIA 2026).

The president also had a financial interest in NVIDIA. His financial disclosures indicated a multimillion-dollar holding in the months before he intervened. Other supporters had business or investment ties of their own. Gavin Baker and Brad Gerstner, whose firms held NVIDIA shares, wrote directly to the board. Technology executives backed a public petition for Huang's return. Senator Elizabeth Warren, the ranking member of the Senate Banking Committee, called the reinstatement "reckless" and said NVIDIA and its board still owed Congress answers about the company's compliance with U.S. export controls (Kornfield 2026; The Times 2026; The Wall Street Journal 2026b; U.S. Senate Committee on Banking, Housing, and Urban Affairs 2026).

Would an executive without the president's personal backing, or friends and allies with comparable financial and business influence, have received the same consideration?

Person	Documented connection
Donald Trump	Trump personally urged the board to reinstate Huang. The Washington Post estimated from Trump's financial disclosures that he held between $13 million and $62 million in NVIDIA stock at the end of August 2026. The Wall Street Journal subsequently estimated that his stake was worth as much as $83 million in early October. Both estimates predate the November 23 vote (The Wall Street Journal 2026a; Kornfield 2026; The Wall Street Journal 2026c).

Person	Documented connection
Donald Trump Jr.	According to the White House, Trump Jr. oversaw his father's investment accounts, while independent financial managers handled the portfolio (The Wall Street Journal 2026c).
Elon Musk	The Stand with Jensen campaign listed Musk as a supporter. His company xAI built its Colossus supercomputer with 100,000 NVIDIA graphics processors and used NVIDIA networking equipment to connect them (Stand with Jensen 2026a; NVIDIA 2024).
Gavin Baker	Baker's investment firm, Atreides Management, held NVIDIA stock. Baker told CNBC that he had discussed China with Huang many times over the years. He and Brad Gerstner wrote to NVIDIA's board urging directors to keep Huang's return under consideration (CNBC 2026; The Times 2026; Stand with Jensen 2026b).
Brad Gerstner	Gerstner led Altimeter Capital, an NVIDIA shareholder. He joined Baker in asking the board to keep open the option of reinstating Huang. A November 20 shareholder letter put the two firms' combined NVIDIA holdings at approximately $2.1 billion (The Times 2026; Stand with Jensen 2026b).
Tobias Lütke	Lütke, Shopify's chief executive, signed the petition for Huang's return. Shopify uses NVIDIA models, software, and processors for its AI products and obtains some of that computing capacity through the cloud provider Nebius (The Wall Street Journal 2026b; Shopify 2026).
Tim Sweeney	Sweeney, chief executive of Epic Games, signed the petition. Epic develops Unreal Engine, and NVIDIA supplies software that developers use to integrate its graphics technology into the engine (The Wall Street Journal 2026b; NVIDIA Developer n.d.).
Amjad Masad	The campaign listed Masad, Replit's chief executive, as a shareholder. An NVIDIA employee used Replit to build the petition website. Masad signed the petition and personally changed the site's code so it could accept signatures faster (Stand with Jensen 2026a; The Wall Street Journal 2026b).
Travis Kalanick	Kalanick, chief executive of Atoms and co-founder of Uber, signed the petition. He said he wrote directly to Huang and offered to rally supporters. The campaign listed his self-reported affiliation as "partner." (The Wall Street Journal 2026b; Stand with Jensen 2026a).

8.5 Conclusion

This chapter finds that contemporary cases demand a wider view of intimate access. Political cultivation can seek social networks and future influence. Corporate relationships can intersect with customer access, supply chains, cloud infrastructure, and export controls. A

traditional espionage operation such as Pollard's can provide a comparison standard for direct collection, but it should not be mistaken for a seduction operation.

The thesis's central proposition is therefore supported with limits: intimacy may be a route to information and organizational influence, but the existence of a relationship is only the beginning of the inquiry. The historian must trace tasking, access, transfer, use, and consequence.

DOI: **10.5281/zenodo.24482572**

Chapter 9.
The Digital Honeytrap: Online Intimacy, Sextortion, and Synthetic Kompromat

9.1 Scope and definitions

This chapter examines how digital communications have altered the practice and evidence of intimate intelligence operations. It considers online relationship cultivation, false identities, digital sextortion, surveillance of publicly available personal information, and synthetic intimate imagery. It asks what has changed in the movement from in-person relationships to platform-mediated contact, what has remained continuous, and what can be demonstrated about intelligence acquired through such contact.

The chapter uses *digital intimate manipulation* as an umbrella term for online deception that uses romantic, sexual, or emotionally close communication to seek access, information, money, compliance, or compromising material. A *digital honeypot* in this thesis means a deceptive online identity or relationship used to cultivate a target for intelligence or leverage. This differs from a computer-security honeypot, which is a decoy system designed to attract cyber intruders. *Sextortion* refers to threats involving actual or purported sexual material used to compel payment or other compliance. *Synthetic intimate imagery* refers to fabricated or materially altered images or video depicting an identifiable person in a sexual context without that person's consent. These categories overlap in some cases, but none should be treated as a synonym for espionage.

Four propositions must remain separate. First, that a person communicated with a false or deceptive online identity. Second, that the interaction was romantic or sexual in character. Third, that the contact was directed by a state intelligence service. Fourth, that the target transferred information or took action that produced a demonstrable consequence. A case may establish one proposition without establishing the others. The digital medium can make an interaction appear intimate while obscuring who operated the profile, where the operator was located, and whether an intelligence service directed the exchange.

The evidence classifications established in Chapter 2 apply here. The chapter distinguishes a documented espionage operation from reported intelligence attribution, criminal romance fraud, ordinary coercive abuse, and the use of synthetic imagery. It also treats public reporting and official statements according to what they establish. A government announcement can document an arrest, charge, conviction, or sentence. It does not automatically establish every

DOI: **10.5281/zenodo.24482572**

allegation made during an investigation. A guilty plea can establish the defendant's admitted conduct without identifying the recipient's true identity or institutional sponsor.

9.2 From proximity to platform-mediated intimacy

Earlier chapters traced intimate intelligence from courtship, social access, and long-term personal relationships to documented recruitment and compromise. Digital communication did not invent the underlying vulnerabilities. Attention, recognition, reciprocity, secrecy, sexual desire, loneliness, ambition, fear of exposure, and the wish to be trusted remain human experiences. What the digital environment changes is the cost, speed, reach, and persistence of the contact.

A prospective operator can use a profile assembled from photographs, public posts, employment information, and other online traces to present a plausible identity. The interaction can begin without physical proximity and continue across multiple accounts or services. A relationship may develop through text, voice, video, images, or shared online activity. The person on the other end may be an individual, a team, a criminal network, or an unknown intermediary. The target may therefore experience a continuous personal relationship while the operation, if there is one, is distributed across people and systems.

This structure changes the meaning of access. In face-to-face recruitment, access may depend on repeated meetings, physical presence, and social observation. Online contact can create a private channel quickly, after which the parties may move between platforms. A target's public digital footprint can help a deceiver identify interests, professional role, family connections, travel, routines, or status. The FBI has warned that criminals use public information from social media and dating platforms to understand and target people, and that romance schemes can seek personal information as well as money (FBI Chicago 2026). These warnings document a broad criminal risk. They do not show that every person who uses such information is an intelligence officer.

Digital contact also leaves records. Messages, account metadata, images, payment trails, platform logs, and device evidence may allow investigators to reconstruct a relationship after it has ended. Yet the same record can be incomplete, manipulated, deleted, or held by a service outside the investigator's jurisdiction. An online persona may be quickly replaced. The speed of account creation and the movement of communications across services complicate attribution. These conditions can make a digital operation easier to initiate and harder to attribute with confidence.

DOI: **10.5281/zenodo.24482572**

A recurring pattern is that emotional trust can become an access channel. A lover, confidant, or admirer may be granted personal or professional information that a stranger would not receive. The digital form can compress the time between first contact and a request for sensitive information, but duration alone does not determine whether a relationship is genuine or operational. A long exchange can still be fraudulent; a short exchange can expose sensitive information. The analytical question is what the relationship enabled and what the evidence shows was actually obtained.

9.3 David Slater: classified disclosure through a dating platform

The case of David Franklin Slater provides a documented example of classified information moving through a digital relationship channel. Slater, a retired U.S. Army lieutenant colonel, later worked as a civilian employee assigned to U.S. Strategic Command at Offutt Air Force Base. The Justice Department stated that he held a Top Secret clearance and worked in a classified space. From approximately February through April 2022, he used a foreign online dating platform to communicate with a person who claimed to be a woman living in Ukraine (U.S. Department of Justice 2024; 2025).

According to the indictment and the Justice Department's account of Slater's guilty plea, the online correspondent repeatedly asked him for sensitive, non-public, and classified information. The messages used romantic language, including calling him her "secret informant love" and "secret agent." Slater had attended briefings on Russia's war against Ukraine, some classified up to Top Secret/Sensitive Compartmented Information. The Justice Department stated that he transmitted classified information concerning military targets and Russian military capabilities. Slater pleaded guilty in July 2025 to conspiring to transmit national defense information. On October 8, 2025, he was sentenced to 70 months in prison, one year of supervised release, and a $25,000 fine (U.S. Department of Justice 2025; U.S. Air Force Office of Special Investigations 2025).

The case establishes a digital romantic channel, repeated requests, actual transmission of classified information, a guilty plea, and a prison sentence. It does not establish publicly that the correspondent was a woman, lived in Ukraine, or represented a foreign intelligence service. The legal record refers to a co-conspirator and a foreign online persona, but the person behind the identity and any state sponsor have not been publicly identified. The case is therefore **A for conspiracy to transmit classified national defense information through an online dating platform and unresolved for attribution to a foreign intelligence service.** It is strong evidence that digital intimacy can be used to elicit protected information. It is not proof that a particular state ran the operation.

The intelligence gain can be described, but not fully valued. The official account says information regarding military targets and Russian military capabilities was transmitted. It does not publicly quantify the number of messages, the full set of documents or details, whether the recipient used the material, or the operational harm that followed. The sentence indicates the seriousness with which the court treated the conspiracy, but the sentence length is not a measure of the intelligence value of the information. The public record proves transfer; it does not disclose a complete damage assessment.

Slater's conduct also differs from several classic honeytrap narratives. The available record does not establish that the correspondent blackmailed him with sexual images, threatened exposure, or physically met him. The mechanism visible in the prosecution is attention, romantic language, repeated solicitation, and his voluntary transmission of classified information. That distinction matters because intimate recruitment does not always depend on entrapment or coercion. A person may disclose secrets to preserve a relationship, feel valued, perform a desired role, or respond to persistent requests. Those are possible explanatory mechanisms, not diagnoses of Slater. The case record establishes his conduct and the messages described by prosecutors; it cannot establish his private psychological state beyond what he admitted in court.

Slater pleaded guilty and received a 70-month federal prison sentence for conspiring to transmit classified national defense information. The sentence and admitted transfer are documented, but the recipient's identity and state affiliation remain publicly unknown. The sources cited here do not describe a spouse, children, or family consequences, and they do not quantify the operational harm from the material. His legal and professional consequences can be stated; the private family aftermath and the recipient's fate cannot. (U.S. Department of Justice 2025; U.S. Air Force Office of Special Investigations 2025.)

9.4 Saurabh Sharma and the digital false persona

A second documented case, from India, concerns a state-directed digital recruitment network; the public account does not establish a sexual relationship. The National Investigation Agency reported that former Indian Army signalman Saurabh Sharma was convicted and sentenced by a special court in Lucknow in August 2024 in a Pakistan-operated espionage case. The agency said a pseudonymous entity called "Neha Sharma," operated by Pakistan Defence/ISI agents, lured Sharma into a spying network. It reported that Sharma shared restricted and confidential information about the Indian Army, including information concerning military installations, and received funds from multiple sources, including Pakistani sources and a co-accused (National Investigation Agency 2024).

The NIA's release establishes that an Indian special court convicted Sharma and that investigators attributed the false persona to Pakistan Defence/ISI agents. It reports the category of information transferred and the presence of payments, though it provides no itemized count, technical damage assessment, or public account of how the information was used. The case is classified **A for the convicted Pakistan-operated espionage scheme as described by the NIA**. It is not classified as a proven sexual honeytrap. The publicly available NIA statement uses the language of luring through a pseudonymous entity, but it does not specify a romantic or sexual relationship, intimate images, blackmail, or the precise emotional mechanism. Calling it a honeytrap in the narrow intimate sense would exceed the record.

The distinction is analytically useful. Digital false identities can recruit or manipulate a source without romance. An online persona may create attention, trust, ideological affinity, or financial inducement. When a case is described in the press as a honeytrap, the thesis must still ask what the official case record says the relationship consisted of. The use of a woman's name or image is not proof that a woman operated the account, and a gendered profile does not establish the sex, identity, or institutional role of the operator.

A related Indian case involving Satendra Siwal shows the limits of public attribution while proceedings remain unresolved. Siwal, an employee posted at the Indian Embassy in Moscow, was arrested in February 2024 and charged under national-security and Official Secrets Act provisions. Indian reporting, citing the Uttar Pradesh Anti-Terrorist Squad, said a woman using a social media identity had befriended him and allegedly induced him to provide information for money. A 2026 Allahabad High Court decision records that charges had been framed in 2024 and that Siwal challenged one of them; the court dismissed his procedural petition, leaving the case to proceed. That ruling did not determine guilt (Indian Express 2024; *Satendra Siwal v. State of Uttar Pradesh* 2026).

The Siwal matter is therefore classified **C: an active espionage allegation with reported online romantic cultivation, not a completed judicial finding of guilt**. The state allegations, account identities, and alleged transfer of classified material remain distinct from what a trial judgment may eventually establish. It is useful as a case to follow, but cannot be presented as a proven operation or a confirmed intelligence success at this stage.

The National Investigation Agency reported that a special court convicted Sharma in August 2024 and imposed sentences of up to five years' imprisonment, along with fines. The agency attributed the online persona to Pakistan-linked Defence/ISI operators, while the public release does not identify the person who communicated with him. The available sources do not establish family consequences for Sharma or personal consequences for the operator, whose

identity remains unknown. The documented sentence should not be expanded into claims about those private outcomes. (National Investigation Agency 2024.)

