Spies in a Barrel: When to Reel in Espionage

Afiq bin Oslan* & T. Ryan Johnson†

August 21, 2024

Abstract

How do secrets affect international order? We present a formal model of counter-intelligence as policy. In our model, the state can learn foreign agent activities from choices in preceding periods. Agents can moderate these actions to suppress the likelihood of discovery. States will only intervene when espionage exceeds a tacitly-agreed threshold, and excesses emerge when agents cannot be incentivized to moderate activity. (Non-)intervention or escalation depends on executive capacity to detect, future benefits of positive ties, and restraint of the intelligence community. Egregious punishment of spies and blowback from an executive's audience make avoiding escalation harder, and intelligence leaks produce ambiguous effects. We discuss these findings in the context of historical and popular accounts of covert activities revealed to the public.

Keywords— secrecy, foreign policy, political economy, game theory

Word count— 8929 words

JEL Classifications— C73 · F52

*Department of Public Economics, Max Planck Institute for Tax Law and Public Finance, Munich, Germany. ORCiD: 0000-0002-1278-0687. Corresponding author. Email: afiq.bin-oslan@tax.mpg.de.

†Department of Political Science, Washington University in Saint Louis, USA. ORCiD: 0000-0001-8452-5688. Email: thomas.johnson@wustl.edu.

1 Introduction

Intelligence and counterintelligence are prominent in nearly all inter-state relations. Current scholarship on secrecy in International Relations (Carnegie, 2021; Carson, 2016, 2020) argues that states use covert acts because secrecy prevents escalation. If both sides deny and feign ignorance even when underhanded activity is uncovered, then a facade of normalcy can be maintained. This facade protects other state interests —such as trade and other forms of cooperation— from being disrupted.

In this paper, we pursue a formal model of the strategic value in turning a blind eye to espionage or other activity considered covert due to its limited audience. We address these questions using simple tools of political economy and game theory, and we frame consequences associated with decisions with respect to hostile, rivalrous, and friendly relations between states. Unlike existing scholarship, we emphasize strategic value of secrecy for friend and foe alike. We begin with an example of escalation between covert rivals.

On April 17, 1961, the United States launched an invasion of Cuba intended to depose Cuban supremo Fidel Castro. The operation, known as the Bay of Pigs, was a complete disaster.

The Bay of Pigs was different from every previous military incursion taken by the United States in recent history. The invasion was undertaken by CIA officers leading Cuban para-military recruits. Cuba had not antagonized the United States into conflict. The United States was the aggressor, and this was a shock to the American public. Worst of all for President John F. Kennedy: Cuba readily quashed the invasion, bringing into question the norm of American supremacy in armed conflict and leaving a lasting impact on American public perspective on the presidency. Jones (2008) provides an excellent account surrounding its history.

The Kennedy administration was no stranger to covert action to achieve their goals. However, the reaction from the American public was a response that the Kennedy administration was unprepared to handle. President Kennedy was humiliated. Though

he took full responsibility as Commander-in-Chief, Kennedy was privately furious with the Joint Chiefs of Staff and CIA, having lamented, "All my life I've known better than to depend on the experts. How could I have been so stupid?" (Jones, 2008, pp. 131-132). The intelligence community and its proposal to invade Cuba with a CIA-backed band of brigadistas had failed him. It seems reasonable to assume that, albeit with the benefit of hindsight, Kennedy would have preferred to forego the invasion in favour of better ensuring that US intentions for Castro remained what we will term an "Open Secret". The indiscretion demonstrated by the intelligence community bypassed this preference of the administration.

A requiem of the events surrounding the Bay of Pigs three decades later by Arthur Schlesinger Jr. —historian, Kennedy advisor, and Assistant Secretary of State during the Bay of Pigs— is particularly illustrative.

> "On the question of whether the CIA was a rogue elephant, [...] I believe that all intelligence agencies become rogue elephants, in whatever country, whether it is the United States, France, Israel, the Soviet Union, or elsewhere. After a time, people in intelligence agencies come to feel that they know the requirements of national security better than transient elected officials who, in the view of many intelligence professionals, are in office too short a time to know what the game is all about. They also tend to take advantage of the lack of oversight.
>
> [...]
>
> I think it is inherent in the nature of intelligence agencies to turn their techniques of disinformation and dissembling — which they are taught to use against the enemy — to turn them against colleagues or agencies that might disagree with their favored course of action.
>
> [...]
>
> But there are also plenty of operators who get excited by the lack of accountability, the money they are given, and by the sense of adventure. Many of

> the players in the Bay of Pigs from inside the agency seem to me to have fallen prey to one or more of these temptations."
>
> —Arthur Schlesinger Jr. in Blight and Kornbluh (1998, pp. 138-139).

Rafael Quintero, a frequent CIA collaborator for many anti-Castro operations undertaken by the US, became familiar with how overzealous operators can impact covert designs. He describes how the story of American military supremacy prior to the Bay of Pigs influenced him and his colleagues to participate in the invasion with the CIA's support.

> "In those days, the Cubans thought of the Americans in what I call the 'John Wayne syndrome.' ... We thought the Americans worked the way John Wayne worked in his movies. Of course, this was naive, but this was the way most of us felt. I mean: the Americans hated communism and, like John Wayne, they never lost — ever."
>
> —Rafael Quintero in Blight and Kornbluh (1998, p. 1).

Quintero describes motivation that tended towards the mythological, but many other incentive pathways can affect the quality of effort and level of risk that operators are willing to undertake. For example, deterrents such as Russia's propensity to poison or defenestrate enemies of the state (Gioe, Goodman and Frey, 2019) surely influence would-be foreign agents. And some individuals can be persuaded towards traitorous action with quid pro quo arrangements.

In this paper, we abstract the idiosyncrasies of the Bay of Pigs and other cases of covert action from history to explore what provides incentive to an executive like Kennedy, what motivates operators like the anti-Castro Cubans, and how such influences contribute to some events staying in the shadows while others are escalated. Our focus is on the robustness of an Open Secrets status quo where foreign agents moderate their behavior in line with Executive preference to avoid escalation.

To this end, we embed counterintelligence into a game of espionage. We model secrets in international affairs as a four player game: two players from two states.

Each state has a Case Officer, responsible for pursuing intelligence in the other state, and an Executive, responsible for setting a counterintelligence policy. Executives must decide how much foreign transgression they are willing to ignore in the interest of protecting the broader relationship between the two states. Case Officers, in turn, must decide if they wish to respect these thresholds, or if the mission at hand is more lucrative than the preservation of good relations.

We refer to all players choosing to respect the established thresholds against spying as an Open Secrets Equilibrium. In such an outcome, both states agree to conceal transgressions of their rivals in the interest of maintaining existing relations. The states are hence not keeping secrets from each other, but rather they are keeping each other's secrets from the rest of the world—which may be their respective public or the international community—who might prefer to see spying and related covert activities punished. The results of the model suggest that the more reasons states have to be friends, the more likely it is that they will keep each others' secrets to maintain relations.

