KEEPING IT SECRET: SURVEILLANCE, INFORMANT NETWORKS, AND THE PROTECTION OF INFORMANTS IN AUTHORITARIAN REGIMES

HOWARD LIU, CHING-HSUAN SU, AND YI-TING WANG

Abstract. Authoritarian regimes rely heavily on informant networks to infiltrate and surveil dissident organizations. While the role of informants in state repression is well-documented, existing research often overlooks how secret police use the intelligence gathered from informants without compromising their identities. In this article, we examine the conditions under which secret police agencies seek to protect informants from exposure. We argue that agencies face a tradeoff between the risks of exposing informants and the costs of implementing protection, often prioritizing protection for informants who are deeply embedded in dissident networks and provide rare, high-value intelligence. Using declassified surveillance reports from 1970s Taiwan, we find that protection is most likely when informants are close to well-connected dissidents, interact with behind-the-scenes activists, or provide sensitive information about internal conflicts. Deeply embedded informants offer high-value intelligence but face greater risks of exposure, making them especially worth protecting. These findings contribute to research on surveillance and repression by showing how secret police manage the risks of informant exposure while leveraging human intelligence to counter dissent.

Keywords: surveillance, infiltration, informant networks, secret police, repression, authoritarian politics

(Howard Liu) University of South Carolina
(Ching-Hsuan Su) National Pingtung University, Taiwan
(Yi-Ting Wang) National Cheng Kung University, Taiwan

Authoritarian regimes maintain their rule through an intricate web of surveillance, often orchestrated by security agencies–especially secret police agencies–that recruit ordinary citizens as informants and spies. These agencies play a central role in gathering intelligence: they rely on recruited informants to secretly monitor society, identify dissidents, and supply information that facilitates repression and fosters an atmosphere of fear (Dragu and Przeworski, 2019; Greitens, 2016; Scharpf and Gläßel, 2020). These surveillance practices are commonly categorized as infiltration, a nonviolent and covert tactic in which agents and informants are embedded within society to secure compliance, operating as part of a broader repertoire of authoritarian control (Hassan et al., 2022). The scale of infiltration carried out by secret police is often striking. In East Germany, for example, declassified Stasi records reveal that, before the regime's collapse, approximately 200,000 informants–one for every 100 citizens–were actively engaged in surveillance (Müller-Enbergs, 2008). Similarly, in communist Poland during the 1980s, archival evidence suggests that up to 200,000 individuals collaborated with secret services at some point, amounting to roughly one informant for every 200 citizens. This extensive network of informants not only allowed regimes to infiltrate society but also created a chilling effect, ensuring that resistance to the ruling power was both rare and perilous.

Surveillance has drawn growing attention in political research. Over the past decade, scholars have explored a range of surveillance practices, from physical surveillance (Hager and krakowski, 2022; Choulis et al., 2024; Nalepa and Pop-Eleches, 2022) to digital monitoring (Gohdes, 2020; Chau et al., 2024). A central argument in this literature is that surveillance helps resolve the classic *information problem*: the challenge regimes face in identifying dissent and monitoring opposition when they lack reliable intelligence to enable targeted repression (Xu, 2021; Liu and Sullivan, 2021). While this scholarship has advanced our understanding of surveillance as a tool of authoritarian rule, it tends to overlook a fundamental dilemma faced by the secret police: how can they act on the intelligence gathered from informants without compromising their identities? Acting on insider tips often endangers the identity of the source, especially when repression follows highly specific information known only to a

few individuals. This tension between the utility of intelligence and the need to protect its origin remains undertheorized and empirically unexamined.

In this article, we offer an early contribution to the study of informant protection in authoritarian surveillance by examining the conditions under which certain informants are prioritized for protection. We argue that secret police agencies have strong incentives to implement protective measures such as delaying repressive actions or limiting cross-checks between sources, in order to avoid exposing their informants when acting on the intelligence. These precautions, however, come at a cost. Delays may give dissidents time to escape or relocate, while limiting verification of intelligence increases the likelihood of governments acting on false or misleading information. To navigate this tradeoff, secret police tend not to protect all informants equally. Instead, they prioritize safeguarding those who provide access to otherwise inaccessible, high-value intelligence. Protection is thus selective, often concentrated on informants who are deeply embedded within dissident networks. Deep penetration enhances the strategic utility of intelligence, but it also increases the risk of informants' exposure when their intelligence is utilized. Deeply embedded informants–those close to *well-connected dissidents*, linked to *behind-the-scenes activists*, or aware of *internal conflicts*–are especially valuable and warrant special protection. Carefully handling the intelligence they provide helps ensure the continued flow of critical information while minimizing the chance of compromising these vital assets.

We test these expectations using recently declassified surveillance archives documenting the monitoring of Taiwan's prominent opposition activists during its authoritarian period (1949–1990). These official reports from secret police agencies offer a unique opportunity to examine the inner workings of a surveillance apparatus, including informants' social connections, the content of their intelligence, and the corresponding actions taken by security agents. The data capture the peak of surveillance activities in the late 1970s when Taiwan's authoritarian government operated an extensive surveillance network of over 83,000 informants nationwide, generating 190,000–200,000 reports annually (Transitional Justice Commission, 2022, p. 428). This pervasive surveillance infiltrated nearly every sector of society, including

universities, churches, neighborhoods, media, and professional associations, fostering an environment where people believed that "informants were right beside you." For this study, we digitized and coded a detailed surveillance file on one of Taiwan's most prominent opposition activists from the 1970s, during the height of the regime's surveillance operations. Our analysis sheds light on the often-hidden processes by which secret police agencies assess, screen, and protect their informants within the surveillance network. Our work provides important insights into the mechanisms of authoritarian control, offering a much-needed understanding of how repressive regimes maintain power through surveillance and strategic intelligence management.

Surveillance, Dissident Infiltration, and Informant Protection

Information is a vital resource for authoritarian regimes, enabling them to identify enemies, uncover subversive activities, and preemptively suppress dissent to maintain political control. Yet in autocracies, where dissent is repressed and open communication is restricted, reliable intelligence is inherently scarce (Geddes et al., 2018). This scarcity poses a challenge to the regime, as dissident groups often operate clandestinely to evade detection. To overcome this obstacle, regimes often rely on their surveillance networks, which typically include both formal secret police agencies and informal networks of recruited informants (Piotrowska, 2020; Thomson, 2023; Steinert, 2023; Mehrl and Choulis, 2024; Liu and Peldon, 2025). Informants are particularly valuable for intelligence gathering because they offer unique advantages that external secret police often lack. Unlike state agents, who operate as outsiders and have a high risk of exposure when trying to infiltrate dissident networks, informants are ordinary citizens embedded within the social circles of dissidents. Their access to private conversations, closed gatherings, and informal networks allows them to gather insider intelligence with minimal suspicion. Moreover, their familiarity with the group's language, norms, and internal dynamics enhances their ability to accurately interpret political behavior and identify key actors for secret police to target. Because their role as regime collaborators is often

hidden even from their close associates, informants can sustain long-term surveillance from within, making them valuable assets for intelligence operations.