9.5 Romance fraud and sextortion: a neighboring threat, not automatically espionage

The scale of online relationship fraud provides context for why digital intimacy has become a security concern. It does not establish that the perpetrators are intelligence services. In its 2024 annual report, the FBI Internet Crime Complaint Center recorded 17,910 confidence- or romance-fraud complaints and reported losses of $672,009,052 in the United States. The FBI emphasizes that these are complaints received through its reporting system. They are not a count of all incidents, all victims, or all online relationships, and they should not be used as a measure of espionage activity (Federal Bureau of Investigation, Internet Crime Complaint Center 2025).

Academic reviews of online romance fraud describe a pattern in which perpetrators construct a false identity, establish emotional credibility, move the exchange into a more private channel, and then introduce financial requests or other demands. The sequence is not always linear, and offenders adapt their stories to the victim. A systematic review by Bilz, Shepherd, and Johnson found that the research base encompasses multiple disciplines and methods, while also identifying gaps in knowledge about the full extent and process of romance scams (Bilz, Shepherd, and Johnson 2023). Research on victims describes both material losses and the loss of a relationship believed to be genuine. Shame, self-blame, and fear of being judged can discourage reporting, leaving official totals incomplete (Whitty and Buchanan 2016; Ray and Henry 2025).

The psychological processes relevant to this thesis overlap with those identified in earlier chapters. A deceptive correspondent may provide steady attention, validation, a sense of exceptional connection, or support during a period of stress. Requests may grow gradually. The target may keep the exchange secret because it feels private, because the relationship is illicit, or because disclosure could threaten a career or marriage. If the relationship turns coercive, embarrassment can be used to isolate the target. These mechanisms are supported by research on romance fraud and sextortion as broad crime categories. They should not be projected onto a named espionage target unless case evidence supports them.

Sextortion makes intimate material an instrument of compulsion. The material may be an authentic image voluntarily shared in a relationship, an image captured without consent, an altered image, or a fabricated claim that such material exists. The FBI describes schemes in

which offenders impersonate romantic interests, persuade victims to send sexual material, and then demand payment under threat of disclosure. It also warns that offenders may fabricate explicit imagery by combining a victim's face with another image (Federal Bureau of Investigation n.d.-a). Such cases are evidence of criminal extortion and digital coercion. They are not, without further evidence, evidence of an intelligence operation.

This is the key boundary for the thesis. A threat can create leverage even when the original intimate interaction was not intelligence-directed. A criminal may seek money, an abusive partner may seek control, and a state service may seek information or compliance. The surface mechanism can look similar, but the objective, command structure, and institutional use differ. Classification must follow evidence of sponsorship and purpose, not the emotional intensity of the relationship or the apparent sensitivity of the victim.

The examples and statistics in this section describe broad categories of fraud and abuse rather than a named intelligence case. They establish reported financial loss and documented psychological and reputational harms across victims, but they do not permit a case-by-case account of any one victim's family or later life. Those individual outcomes are unknown in the aggregate sources reviewed here, and should not be inferred from complaint totals. (Federal Bureau of Investigation, Internet Crime Complaint Center 2025; Whitty and Buchanan 2016; Ray and Henry 2025.)

9.6 Synthetic intimacy and the changing meaning of kompromat

Digital tools have expanded the kinds of compromising material that can be created and circulated. A traditional compromising photograph purports to document an event. A fabricated image may depict an event that never occurred, but still be used to threaten the subject, damage a reputation, or prompt institutions to act defensively. Synthetic content therefore changes both the production cost of compromising material and the burden of verification.

Three forms should be distinguished. **Captured material** records a real interaction or image without consent. **Repurposed material** takes a genuine photograph, message, or recording and changes its context. **Synthetic material** fabricates or substantially alters a sexual image or video. The first two depend on access to a real image or event; the third may be generated from an ordinary public photograph. In all three, the threat of disclosure may matter more than the image's evidentiary truth. A fabricated image can still cause fear because a victim may expect family, colleagues, voters, executives, or the public to believe it.

The availability of synthetic imagery complicates the evidentiary logic of historical kompromat. In earlier cases, the existence of a photograph could be treated as evidence that an encounter occurred, though its context and provenance still required investigation. In the synthetic era, image existence cannot establish an encounter. Metadata, chain of custody, source files, forensic analysis, and corroborating records become central. A leaked image may itself be part of an operation designed to create suspicion. This does not mean every sexual image is fabricated. It means the evidence must be tested rather than assumed to be authentic.

By 2025 and 2026, governments had begun responding to these harms through new laws and platform duties. The U.S. TAKE IT DOWN Act, enacted in May 2025, criminalizes the intentional publication of certain nonconsensual intimate visual depictions, including digital forgeries, and requires covered platforms to establish procedures for removing reported material within a statutory period (United States Congress 2025; Congressional Research Service 2025). In the United Kingdom, the Data (Use and Access) Act 2025 introduced offences relating to creating or requesting nonconsensual purported intimate images, and the Crime and Policing Act 2026 added provisions addressing intimate-image generators and platform removal duties. The UK government described duties requiring covered platforms to remove validly reported intimate-image material within 48 hours (United Kingdom 2025; United Kingdom 2026).

These laws recognize that synthetic images can cause harm without depicting a real sexual event. They do not turn nonconsensual image abuse into intelligence activity. Their relevance to the thesis is institutional: private vulnerability can be weaponized through the creation, threatened distribution, or deliberate fabrication of intimate material, and states are beginning to define legal duties around that power. The laws also reveal a tension. Rapid removal can reduce circulation, but evidence preservation is necessary for investigation and prosecution. Platforms, law enforcement, and victims must navigate the conflict between limiting exposure and documenting the operation.

As of November 2026, public evidence does not establish a general pattern in which state intelligence services use AI-generated sexual images as a standard recruitment or blackmail method. The capacity exists, and cybercriminals have used fabricated intimate imagery in extortion. The thesis can analyze synthetic kompromat as an emerging capability and risk, but it must not convert capability into an established intelligence campaign without case-specific evidence.

DOI: **10.5281/zenodo.24482572**

9.7 Gender, anonymity, and the apparent seductress

Online deception can reproduce the image of a woman seducing a man while concealing who created the image, wrote the messages, or directed the contact. In Slater's case, the recipient presented as a woman in Ukraine, but the person behind the account remains unidentified in the public record. In the NIA account of Sharma's case, a persona using a woman's name was attributed to Pakistan-linked operators, but the public release does not establish who performed the interaction. In both examples, the apparent gender of the profile is evidence about the persona, not the operator.

Gender analysis must account for the difference between a persona and the person operating it. Historically, some services used women to approach men, while East German Romeo operations used male agents to cultivate women. Digital identities make gender presentation even more separable from the operational agent. A profile can be created, maintained, and answered by different people. An image can be stolen or synthetic. The target may respond to a gendered persona without ever interacting with the person pictured. Claims about female culpability should therefore be grounded in proof of the operator's identity, not inferred from the profile's name or appearance.

The digital environment also changes the role of the target. A target may be selected because of professional access, but vulnerability may arise from private needs that are not visible in formal security screening. A person may disclose information to maintain approval, impress an imagined partner, respond to a false emergency, or avoid exposure. These are not uniquely male or uniquely female responses. Gender expectations can shape the kind of persona that appears plausible and the form of shame that a threat invokes, but they do not provide a universal explanation for susceptibility.

This chapter therefore extends Chapter 4's critique of the seductress myth. In a digital operation, a fabricated female identity may be operationally useful without a female agent's participation. Conversely, a woman can be the target, source, or victim of intimate deception. The operation must be reconstructed from records of account control, communications, payments, tasking, and corroborated activity. Persona and person are not interchangeable categories.

9.8 What digital operations demonstrably obtain

The digital cases show why intelligence gain must be measured in stages. Access is not the same as information collected. Information collected is not the same as information delivered

DOI: **10.5281/zenodo.24482572**

to a state service. Delivery is not the same as use. Use is not the same as a demonstrable effect on a decision. A sound assessment should record each stage separately.

Access. The relationship creates a communications channel or gains proximity to a person, office, or network. Access may be socially valuable even if no classified material is acquired.

Information elicited. The target reveals facts, documents, opinions, schedules, contacts, or institutional routines. A public record should identify what was actually disclosed rather than what the operation might have sought.

Transfer. Investigators establish that the information reached an unauthorized recipient or handler. In the Slater case, the guilty plea and official account establish that classified national defense information was transmitted. In the Sharma case, the NIA reported the conviction and the transfer of information concerning military installations.

Attribution. Investigators identify who operated the account and whether a state service directed or received the material. Slater's recipient remains publicly unidentified. The NIA attributed Sharma's false persona to Pakistani Defence/ISI agents. Attribution therefore varies by case.

Operational effect. Records show whether the information was used, whether the service changed a plan, whether a source or asset was compromised, or whether a decision was influenced. The public record in these cases does not quantify such effects.

This framework blocks two common errors. The first is to treat an attractive or intimate relationship as proof that a target was compromised. The second is to treat an official's access or a suspect's arrest as proof that a foreign service obtained useful intelligence. A successful operation may be hidden, and a detected operation may have yielded little. The available record is shaped by classification, prosecutorial choices, institutional disclosure, and the willingness of victims or targets to report.

The Slater case documents a transfer of classified information through a dating platform, but public records do not establish state direction or provide a full damage assessment. Sharma was convicted in an operation the NIA attributed to Pakistan-linked actors; its public statement does not quantify the intelligence's operational value. The Siwal case contains allegations of online cultivation and classified disclosure, but proceedings had not produced a final guilt determination as of the latest court record cited here. Romance-fraud and sextortion statistics measure reported criminal complaints and losses, not intelligence collected. None of these sources supplies a denominator for all digital honeypot attempts, so no overall success rate can responsibly be calculated.

DOI: **10.5281/zenodo.24482572**

9.9 Institutional and personal consequences

Digital intimate operations can create consequences at several levels. For an individual, the exposure of an online relationship may cause reputational, financial, emotional, professional, and legal harm. A person who knowingly discloses classified information may face prosecution and imprisonment, as Slater did. A person deceived into sharing images or money may experience shame, fear, and loss of trust, even when no classified information is involved. When a fabricated image spreads, the subject may face reputational damage despite the absence of an authentic sexual event.

For an institution, discovery can reveal weaknesses in security education, reporting channels, supervision, online exposure, or procedures for handling personal relationships. A defensive response can also create a second harm if officials blame the target, dismiss a victim's experience, or treat the existence of an image as proof of misconduct. Clear procedures should preserve evidence, refer suspected espionage to counterintelligence authorities, and distinguish a security inquiry from a judgment about a person's private life.

At the national level, a digital relationship can become a channel for military information, a source of leverage, or a pretext for public controversy. These outcomes are not equivalent. A classified transfer may create direct security risks. A blackmail threat may change a target's behavior without any information being disclosed. A fabricated image may be deployed to damage credibility or provoke institutional disruption. The thesis should treat each as a possible effect and require evidence before claiming that it occurred in a specific case.

Digital content also travels beyond the control of the original operator. Once copied, it can be redistributed by criminal networks, political actors, media outlets, or unrelated individuals. A single deception may therefore produce consequences far beyond the operator's original purpose. Conversely, a viral scandal may be incorrectly attributed to a foreign intelligence service when available evidence points to personal abuse, criminal extortion, or opportunistic political exploitation. Attribution remains a core research problem.

9.10 Comparative findings

The move from physical intimacy to digital intimacy is a change in operational environment, not a change in human nature. Earlier cases depended on the slow formation of personal trust, social access, and the material vulnerability of secrecy. Digital contact allows a false identity to reach a target at a distance, construct a tailored persona, ask for information through private channels, and preserve or threaten to circulate intimate material. It also makes

identity and provenance harder to establish, while leaving digital traces that can support investigation.

The strongest demonstrated digital case in this chapter is Slater's: online romantic presentation, repeated solicitation, transfer of classified information, guilty plea, conviction, and sentence. The strongest state-attributed false-persona case is Sharma's, for which the NIA reported a conviction and attributed the persona to Pakistan Defence/ISI agents, while the public evidence does not demonstrate a romantic or sexual element. The Siwal matter shows why current allegations must remain provisional until adjudicated. Together, the cases support a broad account of digital intimate influence while requiring narrower descriptions of what each record proves.

The chapter also finds that digital sextortion and synthetic intimate imagery are closely related to the thesis's study of kompromat but should not be merged with intelligence operations. Online criminals exploit emotional trust and sexual shame for money. Abusive partners may use images to control another person. Fabricated images can threaten reputations without documenting a real encounter. Intelligence services may use related mechanisms, but a case-specific record must establish that involvement. The fact that tactics overlap does not make the actors or objectives interchangeable.

Finally, digital intimacy makes the gendered seductress story less reliable as an explanation. A female profile may be a false persona operated by someone of any gender, or by a group. The same platforms can be used to target men and women, and the requested leverage may be information, money, access, or compliance. Across these cases, the subject is the use of trust and private vulnerability to gain institutional access, not any supposed gender-specific ability to seduce.

9.11 Conclusion

Digital platforms have not made intimate intelligence obsolete or transformed it into a purely technical problem. They have extended intimacy across distance, made persona construction easier, created persistent communication records, and expanded the possibilities for surveillance, solicitation, and threatened disclosure. The core mechanism remains social: a person comes to trust, depend on, desire, fear, or protect someone who may be using that relationship to obtain access or control.

The evidence in this chapter supports a measured conclusion. Digital romantic contact can precede the transfer of classified information, as the Slater case establishes. The NIA attributed Sharma's recruitment to a false online identity within a Pakistan-linked espionage network, but

the public record does not establish a sexual relationship. Other cases remain allegations. Sextortion and synthetic intimate imagery show how private material can be weaponized, but they cannot be counted as intelligence operations absent proof of state direction and intelligence purpose.

The next stage of the thesis should compare the historical cases across motive, recruitment method, gender, information obtained, leverage, institutional effects, and the visibility of evidence. The central argument remains a proposition to test: intimacy can become a route through which information, leverage, and institutional power move. The digital record shows that the route has widened, but the burden of proof remains the same.