This result may be slightly unintuitive: it suggests that secrets in International Relations should be more common between friends than they are between enemies. Yet, such logic seems consistent with what we observe. Transgressions carry small risk between allies as they are less likely to expose each other's faults, but committing even the smallest wrongs can instigate a diplomatic breakdown or even conflict when state relations are already hostile. After establishing equilibrium behavior, we discuss several extensions and how they could make Open Secrets more or less likely.

The study of secrets is a small but rich area of International Relations. Major contributions are largely qualitative in nature and have provided insight into the strategic nature through which states employ secrecy in international affairs. We contribute to this literature in two ways. First, the frontier of secrecy scholarship focuses on secret combat or military activity—Carnegie (2021) provides a review. We extend the broad conclusions of this literature to also apply to peace time usage of espionage. Second, we discuss secrets in the context of strategic counterintelligence. We contribute the

first game theoretic treatment of intelligence with respect to a political economy.

2 Secrets and International Organization

Successful strategic intelligence conveys advantage over the use of military, diplomacy, and economy as tools to mediate conflict. For example, misrepresentation of intelligence is expected among adversaries, especially for deception surrounding military capability or military operations in civil or interstate conflict. The generalized study of collusion among rivals to maintain secrets has been a recent innovation in International Relations literature (Carson, 2020), but collusion to maintain secrets among tepid rivals or staunch allies remains understated. Allies also have reasons to deceive or withold information.

Discretion between friends is crucial to understanding the value of secrets in international affairs. So is the context in which friendship occurs. We generalize secrecy and collusion between friend and foe alike as a way to maintain normal relations. These normal relations could be militaristic, diplomatic, or economic in nature, but at minimum they embody a status quo that at least one state prefers to maintain. Examples include limiting the intensity of covert attacks to maintain limited conflict or overlooking the theft of trade secrets to continue trade relations.

2.1 Intelligence and Counterintelligence

This paper applies political economy to study when and how interstate relations affect and are affected by the actions of an intelligence community. We pay close attention to the decision-making power held by an executive who acts on information revealed about a foreign state, which may or may not be a hostile rival.

Detection, deterrence, deception, and neutralization of future threats shape the application of intelligence for counterintelligence operations. Security studies and historical accounts of covert actions tend to discuss actions taken by intelligence services as offensive or defensive in nature, but practitioners find feedback loops in counterin-

telligence to be inescapable. In lieu of an offensive or defensive dichotomy, we embrace the simultaneity of the counterintelligence problem in a game theoretic representation.

Counterintelligence has been defined a number of ways depending on the purpose of the study.[1] To build our formal theory, we prefer,

> "Counterintelligence is the study of the organization and behavior of the intelligence services of foreign states and entities, and the application of the resulting knowledge" (Ehrman, 2009, p. 6),

and hence use "counterintelligence" to broadly refer to a state or a state agency's response to intelligence gathering by an outside force.[2]

When defining counterintelligence, Ehrman (2009) delineates two areas of applied counterintelligence: counterintelligence operations and counterespionage. Counterintelligence operations are those "undertaken to collect information about intelligence services", "are a specialized subset of intelligence operations in general", and "when successful can create endless feedback loops" (Ehrman, 2009, p. 15). Counterespionage, on the other hand, is defined as "investigations or operations undertaken to uncover a spy" (Ehrman, 2009, pp. 16-17). These definitions are not mutually exclusive, but as previously stated, this paper focuses on the former: executive response to detected espionage as a counterintelligence operation. We address potential for a formal model of counterespionage towards the end of the paper.

2.2 Secrets in International Relations

A typical argument in International Relations is that leaders will go public with their demands because doing so ties their hands (Schelling, 1966). Watchful audiences will force leaders to escalate or retaliate if demands are not met, and this mechanism makes any threats that accompany demands more credible (Fearon, 1994, 1995, 1997; Ramsay,

[1] Varouhakis (2011), for example, assesses counterintelligence theory from an organizational behavior perspective.

[2] See Johnson (2009); Bridgeman (2009) for similar definitions and Olson (2001); Wettering (2000) for alternative definitions.

2004; Schultz, 1998; Smith, 1998). Yet, there is still much in International Relations accomplished outside of public view. Beyond closed-door diplomacy, the prevalence of covert operations, secret agreements and classified documents suggests that there are circumstances where states may not be willing to risk escalation to have their demands met (Baum, 2004; Kurizaki, 2007; Poznansky, 2019; Tarar and Leventoğlu, 2009).

Secrecy is the "intentional concealment of information from one or more audiences" (Carson, 2020, p.5). Covert activity is an essential component to ensure that limited competition remains limited as it provides the opportunity for backdoor concessions and avoiding unintended escalation. Covert activity achieves this by avoiding pressure to resist or retaliate from a domestic audience, a watching ally, or an anxious enemy. This can be particularly important if one or more great powers are involved as escalation may set-off an uncontrollable chain reaction (Schelling, 1966; Smoke, 1977).

The study of secrecy in International Relations is a relatively underdeveloped literature. Existing contributions are rich but narrow, primarily focusing on covert elements in combat or military operations. See Carnegie (2021) for a review. However, the use of secrecy in International Relations should be considered more regular and commonplace. After all, states are continuously looking to gain intelligence on one another even in peacetime. We emphasize on this latter context as the primary contribution of our model to the understanding of how secrets affect international relations.

2.3 Collusion and Counterintelligence

Notably, Carson's (2020) definition of secrecy does not require concealment from all parties. Secrecy also captures the possibility of discretion and secret cooperation. For example, a state may abstain from revealing each other's secrets to the public or to other states. Two features of state relations are necessary for the possibility of secret collaboration. On one hand, leaders must be able to abide by thresholds "to control external reactions and avoid unintended escalation" (Carson, 2016, p.113). The complement must also be true and is the focus of our paper. Leaders of states targeted by foreign espionage must make it appear that adversaries are abiding by expected

thresholds to avoid pressure to escalate or retaliate. Linking these two features of interstate relations may produce circumstances where states tacitly collude to keep their competition under wraps, resulting in what Carson (2020) calls "secret wars".

We build on the work of Carson (2020) where states may collude with adversaries in keeping each other's secrets. However, we turn the focus away from combat operations and instead focus on intelligence gathering. We argue that two states — whether or not they are adversaries — may tacitly agree to overlook a limited amount of spying and intelligence gathering in order to maintain the benefits of a cordial public-facing relationship.