However, secret police often face an operational dilemma in handling the intelligence they gather: they must act on it to suppress dissent, but doing so can endanger the very sources that make such action possible. Acting on insider tips–particularly when it involves highly specific or sensitive details–can alert dissidents to the presence of informants within their ranks. Verification procedures, such as cross-checking reports with other internal sources, can also inadvertently expose access or reveal which individuals had the knowledge. Once dissent members begin to infer how the secret police acquired certain intelligence, they may change tactics, sever ties with suspected informants, restrict internal communication, or retaliate against perceived collaborators (Sullivan and Davenport, 2018). These defensive responses disrupt the flow of information and undermine the secret police's capacity to maintain surveillance. This challenge echoes what international relations scholars describe as the "disclosure dilemma" in secret intelligence operations: acting on intelligence may yield strategic benefits but risks revealing the underlying sources or methods (Carnegie and Carson, 2019). The stakes are particularly high with human informants. The better a source's access, the more difficult it becomes to use that intelligence without compromising the source's identity (Dylan and Maguire, 2022).

To keep intelligence sources secret, secret police often employ precautionary measures to protect the identities of informants and avoid backward tracing. That is, preventing dissidents from inferring who leaked sensitive information based on state actions. Anonymity is critical to the success of infiltration (Nalepa and Pop-Eleches, 2022). Once exposed, informants may face harm, social ostracism, or even death, and the regime can lose access to valuable intelligence permanently. Common precautionary measures include delayed state actions, such as waiting days or even weeks after receiving intelligence before intervening, to obscure the link between the tip and the response. Secret police can also limit cross-verification by avoiding the triangulation of reports across different informants, thereby

reducing the chance of backward tracing to the original informant. Additionally, they sometimes fabricate alternative narratives for how intelligence was acquired, such as citing intercepted communications or anonymous public tips, to mask the true origin. These measures help maintain informants' anonymity and preserve the regime's long-term capacity for covert surveillance and repression.

These precautionary measures, however, come at a cost. Delayed state actions give dissidents time to escape, relocate, or destroy evidence, making future repression more difficult and resource-intensive. Likewise, reducing cross-verification of intelligence makes it more likely for secret police to act on false or misleading information, leading to the repression of wrong, innocent individuals and missing actual targets. There is also an opportunity cost: time and resources spent pursuing false information could have been more effectively used if secret police agencies had first verified the information and acted on more reliable intelligence. These costs are far from negligible, especially when the regime aims to dismantle dissident networks and prevent mobilization in a timely and effective manner.

Implementing costly precautionary measures for every informant will significantly burden secret police agencies by slowing down state responses, weakening deterrence, straining interagency coordination, and increasing the likelihood of intelligence becoming outdated. To navigate this tradeoff, secret police typically do not treat all informants equally. Instead, they prioritize the protection of those informants who supply rare, high-value intelligence. Informants deeply embedded in dissident networks offer especially valuable intelligence, but their close proximity to key dissidents and sensitive information also makes them particularly vulnerable to exposure. The deeper the penetration, the more strategically useful—but also more traceable—the intelligence becomes (Su, 2020). As a result, protective measures tend to concentrate on informants who provide privileged access to otherwise unreachable information deep within dissident networks. In the following, we identify three key features that distinguish such informants: the connectivity of their sources, the type of sources they access, and the content of the intelligence their sources provide.[1]

[1]Informants and their sources (or what we term *informants' sources*) occupy distinct roles. Informants are individuals who collaborate with the secret police, whereas informants' sources are dissident actors

Connectivity of informants' sources. For clandestine dissident organizations, insider information is far more valuable to secret police than observations from external sources (Lyall et al., 2015). Individuals deeply embedded within dissident networks serve as especially valuable intelligence sources. As Piotrowska (2024) notes, the Stasi recognized that informants with close social ties to dissidents could access more meaningful and actionable intelligence than those without such connections. This is because dissident organizations often operate as tightly knit networks, where an individual's position shapes their access to sensitive information. Those who are *well-connected*—frequently interacting with and maintaining close ties to many activists—are often key figures within the movement and are more likely to possess high-value intelligence about opposition strategies, plans, and identities (Liu, 2022). In environments where public information is limited or censored, informants' interpersonal networks become crucial conduits for accessing high-value targets and intelligence.

However, these well-connected central figures are typically closely guarded within underground movements, making them difficult for regimes to reach. Access becomes more feasible when government informants are themselves deeply embedded in dissident circles, as trusted insiders are better positioned to interact with high-level actors who would otherwise remain inaccessible to external surveillance. Deep penetration of opposition networks thus becomes a necessary condition for collecting intelligence on the most valuable and well-guarded figures. Yet this access also increases risks: reporting on central dissidents raises the likelihood that others within the network can identify the leak. When repression closely follows the disclosure of sensitive information involving many network members, it creates more reference points for dissidents to triangulate who had access and, by extension, who informed. Based on this logic, we derive the following hypothesis regarding the connectivity of informants' sources and the secret police's tendency to protect their identities from exposure:

who do not cooperate with the regime but inadvertently share information with informants—often due to trust, deception, or negligence. Regimes have incentives to protect the identity of their informants, not the dissidents who unknowingly provide them with intelligence. Accordingly, our hypotheses focus on three features of informants' sources—connectivity, type, and information content—as proxies for the depth of an informant's embeddedness in dissident networks and the corresponding value of protecting them.

H1: Informant protection is more likely for those who have access to well-connected central activists than those who do not.

Type of informants' sources. In addition to connectivity, the type of informants' sources also matters. Dissidents within dissent organizations assume diverse roles, from high-profile leaders to behind-the-scenes operatives (Parkinson, 2013; Sullivan, 2016). Frontline dissidents often serve as the public face of opposition, participating in visible challenges to the regime and engaging in overt activities. For example, in autocracies permitting limited electoral competition, opposition candidates sometimes win elections (Gandhi and Lust-Okar, 2009), assuming prominent and highly visible roles of resistance. While intelligence about these figures is useful, their public nature makes their activities relatively easier for security agencies to monitor through public records, media coverage, or routine surveillance. Moreover, as obvious targets of regime scrutiny, high-profile dissidents are often highly aware of being watched, leading them to exercise caution in their actions and communications. This heightened vigilance reduces the likelihood that informants can obtain sensitive or novel intelligence from them.

In contrast, *behind-the-scenes activists* operate discreetly, sustaining dissent organizations through critical but less visible activities. These individuals coordinate finances, organize meetings, recruit members, facilitate communication, and manage logistics (Parkinson, 2013). Such clandestine efforts are indispensable for maintaining the networks that enable opposition groups to function effectively (Sullivan, 2016). Unlike high-profile figures, these actors–such as aides to elected politicians or logistical support staff–work in the shadows, with their identities and activities often hidden from public view. Their organizational roles grant them access to underground networks, informal interactions, and logistical structures that are difficult to detect through conventional surveillance or engagement with frontline leaders. Intelligence gathered from these behind-the-scenes actors is particularly valuable because it reveals operational details and support mechanisms critical to the survival of dissent groups. Such information enables the regime and its secret police to identify and

disrupt the logistical and financial infrastructure that sustains resistance, thereby weakening dissent movements. Informants who can access such covert actors often penetrate deeply into organizational cores. This level of embeddedness, however, also heightens their risk of exposure, as frequent interactions with key organizers increase the chances that dissidents may trace leaks back to them. Consequently, informants who interact with these covert actors not only provide intelligence of far greater strategic importance than those reporting on public figures, but also require protective measures due to their heightened exposure risk. Based on this reasoning, we propose the following hypothesis:

H2: Informant protection is more likely for those who have access to behind-the-scenes activists than those who do not.