DOI: **10.5281/zenodo.24482572**

Chapter 10.
Comparing Information Gains and Consequences

10.1 Purpose of the comparison

The preceding chapters have followed cases across different periods, intelligence services, political settings, and forms of intimate influence. This chapter compares their outcomes. It asks what information or access was demonstrably acquired, whether a relationship altered a decision or operational condition, and what consequences can be traced for individuals and institutions. The question is not whether intimacy can be useful in espionage. The case record shows that it can. The harder question is how often it produced a measurable gain, what kind of gain it produced, and how far the consequences can be attributed to the relationship itself.

The comparison supports a more discriminating account than the familiar image of the successful seductress or irresistible "honey trap." Intimate contact served different operational functions. It helped recruit insiders, sustain document-transfer channels, create leverage through shame or fear, facilitate movement or capture, and provide social access to political networks. In some cases, evidence establishes that classified information crossed a boundary. In others, it establishes contact, an intelligence concern, or a scandal, but not a transfer of secrets or a policy change. These outcomes are not equivalent.

The evidence classifications in Chapter 2 continue to apply case by case. A documented conviction may establish transfer but not the recipient's subsequent use of the material. A government assessment may identify a serious counterintelligence concern without making its underlying evidence public. An official inquiry may find that conduct created a security risk, or may conclude that no security breach occurred. A public scandal may change political careers even where espionage is not established. The following comparison therefore records four separate variables: access or leverage obtained, information or action demonstrated, consequences documented, and remaining evidentiary limits.

10.2 A comparative framework for intelligence gain

The phrase "intelligence gain" can obscure several distinct steps. A service may gain access to a person or network without receiving protected information. A target may reveal information that is already public, inaccurate, or operationally useless. A document may be transferred without evidence that a foreign service exploited it. A successful capture may

DOI: **10.5281/zenodo.24482572**

prevent a person from speaking freely, yet acquire no new intelligence. Conversely, a relationship may change a target's behavior without any document changing hands.

For this chapter, outcomes are assessed along five linked but separate dimensions:

Access. Did the relationship create proximity to a person, office, institution, or political network that the operator otherwise lacked?

Information transfer. Is there evidence that classified or otherwise protected information actually reached an unauthorized recipient? When records give a count, does that count refer to documents photographed, documents recovered, documents delivered, or documents assessed after the event?

Operational use. Is there evidence that the recipient used the information, changed a plan, compromised a source, or altered an operation? An intelligence service's collection of material does not by itself prove its use.

Leverage or control. Did the relationship or compromising material lead to an observable act, such as continued cooperation, silence, a meeting, a change in travel, or compliance with a demand?

Consequences. What harm or change can be linked to the operation: loss of sources, security redesign, prosecutions, imprisonment, resignation, diplomatic tension, economic effects, or enduring public stigma?

These dimensions do not form a single numerical score. The public record does not provide a common denominator for attempted operations, failed approaches, undetected relationships, and successful transfers. It also does not assign comparable monetary or strategic values to the information in different cases. A numerical success rate would therefore create precision unsupported by the evidence. The comparative objective is to identify recurring mechanisms and the limits of what can responsibly be said.

10.3 Cases with documented information transfer

Vassall: evidence of collection, institutional failure, and unequal certainty about damage

John Vassall's case provides unusually concrete evidence of document handling and unusually clear evidence of institutional vulnerability. In November 1962, parliamentary reporting described 140 photographic exposures from 17 separate secret Admiralty documents, dated between July and September of that year. The Director of Naval Security

characterized the disclosure as a grave danger to the state. The Radcliffe Tribunal examined Vassall's recruitment by Soviet intelligence and criticized weaknesses in personnel selection, security procedures, and the handling of warnings (House of Commons 1962; National Archives n.d.).

The figure of 140 exposures is not a count of 140 unique documents, nor does a seized roll of film by itself establish the full volume previously delivered to Soviet handlers. It is a measure of material documented in the investigation. This distinction matters because later retellings often collapse what investigators found, what Vassall photographed, and what Soviet intelligence received into a single total. The operation's demonstrable value lies in the unauthorized access and photographic transfer of secret Admiralty material. The full operational use of each item remains less visible in the public record.

The institutional consequence was not limited to Vassall's prosecution and imprisonment. The Radcliffe inquiry exposed a system that had failed to assess the risks of an overseas posting and to connect relevant information across agencies. Parliamentary discussion of the report emphasized inadequate security at the Admiralty and at the British Embassy in Moscow. The case therefore supports an institutional explanation alongside individual responsibility: the service exploited a vulnerability, but administrative decisions shaped the opportunity and delayed detection. Vassall received an eighteen-year sentence and was released in 1972 (Hansard 1963a; National Archives n.d.; National Archives 2026).

The East German Romeo operations: sustained access through trusted relationships

The Stasi's so-called Romeo operations show a different model. Rather than acquire a short burst of information through an affair or blackmail, male officers cultivated relationships with women employed in West German government offices and other institutions. The CIA's retrospective account describes individual cases in which secretaries passed chancellery or foreign-service documents over periods of years. It also reports that one woman working at the American Embassy passed thousands of documents during a twelve-year relationship, while other cases involved access to decoded diplomatic traffic or West German intelligence files (Central Intelligence Agency n.d.-b).

The CIA account is a useful official synthesis, but it is a retrospective narrative rather than a published Stasi operational file. Its vivid individual stories should therefore be treated as leads for comparison, not as a complete statistical record of all Romeos or all documents transferred. The cases nevertheless demonstrate a durable mechanism: affection and apparent commitment helped sustain a human channel into offices whose routine paperwork carried

diplomatic and intelligence value. In this model, the relationship itself was not the final product. It maintained the source's access and willingness to copy material.

The women's prosecution and exposure after German reunification provide a record of personal and legal consequences. The source describes multiple prosecutions over several decades and notes that intelligence officers often escaped the same public accountability as the sources they recruited. The asymmetry is relevant to the thesis. A service could obtain years of access while the recruited partner bore the visible legal and reputational costs once the operation was uncovered. The public record is less complete on how particular documents changed specific West German decisions, so access and transfer are better established than decision impact.

Lonetree: intimate recruitment joined to physical access and classified disclosure

Clayton Lonetree's prosecution is the clearest judicially documented case in this group linking a relationship to information transfer and access to restricted spaces. A 1986 State Department memorandum described his recruitment by the "uncle" of a Soviet embassy employee with whom he had a sexual relationship, and reported that he had provided classified documents and information about the Moscow embassy. Later court records established that Lonetree was convicted of identifying covert U.S. intelligence agents and providing floor plans and office assignments for U.S. embassies in Moscow and Vienna. The court-martial sentence was severe, though the initial thirty-year sentence was later reduced (National Security Council 1986; United States v. Lonetree 1990).

The publicly documented gain therefore included more than a single classified paper: it included identities, layouts, and security-relevant knowledge about diplomatic facilities. Established conduct must be separated from unproven allegations. Early allegations that the Soviets had been admitted into sensitive embassy areas and that listening devices had been planted were subject to separate evidentiary questions. The final judicial findings support the transfer of agent identities and embassy information; they should not be expanded to include every allegation circulated during the investigation.

The institutional consequences were substantial and measurable. The State Department ordered the Moscow embassy to stop transmitting classified communications and processing classified information. The secure equipment and conference rooms were removed to Washington for inspection, a response involving approximately 120 crates of communications equipment (Department of State 2016). The documented sequence links intimate recruitment to insider access, security disruption, and costly remediation. The court-martial's original thirty-year sentence was reduced to twenty-five years, and later sentence adjustments and

time served led to his release after eight years. The judicial record does not establish that every item Lonetree disclosed was used by Soviet intelligence or identify each operational loss that followed (United States v. Lonetree 1990, 1992).

Scranage and Soussoudis: intimate access, identities, and institutional exposure

Sharon Scranage, a CIA employee stationed in Ghana, gave classified information to Michael Soussoudis, a Ghanaian intelligence officer and her partner. The FBI records that she provided information including the identities of CIA affiliates and details about communications, radio, and military equipment. She pleaded guilty and was sentenced to five years in prison; Soussoudis was also prosecuted (Central Intelligence Agency 1990; The Washington Post 1985a, 1985b).

This case establishes that an intimate relationship became a channel through which classified information was passed. The public FBI summary does not provide a complete inventory of every identity or document, nor a full damage assessment tracing each disclosure to a later operational outcome. Accounts of threats and coercion must be evaluated against court records and contemporaneous reporting rather than assumed from the fact of a relationship. The firm comparative finding is narrower: classified identities and technical information were exposed through a relationship with a member of the host country's intelligence service.

Scranage's prosecution and imprisonment and the exposure of intelligence contacts were consequences at different levels. Contemporary reporting described concern that Ghanaian informants could be harmed, but the public record does not provide a reliable total of sources harmed or intelligence opportunities lost. The case illustrates why source protection is a more consequential measure than the number of pages copied. A small amount of identifying information can endanger a human source, while a large packet of technical material may have limited operational value if it is obsolete or already known (Central Intelligence Agency 1990; The Washington Post 1985a, 1985c, 1985d).

Boursicot and Shi Pei Pu: conviction does not resolve the relationship's beginning

Trial testimony and contemporary reporting conflict over the sensitivity and value of the material. Boursicot described much of it as public or of little sensitivity, while prosecutors and a counterintelligence witness disputed that account. The record does not establish how many documents were classified, how many were useful to Chinese intelligence, or whether they altered French diplomatic decisions. It establishes an information channel while leaving the

material's utility and the relationship's original purpose unsettled (Le Monde 1986a, 1986b; Bernstein 1986).

The trial's document figure should be treated as a reported count, not as a measure of value. The consequences that can be stated with confidence are arrest, conviction, imprisonment, media exposure, and the lasting public recasting of the relationship as a sexual mystery. The case is thus strong evidence for espionage linked to an intimate relationship but weaker evidence for the operational value of the material and the relationship's original purpose.

10.4 Access, capture, and scandal without demonstrated intelligence gain

Vanunu: a relationship facilitated capture, not the acquisition of the original secret

The Vanunu case is a critical test of loose use of the word "honeypot." By 1986, Mordechai Vanunu had already supplied photographs and information about Israel's Dimona nuclear facility to the Sunday Times. The British Parliament's contemporaneous discussion confirms that his account was published on October 5, 1986, before he disappeared in Rome and was returned to Israel. Published accounts identify a woman known as "Cindy" as the lure that helped bring him to Rome, though the precise operational chain and identity are not fully documented in a public Israeli after-action record (House of Commons 1986; Chapter 7).

The intimate approach is therefore best assessed as a reported movement and capture mechanism. It did not produce the original nuclear disclosure, and no public record shows that it obtained additional technical material from Vanunu. Its direct operational outcome was his return to Israeli custody. His prosecution and eighteen-year imprisonment, the international dispute over his capture, and renewed scrutiny of Israel's nuclear policy were personal and political consequences. Whether capture prevented further disclosures cannot be measured confidently because the public record does not reveal what additional information he retained or would otherwise have released.

Profumo and Keeler: political consequences exceed proven intelligence acquisition

The Profumo affair shows how political damage can occur even when a sexual entrapment operation is unproven. John Profumo's relationship with Christine Keeler overlapped with her contact with Soviet naval attaché Yevgeny Ivanov. The scandal raised a legitimate question about the risk of disclosure, but Lord Denning's inquiry concluded that no security risk had arisen. The inquiry and parliamentary record do not establish that Keeler was acting under

Soviet direction as part of a planned intelligence operation (Lord Denning 1963; UK Parliament n.d.).

Profumo's false statement to the House of Commons, resignation, and the damage to the Macmillan government's credibility were real political consequences. They should not be mistaken for proof that Soviet intelligence obtained British secrets through Keeler. This distinction is central to the thesis: a relationship can trigger institutional crisis through exposure, perceived risk, and political distrust even when the alleged intelligence gain is absent or unproven.

Mata Hari: the consequences of accusation and myth

Mata Hari's case belongs in the comparison as an example of uncertain operational gain alongside exceptionally severe personal consequences. The French military tribunal convicted and executed her in 1917. The French Defence Historical Service summarizes the official record while also noting scholarship that questions whether she ever meaningfully spied. Julie Wheelwright's historiographical work shows how the public figure of the "spy-courtesan" came to embody anxieties about women, sexuality, and national betrayal (Service historique de la Défense n.d.; Wheelwright 2016).

No defensible public accounting shows that Mata Hari delivered intelligence of strategic value commensurate with the claims made against her. Her execution is certain; the scale and utility of her intelligence work are contested. The case therefore warns against measuring success by the severity of punishment or the notoriety of a name. It also shows how a story about sexual access can be politically useful to authorities and later popular culture even when the intelligence yield is doubtful.

10.5 Comparison cases outside intimate recruitment

Pollard: the benchmark for documented acquisition and assessed damage

Jonathan Pollard is included as a comparison standard, not as an intimate operation. His relationship with his wife did not recruit him for Israeli intelligence. The evidence instead includes an espionage conviction, identified handlers, tasking, payments, and a declassified intelligence-community damage assessment. That assessment reported that Pollard compromised more than 800 classified publications and more than 1,000 classified messages and cables, and analyzed risks to sources, methods, intelligence sharing, and U.S. foreign-policy interests (Director of Central Intelligence 1987; Weinberger 1987; United States v. Pollard 1992).

DOI: **10.5281/zenodo.24482572**

The damage assessment records that Israeli case officers told Pollard his intelligence had critically supported Israel's October 1985 air attack on PLO headquarters near Tunis. The report records what his handlers told him, but it does not independently reconstruct how specific documents shaped the operation. The assessment also identifies risks to sources, methods, intelligence sharing, and U.S. foreign-policy interests. Public releases remain redacted, and they do not show the use of every item or provide a complete reconstruction of every downstream effect (Director of Central Intelligence 1987). The case prevents the thesis from making intimacy do explanatory work that belongs to other factors. Ideology, access, handlers, payment, and systematic tasking can produce large transfers without romantic manipulation.

Fang and Swalwell: political access and contact are not proof of espionage transfer

Fang and Swalwell provide a comparison case for political access without publicly demonstrated transfer. Reporting, the defensive briefing, released interview summaries, and the Ethics Committee outcome are documented, but they do not establish knowing cooperation or Chinese intelligence direction. Chapter 8 presents the underlying record (Axios 2020a; House Committee on Ethics 2023b; White House Government Transparency Task Force 2026b).