By our definition, counterintelligence broadly refers to state response to intelligence gathering by an outside force. We abstract threat neutralization by a state as lifting the facade of normal relations and ending espionage for everyone in the game. Under this abstraction, we focus on two responses that an executive can take as we develop the game. We stylise these responses to be "like shooting fish in a barrel", an English idiom describing a straightforward task. For a potential catch in hand, we analyze when the strategic executive might *Let Swim* to play another round or *Reel In* their catch. These stylized actions correspond to whether the executive escalates upon detection by ending the game or allows both their spy and the detected foreign agent to continue the game upon receipt of an exogenous benefit.

When might a target state reel in discovered spies and expose the underhanded ambitions of foreign powers? When the adversary's covert activity substantially alters the strategic status quo (Carson, 2016, p.127). If the adversary does not abide by established thresholds, the target state may no longer feel it beneficial to avoid escalation. In such scenarios, losses from covert incursion begin to outweigh the benefits of maintaining normal relations.

2.4 Principals and Agents

We use the Ehrmann definition of counterintelligence to motivate our formal theory. However, another definition of counterintelligence with respect to the policy process is

useful to distinguish effects in our model from what is expected in a principal-agent framework.

Counterintelligence as a policy process can be summarized as "detect, study, act" (Bridgeman, 2009, p. 129). Counterintelligence detects a previously unknown aspect of a rival state. The new information is studied and incorporated into a plan to confer advantage over the rival. An intelligence service brings processed information as policy to the attention of the executive, and finally the executive must decide whether to act on the proposal.

In our exploration of counterintelligence as actionable policy, we bury the "study" component from the Bridgeman definition as something that intelligence services do independently and flawlessly. Our model thus reduces the counterintelligence process to "detect, act" and the executive does not have the ability to question the validity of the information given to them, as President Kennedy did in retrospect. While this is undoubtedly a simplification, Schlesinger's insights into rogue elephants suggests that our abstracting away from these processes may be reasonably founded.

Detection implies that our model belongs to a class of monitoring problems, while discretion to act generates strategic behavior among players of the game. However, our model lacks principal-agent dynamics for three reasons. First, effort taken by a Case Officer does not directly influence supervisor payoffs. Second, our model has no way for the Executive to monitor — even imperfectly — the level of effort taken by their subordinate. Finally, our model has no mechanism for the Executive to hold their subordinate accountable to a preferred level of effort. The absence of these features constrain our model to focus on counterintelligence decisions. We take Schlesinger's words to heart and assume that intelligence service personnel may be inherently rogue agents operating at their own discretion, untethered to Executive goals.

Detection and discretion to act focuses our analysis on intelligence as policy, which distinguishes our model from a principal-agent relationship. Despite these differences, extensions can be made to capture many real-world dynamics of interest. Domestic and international pressure can force Executives to bow to public demands. An Executive

can deter rival Case Officers through punishment, and treacherous case officers who trade in secrets can affect interstate relations. These extensions will follow separately after first presenting our baseline model.

3 An Infinite-Horizon Game of Secrets

3.1 A Simple Example

Let there be two States: $i \in \{A, B\}$. The game has two players each affiliated with the two States: a Case Officer (or Officer, CO), and an Executive (E). The game thus has a total of four players, $\{CO_A, CO_B, E_A, E_B\}$, that play an infinite horizon game of secrets. Periods of the game are indexed by t.

At the start of every period t, the Officers choose an amount of effort to invest into their activities $x_{i,t} \in [0, 1]$. This might be in reference to the size of the spy network they create and maintain in the host state, the value of the information they pursue, or the amount of risks they take in their tradecraft.

The scale of an Officer's activities determines how likely they are to be discovered by counterintelligence. In any period t, an Executive is activated to pursue counterintelligence with probability $x_{-i,t}$. In periods when they are not activated, Executives have no choices to make. When activated, an Executive can choose to neutralize the threat and *Reel In* the spy network, terminating its activities to protect state secrets. Reeling in the spy ends the game. Such a design implies that not only does the Executive take the opportunity to stop spying in their home state, but also withdraws any of their own spies in fear of retaliation. Alternatively, this abstraction of threat neutralization can be considered an endogenisation of a downstream effect where the other state tightens security in response. Choosing to *Reel In* is thus synonymous with a change in the status quo between the two States.

Alternatively, the Executive may choose to *Let Swim*, allowing the spying to continue but also using the opportunity to continue their own intelligence gathering. Let-

ting the detected spy swim continues the game into the next period. In context, what the Executive is allowing to swim may not be a particular individual spy, but the spying operation as a whole. Choosing to *Let Swim* is thus choosing to maintain the status quo.

Thus, our design models secrets during normal relations between states. The majority of the game takes place under friendly or neutral inter-state relations, but as soon as spying is revealed, states may choose to make a big deal of it. Notably, relations will only break down if a state chooses to counter the spying; relations do not immediately suffer upon discovery of spies. States are thus choosing between maintaining relations and ignoring the spying, or acting upon the spying at the risk of a public breakdown of inter-state relations.

Officers pay-offs are straightforward: they gain intelligence that matches their effort. Thus, $U_{CO_i}(x_{i,t}) = x_{i,t}$.

The Executive incurs negative utility equal to the amount of spying taking place and receives $-x_{-i,t}$ every period. In periods where they let the spies swim, the Executive gains an exogenously determined benefit $\alpha_i \in [0, 1]$. This exogenous benefit can be defined in many ways, but should generally be considered the Executive's value of protecting interests that would have been threatened had espionage been exposed at the risk of escalation. Let $s_{i,t} \in \{0, 1\}$ indicate whether Executive i played Let Swim in period t. Host pay-offs are then

$$U_{E_i}(x_{-i,t}, s_{i,t}) = s_{i,t}\alpha_i - x_{-i,t}$$

Pay-offs are realised at the end of every period, and future pay-offs are discounted by $\delta \in (0, 1)$ common to all players. Since Executives are only able to act when a spy is detected, our design is equivalent to saying that Executives only learn of their past utility the moment they are activated. That is, Executives learn how much past intelligence has been stolen only when they discover the spies. If an Executive is not activated and has no choice to make, then that is formally equivalent to not knowing

anything since they cannot do anything about it anyway.

The description of the game is complete. The timing of the game is as follows.

1. Set $t = 0$.
2. Increase t by 1. Both Case Officers choose $x_{i,t} \in [0, 1]$.
3. With probability $x_{-i,t}$, Executive i is activated. Activated Executives simultaneously choose either *Reel In* or *Let Swim*. If any Executives play *Reel In*, the game ends. Otherwise, return to step 2.

The solution concept is sub-game perfect Nash equilibrium.

3.2 Solution

An infinite horizon design allows for many potential solutions. Our primary interest is in the Open Secrets outcome where both Executives tolerate spying so long as it remains within certain thresholds. Such an equilibrium conforms to the prevailing view in International Relations that states would tolerate some level of espionage in exchange for non-escalation (Carson, 2016, 2020). By scrutinising conditions for Open Secrets, we will also be able to understand when mutual restraint is insufficient to deter counterintelligence responses that lead to escalation.