Content of source's intelligence. The substantive content of information also plays a key role in determining an informant's importance. Reports on *internal conflicts*, such as negative interpersonal relations, disagreements, and criticisms among dissent members, represent critical information for the regime and its secret police. Regimes are acutely aware that a unified dissent poses a significant threat, and they frequently deploy strategies to divide the opposition groups, making them easier to suppress (Lust-Okar, 2004; Ong, 2022). Intelligence on internal conflicts allows the state to exploit personal frictions and deepen divisions, thereby weakening the cohesion of regime adversaries.

However, information on internal conflicts and negative relationships is inherently more difficult to obtain. Collaborative activities, such as recruitment or protests, typically involve broader participation, making them more observable and less sensitive to disclosure. In contrast, discussions of internal conflicts and criticisms tend to occur within trusted and private circles. Dissent members are acutely aware that revealing internal tensions can be exploited by the regime and are therefore cautious about sharing such information. These conversations are often confined to close-knit groups, making them less accessible through routine surveillance. It requires informants to be deeply embedded within dissidents' inner networks, close enough to be trusted with sensitive and potentially damaging information.

Informants who report on negative interactions thus provide rare and valuable intelligence into the internal dynamics and weaknesses of opposition groups–details that are otherwise difficult to uncover. Because of the strategic value and the risks involved, these informants are especially likely to warrant special protection. Based on this logic, we propose the following hypothesis:

H3: Informant protection is more likely for those who can inform internal conflicts within dissident networks than those who cannot.

Data, Measures, and Models

We evaluate our theoretical expectations using declassified archives on state surveillance in a highly repressive regime. Taiwan's authoritarian period, spanning 1949–1990, was characterized by a regime seeking to maintain control over its remaining territory after a failed civil war against Mao's Communist Party. This context provides a rare and valuable opportunity to study how regimes and their security apparatus leverage repression and mass surveillance to constrain dissent. In the late 1970s, increasing mobilization and dissent from opposition groups challenged the regime. Despite the prohibition on establishing opposition parties, dissidents managed to participate and compete in local elections, although very few legislative seats were open and the process was marred by widespread fraud. The ruling Kuomintang party (KMT) maintained strict authoritarian control, and by the late 1970s, its monitoring and informant networks had become highly developed and operationally mature. According to the Taiwanese Transitional Justice Commission's report, by the 1980s, the government had established an intelligence network of more than 83,000 informants nationwide to monitor potential dissidents and their networks.[2] The massive surveillance network and an influx of information compelled security agencies to prune their informant network to enhance intelligence quality. These features provide an ideal context for us to test our hypotheses.

[2]This figure only includes informants recruited by the Investigation Bureau. Additional informants were recruited by agencies like the Garrison Command and National Security Bureau, suggesting a higher actual number.

Our analysis focuses on 230 surveillance reports targeting a key opposition figure Chen Chu (陳菊) from 1977–1979, produced under a surveillance project, the Project Chinggu (青谷專案), dedicated to monitoring Chen during the height of opposition movements in the late 1970s.[3] Each report documents intelligence gathered by typically an informant and reported by a secret police officer, all under aliases. The reports include detailed information on the reported time, location, content, and review comments from the officer, which indicate their assessments and reactions to the intelligence provided.[4]

Dependent variable. We measure our dependent variable, *Informant protection request*, based on review comments attached to each surveillance report. Security agencies sometimes recommend caution when acting on intelligence to avoid exposing the identity of their informant. This can include delaying arrests or deferring the use of specific information to prevent backward tracing. Specifically, our dependent variable captures whether a secret police officer requested that the intelligence be handled carefully to protect the identity of the informant who provided it and avoid their exposure.[5] We treat reports as the unit of analysis because each surveillance report is typically linked to a single informant. This ensures that any protection request corresponds to one informant in one report, avoiding concerns that a single request could apply to multiple informants within the same report.[6] We code this variable as 1 if such a request is made, and 0 otherwise.

Explanatory variables. For the first hypothesis, we measure the informant's ability to gain access to well-connected activists. To define connectivity, we first identify informant's sources

[3]We obtained these surveillance reports from Taiwan's *National Human Rights Museum* through our research collaboration with the Museum. The full corpus of surveillance reports is available at Taiwan's National Archives.

[4]More details about the context of the case and the surveillance reports are included in Appendix Section 1.

[5]For example, in one surveillance report, it is noted that we "request that superiors exercise caution and ensure the confidentiality of both the origin and the content when handling this intelligence, in order to avoid exposing our 'inside informant.'" (要求上級處理本情報時，宜請注意來源及內容保密，避免暴露「內線」). See the original report in Appendix Figure A.2.

[6]Unfortunately, many informants' names are redacted in the declassified documents or replaced with generic labels such as "informant", "operations personnel", or "internal associate." This limits our ability to uniquely identify individual informants and to test or control for informant-level effects on the likelihood of protection requests.

and then build the source's social network. Each informant in each report specifies the individuals who provided the underlying intelligence, allowing us to identify these source individuals by systematically reviewing the content of the reports. Next, we construct the source's social networks, with ties between nodes (activists) established based on documented interactions such as meetings, joint activities, or communications described in the reports. The networks are constructed in two ways to address simultaneity concerns: (1) using all reports available up to $t-1$ of each surveillance report and (2) using reports from the previous month. Lastly, we measure the connectivity of these information sources. The variable, *Centrality of the sources*, was created by calculating their eigenvector centrality. Eigenvector centrality assigns greater importance to nodes that are connected to other highly connected nodes, providing a useful measure of an information source's influence and connectedness within the network.[7] Since some reports reference multiple informants' sources, we use both the mean and maximum eigenvector centrality of all sources mentioned in a report in the analysis. Figure 1 shows two sample informant's source networks in surveillance reports.

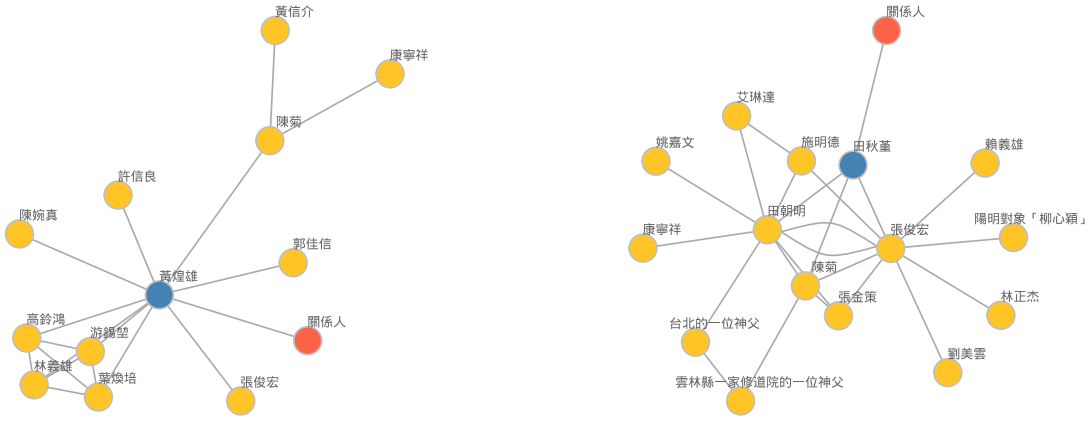

Figure 1. Dissident networks in two surveillance reports

Note: The red nodes represent *informants*, the blue nodes represent the *informants' sources*, and the yellow nodes represent *activists* within the network. A tie between two nodes indicates evidence of interaction, such as meetings, joint activities, or communication, as documented in the surveillance reports.