Alice Huang, NVIDIA, and Megaspeed: an unresolved high-stakes allegation

The Alice Huang episode belongs in the comparison as an unresolved allegation with documented institutional responses. Chapter 8 presents the reporting and official statements. The public record does not establish Chinese tasking, an information transfer, or an export-control violation; the case therefore shows how an intelligence concern and its consequences can remain distinct from a proven intimate operation (Reuters 2026b, 2026g, 2026i; Singapore Ministry of Home Affairs 2026b).

10.6 Digital cases and the limits of outcome attribution

Chapter 9 showed that online contact can produce a demonstrable classified transfer while leaving the recipient's identity or sponsor unknown. David Slater pleaded guilty to transmitting classified national defense information through an online dating relationship, and the Air Force Office of Special Investigations later reported his sentence. The public record establishes the transfer and sentence; it does not identify the recipient as an intelligence officer or prove state direction. The Saurabh Sharma case differs: India's National Investigation Agency reported a conviction and attributed the pseudonymous "Neha Sharma" persona to Pakistan's Defence/ISI

agents, but the public statement does not establish a romantic or sexual relationship. The Satendra Siwal matter remains an allegation and pending prosecution, not a final finding of guilt (U.S. Department of Justice 2025; U.S. Air Force Office of Special Investigations 2025; National Investigation Agency 2024; Satendra Siwal v. State of Uttar Pradesh 2026).

These cases demonstrate why online deception should be evaluated through the same stages as historical operations: access, information elicited, transfer, attribution, and operational effect. Slater supplies evidence of transfer without public state attribution. Sharma supplies an official state attribution and conviction without a demonstrated intimate relationship. Siwal supplies a live legal allegation without an adjudicated final outcome. Romance scams and sextortion create personal and financial harm, but complaint and loss statistics cannot be reclassified as espionage results. Similar tools do not establish shared actors, motives, or outcomes.

The digital cases also broaden the meaning of consequence. Nonconsensual intimate material can be used to demand money, silence a victim, or damage a reputation without yielding national-security information. Synthetic material can create apparent compromise without a genuine encounter. The legal and institutional consequences may be serious, but they belong in an intelligence analysis only when a case-specific record establishes state direction or intelligence purpose. Otherwise, these phenomena are relevant as adjacent forms of coercion and as conditions that can create security vulnerabilities, not as proven intelligence operations.

10.7 What the comparison says about historical change

Across the cases, human motives recur, but the methods used to study and exploit them change with institutional capacity and technology. Intimacy can create trust, obligations, secrecy, and access. A service may exploit an existing relationship or construct a deceptive one. What changes over time is the social position of targets, the means of contact, the record left behind, the legal treatment of sexuality, and the institutional capacity to monitor or exploit information.

The premodern and early modern cases discussed in Chapter 2 document political information moving through kinship, courtship, patronage, household service, and trusted correspondence. Those examples establish a long history of personal access as an intelligence channel. They do not establish a continuous, standardized “honeypot” method operating unchanged across centuries. The surviving evidence is shaped by court records, diplomatic letters, memoirs, and later storytelling. Earlier examples can support historical continuity at

DOI: **10.5281/zenodo.24482572**

the level of social access and private information, while modern archival cases support more precise claims about service direction, sexual leverage, and document transfer.

The gender pattern also changes when the cases are compared rather than retold individually. Mata Hari's notoriety helped make the female seductress the popular face of espionage, even while the East German Romeo cases document male agents cultivating women with institutional access. Lonetree and Vassall were men targeted through sexual vulnerability. Scranage was a woman who transferred information to a male partner. Digital false identities weaken the assumption that a female-looking persona implies a female operative. The historical evidence supports gendered operational patterns in particular institutions, not an inherent female capacity for seduction or an exclusively male capacity to be targeted.

The comparison further shows that successful operations need not look like sex scandals. The longest-running and most productive Romeo cases depended on ordinary, sustained relationships and workplace access. Pollard's large-scale transfer depended on tasking, ideological commitment, and opportunity without a recruitment romance. Vanunu's reported romantic lure served capture rather than acquisition. The public imagination tends to emphasize the sexual moment; the operational record often turns on access control, repeated document handling, compromised identities, and institutional oversight.

10.8 Personal and institutional consequences are not interchangeable

The cases produce consequences at several levels, but not every effect can be traced to the same cause. Personal consequences include imprisonment, loss of employment, shame, relationship trauma, isolation, and long-term public stigma. Institutional consequences include exposure of human sources, suspension of secure communications, changes to vetting and reporting, internal investigations, and the cost of replacing equipment or rebuilding trust. Political consequences include resignations, parliamentary inquiries, public controversy, and damage to government credibility. Strategic consequences may include compromised collection methods, adversary insight into allied capabilities, or changes in diplomatic relations.

The evidence is strongest for consequences recorded in court judgments, official inquiries, agency histories, and parliamentary proceedings. It is weaker when a source asserts that an operation changed national policy, caused an election outcome, or determined a military decision without documentary support. In the cases reviewed here, the consequences of prosecution and exposure are generally easier to establish than the downstream use of acquired intelligence. The Vassall, Lonetree, and Scranage records show actual disclosures and institutional responses, yet do not make every subsequent loss publicly traceable. The Pollard

DOI: **10.5281/zenodo.24482572**

assessment explicitly describes broad risk, while redactions limit independent verification of some effects. In the unresolved NVIDIA case, the scale of the surrounding political reaction cannot substitute for evidence of a transfer.

Consequences also fall unevenly. Recruited sources and deceived targets can be prosecuted or publicly shamed while handlers and institutions remain less visible. Victims of sextortion may be blamed for private material that was created or shared without consent. An institution can respond to a security breach by scrutinizing an individual's sexuality while neglecting the policies that created excessive access or weak supervision. An account of intimate intelligence must therefore examine both the person who disclosed information and the systems that enabled, exploited, or failed to detect the disclosure.

10.9 Why some cases become visible

Public visibility is not a reliable measure of frequency or success. Cases tend to become visible when an operation fails, a source defects, an arrest produces court records, a government conducts an inquiry, a political scandal becomes public, or a later declassification release changes what can be said. Successful operations can remain concealed. Failed operations can leave dramatic public traces despite yielding little useful information. A famous scandal may remain in public memory because it can be told as a compelling story, while a productive and routine source may remain unknown.

The visibility of a case also shapes its gender narrative. A female target or operative whose sexuality is central to public storytelling can become a symbol, as Mata Hari did, while male recruiters, officials who enabled access, and institutional deficiencies receive less attention. Conversely, male victims of sexual blackmail may be obscured by stigma or legal norms. The archive is not a neutral census of intimate intelligence. It is a record of what institutions documented, prosecuted, released, and remembered.

This selection effect prevents the thesis from estimating the overall prevalence or success rate of intimate operations. It also requires caution when comparing centuries. Early records are often less complete, categories of sexuality and espionage have changed, and state archives open selectively. The defensible claim is historical recurrence of personal access and private leverage, alongside documented periods and cases in which services deliberately organized intimate recruitment. The evidence does not support a timeless, universal technique with a stable rate of success.

DOI: **10.5281/zenodo.24482572**

Chapter 11.
Findings, Limits, and the Architecture of Intimate Power

11.1 The question the thesis can answer

This thesis set out to investigate how private relationships have intersected with intelligence collection, recruitment, coercion, and institutional power across history. Its conclusion is affirmative but qualified. Human relationships have long created routes to information and influence. In particular cases, intelligence organizations deliberately cultivated romantic or sexual relationships, exploited existing attachments, or used private material to compel cooperation. Yet the evidence does not support one timeless "honey trap" method repeated unchanged from antiquity to the digital present. The historical continuity lies in the use of human access and trust. The operational forms, gender expectations, state structures, technologies, and evidentiary records changed.

The central proposition is therefore supported in a conditional form: private intimacy can become a channel through which information, leverage, and institutional power move between individuals and organizations. A historical claim that a particular relationship moved a secret, altered a decision, or changed an institution must still be demonstrated case by case. Intimacy is neither proof of espionage nor a sufficient explanation for an intelligence outcome.

This distinction answers the thesis's main methodological challenge. The subject is emotionally compelling, but narrative force is not evidence. A public scandal can be politically consequential without producing intelligence. A person can pass secrets through an online relationship without the recipient's state affiliation being publicly established. A service may use a relationship to capture someone after the important information has already been disclosed elsewhere. A famous accusation can leave behind more cultural memory than reliable evidence of intelligence gain. The analysis must therefore distinguish access, recruitment, transfer, operational use, leverage, capture, and consequence.

11.2 The architecture: from social access to institutional effect

Across the cases, intimate influence can be understood as a sequence of possible connections rather than a single tactic. First comes access. Family networks, court service, diplomacy, military posting, clerical work, corporate relationships, and online platforms can bring people into contact with individuals or institutions they could not otherwise reach. Second comes trust, attraction, reciprocity, emotional dependence, or perceived obligation.

DOI: **10.5281/zenodo.24482572**

Third, an actor may seek information, continued access, a meeting, movement to a location, silence, or compliance. A later stage may involve a transfer of material, recruitment, coercion, or the use of compromising information. Only some operations proceed through every stage, and the sequence does not establish that all relationships were planned from the outset.

The premodern and early modern evidence supports a long history of information moving through households, kinship, service, correspondence, courtship, and social networks. The Flemish agents of 1488-1489, the women operating in early modern British intelligence networks, and women in diplomatic households show that political information depended on mobility and relationships as well as formal office (Demets and Haemers 2022; Akkerman 2018; Do Paço 2022). These cases establish women's participation in intelligence work and the political value of access. They do not establish that every such woman was a seductress or that modern state-directed sexual entrapment existed in the same form centuries earlier.

Modern intelligence systems made some forms of relational cultivation more organized and traceable. The East German Romeo operations used male officers to build sustained relationships with women employed in West German institutions. Some sources passed documents over years, making the relationship a durable access channel rather than a brief sexual compromise (Central Intelligence Agency n.d.-b; Maddrell 2014). John Vassall's recruitment involved the exploitation of sexual stigma and compromising exposure in a period when same-sex conduct was criminalized. Clayton Lonetree was recruited through a Soviet embassy employee and her relative, then passed classified information. Sharon Scranage gave classified material to her Ghanaian partner, Michael Soussoudis. These cases differ in method and motive, but they demonstrate that both men and women could be placed in operational roles, targeted, or drawn into relationships that became intelligence channels (House of Commons 1962; National Security Council 1986; United States v. Lonetree 1990, 1992; Central Intelligence Agency 1990; The Washington Post 1985a, 1985b).

Intimacy did not always defeat security. Access and trust could lower barriers to collection when institutions concentrated valuable information in a person, office, or relationship. The institution shapes the stakes. Clearance boundaries, work routines, source protection, reporting procedures, and counterintelligence coordination determine whether one person's conduct becomes an isolated breach or a wider vulnerability. The Radcliffe inquiry into Vassall and the U.S. response to the Lonetree case show that institutional failures can magnify personal disclosures and increase the cost of remediation. Individual responsibility and institutional responsibility can coexist.

DOI: **10.5281/zenodo.24482572**

11.3 Psychology explains vulnerability without diagnosing the target

The psychological research reviewed in this thesis helps explain how intimacy can facilitate disclosure and influence. Self-disclosure and perceived responsiveness are associated with the development of closeness; reciprocity and social influence can shape compliance; attachment and belonging can make a relationship meaningful and difficult to abandon (Collins and Miller 1994; Laurenceau, Barrett, and Pietromonaco 1998; Cialdini and Goldstein 2004). These findings describe general interpersonal processes. They do not establish that any named person was susceptible for a particular reason, and they do not prove that a relationship was operationally directed.

The cases resist a single psychological profile. Some people acted for money, ideology, career advancement, resentment, affection, coercion, or mixed reasons. Some were deceived about the identity or purpose of a partner. Others knowingly cooperated, sometimes after a relationship already existed. Shame, secrecy, fear of exposure, and the social or legal consequences of sexuality could become leverage, as in Vassall's case. But consensual intimacy is not consent to espionage, and sexual conduct alone is not evidence of compromise. Labels such as "narcissist," "sexually impulsive," or "gullible" would convert explanation into ungrounded diagnosis.

The more useful psychological question is situational: what did the relationship make possible, what request followed, how did the target understand the request, what pressure or obligation existed, and what could the target realistically refuse? That question preserves human agency without assuming that participation was fully free. It also avoids treating emotional attachment as an operational weakness in itself. The vulnerability may lie in an institution's excessive concentration of access, its failure to provide safe reporting routes, or an adversary's ability to exploit legal stigma and fear.

Medieval and early modern actors could read and exploit behavior through practical knowledge of status, loyalty, ambition, affection, obligation, fear, and reputation. The surviving sources do not show a formal psychological discipline or standardized intelligence curriculum shaping those cases.

By the twentieth century, some intelligence organizations had made human assessment and interpersonal tradecraft more systematic. A Stasi training document analyzed secretaries' work routines, institutional access, and occupational vulnerabilities. A declassified CIA account described operations officers receiving extensive training in specialized tradecraft and interpersonal relations. These records document institutional study and modern training, not that every agent studied academic psychology or used identical methods (Bundesarchiv, Stasi

Records Archive n.d.; Central Intelligence Agency n.d.-a). Later U.S. Department of Defense policy formalized HUMINT training and certification requirements (United States Department of Defense 2015). The continuity is practical recognition that people respond to relationships and pressure. The historical change is the organization, systematization, and deliberate teaching of that knowledge.

Intimate espionage is a deliberate exploitation of human behavior. The operative's purpose is to learn what matters to the target and use that knowledge to obtain access, information, cooperation, or leverage. In directed intimate operations, deception is part of the method: an operative may conceal identity and purpose, feign affection, mirror the target's interests, offer validation, or make requests that grow from personal disclosure into access to protected information. The Romeo operations show how a service used feigned love and promises of marriage to cultivate sources with government access. The relationship was not simply personal; it was used to reach information through trust and attachment (Stasi Records Archive, n.d.; Maddrell 2014, 182–83).