We begin by considering Officer choice. Limiting our considerations to stationary strategies, only two Officer choices are rationalisable. First, the Officer can maximally expand their efforts ($x_{i,t} = 1$) to pursue short-term gains. Such a choice will lead Officer activities to be discovered immediately and they will be summarily expelled from their post as the threat they pose is too great. Second, the Officer can restrain their spy network just enough ($x_{i,t} = x^\star$) that the rival Executive turns a blind eye—respecting the Open Secrets arrangement—and playing a long-game of espionage.

What does this restrained level of espionage look like? The threshold depends on the utility of the target state's Executive and can be found at the indifference point between their choices. Under the current pay-off structure and with Officers playing

stationary $x_{i,t}$, this is

$$\begin{aligned}
\mathbb{E}\,U_{E_{-i}}(\text{Reel In}) &= \mathbb{E}\,U_{E_{-i}}(\text{Lets Swim}) \\
-x_{i,t} &= \alpha_{-i} - x_{i,t} + \frac{\delta(x_{i,t}\alpha_{-i} - x_{i,t})}{1-\delta} \\
x_i^\star &= \frac{\alpha_{-i}(1-\delta)}{\delta(1-\alpha_{-i})}
\end{aligned}$$

Proposition 1. ***Open Secrets Equilibrium****: There exists a sub-game perfect Nash equilibrium to the game where, given* $\delta \leq \frac{\alpha_{-i}}{1-\alpha_{-i}}$ *for all* i*, both Case Officers play* $x_{i,t} = x_i^\star$ *in every* t*, and activated host Executives play Reel In when* $x_{-i,t} > x_{-i}^\star$ *and Lets Swim otherwise in every* t*.*

The Open Secrets Equilibrium in Proposition 1 depends on whether Officers are willing to maintain this restricted espionage level. The equilibrium condition is derived by comparing Officer pay-off associated with restrained effort to the pay-off associated with mounting a full-blown spy operation ($x_{i,t} = 1$) for one period before Executive $-i$ shuts everything down and reels in the officer immediately after.

$$\begin{aligned}
\mathbb{E}\,U_{CO_i}(x_{i,t} = x^\star) &\geq \mathbb{E}\,U_{CO_i}(x_{i,t} = 1) \\
\frac{x_i^\star}{1-\delta} &\geq 1 \\
\frac{\frac{\alpha_{-i}(1-\delta)}{\delta(1-\alpha_{-i})}}{1-\delta} &\geq 1 \\
\delta &\leq \frac{\alpha_{-i}}{1-\alpha_{-i}} \equiv T_i^\star
\end{aligned}$$

Conversely, the equilibrium fails when $\delta > \frac{\alpha_{-i}}{1-\alpha_{-i}}$ for either i. That is, Open Secrets break down when either there is insufficient exogenous benefit to maintaining the facade for one of the state's Executives (low α) or players place high value on future pay-offs (high δ).

For completeness, we offer the Executive's equilibrium pay-off under Open Secrets.

$$\mathbb{E}\,U_{E_i}(\text{Open Secrets}) = \frac{x_{-i}^\star\alpha_i - x_{-i}^\star}{1-\delta} = -\frac{\alpha_i}{\delta}$$

Notice here that the Executive's expected equilibrium pay-off is negative. This aspect of the design explains why Open Secrets is found to be more likely when players are short-sighted (low δ). A particularly far-sighted executive may not see the maintenance of present good relations worthwhile compared to the long-term losses to spying. This particular comparative static is slightly unintuitive because if the Officer's interests are taken in isolation, one might presume that short-sighted players are less likely to respect Open Secrets as they will be more tempted to take what they can and run. The interaction of Officer's interests with the Executive's interests reverses this expectation.

3.3 An Application

In its current state, the example model is primitive. However, there is already a clear and important pattern: The more reasons you have to be friends, the more likely you are to have secrets to maintain relations. This fact manifests in how Open Secrets is easier to maintain as α_i increases for all i, even if the increases vary in magnitude. By contrast, when there are not many reasons for a friendship to continue, states and their agents may be more than happy to push boundaries with operations that would otherwise be covert.

This result should not be too surprising. After all, friendly states are not keeping secrets from each other. Rather, states are keeping each other's secrets from the rest of the world. When the facade of friendship or the appearance of limited conflict is valuable, two states will underplay each other's indiscretions. One such example is how governments across the world will tolerate extensive Chinese interference for the sake of maintaining trade relations.

In November 2021, Xu Yanjun became the first Chinese intelligence officer extradited to the US to be trialled for and convicted of espionage. Xu's downfall is a success story of US counterintelligence. Xu targeted American aviation companies, their employees, and their proprietary information. One of Xu's assets was an engineer with GE Aviation, now known as GE Aerospace. In June 2017, this engineer brought sensitive

materials to China to give a guest lecture at a university in Nanjing at Xu's invitation. As neither the carrying of materials nor the lecture were authorised by his employers, this visit prompted a counterintelligence investigation that eventually cornered Xu in Belgium.[3]

In the wake of Xu's conviction, FBI Director Christopher Wray is alludes to the need for measured response to espionage.

> "If you're basing what you think American policy should be on the assumption that China's goal is just simply to eliminate competition, I think that's alarmist and it's going to lead you to adopt policies which are actually self-defeating. And I think you can come up with a relatively nuanced, sophisticated, smart strategy that doesn't lead you just simply to say: what we need is '*Fortress America*'."
>
> —FBI Director Christopher Wray in Javers et al. (2023)

Current scholarship on secrecy in International Relations (Carnegie, 2021; Carson, 2016, 2020) affirms Wray's preference for nuance and sophistication. States use espionage because secrecy prevents escalation: if both sides deny and feign ignorance even when spying is uncovered, then a facade of normalcy can be maintained. This facade protects other state interests—such as trade, which Wray emphasised—from being interrupted.

From this perspective, Xu's capture, extradition, trial and conviction may actually represent a small break from the spying norm. There are perhaps two aspects in which Xu's behaviour may have prompted this norm-breaking: Xu was too greedy and too sloppy. The potential loss of aeronautical engineering secrets was possibly too much for the US to ignore, and Xu's pursuit of this particular asset left behind too many clues that lead to successful counterintelligence. To prevent Xu from causing more harm, the US was forced to lift the veil of secrecy and respond with a formal judicial process.

While Xu may have been caught, broader Chinese presence in America's sphere was left to swim. Despite Xu's fecundity, his actions were not enough to cause American

[3]See U.S. Department of Justice (2022) for details of the case.

leadership to "fortress" America. As stated by Director Wray, the US is not shutting down its relations with China anytime soon. The US chose not to follow through on action against China and normal relations were maintained. That is, despite seeing what might be interpreted as a reasonably high x_{-i}, the US did not deem it a severe enough transgression to sour trade relations with China. The α in the US pay-off — the value of trade with China — is much too high.