For the second hypothesis, we measure the informant's ability to gain access to behind-the-scenes activists. To code this type of behind-the-scenes sources, we collected memoirs and

[7]Appendix Table A.6 shows consistent results using degree centrality of sources.

biographies of each identified activist within the networks. We classify personal assistants, secretaries, and staff to opposition elected officials as behind-the-scenes activists, as they occupy less visible but essential roles in sustaining dissident networks, such as managing logistics and coordinating finances. Conversely, we classify opposition elected officials as high-profile public activists, as they represent the visible face of resistance, engage in open challenges to the regime, and are more easily observed by state agencies. To operationalize these distinctions, we create two binary variables: *Personal assistants as the sources* and *High-profile activists as the sources*. Reports where the sources did not fall into either category–typically family members or relatives uninvolved in dissident activities–are coded as 0 for both indicators. For robustness, we conducted additional analyses excluding reports in which all sources fell outside these categories or where sources included both assistants and politicians. The results remain consistent.

For the third hypothesis, we measure intelligence content that informs internal conflicts and divisions. Specifically, we create a binary indicator, *Negative interactions*, to capture whether a report documents instances of internal conflicts within activist networks, such as disputes, blame, or criticisms among dissidents. This variable is operationalized in two ways: one includes all negative interactions, while the other focuses specifically on those involving prominent opposition figures, such as county mayors, provincial councilors, and legislators–the highest elected positions available to opposition candidates at the time. Negative interactions involving these high-profile figures were likely of particular interest to state agencies, as such conflicts offered valuable opportunities for the regime and its secret police to exploit and demobilize the opposition.

Covariates. We also control for some potential confounders. *Number of actors mentioned* counts the dissidents referenced in the report. Reports with more actors tend to raise the secret police's concerns and are also more likely to include negative interactions, potentially confounding the expected relationships. A binary indicator for *students* indicates whether the report mentions student involvement, a group often seen as heightening the government's

perceived risk. A binary indicator for *public* denotes whether the informants obtained intelligence during public activities, including campaign speeches, public gatherings, or fundraising dinners open to the general public, to ensure the circumstances of information gathering do not confound the effect of network positions on protection outcomes. *Level of intelligence* captures the originating security agency's assessment of a report's reliability and accuracy. However, this measure likely reflects personal biases of the individual officer providing this initial rating. It is also relatively coarse: about 85% of reports fall into just two categories, and rating patterns vary systematically across agencies.[8] We include it to account for potential confounding but caution against overinterpreting its meaning.

We also include cubic polynomials to account for temporal dependence in the reports (Carter and Signorino, 2010). Fixed effects for security agency producing the report (Garrison Command, Investigation Bureau, or National Security Bureau) are also included to account for potential differences in informant protection protocols across agencies. Coding rules and descriptive statistics of the variables are documented in Tables A.1 and A.2.

We employ logit regressions given the binary nature of our dependent variable, with individual surveillance reports as the unit of analysis. Standard errors are clustered at the reporter level.

Results

Figure 2 presents the results. The left panel shows the relationship between *Centrality of the sources* and the likelihood of informant protection. It displays six models, incorporating three sets of control variables–no controls, temporal trends with authority fixed effects, and full controls–and two measures of connection: the mean eigenvector centrality of sources

[8]Taiwan's security agencies employ a system resembling the Admiralty Code (or the NATO System), which assesses "source reliability" and "information credibility". We combine them into an eight-point ordinal scale. While common in intelligence practice, this system is often criticized for its vagueness and subjectivity (Irwin and Mandel, 2019). Internal manuals from Taiwan's Investigation Bureau echo these concerns and advise against overinterpreting the ratings (Bureau, 1959, 1974). The manuals also note that domestic intelligence is generally rated as more reliable than foreign or battlefield intelligence, which helps explain the more uniform rating patterns observed in reports on domestic dissidents.

across all reports up to time $t-1$ and within the past month.[9] Across all models, higher source connectedness is positively and significantly associated with protections. One standard deviation increase in the connectedness of informants' sources raises the likelihood of informant protection by 1.6 to 2.1 times.

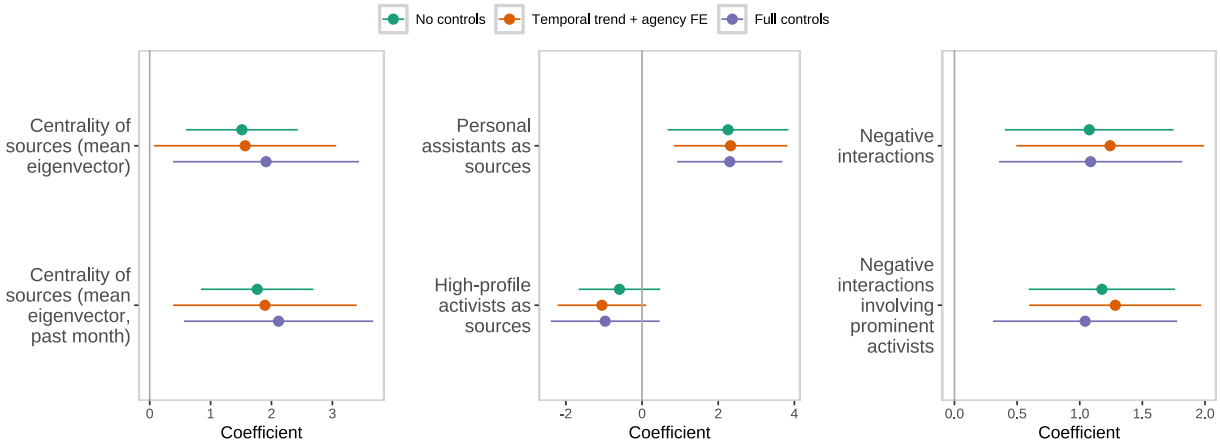

Figure 2. Features of informants' sources and informant protection requests

Note: The left panel presents estimates from models in Appendix Table A.4, examining the effects of sources' network centrality. The middle panel shows estimates from Models 1–3 in Appendix Table A.7, analyzing the effects of sources' types. The right panel provides estimates from models in Appendix Table A.8, evaluating the impact of reports mentioning negative interactions within dissident networks. Circles represent point estimates, and solid lines denote 95% CIs clustered at the reporter level. Full controls include authority fixed effects, temporal trends, the number of actors mentioned, student involvement, public circumstances, and intelligence level.