Authority does not make a person immune to manipulation. Status, expertise, ambition, ego, desire for recognition, sexual or romantic interest, loyalty, and the need to belong can all shape decisions. Secrecy can keep a target from seeking advice. Stigma can make disclosure feel more dangerous than continued cooperation. Attachment can make refusal feel like betrayal, while blackmail can turn fear of exposure into direct pressure. These mechanisms help explain why someone may trust, protect, or cooperate with an intimate partner even when the stakes are high.

Awareness can help a target recognize warning signs such as intense flattery, concealed identity, demands for secrecy, inconsistencies, or requests that keep escalating. But being deceived does not prove that a target was foolish or consenting. The operative chooses to exploit human behavior; the target's authority does not erase that choice or the deception used against them.

11.4 Gender shaped the craft and the story told about it

The thesis does not support the idea that women are uniquely responsible for intimate espionage. Women acted as messengers, informants, couriers, agents, analysts, codebreakers, political intermediaries, and operatives. Men also cultivated women for institutional access. Men were targets of sexual blackmail and romantic deception. Women could be targets, recruiters, partners, or people whose relationships were exploited by others. The Romeo operations make the male-agent pattern especially clear; Scranage was a female intelligence

employee who passed information to a male partner. In the reported Vanunu operation, a female operative helped capture a male target.

Gender mattered because it shaped who could travel, enter a household, work in an office, gain trust, or be believed. It also shaped which stories became memorable. Mata Hari's prosecution and execution produced a persistent image of the sexually dangerous female spy, although the intelligence yield attributed to her remains disputed. Male recruiters and institutional failures have often been less visible in popular retellings. In Vassall's case, stigma attached to same-sex conduct was used against a male target. In the digital environment, a false online persona can perform a gendered identity regardless of the operator's actual identity. The appearance of a woman is not proof that a woman operated the account.

The historical conclusion is thus about gendered opportunity and representation, not inherent capacity. The "seductress" stereotype can obscure trained women operatives, male recruiters, male victims, genuine relationships later exploited, and institutional systems that made access possible. A sound case history records who initiated contact, what each person knew, when intelligence purpose arose, and how later accounts assigned blame.

11.5 What the cases show about information actually obtained

The research finds several documented pathways to information, but it cannot produce a defensible overall success rate. The public record does not offer a denominator that includes failed approaches, undetected operations, relationships that yielded nothing, and cases that were never exposed. Nor do governments and archives classify these incidents consistently. A percentage would imply a precision the evidence cannot support.

The strongest general finding is that transfer is better documented than strategic use. Court records and inquiries can establish what a person disclosed or what investigators recovered. They less often show precisely which recipient used each item, which decision changed because of it, or what military, diplomatic, or commercial outcome followed. The amount discovered by investigators is not automatically the amount delivered to a foreign service, and the amount delivered is not automatically the amount used. The thesis therefore measures information gains by the strongest public evidence available and treats claims about downstream impact separately.

11.6 Consequences were real but unevenly traceable

The case chapters document prosecutions, exposure, security changes, inquiries, resignations, and public scrutiny more clearly than they document private family effects or the

DOI: **10.5281/zenodo.24482572**

item-by-item use of acquired information. These outcomes establish consequences for people and institutions; they do not, by themselves, prove that an intimate relationship produced an intelligence gain.

11.7 Limits of this investigation

This is an independent historical and psychological investigation. It relies on accessible primary documents, court records, official inquiries, archival collections, declassified files, scholarly research, and credible reporting. The quality and completeness of those sources vary sharply across time and national context. The research cannot inspect closed intelligence archives, verify every classified claim, or reconstruct all private conversations that led to a disclosure.

The medieval and early modern cases are not directly comparable to twentieth-century intelligence services. They illuminate the longer history of social access and information networks, but they do not permit a claim that modern, centralized honeypot operations existed unchanged across the centuries. The Cold War record is richer in formal inquiries, prosecutions, and declassified documents, but it remains selective. Contemporary corporate and political allegations are especially vulnerable to partisan framing, secrecy, and incomplete investigations. The psychological literature supports general mechanisms but cannot identify an individual's motives without evidence specific to that person.

The thesis also cannot calculate a global prevalence rate or a general success rate. It does not claim that every disclosed secret was used, that every relationship was initiated by an intelligence service, or that every official allegation is accurate. Some individual cases may be revised as archives open or litigation concludes. The NVIDIA and Megaspeed case is the clearest present example of a high-stakes matter whose public evidence is still developing. These limitations narrow the conclusions; they do not nullify the documented cases.

11.8 Final findings

The investigation yields six final findings.

First, intimate and social access are recurring parts of intelligence history, but deliberate sexual entrapment is period-specific. The record from antiquity through early modern Europe shows information moving through households, service, courtship, correspondence, diplomacy, and social networks. Modern services sometimes organized romantic recruitment and sexual compromise more explicitly. The continuity is human access, not an unchanged operational doctrine.

DOI: **10.5281/zenodo.24482572**

Second, the craft is not inherently female. Women and men have served as operatives, recruited sources, intermediaries, partners, targets, and victims. Gender norms influence access and public interpretation, but do not assign espionage capacity to one sex. The seductive woman became a durable cultural image that often concealed broader networks and institutional choices.

Third, psychological vulnerability is relational and institutional, and the methods used to understand and exploit it changed over time. Earlier actors relied on practical observation and experience; twentieth-century intelligence organizations increasingly systematized target study and interpersonal tradecraft through institutional training. Trust, reciprocal disclosure, attachment, secrecy, stigma, and fear can influence decisions. None provides a universal profile or proves culpability. Security systems determine how far an individual relationship can reach into protected information and whether warning signs can be acted upon.

Fourth, demonstrated transfer is more common in the public record than demonstrated strategic effect. Several cases establish the passage of classified information, and Pollard shows how a large-scale acquisition can be described through legal and intelligence records. Even there, redactions and reliance on handler accounts limit reconstruction of downstream use. Claims that intimacy changed a military, political, corporate, or diplomatic decision require separate proof.

Fifth, consequences can be substantial even when intelligence gain is uncertain. Capture, imprisonment, institutional disruption, resignation, diplomatic exchange, public stigma, and corporate scrutiny are distinct outcomes. A scandal can damage an institution without proving a foreign service directed it. A relationship can facilitate capture without producing the information that initiated the case. Harm must be measured at the level the evidence supports.

Sixth, digital media expand reach and alter evidence, not the burden of proof. Online platforms enable contact across distance, persistent communication, false identities, and rapid circulation of intimate material. Digital records can preserve requests and transfers, but identities and state sponsorship may remain uncertain. Sextortion and synthetic intimate imagery create serious forms of coercion that belong beside the history of intelligence without being conflated with it.

The title's "architecture" refers to the arrangement of relationships, access, information, secrecy, leverage, and institutional rules through which private life can become politically consequential. The research does not show that intimacy automatically yields secrets or control. It shows that institutions and intelligence actors have repeatedly recognized the value

DOI: **10.5281/zenodo.24482572**

of human access, and that relationships can become channels when opportunity, motive, operational design, and vulnerability align. The historical claim remains strongest when stated with restraint: private intimacy can move information, leverage, and institutional power, but the evidence must establish what moved, who directed it, and what changed.

DOI: **10.5281/zenodo.24482572**

Author's Statement

In my view, spying has long been a craft used to obtain information, access, or advantage for a state, a political actor, or another interested party. Its methods have evolved. Men and women have served as agents, sources, intermediaries, and targets. Modern intelligence work has increasingly applied organized target study and psychological knowledge to identify what a person wants, fears, or may be persuaded to protect. Yet the human vulnerabilities that can be reached through attention, desire, ego, trust, or ambition have not disappeared. A target who feels admired or uniquely understood may overlook warning signs and the consequences for colleagues, family, professional life, or the institution entrusted to them. That does not make every target foolish or prove that every intimate relationship was an operation; each case still depends on its evidence.

The stakes now extend beyond governments to corporate and industrial espionage, where confidential information, proprietary knowledge, and advanced technology can be copied, transferred, or exploited. The spy's craft can demand mastery of deception and illusion, and a willingness to set conscience aside in pursuit of an objective. The methods and tools change, but the human cost can reach the target, the operative, their families, companies, institutions, and the public. My closing thought is simple: "Play by fire, pay by fire."

DOI: **10.5281/zenodo.24482572**

References

ABC News. 2026. “New FBI Files Reveal Former Rep. Eric Swalwell Admitted Relationship with Suspected Chinese Operative Christine Fang.” August 17, 2026. https://abc7.com/amp/post/new-fbi-files-reveal-former-rep-eric-swalwell-admitted-relationship-suspected-chinese-operative-christine-fang/19694681/.

Akkerman, Nadine. 2018. *Invisible Agents: Women and Espionage in Seventeenth-Century Britain*. Oxford: Oxford University Press.

Allen, Gemma. 2019. “The Rise of the Ambassadress: English Ambassadorial Wives and Early Modern Diplomatic Culture.” *The Historical Journal* 62 (3): 617-638. https://doi.org/10.1017/S0018246X1800016X.

Aristotle. 1885. The Politics of Aristotle. Translated into English, with introduction, marginal analysis, essays, notes, and indices, by Benjamin Jowett. Oxford: Clarendon Press.

Aristotle. 1944. Politics. Translated by Harris Rackham. Loeb Classical Library 264. London: William Heinemann; Cambridge, MA: Harvard University Press.

Axios. 2020a. “Feds worried Chinese spy Fang Fang targeted California politicians.” December 8, 2020. https://www.axios.com/2020/12/08/china-spy-fang-fang-california-politicians.

Axios. 2020b. “How a Suspected Chinese Spy Gained Access to California Politics.” December 8, 2020. https://www.axios.com/2020/12/08/china-spy-california-politicians.

Bailey, Jordyn. 2024. *Surveilling Sex: Prostitution and the East German Stasi, 1950-1989*. PhD diss., University of New Brunswick.

Balu, Raphaële. 2020. “Anne-Marie Walters vs. George Starr: Reflections on Gendered Representations within the Special Operations Executive.” *British Journal for Military History* 6 (3): 66-84. https://doi.org/10.25602/GOLD.bjmh.v6i3.1426.

Bernstein, Richard. 1986. “France Jails 2 in Odd Case of Espionage.” New York Times, May 11, 1986. Clipping reproduced in CIA Reading Room. https://www.cia.gov/readingroom/docs/CIA-RDP90-00965R000100490003-8.pdf.

Bilz, Alexander, Lynsay A. Shepherd, and Graham I. Johnson. 2023. “Tainted Love: A Systematic Literature Review of Online Romance Scam Research.” *Interacting with Computers* 35 (6): 773-788. https://doi.org/10.1093/iwc/iwad048.

Blaylock, Isabel J. 2025. “In the Name of National Security: The Federal Surveillance and Weaponization of Sex in Cold War America.” Undergraduate honors thesis, University of Richmond.

Bloomer, Stephanie A. 2016. “Exploring the Susceptibility of High Sensation Seeking Individuals to Honey Trap Operations for the Purpose of Targeting and the Development of Self-Protective Countermeasures.” MA capstone thesis, American Public University System.

British Security Coordination. 1998. *British Security Coordination: The Secret History of British Intelligence in the Americas, 1940-1945*. New York: Fromm International.

Bundesarchiv, Stasi Records Archive. n.d. “Training Material with Selected Findings about the Occupational Group of Secretaries.” Stasi Mediathek. Accessed November 16, 2026. https://www.stasi-mediathek.de/medien/schulungsmaterial-mit-ausgewaehlten-erkenntnissen-ueber-die-berufsgruppe-der-sekretaerinnen/.

Central Intelligence Agency. n.d.-a. “A Vital Institution and a Distinguished Tradition.” CIA Reading Room. Declassified in part March 13, 2013. https://www.cia.gov/readingroom/docs/CIA-RDP90-00530R000701680004-1.pdf.

CBS News. 2026. “Ex-Nvidia CEO Jensen Huang Agrees to Testify as Congress Raises Concerns about Affair with Suspected Chinese Spy.” November 17, 2026. https://www.cbsnews.com/news/house-republicans-nvidia-jensen-huang-testimony/.

Central Intelligence Agency. n.d.-b. “Romeo Spies.” Accessed November 16, 2026. https://www.cia.gov/stories/story/romeo-spies/.

Central Intelligence Agency. 1990. “The Scranage Case: CIA, Ghana, and the [title redacted].” *Studies in Intelligence* 34 (Fall). Declassified July 29, 2014. https://www.cia.gov/readingroom/docs/DOC_0000624354.pdf.

Christl, Maria-Ernestina, Kim-Chi Tran Pham, Adi Rosenthal, and Anne P. DePrince. 2024. “When Institutions Harm Those Who Depend on Them: A Scoping Review of Institutional Betrayal.” *Trauma, Violence, & Abuse* 25 (4): 2797-2813. https://doi.org/10.1177/15248380241226627.

Churchill Archives Centre. n.d. “The Papers of Vasiliy Mitrokhin.” University of Cambridge. Accessed November 16, 2026. https://archives.chu.cam.ac.uk/collections/mitrokhin/.

Cialdini, Robert B., and Noah J. Goldstein. 2004. “Social Influence: Compliance and Conformity.” *Annual Review of Psychology* 55: 591-621. https://doi.org/10.1146/annurev.psych.55.090902.142015.

CNBC. 2026. “First on CNBC: Excerpts from interview with Atreides Management managing partner and CIO Gavin Baker.” https://pressroom.versantmedia.com/cnbc/press-releases/first-cnbc-excerpts-atreides-management-managing-partner-cio-gavin-baker-speaks.

Collins, Nancy L., and Lynn Carol Miller. 1994. “Self-Disclosure and Liking: A Meta-Analytic Review.” *Psychological Bulletin* 116 (3): 457-475. https://doi.org/10.1037/0033-2909.116.3.457.

Congressional Research Service. 2025. *The TAKE IT DOWN Act: A Federal Criminal Prohibition and Platform Requirements for Nonconsensual Intimate Visual Depictions*. Legal Sidebar LSB11314. May 2025. https://crsreports.congress.gov/product/pdf/LSB/LSB11314.

Curry, Anne. 2009. “Soldiers’ Wives in the Hundred Years War.” In *Soldiers, Nobles and Gentlemen: Essays in Honour of Maurice Keen*, edited by Peter Coss and Christopher Tyerman, 198-214. Woodbridge: Boydell Press.