4 Extensions

An interesting feature of the game revealed by the analysis in Section 3 is that the breakdown of Open Secrets appears to be an Officer-level decision. Both Officers must decide to restrict their espionage for the game to continue. Furthermore, the model has no mechanism for the Executive to compel its Officer. As it stands, the game is the most conservative design of the detection-deterrence relationship, where the principal-agent problem between the executive and the intelligence community is left unsolved.

While the economy of the model is set by the strategic behavior of intelligence officers, the politics surrounding the infinite-horizon game of secrets are a consequence of the actions taken by Executives. A willingness to maintain Open Secrets is tacit collusion between policy makers in the model, and a willingness to act on newly detected espionage is constrained by Executive preference. For this reason, we first explore model extensions that influence executive behavior. Response from external observers towards revealed covert action could encourage or suppress Executive desire to pull the reel. We thus explore the possibilities of both blowback from a critical audience and exaltation from domestic patriots when a state's espionage is revealed.

We then turn to scrutinising mechanisms that Executives may use to compel Officers— both those operating for and against them. A state's Executive may deter excessive rival intelligence activity by tightening laws against spies. Spies that risk capital punishment may be less willing to take risks than spies that only risk expulsion. We then also consider the possibility of treacherous Case Officers that work at the expense of

their Executive.

4.1 Public Pressure

Consider a model extension where critical onlookers dislike when their government interferes in foreign affairs through covert action. This is a generalization of American public response to the Bay of Pigs. Recall that our model perfectly translates Case Officer effort into proportional success, even when the foreign Executive detects espionage. This extension makes the detection of covert activity simultaneous with public discovery — and public reaction, for better or worse — to see how this effects Open Secrets.

We modify the base game with the straightforward addition of a new exogenous parameter. Consider $\gamma > 0$, a penalty the Executive must pay whenever their Case Officer is discovered abroad. We assume that any news of unanticipated covert activity undertaken is bad news for the perpetrator when revealed to the public, which is the most consistent sentiment associated with popular accounts of espionage gone wrong.

For simplicity, let $\alpha_A = \alpha_B \equiv \alpha$ for this extension so that both Executives share the same exogenous benefit of continuing the game. In turn, this implies the two Case Officers share the same critical level of spying $x^\dagger$. We first consider the Executive's equilibrium tolerance for spying when their principled public reacts negatively to the revelation of covert activity abroad.[4] We refer to negative public response as blowback.

$$\begin{aligned}
\mathbb{E}\, U_{E_{-i}}(\text{Reel In}) &= \mathbb{E}\, U_{E_{-i}}(\text{Let Swim} \mid \text{with Public Response}) \\
-x_{i,t} &= \alpha - \gamma x_{-i,t} - x_{i,t} + \frac{\delta(x_{i,t}\alpha - \gamma x_{-i,t} - x_{i,t})}{1-\delta} \\
x^\dagger &= \frac{\alpha(1-\delta)}{\delta(1-\alpha)+\gamma}
\end{aligned}$$

An audience with a distaste for spycraft thus reduces the equilibrium level of spying deemed acceptable by the Executive, evident from the larger denominator in Executive

[4]Note that the derivation below betrays an assumption that Executive i does not know the fate of their compatriot Officer i at the point where they must make their counterintelligence response, hence the appearance of $\gamma x_{-i,t}$ in both current period and future period utility of Let Swim with Public Response.

critical values. The change in the Executive's equilibrium threshold for spying also corresponds with a slight change in the equilibrium condition for Case Officer effort, as follows.

$$\begin{aligned} \mathbb{E}\, U_{CO_i}(x_{i,t} = x^\dagger) &\geq \mathbb{E}\, U_{CO_i}(x_{i,t} = 1 \mid \text{with Public Response}) \\ \frac{x^\dagger}{1-\delta} &\geq 1 \\ \delta &\leq \frac{\alpha - \gamma}{1 - \alpha} \end{aligned}$$

The lower tolerance to spying makes Open Secrets more difficult to achieve, as seen by the smaller numerator in Officer critical values. Officers value long-term intelligence less due to the stricter thresholds, so they are less likely to respect the thresholds that maintain Open Secrets. Thus, blowback makes Open Secrets less likely.

Some audiences may have an appetite for espionage. If so, the term blowback is no longer appropriate. This alternative reflects the possibility that an Executive's public could relish seeing evidence of action being taken against a public enemy whenever their Case Officer is exposed abroad.

Modern Russia is the paradigm of a nation that exalts intelligence operations. When it comes to patriotic hacking, "the Russians have elevated it to an art form" (Gutman-Wei, 2022). Falkov (2022) argues that Russia has been an "intelligence-exalting strategic culture" since at least the 1920s. Such a culture might prompt Russian citizens to pursue cyberattacks on foreign assets unprompted by the government. Russian intelligence services turn a blind eye to those who follow simple rules: don't hack the homeland, and say yes to favors. Patriotic hackers who follow these rules will never face legal repercussions and often share in the loot (Lewis, 2022). This would fit the conservative design of our model since such a scenario is a good example of when the state executive may not have direct control over their spies yet reaps the benefits of their actions —for better or for worse.

How does this "exaltant" public—to borrow Falkov's turn of phrase—affect strategic counterintelligence? The game variant needed to consider this is near identical to the

Blowback extension, but now $\gamma < 0$. What we learn here is thus just the inverse of preceding results. This time, Executives allows for a higher equilibrium level of spying. This in turn increases the equilibrium pay-off of the Officers, making it more profitable for them to adhere to Open Secrets. Thus, an Exaltant Public makes Open Secrets more likely.

We state the findings of the Public Response extension — regardless of whether the response is positive or negative — as Proposition 2. The proposition is provided for a range of public response parameters $\gamma \in [-1, 1]$.

Proposition 2. ***Open Secrets Equilibrium with Public Response****: There exists a sub-game perfect Nash equilibrium to the Public Response extension where, given* $\delta \leq \frac{\alpha-\gamma}{1-\alpha}$ *for all* i*, both Case Officers play* $x_{i,t} = x^{\dagger}$ *in every* t*, and activated host Executives play Reel In when* $x_{-i,t} > x^{\dagger}$ *and Let Swim otherwise in every* t*.*

4.2 Punishment

Punishments are an obvious deterrent. We now explore when an Executive would prefer adopting one punishment policy over another. Suppose there are two policy alternatives to letting a non-compliant rival spy go unpunished: an Always Punish policy where rival spies are always punished when detected, or a Selectively Punish policy where punishment only occurs when the reel is pulled. What level of punishment should an Executive choose to provide incentive to respect an Open Secrets Equilibrium?

4.2.1 Punishing on Detection

Consider the baseline design, where there are no punishment policies in place. In particular, we are interested in parameterisations where Proposition 1 is not possible — that is, when $\delta > \min\{T_A^{\star}, T_B^{\star}\}$. In such cases, Open Secrets would not be normally achieved. Introducing punishment allows the Executive to compel Officers into moderation and broaden the threshold for Open Secrets.