The middle panel shows the relationship between the type of informants' sources and the likelihood of informant protection. Across these three model specifications, informants connected to behind-the-scenes activists, measured as *Personal assistants as sources*, are associated with a significantly higher likelihood of protection compared to other sources. Models 4–6 in Appendix Table A.7, which exclude reports listing both assistants and high-profile activists as information sources, yield similar results.[10]

The right panel shows that reports mentioning *Negative interactions* within dissident networks significantly increase the likelihood of informant protection. This finding holds when

[9] Appendix Tables A.5 and A.6 provide consistent results using maximum eigenvector centrality and mean degree centrality of sources.

[10] When such reports are excluded, we see that informants connected to high-profile activists are significantly less likely to receive protection, likely reflecting their visibility and routine monitoring by secret police agencies.

the analysis is restricted to negative interactions involving prominent activists, as shown in Models 4–6 in Appendix Table A.8. Taken together, these results support our hypotheses that informants gathering intelligence from well-connected sources, behind-the-scenes sources, and those reporting divisive content are more likely to be protected by security agencies.[11]

Conclusion

Using original data from declassified surveillance reports, this research note offers one of the first analyses of how secret police assess intelligence quality and protect long-term assets within their surveillance networks. We find that informant protection measures are tied to their ability to access well-connected dissidents, behind-the-scenes figures who possess hidden information, and content on internal conflicts that can fuel divisions. Informants with access to these critical individuals and sensitive information are more likely to receive protection within the regime's intelligence system. In the world of widespread authoritarian surveillance, this finding carries critical implications for authoritarian survival. It suggests that, rather than simply seeking more information, secret police prioritize their emphasis and protection on high-quality intelligence provided by informants deeply embedded in the opposition networks. These results encourage research to consider the critical consequences of intelligence usage in repression. Intelligence assets require time to develop within the network, with high-value assets demanding even more time. Given that informants operate covertly within the activist network, acting on intelligence without caution could risk exposing their crucial assets and jeopardizing surveillance operations. By uncovering the decision-making processes of intelligence asset protection, this study speaks to the inner

[11]We also conduct a separate analysis including all three explanatory variables in the model as a robustness check. The results are shown in Appendix Table A.9. We find that the centrality measure loses statistical significance at conventional levels, and it is driven by the rare presence of Chen Chu as an information source—who was both highly connected and served as a personal assistant within the opposition network. After removing reports mentioning Chen Chu as an informant's sole source (12 % of our data), all three explanatory variables remain statistically significant and aligned with our theoretical expectations. Nonetheless, we acknowledge that this outlier influences the results and advise interpreting the centrality findings with caution.

workings of state surveillance, a topic of increasing relevance in an era of digital surveillance and increasingly sophisticated state repression against regimes' enemies.

References

Bureau, I. (1959). *On the Problem of Intelligence Processing*. Investigation Bureau.

Bureau, I. (1974). *Four Lectures on Methods of Work*. Investigation Bureau.

Carnegie, A. and Carson, A. (2019). The disclosure dilemma: nuclear intelligence and international organizations. *American Journal of Political Science*, 63(2):269–285.

Carter, D. B. and Signorino, C. S. (2010). Back to the future: Modeling time dependence in binary data. *Political Analysis*, 18(3):271–292.

Chau, T.-H., Hassan, M., and Little, A. T. (2024). Communication, coordination, and surveillance in the shadow of repression. *American Journal of Political Science*.

Choulis, I., Escribà-Folch, A., and Mehrl, M. (2024). Preventing dissent: Secret police and protests in dictatorships. *The Journal of Politics*, 86(3):000–000.

Dragu, T. and Przeworski, A. (2019). Preventive repression: Two types of moral hazard. *American Political Science Review*, 113(1):77–87.

Dylan, H. and Maguire, T. J. (2022). Secret intelligence and public diplomacy in the ukraine war. *Survival*, 64(4):33–74.

Gandhi, J. and Lust-Okar, E. (2009). Elections under authoritarianism. *Annual Review of Political Science*, 12:403—422.

Geddes, B., Wright, J., and Frantz, E. (2018). *How Dictatorships Work: Power, Personalization, and Collapse*. Cambridge University Press.

Gohdes, A. R. (2020). Repression technology: Internet accessibility and state violence. *American Journal of Political Science*, 64(3):488–503.

Greitens, S. C. (2016). *Dictators and Their Secret Police: Coercive Institutions and State Violence*. Cambridge University Press.

Hager, A. and krakowski, K. (2022). Does state repression spark protests? evidence from secret police surveillance in communist poland. *American Political Science Review*, pages 1–16.

Hassan, M., Mattingly, D., and Nugent, E. R. (2022). Political control. *Annual Review of Political Science*, 25(1):155–174.

Irwin, D. and Mandel, D. R. (2019). Improving information evaluation for intelligence production. *Intelligence and National Security*, 34(4):503–525.

Liu, H. (2022). Dissent networks, state repression, and strategic clemency for defection. *Journal of Conflict Resolution*, 66(7-8):1292–1319.

Liu, H. and Peldon, D. (2025). Surveillance studies. In *De Gruyter Handbook of Political Control*. De Gruyter.

Liu, H. and Sullivan, C. M. (2021). And the heat goes on: Police repression and the modalities of power. *Journal of Conflict Resolution*, 65(10):1657–1679.

Lust-Okar, E. (2004). Divided they rule: The management and manipulation of political opposition. *Comparative politics*, pages 159–179.

Lyall, J., Shiraito, Y., and Imai, K. (2015). Coethnic bias and wartime informing. *The Journal of Politics*, 77(3):833–848.

Mehrl, M. and Choulis, I. (2024). Secret police organizations and state repression. *Journal of Conflict Resolution*, 68(5):993–1016.

Müller-Enbergs, H. (2008). *Die inoffiziellen Mitarbeiter[The Unofficial Collaborators]*. Deutsche Nationalbibliothek.

Nalepa, M. and Pop-Eleches, G. (2022). Authoritarian infiltration of organizations: causes and consequences. *The Journal of Politics*, 84(2):861–873.

Ong, E. (2022). *Opposing power: building opposition alliances in electoral autocracies*. University of Michigan Press.

Parkinson, S. E. (2013). Organizing rebellion: Rethinking high-risk mobilization and social networks in war. *American Political Science Review*, 107(3):418–432.

Piotrowska, B. M. (2020). The price of collaboration: How authoritarian states retain control. *Comparative Political Studies*, 53(13):2091–2117.

Piotrowska, B. M. (2024). Reaching the converted: Understanding the informant enrollment methods. *Available at SSRN 4832186*.

Scharpf, A. and Gläßel, C. (2020). Why underachievers dominate secret police organizations: Evidence from autocratic argentina. *American Journal of Political Science*, 64(4):791–806.

Steinert, C. V. (2023). The impact of domestic surveillance on political imprisonment: Evidence from the german democratic republic. *Journal of Conflict Resolution*, 67(1):38–65.

Su, C.-H. (2020). How is surveillance carried out? the case of chen chu in the ching-gu project (監視怎麼做？以《青谷專案》中陳菊的動態爲例). In *Political Archives Collection and Preliminary Research Conference*, National Taiwan University, Taipei, Taiwan. In Chinese.