Debruyne, Emmanuel. 2014. “Espionage.” In *1914-1918 Online: International Encyclopedia of the First World War*. https://encyclopedia.1914-1918-online.net/article/espionage/.

Demets, Lisa, and Jelle Haemers. 2022. “‘Omme maren te vernemene van den Duutschen’: Vrouwen als spionnen en boodschappers in de Vlaamse Opstand (1488-1489).” *Tijdschrift voor Geschiedenis* 135 (1): 22-42. https://doi.org/10.5117/TvG2022.1.003.DEME.

Demets, Lisa, and Jelle Haemers. 2025. “Women, War and Intelligence in Ypres and the Flemish West Quarter (1488-1489).” *Intelligence and National Security* 40 (4): 627-647. https://doi.org/10.1080/02684527.2025.2506279.

Department of Justice and Department of Commerce. 2026. “Joint Statement from Department of Commerce and Department of Justice on Megaspeed Investigation.” November 17, 2026. https://www.justice.gov/opa/pr/joint-statement-department-commerce-and-department-justice-megaspeed-investigation.

Department of State. 2016. “DSS Historical Fact of the Day: Clayton Lonetree.” March 25, 2016. https://2009-2017.state.gov/m/ds/c69942.htm.

Director of Central Intelligence. 1987. *The Jonathan Jay Pollard Espionage Case: A Damage Assessment*. October 30, 1987; declassified and released by the National Archives and Records Administration. https://www.archives.gov/files/declassification/iscap/pdf/2007-010-doc1.pdf.

Do Paço, David. 2022. “Women in Diplomacy in Late Eighteenth-Century Istanbul.” *The Historical Journal* 65 (3): 640-662. https://doi.org/10.1017/S0018246X21000479.

Drumhiller, Nicole K. 2025. “Women in Intelligence: A Limited Systematic Review.” *Intelligence and National Security* 40 (4): 605-626. https://doi.org/10.1080/02684527.2025.2506278.

Eco, Umberto. 2015. *How to Write a Thesis*. Translated by Caterina Mongiat Farina and Geoff Farina. Cambridge, MA: MIT Press. Originally published in Italian in 1977.

English Heritage. n.d.-a “Jane Whorwood: Royalist Spy.” Accessed November 16, 2026. https://www.english-heritage.org.uk/visit/places/carisbrooke-castle/history/jane-whorwood/.

English Heritage. n.d.-b “Margoth: A Cross-Dressing Medieval Spy at Kenilworth Castle.” Accessed November 16, 2026. https://www.english-heritage.org.uk/visit/places/kenilworth-castle/history-and-stories/cross-dressing-spy/.

Farsi, Arghawan, and Luděk Michálek. 2023. *Skryté vlaštovky: Role ženských agentek v íránských zpravodajských praktikách [Hidden Swallows: The Role of Female Agents in Iranian Intelligence Practices]*. Master’s thesis, Charles University.

FBI Chicago. 2026. “FBI Chicago Releases Public Service Announcement Raising Awareness on Romance Scams and Confidence Fraud.” February 13, 2026. https://www.fbi.gov/contact-us/field-offices/chicago/news/fbi-chicago-releases-public-service-announcement-raising-awareness-on-romance-scams-and-confidence-fraud.

Federal Bureau of Investigation. n.d.-a. “Financially Motivated Sextortion.” https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/sextortion/financially-motivated-sextortion.

Federal Bureau of Investigation. n.d.-b. “Year of the Spy (1985): Jonathan Jay Pollard.” Accessed November 16, 2026. https://www.fbi.gov/history/cases-and-criminals/year-of-the-spy-1985.

Federal Bureau of Investigation, Internet Crime Complaint Center. 2025. *2024 Internet Crime Report*. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

Financial Times. 2026. “Nvidia reinstates Jensen Huang as chief executive.” https://www.ft.com/content/08914b05-bbfa-478d-b38a-549acfc1aae6.

Follorou, Jacques. 2025. “The KGB’s Spy inside France’s Cold War Counter-Espionage.” *Le Monde*, January 5, 2025. https://www.lemonde.fr/en/history/article/2025/01/05/the-kgb-s-spy-inside-france-s-cold-war-counter-espionage_6736726_157.html.

Fritts, Robert E. 2004. “Interview with Robert E. Fritts.” Foreign Affairs Oral History Collection, Association for Diplomatic Studies and Training. https://tile.loc.gov/storage-services/service/mss/mfdip/2004/2004fri04/2004fri04.pdf.

Fry, Helen. 2023. *Women in Intelligence: The Hidden History of Two World Wars*. New Haven: Yale University Press.

Grawe, Lukas. 2025. “Espionage, Sabotage, Propaganda: German Military Attachés in Neutral Countries and Their Organisation and Tasks During the First World War.” *Journal of Intelligence History* 24 (3): 261-284. https://doi.org/10.1080/16161262.2024.2387982.

Haemers, Jelle. 2024. “Women and War: Female Spies and Messengers in the Late-Medieval Low Countries.” *Journal of Women’s History* 36 (2): 10-29. https://doi.org/10.1353/jowh.2024.a929066.

Hansard. 1962. “The Vassall Case and Naval Security.” House of Lords, October 31, 1962. https://api.parliament.uk/historic-hansard/lords/1962/oct/31/the-vassall-case-and-naval-security.

Hansard. 1963a. “The Radcliffe Report and Tribunals of Inquiry.” House of Lords Debates, May 8, 1963, vol. 248, cols. 699-756. https://api.parliament.uk/historic-hansard/lords/1963/may/08/the-radcliffe-report-and-tribunals-of.

Hansard. 1963b. “Vassall Case (Tribunal’s Report).” House of Commons Debates, April 25, 1963, vol. 676, cols. 423-425. https://api.parliament.uk/historic-hansard/commons/1963/apr/25/vassall-case-tribunals-report.

Harris, Kayci Olson. 2021. *Pas de Deux: Cold War Dance Tours and Franco-Soviet Cultural Interaction, 1953-1975*. PhD diss., University of Wisconsin-Madison. https://asset.library.wisc.edu/1711.dl/TOVUHCGA5ZZMQ8L/R/file-b705b.pdf.

House Committee on Ethics. 2023a. “Letter to Representative Eric Swalwell.” May 22, 2023. https://static.foxnews.com/foxnews.com/content/uploads/2023/05/COE-to-swalwell.pdf.

House Committee on Ethics. 2023b. “Statement Regarding Representative Eric Swalwell.” May 23, 2023. Letter concluding that the Committee would take no further action, reproduced in Mariana Alfaro, “House Ethics Committee Closes Swalwell Investigation with No Further Action,” Washington Post, May 23, 2023. https://www.washingtonpost.com/politics/2023/05/23/swalwell-ethics-investigation-closed/.

House of Commons. 1962. “Vassall Case.” Hansard, November 2, 1962. https://hansard.parliament.uk/commons/1962-11-02/debates/3c5d37a1-194b-4b5a-9b46-94829fa8b8bd/CommonsChamber.

House of Commons. 1986. “Mr Mordechai Vanunu.” Hansard, November 18, 1986. https://hansard.parliament.uk/Commons/1986-11-18/debates/2eeb373a-ce8e-443f-97a9-086e85ff864f/MrMordechaiVanunu.

House Select Committee on China. 2026. “Moolenaar, Mast, and Crawford Seek Briefing from Jensen Huang on Ties to Chinese Intelligence Asset.” November 5, 2026. https://chinaselectcommittee.house.gov/media/press-releases/moolenaar-mast-and-crawford-seek-briefing-from-jensen-huang-on-ties-to-chinese-intelligence-asset.

Huneke, Samuel Clowes. 2023. “The Surveillance of Subcultures: Gay Spies, Everyday Life, and Cold War Intelligence in Divided Berlin.” *Journal of Social History* 56 (3): 559-582. https://doi.org/10.1093/jsh/shac030.

Indian Express. 2024. “Indian Embassy Employee Shared Secret Military Documents after Being Honey-Trapped: UP ATS.” February 14, 2024. https://indianexpress.com/article/india/indian-embassy-employee-shared-secret-military-documents-honey-trapped-up-ats-9161827/.

Kornfield, Meryl. 2026. “Trump’s stake in Nvidia grew to as much as $62 million before scandal broke out.” https://www.washingtonpost.com/business/2026/11/16/trumps-stake-nvidia-grew-much-62-million-before-scandal-broke-out/.

NVIDIA Developer. n.d.. “Unreal Engine 3D Creation Platform.” https://developer.nvidia.com/game-engines/unreal-engine.

NVIDIA. 2024. “NVIDIA Ethernet Networking Accelerates World’s Largest AI Supercomputer, Built by xAI.” https://nvidianews.nvidia.com/news/spectrum-x-ethernet-networking-xai-colossus.

NVIDIA. 2026. “NVIDIA Board Reinstates Jensen Huang as President, CEO and Board Director.” https://investor.nvidia.com/news/press-release-details/2026/NVIDIA-Board-Reinstates-Jensen-Huang-as-President-CEO-and-Board-Director/default.aspx.

Reuters. 2026j. “Nvidia says no to rehiring Huang and WSJ reports SEC is probing the chipmaker.” https://www.investing.com/news/stock-market-news/nvidia-board-forms-committee-for-national-security-and-export-control-oversight-5032154.

Shopify. 2026. “How Shopify turns open models into task experts.” https://shopify.engineering/open-model-task-experts.

Stand with Jensen. 2026a. “An Open Letter to the NVIDIA Board of Directors.” https://standwithjensen.com/.

Stand with Jensen. 2026b. “Letter to the NVIDIA Board of Directors: Who decides whether Jensen Huang returns.” https://standwithjensen.com/documents/letter-to-nvidia-board-2026-11-20.pdf.

The Guardian. 2026. “Trump says he spoke to Nvidia board directly about Jensen Huang and insists CEO’s return doesn’t pose a national security risk.” https://www.theguardian.com/us-news/live/2026/nov/23/donald-trump-democrats-republicans-presidential-primary-midterms-house-latest-news-updates?page=with%3Ablock-6b0469da8f08cb9a90515679.

The Information. 2026a. “Alice Huang’s Companies Invested in DeepSeek, Promising Nvidia Chips.” November 12, 2026. https://www.theinformation.com/articles/alice-huangs-companies-invested-deepseek-promising-nvidia-chips.

The Information. 2026b. “How Jensen Huang’s Yearslong Ties to Alice Huang Enabled $7 Billion-Plus Nvidia Chip Sales to China.” November 10, 2026. https://www.theinformation.com/articles/jensen-huangs-yearslong-ties-alice-huang-enabled-nvidia-chip-sales-china.

The Information. 2026c. “Nvidia Board Is Launching Investigation After Reporting That CEO Targeted by Chinese Informant.” November 8, 2026. https://www.theinformation.com/briefings/nvidia-board-launching-investigation-reporting-ceo-targeted-chinese-informant.

Iordanou, Ioanna. 2019. *Venice’s Secret Service: Organizing Intelligence in the Renaissance*. Oxford: Oxford University Press.

Jewish Telegraphic Agency (JTA). 1986. “Woman Who Lured Vanunu Named.” October 1986. https://www.jta.org/archive/woman-who-lured-vanunu-named.

Judges. In *The New Oxford Annotated Bible with Apocrypha: New Revised Standard Version*. 5th ed. Oxford: Oxford University Press, 2018.

Judith. In *The New Oxford Annotated Bible with Apocrypha: New Revised Standard Version*. 5th ed. Oxford: Oxford University Press, 2018.

Kazyulina, Regina. 2024. “In Their Words: Soviet Women in the Ranks of Soviet Intelligence during the Second World War.” In *The Eastern Front: War, Myth, and Memory*, edited by Yan Mann and Olga Kucherenko, 177-199. London: Routledge.

Laurenceau, Jean-Philippe, Lisa Feldman Barrett, and Paula R. Pietromonaco. 1998. “Intimacy as an Interpersonal Process: The Importance of Self-Disclosure, Partner Disclosure, and Perceived Partner Responsiveness in Interpersonal Exchanges.” *Journal of Personality and Social Psychology* 74 (5): 1238-1251. https://doi.org/10.1037/0022-3514.74.5.1238.

Le Monde. 1964. “M. Dejean Will Leave His Post on February 10.” February 5, 1964. https://www.lemonde.fr/archives/article/1964/02/05/m-dejean-quittera-son-poste-le-10-fevrier_2129753_1819218.html.

Le Monde. 1986a. “À la cour d’assises de Paris: espionnage à la chinoise.” May 7, 1986. https://www.lemonde.fr/archives/article/1986/05/07/a-la-cour-d-assises-de-paris-espionnage-a-la-chinoise_3117530_1819218.html.

Le Monde. 1986b. “Bernard Boursicot et Shi Peipu sont condamnés à six ans de détention criminelle.” May 8, 1986. https://www.lemonde.fr/archives/article/1986/05/08/bernard-boursicot-et-shi-peipu-sont-condamnes-a-six-ans-de-detention-criminelle_2935244_1819218.html.

Levitsky, Melvyn. 1987. “Memorandum from the Executive Secretary of the Department of State to the President’s Assistant for National Security Affairs (Carlucci): A Second Marine in the Security Guard Espionage Case.” March 23, 1987. *Foreign Relations of the United States, 1981-1988*, Volume VI, Soviet Union, October 1986-January 1989, Document 27. U.S. Department of State, Office of the Historian. https://history.state.gov/historicaldocuments/frus1981-88v06/d27.

Lord Denning. 1963. Report of the Tribunal Appointed to Inquire into the Matters Arising from the Profumo Affair. London: Her Majesty’s Stationery Office.

Los Angeles Times. 1986. “Vanunu Is Seized in Rome, Israel Says He Gave Nuclear Secrets.” October 8, 1986. https://www.latimes.com/archives/la-xpm-1986-10-08-mn-4812-story.html.

Los Angeles Times. 2004. “Israel Frees Nuclear Whistle-Blower Vanunu.” April 21, 2004. https://www.latimes.com/archives/la-xpm-2004-apr-21-fg-vanunu21-story.html.

Lovell, Mary S. 1992. *Cast No Shadow: The Life of the American Spy Who Changed the Course of World War II*. New York: Pantheon Books.