To this effect, consider an extension where Executive A can determine an Always

Punish policy against detected Officers. At the outset (step 0) of this extension, Executive A can choose some $\beta \geq 0$ to serve as a potential punishment that applies for detected Officers of either affiliation. Case Officer i is punished with this β whenever they are detected by rival Executive $-i$, and Executive $-i$ simultaneously pays the same β as a cost to punish. The game otherwise proceeds as the baseline; indeed, fixing $\beta = 0$ would make the two equivalent.

By this design, Officers cannot entirely avoid punishment through moderation, only minimize the chance of being detected to minimize the chance of facing punishment. The new critical spying effort is:

$$\begin{aligned}
\mathbb{E}U_{E_{-i}}(\text{Reel In} \mid \text{Always Punish}) &= \mathbb{E}U_{E_{-i}}(\text{Let Swim} \mid \text{Always Punish}) \\
-\beta - x_{i,t} &= \alpha_{-i} - \beta - x_{i,t} + \frac{\delta(x_{i,t}(\alpha_{-i} - \beta) - x_{i,t})}{1-\delta} \\
x_i^{\oplus} &= \frac{(1-\delta)\alpha_{-i}}{\delta(1 - \alpha_{-i} + \beta)}
\end{aligned}$$

and the new threshold for Officers to prefer the critical effort over maximum effort is

$$\begin{aligned}
\mathbb{E}U_{CO_i}(x_{i,t} = x_i^{\oplus} \mid \text{Always Punish}) &\geq \mathbb{E}U_{CO_i}(x_{i,t} = 1 \mid \text{Always Punish}) \\
\frac{x_i^{\oplus} - x_i^{\oplus}\beta}{1-\delta} &\geq 1 - \beta \\
\delta &\leq \frac{\alpha_{-i}}{1 - \alpha_{-i} + \beta} \equiv T_i^{\oplus}
\end{aligned}$$

Recall that punishment costs imply Executives will only choose to enforce punishment when Open Secrets is not otherwise achievable. Similarly, the Executive will choose the smallest possible β that can compel Officers to minimise this cost if they choose to pay it. These values are found by solving the tolerance threshold $T_i^{\oplus}$ for β,

$$\beta_i^{\oplus} = \frac{\alpha_{-i} - \delta(1 - \alpha_{-i})}{\delta}$$

The greater of the two $\beta_i^{\oplus}$ would then be the necessary β to compel both Officers. Let this be $\beta^{\oplus} \equiv \max\{\beta_A^{\oplus}, \beta_B^{\oplus}\}$.

Executive A will choose to enact Always Punish as policy if their expected utility

strictly improves under the new policy.

$$\begin{aligned}
\mathbb{E}U_{E_A}(\text{Let Swim} \mid x_{B,t} = x_B^{\oplus} \wedge \beta = \beta^{\oplus}) &> \mathbb{E}U_{E_A}(\text{Reel In} \mid x_{B,t} = 1) \\
\mathbb{E}\left(\frac{s_{A,t}(\alpha_A - \beta) - x_{B,t}}{1-\delta}\right) &> -1 \\
\frac{x_B^{\oplus}(\alpha_A - \beta - 1))}{1-\delta} &> -1 \\
-\frac{\alpha_A}{\delta} &> -1 \\
\delta &> \alpha_A
\end{aligned}$$

To ensure that the other Executive also prefers to maintain Open Secrets whilst paying for punishments, a symmetric condition $\delta > \alpha_B$ also applies.

Proposition 3. ***Enforcing Open Secrets with an Always Punish Policy****: There exists a sub-game perfect Nash equilibrium to the Punishment extension where, given* $\delta > \min\{T_A^\star, T_B^\star\}$ *and* $\delta > \max\{\alpha_A, \alpha_B\}$*, Executive A sets punishment* $\beta_i = \beta^{\oplus}$*, both Case Officers play* $x_{i,t} = x_i^{\oplus}$ *in every* t*, and activated host Executives play Reel In when* $x_{-i,t} > x_{-i}^{\oplus}$ *and Let Swim otherwise in every* t*.*

4.2.2 Punishing if the Reel is Pulled

Now consider the Selective Punishment policy, where an Executive limits punishment to events that are exceptionally egregious and demanding escalation. This extension is similar to the previous, except that 1) Executive utility now pays a cost to punish only on reel pull: $U_{E_i} = s_{i,t}(\alpha_i - \beta) - x_{-i,t}$, and, complimentarily, 2) Case Officers are now only punished when the reel is pulled on them by their rival Executive: $U_{CO_i} = x_{i,t} - s_{-i,t}\beta$. This leads to the following effort for Case Officer i in equilibrium under the new policy.

$$\begin{aligned}
\mathbb{E}U_{E_{-i}}(\text{Reel In} \mid \text{Selectively Punish}) &= \mathbb{E}U_{E_{-i}}(\text{Let Swim} \mid \text{Selectively Punish}) \\
-\beta - x_{i,t} &= \alpha_{-i} - x_{i,t} + \frac{\delta(x_{i,t}\alpha_{-i} - x_{i,t})}{1-\delta} \\
x_i^{\otimes} &= \frac{(1-\delta)(\alpha_{-i} + \beta)}{\delta(1-\alpha_{-i})}
\end{aligned}$$

When punishment only happens when the opposing Executive chooses *Reel In*, a Case Officer can moderate their effort and avoid punishment entirely. The effort exerted in a possible Open Secrets equilibrium should be low enough that the detecting Executive will always choose *Let Swim*. Restraint under the new policy regime looks as follows.

$$\begin{aligned}\mathbb{E}U_{CO_i}(x_{i,t} = x_i^{\otimes} \mid \text{Selectively Punish}) &\geq \mathbb{E}U_{CO_i}(x_{i,t} = 1 \mid \text{Selectively Punish}) \\ \frac{x_i^{\otimes}}{1-\delta} &\geq 1-\beta \\ \delta &\leq \frac{\alpha_{-i}+\beta}{(1-\alpha_{-i})(1-\beta)} \equiv T_i^{\otimes}\end{aligned}$$

The level of punishment needed for Open Secrets is again found by solving the tolerance threshold $T_i^{\otimes}$ for punishment.

$$\beta_i^{\otimes} = 1 - \frac{1+\alpha_{-i}}{1+\delta(1-\alpha_{-i})}$$

And again, the greater of the two $\beta_i^{\otimes}$ compels both Officers. Let this be $\beta^{\otimes} \equiv \max\{\beta_A^{\otimes}, \beta_B^{\otimes}\}$. Again, we also solve for when Executive A will prefer to implemented the specified new policy.

$$\begin{aligned}\mathbb{E}U_{E_A}(\text{Let Swim} \mid x_{B,t} = x_B^{\otimes} \wedge \beta = \beta^{\otimes}) &> \mathbb{E}U_{E_A}(\text{Reel In} \mid x_{B,t} = 1) \\ \mathbb{E}\left(\frac{s_{A,t}\alpha_A - x_{B,t}}{1-\delta}\right) &> -1 \\ \frac{x_B^{\otimes}(\alpha_A - 1)}{1-\delta} &> -1 \\ -\frac{\alpha_A + \beta^{\otimes}}{\delta} &> -1 \\ \delta &> \alpha_A + \beta^{\otimes}\end{aligned}$$

This result again also applies symmetrically for Executive B.