Sullivan, C. M. (2016). Political repression and the destruction of dissident organizations: Evidence from the archives of the guatemalan national police. *World Politics*, 68(4):645–676.

Sullivan, C. M. and Davenport, C. (2018). Resistance is mobile: Dynamics of repression, challenger adaptation, and surveillance in us 'red squad' and black nationalist archives. *Journal of Peace Research*, 55(2):175–189.

Thomson, H. (2023). The bureaucratic politics of authoritarian repression: Intra-agency reform and surveillance capacity in communist poland. *Political Science Research and Methods*, pages 1–16.

Transitional Justice Commission, T. (2022). *Mission Conclusion Report, Volume 2*. Taipei: Transitional Justice Commission.

Xu, X. (2021). To repress or to co-opt? authoritarian control in the age of digital surveillance. *American Journal of Political Science*, 65(2):309–325.

KEEPING IT SECRET: SURVEILLANCE, INFORMANT NETWORKS, AND THE PROTECTION OF INFORMANTS IN AUTHORITARIAN REGIMES
ONLINE APPENDIX

1. Case and Context Overview

This study utilizes newly declassified archives on state surveillance and repression during Taiwan's authoritarian period, collected and released by the National Archives Administration. Specifically, we analyze a single surveillance project dedicated to monitoring Chen Chu (陳菊). The monitoring was carried out by the Garrison Command, Investigation Bureau, and National Security Bureau, spanning the period between the Zhongli Incident (中壢事件) in 1977–when a protest against election fraud turned violent–and the Formosa Incident (美麗島事件) in 1979. Figure A.1 presents an example of a declassified surveillance report from this project.

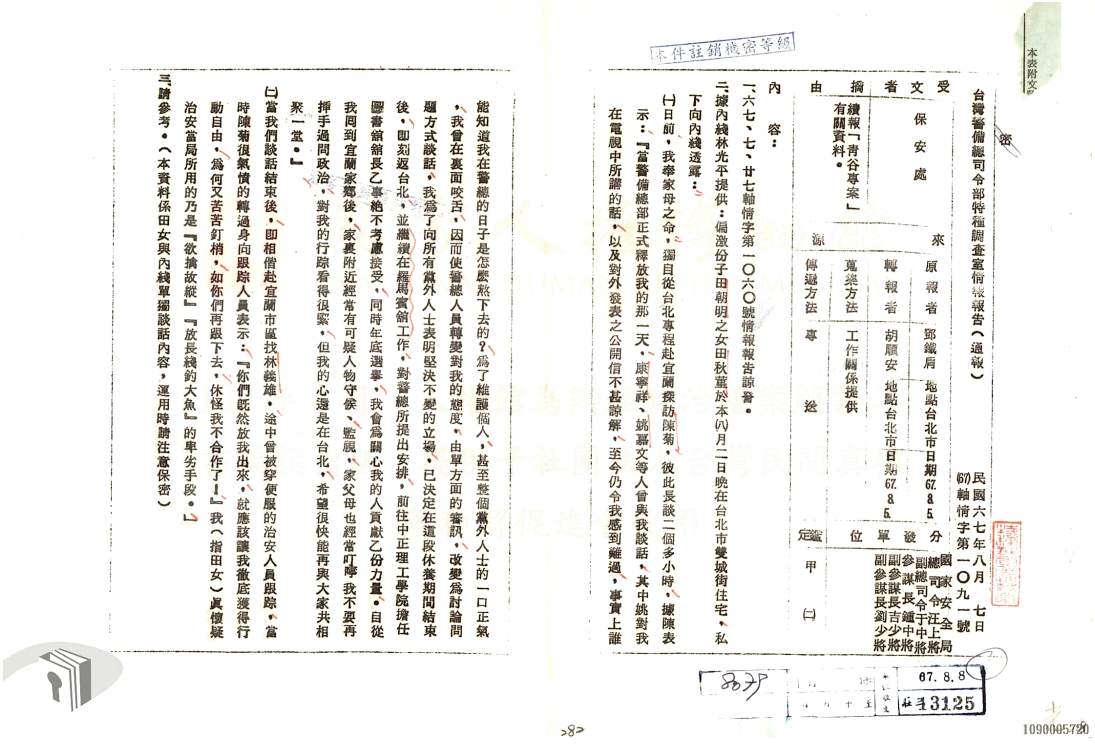

Figure A.1. A sample surveillance report. *Source: Taiwan National Human Rights Museum.*

The late 1970s marked increasing mobilization among dissidents in Taiwan. By this time, the Kuomintang (KMT) had developed a sophisticated monitoring and informant network. Adding to the tension, in 1979, the U.S. formally broke diplomatic relations

with the Republic of China (ROC) and recognized the People's Republic of China (PRC), further undermining the KMT's legitimacy. The Formosa Incident marked a pivotal moment in Taiwan's democratic movement. On December 10, 1979, a pro-democracy protest organized by Formosa Magazine (美麗島雜誌社) escalated into a large demonstration. The magazine's efforts to form an official opposition party posed a direct threat to the regime, prompting a violent crackdown. Key dissidents, including Chen Chu, were arrested, bringing the surveillance project targeting her to an end.

Chen Chu's surveillance project is representative for our analysis for several reasons. As a key organizer, she facilitated communication and collaboration among opposition activists, offering valuable insights into how dissident networks operated during this period. Additionally, Chen Chu was one of eight defendants prosecuted during the Formosa Incident. Her surveillance files are the most extensive and detailed among these key activists, surpassing those of other individuals under surveillance for longer periods. The completeness of her archives provides a solid basis for analyzing the regime's monitoring and intelligence management strategies.