Maddrell, Paul. 2014. “Cooperation between the HV A and the KGB, 1951-1989.” In *The Stasi at Home and Abroad: Domestic Order and Foreign Intelligence*, 171-192. German Historical Institute. https://www.ghi-dc.org/fileadmin/publications/Bulletin_Supplement/Supplement_9/supp9.pdf.

Marshall, Alan. 2015. “‘Memorialls for Mrs Affora’: Aphra Behn and the Restoration Intelligence World.” *Women’s Writing* 22 (1): 13-33. https://doi.org/10.1080/09699082.2014.941181.

Martinez Morales, Jennifer. 2015. *Women and War in Classical Greece*. PhD thesis, University of Liverpool. https://doi.org/10.17638/02042479.

McKenzie, Tiffany, Pamela Henry, and Nikki Rajakaruna. 2026. “Managing Human Sources: Identification and Management of Motivation.” *Psychiatry, Psychology and Law* 33 (3): 683-705. https://doi.org/10.1080/13218719.2025.2454577.

Metropolitan Museum of Art. n.d. “The Countess da Castiglione.” Accessed November 16, 2026. https://www.metmuseum.org/es/essays/the-countess-da-castiglione.

Mikulincer, Mario, and Phillip R. Shaver. 2016. “Adult Attachment, Stress, and Romantic Relationships.” *Current Opinion in Psychology* 13: 19-24. https://doi.org/10.1016/j.copsyc.2016.04.006.

Mikulincer, Mario, and Phillip R. Shaver. 2019. “Attachment Orientations and Emotion Regulation.” *Current Opinion in Psychology* 25: 6-10. https://doi.org/10.1016/j.copsyc.2018.02.006.

Miller, Geoffrey D. 2014. “A Femme Fatale of Whom ‘No One Spoke Ill’: Judith’s Moral Muddle and Her Personification of Yahweh.” *Journal for the Study of the Old Testament* 39 (2): 223-245. https://doi.org/10.1177/0309089214567377.

The National Archives. n.d. “Inquiry into the Case of W. J. C. Vassall, a Clerical Officer in the Admiralty, Who Had Been Recruited by the Russian Intelligence Services and Related Matters (Radcliffe Tribunal), 1962-1963.” Catalogue description for CAB 301/265. Accessed November 16, 2026. https://www.nationalarchives.gov.uk/cabinet-office-files-cab/.

National Archives and Records Administration. 1945. “Report of the Special Interrogation of Frau Hildegarde Beetz, July 7, 1945.” Records of the Office of Strategic Services, Record Group 226, Entry 214. https://www.archives.gov/iwg/declassified-records/rg-226-oss/entry-214.html.

National Archives and Records Administration. 2013. “The Story Behind the Series Title ‘Ciano Papers: Rose Garden.’” *The Text Message*, April 15, 2013. https://text-message.blogs.archives.gov/2013/04/15/the-story-behind-the-series-title-ciano-papers-rose-garden/.

National Archives and Records Administration. 2016. “Papers of Count Galeazzo Ciano.” *Prologue: Pieces of History*, September 21, 2016. https://prologue.blogs.archives.gov/2016/09/21/papers-of-count-galeazzo-ciano/.

National Archives (United Kingdom). n.d. “John Vassall: Victim, Spy, Traitor, Prisoner.” Accessed November 16, 2026. https://www.nationalarchives.gov.uk/whats-on/events/john-vassall-victim-spy-traitor-prisoner/.

The National Archives (United Kingdom). n.d. “Olga Gray and the Woolwich Arsenal Spy Ring.” Accessed November 16, 2026. https://www.nationalarchives.gov.uk/explore-the-collection/stories/olga-gray-and-the-woolwich-arsenal-spy-ring/.

The National Archives (United Kingdom). 1915. “1915 Espionage Charges: R. Rowland and Mrs. L. E. Wertheim.” WO 141/3/1. Catalogue reference.

National Investigation Agency. 2024. “Ex-Army Man Convicted & Sentenced to RI by NIA Lucknow Court in Pak Espionage Case.” August 28, 2024. https://nia.mha.gov.in/sites/default/files/Document/1798_1_PR28082024.pdf.

National Portrait Gallery. n.d. “Secrets and Spies: SOE Women during the Second World War.” Accessed November 16, 2026. https://www.npg.org.uk/collections/reframing-narratives-women-in-portraiture/female-focus-page/secrets-and-spies-soe-women-ww2.

National Security Council. 1986. “Espionage Case at Embassy Moscow.” Paper prepared in the National Security Council, December 31, 1986. In *Foreign Relations of the United States, 1981-1988, Volume VI, Soviet Union, October 1986-January 1989*, document 10. Office of the Historian, U.S. Department of State. https://history.state.gov/historicaldocuments/frus1981-88v06/d10.

National Security Council Staff. 1987. “Memorandum From Barry Kelly of the National Security Council Staff to the President’s Assistant for National Security Affairs (Carlucci), March 24, 1987: Follow-up to Lonetree Espionage Case.” Includes the attached January 15, 1987 assessment by David Major. In Foreign Relations of the United States, 1981-1988, Volume VI, Soviet Union, October 1986-January 1989, document 28. Office of the Historian, U.S. Department of State. https://history.state.gov/historicaldocuments/frus1981-88v06/d28.

NATO Archives. 1963. “Report from the National Security Authority on the Breach of Security to NATO Information Resulting from the Vassall Case.” AC/35-D/521, December 18, 1963. https://archives.nato.int/report-from-the-national-security-authority-on-the-breach-ofsecurity-to-nato-information-resulting-from-the-vassall-case.

NATO Archives. 1964. “The Breach of Security to NATO Information Resulting from the Vassall Case.” AC/35-D/529, January 10, 1964. https://archives.nato.int/the-breach-of-security-to-nato-information-resulting-from-the-vassall-case.

Neequaye, David A., and Pär Anders Granhag. 2024. “Using Shared Experiences to Recruit Committed Human Intelligence Sources: Exploring the Shared Attention Mechanism and the Role of Social Connection.” *Legal and Criminological Psychology* 29 (1): 48-64. https://doi.org/10.1111/lcrp.12251.

Nelson, Samantha. 2025. “‘I Sente a Woman … Beecause a Man Shoulde Have Beene Suspected’: Tudor Women and Military Intelligence (c.1509-1603).” *Intelligence and National Security* 40 (4): 648-669. https://doi.org/10.1080/02684527.2025.2506280.

Peake, Hayden B. 2022. “A Spy Called Cynthia: And a Life in Intelligence.” *Studies in Intelligence* 66 (3), Intelligence Officer’s Bookshelf. https://www.cia.gov/resources/csi/static/StudiesUnclassifiedExtracts-Vol66-No-3-Sep-2022.pdf.

Pető, Andrea. 2020. “A Gender History of Hungarian Intelligence Services during the Cold War.” *Journal of Intelligence History* 19 (2): 197-212. https://doi.org/10.1080/16161262.2020.1774231.

Plutarch. *Life of Alexander*. 48.4-49.1. In *Plutarch’s Lives*, translated by Bernadotte Perrin. Loeb Classical Library. Cambridge, MA: Harvard University Press, 1919.

Poynting, Sarah. 2006. “Deciphering the King: Charles I’s Letters to Jane Whorwood.” *The Seventeenth Century* 21 (1): 128-140. https://doi.org/10.1080/0268117X.2006.10555570.

Proctor, Tammy M. 2003. *Female Intelligence: Women and Espionage in the First World War*. New York: New York University Press.

Radcliffe Tribunal. 1963. Report of the Tribunal Appointed to Inquire into the Vassall Case and Related Matters. April. Cmnd. 2009. London: Her Majesty’s Stationery Office.

Ray, Alana, and Nicola Henry. 2025. “Sextortion: A Scoping Review.” *Trauma, Violence, & Abuse* 26 (1): 138-155. https://doi.org/10.1177/15248380241277271.

Reis, Harry T., and Phillip Shaver. 1988. “Intimacy as an Interpersonal Process.” In *Handbook of Personal Relationships: Theory, Research and Interventions*, edited by Steve Duck, 367-389. Chichester: Wiley.

Reuters. 2026a. “Alice Huang, Chinese Businesswoman Tied to Nvidia CEO Jensen Huang, Went from Finance to Chips.” November 10, 2026. https://www.investing.com/news/stock-market-news/alice-huang-chinese-businesswoman-tied-to-nvidia-ceo-jensen-huang-went-from-finance-to-chips-5014096.

Reuters. 2026b. “Ex-Nvidia CEO Misled Top Lawyer on Affair with Chinese Businesswoman, Sources Say.” November 14, 2026. https://www.reuters.com/world/china/ex-nvidia-ceo-misled-top-lawyer-affair-with-chinese-businesswoman-sources-say-2026-11-14/.

Reuters. 2026c. “Key Republicans Seek Briefing from Nvidia CEO over Chinese Spy Allegations.” November 5, 2026. https://www.investing.com/news/stock-market-news/key-republicans-seek-briefing-from-nvidia-ceo-over-chinese-spy-allegationsdocument-5005367.

Reuters. 2026d. “Nvidia CEO’s Affair with Alleged Spy Aided $7.5 Billion in China Chip Shipments, The Information Reports.” November 10, 2026. https://www.reuters.com/world/china/nvidia-ceos-affair-aided-75-billion-chip-shipments-china-information-reports-2026-11-10/.

Reuters. 2026e. “Nvidia Faces Extraordinary Push to Restore Huang Days After His Exit.” November 16, 2026. https://www.reuters.com/legal/transactional/silicon-valley-leaders-back-call-jensen-huangs-return-nvidia-2026-11-16/.

Reuters. 2026f. “Singapore, US Agree to Keep Discussing Megaspeed as Scrutiny of Nvidia Scandal Widens.” November 16, 2026. https://www.reuters.com/world/asia-pacific/singapore-us-agree-keep-discussing-megaspeed-scrutiny-nvidia-scandal-widens-2026-11-16/.

Reuters. 2026g. “U.S. Justice Department Has Not Concluded Alice Huang Was Chinese Spy, Blanche Says.” November 12, 2026. https://www.reuters.com/world/china/us-justice-department-has-not-concluded-alice-huang-was-chinese-spy-blanche-says-2026-11-12/.

Reuters. 2026h. “US Releases Details of Megaspeed Probe, Says Investigation Began in 2024.”

November 17, 2026. https://www.reuters.com/world/asia-pacific/us-releases-details-of-

megaspeed-probe-says-investigation-began-2024-2026-11-17/.

Reuters. 2026i. “What We Know About Chinese Businesswoman Alice Huang.” November 14, 2026. https://www.investing.com/news/stock-market-news/what-we-know-about-chinese-businesswoman-alice-huang-5026865.

Roldugina, Irina. 2025. “The Cold War and the Soviet KGB’s Same-Sex Entrapment Operations in the 1950s and 1960s: The Perpetrator in Focus.” *Journal of Cold War Studies* 27 (4): 106-135. https://doi.org/10.1162/JCWS.a.1296.

Rushton, Joshua. 2021. Review of *Venice’s Secret Service: Organizing Intelligence in the Renaissance*, by Ioanna Iordanou. *Journal of Intelligence History* 20 (2): 244-246.

Russell, Frank Santi. 2000. *Information Gathering in Classical Greece*. Ann Arbor: University of Michigan Press. https://doi.org/10.3998/mpub.23087.

Salter, Michael, and Lorie Charlesworth. 2006. “Ribbentrop and the Ciano Diaries at the Nuremberg Trial.” *Journal of International Criminal Justice* 4 (1): 103-127. https://doi.org/10.1093/jicj/mqi095.

Satendra Siwal v. State of Uttar Pradesh, Matters Under Article 227 No. 4289 of 2026 (Allahabad High Court, Lucknow Bench, August 13, 2026). https://indiankanoon.org/doc/78479484/.

Senato della Repubblica. 1997. “Risposte scritte ad interrogazioni: risposta all’interrogazione 4-04520 sulla vicenda Mordechai Vanunu.” XIII Legislatura, July 23, 1997. https://www.parlamento.it/service/PDF/PDFServer/DF/17753.pdf.

Service historique de la Défense. n.d. “Mata Hari.” Ministère des Armées. Accessed November 16, 2026. https://www.servicehistorique.sga.defense.gouv.fr/liste-dossiers-individuels/mata-hari and https://www.servicehistorique.sga.defense.gouv.fr/en/node/373974.

Singapore Ministry of Home Affairs. 2026a. “Clarification Statement on Wall Street Journal’s Article.” October 31, 2026. https://www.mha.gov.sg/media-room/newsroom/clarification-statement-on-wall-street-journals-article/.

Singapore Ministry of Home Affairs. 2026b. “Singapore’s Investigations into Alice Huang (Huang Le) and Megaspeed International Pte Ltd.” November 12, 2026. https://www.mha.gov.sg/media-room/newsroom/singapore-investigations-into-alice-huang-huang-le-and-megaspeed-international-pte-ltd/.

Slepian, Michael L., Jinseok S. Chun, and Malia F. Mason. 2017. “The Experience of Secrecy.” *Journal of Personality and Social Psychology* 113 (1): 1-33. https://doi.org/10.1037/pspa0000085.

Smith, V. 2024. *Diplomatic Counsel and the Shaping of Anglo-Scottish Relations (1558-69): The British Perspectives of Nicholas Throckmorton and Thomas Randolph*. PhD thesis, University of Oxford. https://doi.org/10.5287/ora-j0darzxzb.

Stasi Records Archive. n.d. “Agenten,” keyword “Romeo.” *Stasi Media Library*. Accessed November 16, 2026. https://www.stasi-mediathek.de/themen/schlagwort/Agenten/.

Stephenson, Elizabeth, and Susan Harris Rimmer. 2023. “Classified and Secret: Understanding the Literature on Diversity in the Intelligence Sector.” *International Studies Review* 25 (3): viad033. https://doi.org/10.1093/isr/viad033.

Tayler, Alistair, and Henrietta Tayler. 1933. “The Ogilvies of Boyne.” Transactions of the Banffshire Field Club. https://banffshirefieldclub.org.uk/PDFs/BOOK_12/Banffshire_Field_Club_Transactions_1931-1934_-_1933_The_Ogilvies_of_Boyne_WM.pdf.