Proposition 4. ***Enforcing Open Secrets with a Selective Punishment Policy****: There exists a sub-game perfect Nash equilibrium to the Punishment extension where, given* $\delta > \min\{T_A^{\star}, T_B^{\star}\}$ *and* $\delta > \max\{\alpha_A + \beta^{\otimes}, \alpha_B + \beta^{\otimes}\}$*, Executive A sets punishment* $\beta = \beta^{\otimes}$*, both Case Officers play* $x_{i,t} = x_i^{\otimes}$ *in every t, and activated host Executives*

play Reel In when $x_{-i,t} > x_{-i}^{\otimes}$ and Let Swim otherwise in every t.

Recognise that the Executive expects less utility from Open Secrets in equilibrium under a Selectively Punish policy $\left(-\frac{\alpha_i+\beta^{\otimes}}{\delta}\right)$ than under an Always Punish policy $\left(-\frac{\alpha_i}{\delta}\right)$. This manifests due to how different payment structures for the Executive compel Officers to behave differently in response. The Always Punish policy guarantees punishment (and paying for punishment) happens more often. However, because the need to pay is guaranteed for the Executive, such costs reduce Executive tolerance for spying in equilibrium and reduce critical spying in turn. This results in better equilibrium welfare for Executives. By contrast, Selective Punishment has comparatively higher equilibrium critical spying effort. Here, Executives only pay upon reeling in and thus Executives have extra incentive to avoid reeling in order to avoid this cost. Officers can take advantage of this and their equilibrium critical spying effort rises in response, resulting in worse Executive welfare.

For states confronting underhanded international interference, the comparison between these two punishment designs reveals value in rule of law. Strong rules that requires states to punish transgressions regularly, transparently, and with obvious costs like in the Always Punish regime provide a credible signal that states will not tolerate (as many) transgressions — and this is welfare improving. Thus, it may be beneficial for states to create and propagate clear laws regarding their treatment of foreign agents to keep Open Secrets at a manageable level. This applies to laws within any individual state as well as agreements between states pertaining to such norms. The latter, echoed by the choice of a global β in our design, is particularly important between friendly states who are both more likely to be able to agree on such norms and are also more likely to have Open Secrets among themselves.

4.3 Treachery

The most famous mole in American intelligence history may be Robert Hanssen; he is certainly the most destructive. Hanssen was an FBI agent who leaked information

to Soviet and Russian intelligence between 1979 and 2001. Among other damaging revelations, Hanssen offered the identities of double-agents within Soviet intelligence services, leading to their execution. The hunt for Hanssen's identity was prolonged by the simultaneous perfidity of Aldrich Ames within the CIA. When captured, Hanssen asked the arresting FBI agents "What took you so long?" (Olson, 2019, p. 12).

An enterprise specifically interested in betrayal would endogenise both the temptation for and efforts to uncover treachery. Instead, we restrict our focus on how an exogenously-imposed "leaky pipe" on either side of the competitive enterprise can moderate the behavior of Executives and Case Officers. The notion of an intelligence service tolerating treachery in their ranks is absurd. Mole hunts are fervent endeavors. However, mole hunts are not easy. They take time and require certainty. Despite this, the losses inflicted by a mole at large are common knowledge and their damage becomes clear quickly. We thus model how this very specific understanding of treachery exogenously imposed upon an agency affects Open Secrets.

Formally, payoff for Case Officer i now also depends on an exogenous level of common knowledge treachery $y_i \in [0, 1]$. Again, we model the extent of treachery as common knowledge because it can have clear realised effects when in play. The FBI knew there was treachery in their ranks as their assets were being targeted, even if they did not know it was Hanssen specifically. Treachery appears as a benefit to the Case Officer and is only attained when the Executive from $-i$ does not pull the reel. The latter element allows Executives to "plug the leak" by terminating the game (but will also be seen later to be formally convenient). This new treachery component is additive to their original utility and thus Case Officer utility is now:

$$U_{CO_i}(x_{i,t}, y_i, s_{-i,t}) = x_{i,t} + s_{-i,t}y_i$$

As long as the rival Executive does not pull the reel, the treacherous Case Officer will get the pay-off of their malfeasance.

Payoff for the Executive is now modified negatively by the treachery of their com-

patriot Case Officer. If the Host pulls the reel, then they can mitigate the effects of their compatriot Case Officer's treachery, but not the rival Officer's honest effort.

$$U_{E_i}(x_{-i,t}, y_i, s_{i,t}) = s_{i,t}(\alpha_i - y_i) - x_{-i,t}$$

The threshold under the new equilibrium condition with treachery depends on the utility of the target state's Executive relative to the indifference point between pulling the reel or letting the game continue.

$$\begin{aligned}
\mathbb{E}\, U_{E_{-i}}(\text{Reel In} \mid \text{Treachery}) &= \mathbb{E}\, U_{E_{-i}}(\text{Let Swim} \mid \text{Treachery}) \\
-x_{i,t} &= \alpha_{-i} - y_{-i} - x_{i,t} + \frac{\delta(x_{i,t}(\alpha_{-i} - y_{-i}) - x_{i,t})}{1-\delta} \\
x_i^{\ddagger} &= \frac{(\alpha_{-i} - y_{-i})(1-\delta)}{\delta(1 - (\alpha_{-i} - y_{-i}))}
\end{aligned}$$

A treacherous Case Officer is not more likely to be discovered due to their own treachery y_i. This a quirk of how we have chosen to model treachery as exogenous.

However, what we do learn from the design of this extension is that Case Officer effort — regardless of treachery — decreases with rival Case Officer treachery y_{-i}. This is because leaks reduce the appetite of rival Executives for spying in general and Open Secrets specifically. Executive $-i$ now has to worry about utility losses from the exogenous treacherous leaks, so their tolerance for rival spying $x_i^{\ddagger}$ decreases.