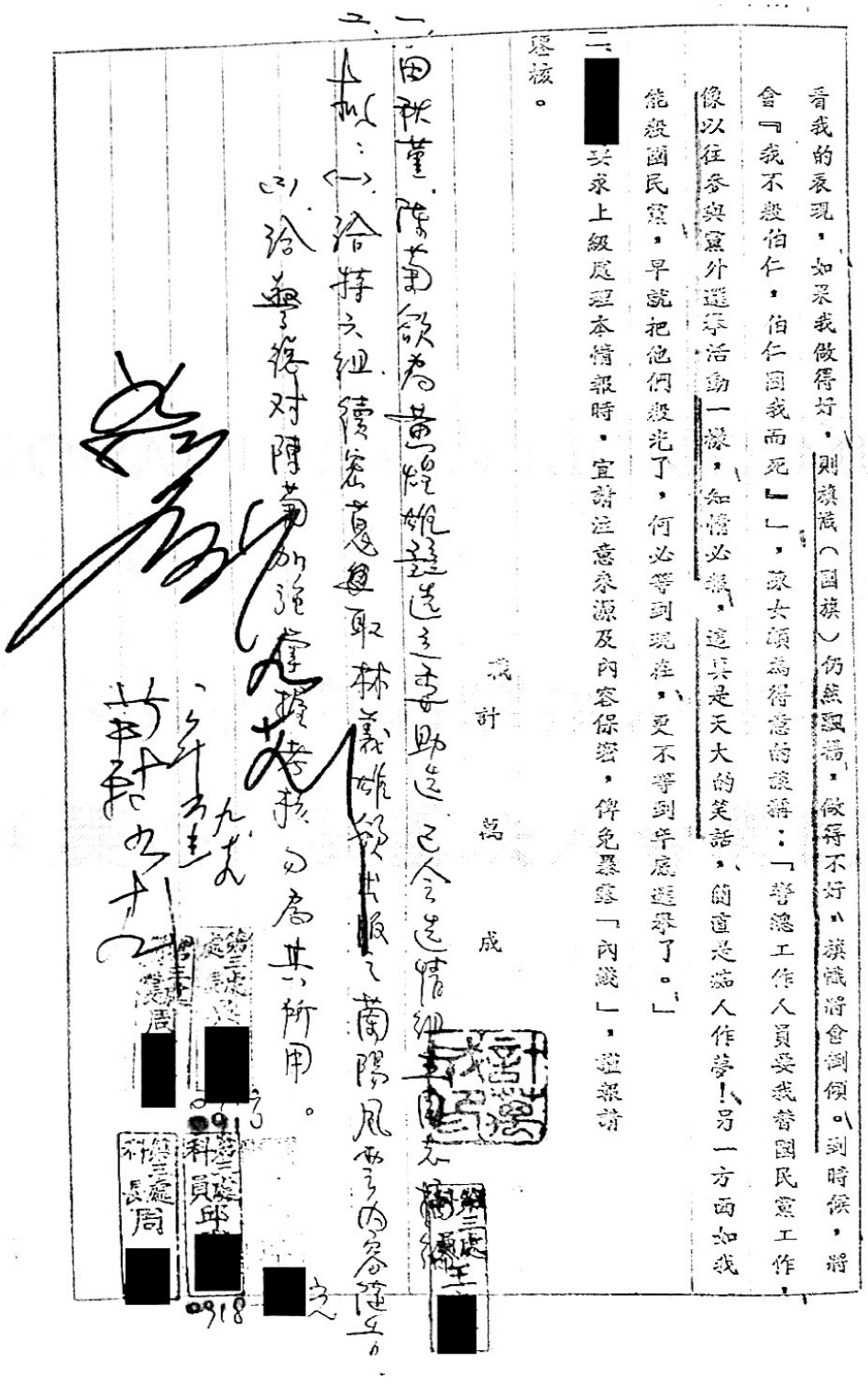

Figure A.2. Surveillance report requesting caution in handling the intelligence.
Source: Taiwan National Human Rights Museum.

2. Descriptive Statistics

Table A.1. Coding rules for all variables used

Variable	Description	Coding rule
Informant protection request	Whether the reviewing officer requests cautious handling to protect the informant's identity	Binary variable coded as 1 if the report includes an explicit mention of a request for protection; 0 otherwise.
Centrality of the sources	Centrality of informant's sources within activist networks	Identify sources mentioned in each report. Construct the sources' network based on documented co-activities (e.g., meetings, joint protests). Compute eigenvector (and degree) centrality of each source using (1) all reports up to time $t-1$, and (2) previous-month reports. Use max and mean of sources' scores per report.
Personal assistants as the sources	Whether the informant's sources are behind-the-scenes assistants	Binary variable coded as 1 if there are any sources identified (via biographies/memoirs) as a personal assistant/staffer to elected opposition officials in each report; 0 otherwise.
Politicians as the sources	Whether the informant's sources are prominent public dissidents	Binary indicator coded as 1 if there are any sources identified was an opposition politician holding elected office (e.g., county mayor, legislator) in each report; 0 otherwise.
Negative interactions	Whether a report documents internal conflicts among dissidents	Binary variable coded as 1 if the report describes any blame, disputes, or criticism among activists in each report. An alternative version of this measure restricts it to conflicts involving elected opposition officials.
Number of actors	Number of dissidents referenced in the report	Count of unique dissidents referenced in the report.
Students	Whether students are referenced in the report	Binary indicator coded as 1 if students are explicitly participants in the report; 0 otherwise.
Public	Whether intelligence was gathered during public/open activities	Binary variable coded as 1 if information was obtained during public activities (e.g., campaign speeches, rallies, fundraisers); 0 otherwise.
Intelligence level	Internal reliability/importance rating of report by agency	Derived from a two-dimensional agency rating system, combining "source reliability" and "content credibility" into an ordinal 8-point scale.
Date	Time trends	Include cubic polynomials of time to account for temporal dependence.
Reporting agency	Agency producing the report	Fixed effects for Garrison Command, Investigation Bureau, and National Security Bureau.

Table A.2. Descriptive statistics

Variable	N	Mean	St. Dev.	Min	Max
Informant protection request	233	0.137	0.345	0	1
Centrality of sources (mean eigenvector)	227	0.283	0.288	0.000	1.000
Centrality of sources (mean eigenvector, past month)	227	0.349	0.307	0.000	1.000
Centrality of sources (max eigenvector)	227	0.499	0.427	0.000	1.000
Centrality of sources (max eigenvector, past month)	227	0.539	0.420	0.000	1.000
Personal assistants as sources	227	0.661	0.474	0	1
High-profile activists as sources	227	0.348	0.477	0	1
Negative interaction	233	0.283	0.452	0	1
Negative interaction (prominent actors)	233	0.223	0.417	0	1
Date	233	500.614	176.037	1	904
Number of actors	233	7.708	6.178	2	46
Public	233	0.052	0.221	0	1
Student	233	0.124	0.331	0	1
Intelligence level	231	5.242	1.487	0	7

Table A.3. Correlations across sources' features

	1.	2.	3.	4.
1. Centrality of sources (mean eigenvector)	1			
2. Personal assistants as sources	0.333	1		
3. High-profile activists as sources	0.160	0.016	1	
4. Negative interaction	0.034	0.022	−0.033	1

3. Additional Analyses

Table A.4. Regression estimates of sources' network centrality on informant protection request

DV	Informant protection request					
	(1)	(2)	(3)	(4)	(5)	(6)
Centrality of sources (mean eigenvector)	1.51**		1.57*		1.91*	
	(0.468)		(0.763)		(0.779)	
Centrality of sources (mean eigenvector, past month)		1.77***		1.89*		2.12**
		(0.471)		(0.769)		(0.793)
N of actors					0.102*	0.091†
					(0.048)	(0.047)
Public					-20.3***	-20.0***
					(1.60)	(1.55)
Students					1.01†	0.998†
					(0.555)	(0.536)
Intelligence level					0.274	0.272
					(0.296)	(0.282)
Constant	-2.31***	-2.53***	-3.44	-3.62	-4.98†	-4.92†
	(0.356)	(0.379)	(3.54)	(3.76)	(2.54)	(2.57)
Agency fixed effects			v	v	v	v
Cubic polynomials for time			v	v	v	v
Observations	227	227	227	227	225	225
Adjusted Pseudo R^2	0.02212	0.03626	0.09283	0.10458	0.11834	0.12647
Akaike Inf. Crit.	182.57	179.96	169.51	167.34	164.26	162.76

Note: Standard errors clustered at the reporter level in parentheses. †p<0.1; *p<0.05; **p<0.01; ***p<0.001

Table A.5. Regression estimates of sources' network centrality on informant protection request