The Times of Israel. 2015. “Nuclear Secret-Spiller Vanunu Recalls His Capture.” May 2015. https://www.timesofisrael.com/liveblog_entry/nuclear-secret-spiller-vanunu-recalls-his-capture/.

The Times of Israel. 2020. “Jonathan Pollard Arrives in Israel, 35 Years after His Arrest for Spying.” December 30, 2020. https://www.timesofisrael.com/jonathan-pollard-arrives-in-israel-35-years-after-his-imprisonment-for-spying.

The Times. 2026. “Trump convinced Nvidia to reinstate Jensen Huang as CEO.” https://www.thetimes.com/business/companies-markets/article/jensen-huang-ceo-nvidia-reinstated-latest-news-zrr6jhqvm.

The Wall Street Journal. 2026a. “Trump Talked With Nvidia Board About Reinstating Jensen Huang.” https://www.wsj.com/livecoverage/stock-market-today-dow-sp-500-nasdaq-11-23-2026/card/trump-talked-with-nvidia-board-about-reinstating-jensen-huang-M37xHvHGISNB1FlhUH7j.

The Wall Street Journal. 2026b. “The Campaign to Bring Back Jensen Huang as Nvidia CEO.” https://www.wsj.com/tech/the-campaign-to-bring-back-jensen-huang-as-nvidia-ceo-e91b0b2c.

The Wall Street Journal. 2026c. “Trump Held Up to $83 Million in Nvidia Stock Before Price Dropped.” https://www.wsj.com/livecoverage/stock-market-today-dow-sp-500-nasdaq-11-16-2026/card/trump-held-up-to-83-million-in-nvidia-stock-before-price-dropped-48Y94LwIforpngbqUaoV.

Todd, Lisa. 2011. “The Soldier’s Wife Who Ran Away with the Russian: Sexual Infidelities in World War I Germany.” *Central European History* 44 (2): 257-278. https://doi.org/10.1017/S0008938911000033.

Toy, Rosemary Florence, and Christopher Smith. 2018. “Women in the Shadow War: Gender, Class and MI5 in the Second World War.” *Women’s History Review* 27 (5): 688-706. https://doi.org/10.1080/09612025.2017.1345714.

U.S. Senate Committee on Banking, Housing, and Urban Affairs. 2026. “Senator Warren Statement on Jensen Huang Reinstatement as NVIDIA CEO.” https://www.banking.senate.gov/newsroom/minority/senator-warren-statement-on-jensen-huang-reinstatement-as-nvidia-ceo.

UK Parliament. n.d. “Lord Denning’s Report into the Profumo Affair.” https://www.parliament.uk/about/living-heritage/transformingsociety/private-lives/relationships/collections1/parliament-and-the-1960s/lord-dennings-report---profumo-scandal/.

UK Parliament. 2017. “The Sexual Offences (Pardons Etc.) Bill 2016-17.” House of Commons Library Briefing Paper CBP-7741. https://researchbriefings.files.parliament.uk/documents/CBP-7741/CBP-7741.pdf.

United Kingdom. 2025. *Data (Use and Access) Act 2025*, c. 18, section 138. https://www.legislation.gov.uk/ukpga/2025/18/section/138.

United Kingdom. 2026. *Crime and Policing Act 2026*, c. 20, sections 99-101. https://www.legislation.gov.uk/ukpga/2026/20/part/5/chapter/4.

United States Air Force Office of Special Investigations. 2025. “Civilian Sentenced 5 Years Following Classified Information Leak.” October 8, 2025. https://www.osi.af.mil/News/Article-Display/Article/4341325/civilian-sentenced-5-years-following-classified-information-leak/.

United States Congress. 2025. *TAKE IT DOWN Act*, Public Law 119-12, 139 Stat. 55. May 19, 2025. https://www.congress.gov/119/plaws/publ12/PLAW-119publ12.pdf.

United States Department of Defense. 2015. Department of Defense Instruction 3305.15, "DoD Human Intelligence (HUMINT) Training and Certification." August 13, 2015, incorporating Change 2, effective August 25, 2020. https://dodcertpmo.defense.gov/Portals/62/330515p.pdf.

United States Department of Justice. 2024. "Air Force Employee Indicted for Unlawful Disclosure of Classified National Defense Information." March 4, 2024. https://www.justice.gov/usao-ne/pr/air-force-employee-indicted-unlawful-disclosure-classified-national-defense-information.

United States Department of Justice. 2025. "Air Force Employee Pleads Guilty to Conspiracy to Disclose Unlawfully Classified National Defense Information." July 10, 2025. https://www.justice.gov/opa/pr/air-force-employee-pleads-guilty-conspiracy-disclose-unlawfully-classified-national-defense.

United States v. Lonetree. 1990. 31 M.J. 849 (U.S. Navy-Marine Corps Court of Military Review); 1992. 35 M.J. 396 (U.S. Court of Military Appeals). https://openjurist.org/35/mj/396/united-states-v-lonetree.

United States v. Pollard. 1992. 959 F.2d 1011 (D.C. Cir.). https://law.justia.com/cases/federal/appellate-courts/F2/959/1011/220032/.

UPI. 1986. "Former Official Convicted in Strange Espionage-Sex Case." May 6, 1986. https://www.upi.com/Archives/1986/05/06/Former-official-convicted-in-strange-espionage-sex-case/2183515736000/.

UPI. 1999. "Sex and Sleaze Scandal Shakes Russia." March 18, 1999. https://www.upi.com/Archives/1999/03/18/UPI-Focus-Sex-and-sleaze-scandal-shakes-Russia/7690921733200/.

U.S. Army. 1945. "Interrogation of Frau Hildegard Beetz." June 14, 1945. Central Intelligence Agency Reading Room, released June 14, 1945. https://www.cia.gov/readingroom/docs/BEETZ%2C%20HILDEGARD%20%20%20VOL.%201_0061.pdf.

U.S. House Committees. 2026a. Letter to Jensen Huang requesting a closed-door briefing, November 4. House Select Committee on the Chinese Communist Party.

U.S. House Committees. 2026b. Letters requesting closed-door, transcribed interviews with Jensen Huang, Tim Teter, and Jeffrey Kessler. November 12. House Committee on Foreign Affairs. https://foreignaffairs.house.gov/news/press-releases/chairmen-mast-moolenaar-and-crawford-send-second-request-to-jensen-huang-and-nvidia-to-brief-congress-on-the-chinese-intelligence-asset.

U.S. Office of the Director of National Intelligence. 2009. *Counterintelligence Reader, Volume III: CI in the Turbulent 1960s and 1970s*. https://www.dni.gov/files/NCSC/documents/ci/CI_Reader_Vol3.pdf.

U.S. Senate. 1970. "Testimony of George Karlin (Yuriy Krotkov)." Hearings before the Subcommittee to Investigate the Administration of the Internal Security Act and Other Internal Security Laws, 91st Congress, 1st Session, Parts 1-3. Washington, DC: U.S. Government Printing Office.

U.S. Senate Committee on Foreign Relations. 2018. *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*. 115th Congress, 2nd session. Washington, DC: U.S. Government Publishing Office. https://www.govinfo.gov/content/pkg/CPRT-115SPRT28110/pdf/CPRT-115SPRT28110.pdf.

The Virginian-Pilot. 1996. "The Story Behind the Scandal at the U.S. Embassy in Moscow." June 23, 1996. https://scholar.lib.vt.edu/VA-news/VA-Pilot/issues/1996/vp960623/06210719.htm.

The Washington Post. 1985a. "CIA Aide, Ghanaian Face Spy Counts." July 12, 1985. https://www.washingtonpost.com/archive/politics/1985/07/12/cia-aide-ghanaian-face-spy-counts/.

The Washington Post. 1985b. "Ex-Clerk Pleads Guilty to Leaking Data in Ghana." September 28, 1985. https://www.washingtonpost.com/archive/local/1985/09/28/ex-clerk-pleads-guilty-to-leaking-data-in-ghana/31562b96-1c17-4998-82a1-e86fed941111/.

The Washington Post. 1985c. "Ghana Expels 8 in Trade of Spy Suspects." November 27, 1985. https://www.washingtonpost.com/archive/politics/1985/11/27/ghana-expels-8-in-trade-of-spy-suspects/ac024449-d914-4b43-ab85-790dafd7c3a4/.

The Washington Post. 1985d. "Routine Polygraph Opened Ghanaian Espionage Probe." July 13, 1985. https://www.washingtonpost.com/archive/politics/1985/07/13/routine-polygraph-opened-ghanaian-espionage-probe/.

The Washington Post. 1985e. "Scranage Dated Ghanaian after Order, FBI Says." July 20, 1985. https://www.washingtonpost.com/archive/politics/1985/07/20/scranage-dated-ghanaian-after-order-fbi-says/53634da2-ee2e-4151-8ebc-55566ca08ee0/.

The Washington Post. 1985f. "U.S., Ghana Trade Spy Suspects." November 26, 1985. https://www.washingtonpost.com/archive/politics/1985/11/26/us-ghana-trade-spy-suspects/d708d1bd-c257-45ee-853e-880de7425270/.

The Washington Post. 1986a. "Term Cut in Ghana Spy Case." April 10, 1986. https://www.washingtonpost.com/archive/politics/1986/04/10/term-cut-in-ghana-spy-case/fb0049eb-f5dd-4b11-ab94-be5190139cd8/.

The Washington Post. 1986b. "Treason Suspect in Israel Flashes Message on Kidnaping." December 23, 1986. https://www.washingtonpost.com/archive/politics/1986/12/23/treason-suspect-in-israel-flashes-message-on-kidnaping/6f45e059-ba5a-4316-8ac1-59d4e5c9fd1c/.

The Washington Post. 1987. "Lonetree Sentenced to 30 Years." August 25, 1987. https://www.washingtonpost.com/archive/politics/1987/08/25/lonetree-sentenced-to-30-years/98ae4456-5bd3-42a4-b41c-d5e0e8707feb/.

The Washington Post. 1988. "Lonetree's Prison Sentence Reduced by Five Years." May 21, 1988. https://www.washingtonpost.com/archive/politics/1988/05/21/lonetrees-prison-sentence-reduced-by-five-years/3bfa6f53-ef75-4a06-95c3-e776a1e03e33/.

The Washington Post. 1999. "Yeltsin Fires His Chief of Staff." March 20, 1999. https://www.washingtonpost.com/archive/politics/1999/03/20/yeltsin-fires-his-chief-of-staff/edd26fed-a476-42df-bb07-553a595f8500/.

The Washington Post. 2017. "By Chance, Meeting the Disgraced 'M. Butterfly' Diplomat Whose Lover Misled Him." August 11, 2017. https://www.washingtonpost.com/entertainment/theater_dance/by-chance-meeting-the-disgraced-m-butterfly-diplomat-whose-lover-misled-him/2017/08/11/7fb44744-77c1-11e7-9eac-d56bd5568db8_story.html.

The Washington Post. 2020. "Parole Ended for Jonathan Pollard, Who Spied for Israel, Freeing Him to Leave the United States." November 20, 2020. https://www.washingtonpost.com/national-

security/parole-ended-for-jonathan-pollard/2020/11/20/6b5e24a8-2b74-11eb-9b14-ad872157ebc9_story.html.

Weil, Rachel. 2020. Review of Invisible Agents: Women and Espionage in Seventeenth-Century Britain, by Nadine Akkerman. American Historical Review 125 (1): 302-303. https://doi.org/10.1093/ahr/rhz745.

Weinberger, Caspar W. 1987. "Declaration of the Secretary of Defense." January 7, 1987. Declassified affidavit concerning Jonathan Pollard's disclosures, National Security Archive. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB407/docs/A-Pollard7c.pdf.

Wheelwright, Julie. 2016. "The Language of Espionage: Mata Hari and the Creation of the Spy-Courtesan." In *Languages and the First World War: Representation and Memory*, edited by Christophe Declercq and Julian Walker, 164-177. London: Palgrave Macmillan. https://doi.org/10.1057/9781137550361_11.

Wheelwright, Julie. 2025. "Doctor, Dancer, Drug Addict? Interwar Spy Writers and the Literary Construction of Germany's Female Intelligence Operatives." *Intelligence and National Security* 40 (4): 670-686. https://doi.org/10.1080/02684527.2025.2506281.

White House Government Transparency Task Force. 2026a. "FBI Case File 56D-SF-4662117: Eric Swalwell and Christine Fang." Declassified August 17, 2026. Redacted FBI file released through the White House Transparency Task Force; copy hosted by Just the News. https://justthenews.com/sites/default/files/2026-08/FBI%2056D-SF-4662117%20Packet%20-%20FINAL%20-%20REDACTED%208.14.26.pdf.

White House Government Transparency Task Force. 2026b. "Rusty Thumbs: Codename for the FBI's Christine Fang File." Declassified FBI materials, August 2026. https://www.whitehouse.gov/transparency/.

Whitty, Monica T., and Tom Buchanan. 2016. "The Online Dating Romance Scam: The Psychological Impact on Victims, Both Financial and Non-Financial." *Criminology & Criminal Justice* 16 (2): 176-194. https://doi.org/10.1177/1748895815603773.

Wilder, Ursula M. 2017. "Why Spy Now? The Psychology of Espionage and Leaking in the Digital Age." *Studies in Intelligence* 61 (2), extracts (June): 1-36. Central Intelligence Agency, Center for the Study of Intelligence. https://www.cia.gov/resources/csi/static/Psych-of-Leaking-Espionage.pdf.

Willems, Yayouk E., Catrin Finkenauer, and Peter Kerkhof. 2020. "The Role of Disclosure in Relationships." *Current Opinion in Psychology* 31: 33-37. https://doi.org/10.1016/j.copsyc.2019.07.032.

Zhang, Amanda. 2021. *Loyalty, Secrecy and Revolutionary Work: Female Underground Operatives and Narratives about Chinese Female Spies before and after 1949*. DPhil thesis, University of Oxford.

Zhang, Amanda. 2023. "Engendered Perceptions: Reconsidering Wartime Female Tewu (Special Agent) Activities and Narratives of 'Honey Traps' in the Early People's Republic of China, 1949-1959." *Journal of Chinese Military History* 12 (2): 188-216. https://doi.org/10.1163/22127453-bja10019.