DV	Informant protection request					
	(1)	(2)	(3)	(4)	(5)	(6)
Centrality of sources (max eigenvector)	1.10* (0.4430)		0.956† (0.5588)		1.06† (0.5669)	
Centrality of sources (max eigenvector, past month)		1.43** (0.4472)		1.25* (0.5777)		1.30* (0.6140)
N of actors					0.0604 (0.0465)	0.0487 (0.0463)
Public					-19.68*** (1.559)	-19.32*** (1.497)
Students					0.949† (0.5433)	0.970† (0.5263)
Intelligence level					0.2555 (0.3170)	0.2508 (0.2996)
Constant	-2.432*** (0.3558)	-2.706*** (0.4025)	-3.347 (3.693)	-3.346 (3.771)	-4.346 (2.665)	-4.281 (2.646)
Agency fixed effects			v	v	v	v
Cubic polynomials for time			v	v	v	v
Observations	227	227	227	227	225	225
Adjusted Pseudo R^2	0.02013	0.03628	0.08444	0.09360	0.10287	0.10779
Akaike Inf. Crit.	182.93	179.95	171.06	169.37	167.11	166.20

Note: Standard errors clustered at the reporter level in parentheses. †p<0.1; *p<0.05; **p<0.01; ***p<0.001

Table A.6. Regression estimates of sources' network centrality on informant protection request

DV	Informant protection request		
	(1)	(2)	(3)
Centrality of sources (mean degree centrality)	0.001†	0.002†	0.002*
	(0.0007)	(0.001)	(0.001)
N of actors			0.093†
			(0.050)
Public			-20.0***
			(1.65)
Students			0.940†
			(0.541)
Intelligence level			0.330
			(0.455)
Constant	-2.01***	-2.67	-4.59
	(0.313)	(2.82)	(2.83)
Agency fixed effects		v	v
Cubic polynomials for time		v	v
Observations	227	227	225
Adjusted Pseudo R^2	0.00484	0.08429	0.10466
Akaike Inf. Crit.	185.76	171.09	166.78

Note: Standard errors clustered at the reporter level in parentheses. †p<0.1; *p<0.05; **p<0.01; ***p<0.001

Table A.7. Regression estimates of sources' types on informant protection request

DV	Informant protection request					
	(1)	(2)	(3)	(4)	(5)	(6)
Personal assistants as sources	2.26**	2.33**	2.30**	1.97*	1.98*	1.72*
	(0.810)	(0.759)	(0.706)	(0.841)	(0.827)	(0.737)
High-profile activists as sources	-0.594	-1.05†	-0.968	-15.4***	-17.5***	-17.7***
(Other sources=0)	(0.546)	(0.594)	(0.731)	(0.743)	(2.54)	(0.803)
N of actors			0.078			0.156
			(0.069)			(0.106)
Public			-19.6***			-16.4***
			(1.88)			(1.04)
Students			0.720			0.237
			(0.521)			(0.790)
Intelligence level			0.261			0.879
			(0.448)			(0.937)
Constant	-3.46***	-3.42	-4.61	-3.20***	-2.04	-15.1
	(0.746)	(5.75)	(4.15)	(0.743)	(17.9)	(18.6)
Agency fixed effects		v	v		v	v
Cubic polynomials for time		v	v		v	v
Observations	227	227	225	174	174	172
Adjusted Pseudo R^2	0.07513	0.15943	0.16461	0.10654	0.24301	0.22669
Akaike Inf. Crit.	172.78	157.21	155.75	126.74	107.69	109.50

Note: In Models 4–6, reports where both personal assistants and high-profile activists are sources are excluded. Standard errors clustered at the reporter level in parentheses. †p<0.1; *p<0.05; **p<0.01; ***p<0.001

Table A.8. Regression estimates of reporting negative interactions on informant protection request

DV	Informant protection request					
	(1)	(2)	(3)	(4)	(5)	(6)
Negative interaction (yes=1)	1.08**		1.24**		1.09**	
	(0.344)		(0.382)		(0.373)	
Negative interaction (prominent actors, yes=1)		1.18***		1.28***		1.04**
		(0.298)		(0.350)		(0.375)
N of actors	0.010	0.019	-0.015	-0.002	0.065	0.068
	(0.022)	(0.022)	(0.025)	(0.025)	(0.052)	(0.053)
Public					-19.5***	-19.1***
					(1.60)	(1.72)
Students					0.684	0.780
					(0.480)	(0.550)
Intelligence level					0.181	0.188
					(0.284)	(0.285)
Constant	-2.31***	-2.35***	-3.84	-3.78	-4.81	-4.62†
	(0.404)	(0.394)	(4.75)	(4.01)	(3.07)	(2.59)
Agency fixed effects		v	v		v	v
Cubic polynomials for time		v	v		v	v
Observations	233	233	233	233	231	231
Adjusted Pseudo R^2	0.02135	0.02689	0.09969	0.10024	0.11407	0.11039
Akaike Inf. Crit.	184.47	183.43	169.86	169.76	166.65	167.34

Note: Standard errors clustered at the reporter level in parentheses. †p<0.1; *p<0.05; **p<0.01; ***p<0.001

Table A.9. Regression estimates of sources' network centrality, types, and reporting negative interactions on informant protection request

DV	Informant protection request					
	(1)	(2)	(3)	(4)	(5)	(6)
Centrality of sources (mean eigenvector, past month)	1.04 (0.650)	1.73* (0.826)	1.20 (0.969)	2.22* (0.966)	1.41 (1.00)	2.46* (1.08)
Personal assistants as sources	2.02* (0.865)	1.04** (0.395)	2.08** (0.743)	0.969* (0.391)	2.16*** (0.649)	1.09*** (0.297)
High-profile activists as sources (Other sources=0)	-0.600 (0.637)	-0.675 (0.674)	-1.06 (0.664)	-1.22 (0.865)	-0.958 (0.657)	-1.09 (0.839)
Negative interaction (yes=1)	1.08*** (0.320)	0.919** (0.326)	1.16*** (0.350)	0.939** (0.330)	1.01** (0.334)	0.802** (0.274)
N of actors	-0.003 (0.030)	-0.007 (0.039)	-0.011 (0.034)	-0.009 (0.040)	0.067 (0.059)	0.079 (0.067)
Public					-19.4*** (1.47)	-20.0*** (1.73)
Students					0.783 (0.484)	0.923** (0.347)
Intelligence level					0.085 (0.214)	0.251 (0.375)
Constant	-4.07*** (0.658)	-3.15*** (0.399)	-4.37 (7.02)	-3.06 (4.97)	-4.99 (5.80)	-4.08 (2.59)
Agency fixed effects			v	v	v	v
Cubic polynomials for time			v	v	v	v
Observations	227	200	227	200	225	199
Adjusted Pseudo R^2	0.09729	0.06016	0.17912	0.12076	0.18997	0.14358
Akaike Inf. Crit.	168.69	154.24	153.58	144.42	151.08	140.47

Note: In Models 2, 4, and 6, reports in which Chen Chu is the sole source of informants are excluded. Standard errors clustered at the reporter level in parentheses. †p<0.1; *p<0.05; **p<0.01; ***p<0.001