Proposition 5. ***Open Secrets Equilibrium with Treachery****: There exists a sub-game perfect Nash equilibrium to the game, given* $\delta \leq \frac{(\alpha_{-i}-y_{-i})(1+y_i)}{1-(\alpha_{-i}-y_{-i})}$ *for all* i*, both Case Officers plays* $x_{i,t} = x_i^{\ddagger}$ *in every* t*, and activated host Executives play Reel In when* $x_{-i,t} > x_{-i}^{\ddagger}$ *and Let Swim otherwise in every* t*.*

Again, the equilibrium condition requires Officers to prefer the restrained effort necessary for Open Secrets to mounting a full-blown operation ($x_{-i,t} = 1$) for one

period before Executive i shuts everything down.

$$\begin{aligned}
\mathbb{E}\, U_{CO_i}(x_{i,t} = x_i^{\ddagger} \mid \text{Treachery}) &\geq \mathbb{E}\, U_{CO_i}(x_{i,t} = 1) \\
\frac{x_i^{\ddagger} + x_i^{\ddagger} y_i}{1-\delta} &\geq 1 \\
\frac{\frac{(\alpha_{-i}-y_{-i})(1-\delta)}{\delta(1-(\alpha_{-i}-y_{-i}))}(1+y_i)}{1-\delta} &\geq 1 \\
\delta &\leq \frac{(\alpha_{-i}-y_{-i})(1+y_i)}{1-(\alpha_{-i}-y_{-i})}
\end{aligned}$$

From this condition, we highlight that when $y_i \geq \alpha_i$, the affiliated Officer's treachery entirely negates their Executive's exogenous benefit of letting the game continue, making Open Secrets impossible.

We explore the effects of changes to treachery with the aid of an example, noting that this is the only extension of our model that causes Case Officer behavior to influence their rival. Suppose Case Officer i increases their treachery by dy_i while rival Case Officer $-i$ maintains their level of treachery at y_{-i}. Case Officer i will not change their own effort because it is not a function of their own treachery. However, the rival Case Officer will decrease effort in response.

$$\frac{\partial x_{-i}^{\ddagger}}{\partial y_i} dy_i = \frac{-(1-\delta)}{\delta(1-(\alpha_i - y_i))^2} dy_i$$

The net effects of a change in treachery depend on which Case Officer has the minimum equilibrium cut-off. If Case Officer i has a patience threshold $T_i^{\ddagger}$, then

$$\frac{\partial T_i^{\ddagger}}{\partial y_i} dy_i = \frac{\alpha_{-i} - y_{-i}}{1-(\alpha_{-i} - y_{-i})} dy_i$$

which implies that an increase in treachery dy_i increases Case Officer patience. On the other hand,

$$\frac{\partial T_{-i}^{\ddagger}}{\partial y_i} dy_i = \frac{-(1-y_i)}{(1-(\alpha_{-i} - y_{-i}))^2} dy_i$$

shows a corresponding decrease to rival Case Officer patience. Which of these two effects dominates can be broken down into two cases.

Suppose Case Officer i is the most impatient so that their level of tolerance sets global patience by which other players abide. If rival Case Officer patience has decreased enough so they are now the most impatient, and if the rival Case Officer has updated patience below the original threshold, then the increase in treachery dy_i decreases the range of δ for which Open Secrets are viable. However, if the rival Case Officer becomes the most impatient at a level above Case Officer i's original threshold, or if Case Officer i remains the most impatient, then the increase in treachery dy_i increases the range of δ for which Open Secrets are viable.

Treachery may neither straightforwardly harm the betrayed nor benefit their adversaries. A more thorough model, dedicated to exploring the many further elements of treachery that were simplified away for this extension, will be needed to pin down shifting strategic considerations involved in this phenomenon. Such an endeavour would likely subsume a treatment of counterespionage in general.

5 Conclusion

To conclude, we emphasize the simplicity of our model, its interpretability, and the capacity for detection and deterrence alone to generate real world behavior. The findings offer insights into the strategic behavior of states and foreign agents regarding espionage, helping political scientists understand how intelligence services and their actions can affect international order. The theoretical framework is flexible enough to be applied to other application areas, broadening the scope of political science research in security and statecraft. If silence speaks volumes, then our model can prove useful.

Many interesting pathways that influence behavior in the game of secrets remain to be explored. To reiterate, our model has focused primarily on modeling detection and deterrence—the possibility of explicit deception is omitted. Our model requires genuine espionage to potentially trigger an Executive response. Without the ability for Case Officers to deceive foreign Executives, our model cannot accommodate false flag operations. In other words, Case Officers do not have a way to bait Executives into

pulling the reel and escalating tensions. Relatedly, we also did not consider explicit collusion between Case Officers of different states for an entirely different flavour of deception.

Our model has also not considered the possibility of diplomacy between Executives. That said, Open Secrets can also be construed to constitute an implicit form of understanding between Executives: one Executive keeps the other's secrets because they know it will be reciprocated. This type of understanding may be even stronger than explicit agreements—but this should, of course, be the subject of further theorising. Additional work can also investigate the differences in outcomes prompted by variations in legal or judicial capacity to handle espionage by a foreign agent. A totalitarian regime could take extra-judicial measures or simply generate the appearance of a trial, whereas a democratic regime would need rely to rely on a well-functioning judicial system. We hope our model here serves as a starting point for all such further complexities.

Statements and Declarations

Conflicts of interest/Competing interests: The authors have no conflicts of interest or competing interests related to the publication of this manuscript.

References

Baum, Matthew A. 2004. "Going private: Public opinion, Presidential rhetoric, and the domestic politics of audience costs in US foreign policy crises." *Journal of Conflict Resolution* 48:603–631.

Blight, James G. and Peter Kornbluh, eds. 1998. *Politics of Illusion: The Bay of Pigs Invasion Reexamined*. Boulder, CO: Lynne Rienner Publishers, Inc.

Bridgeman, Vincent H. 2009. Defense Counterintelligence, Reconceptualization. In

Vaults, Mirrors and Masks: Rediscovering US Counterintelligence, ed. Burton Gerber Jennifer E. Sims. Washington, D.C.: Georgetown University Press pp. 125–148.

Carnegie, Allison. 2021. "Secrecy in International Relations and Foreign Policy." *Annual Review of Political Science* 24:213–233.

Carson, Austin. 2016. "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War." *International Organization* 70(1):103–131.

Carson, Austin. 2020. *Secret Wars: Covert Conflict in International Politics*. Princeton University Press.

Ehrman, John. 2009. "Toward a Theory of CI: What Are We Talking About When We Talk About Counterintelligence?" *Studies in Intelligence* 53:5–20.

Falkov, Yaacov. 2022. "Intelligence-exalting strategic cultures: A case study of the Russian approach." *Intelligence and National Security* 37.

Fearon, James D. 1994. "Domestic political audiences and the escalation of international disputes." *American Political Science Review* 8:577–592.

Fearon, James D. 1995. "Rationalist Explanations for War." *International Organisation* 49:379–415.

Fearon, James D. 1997. "Signaling Foreign Policy Interests: Tying Hands Versus Sinking Costs." *Journal of Conflict Resolution* 41:68–90.

Gioe, David V., Michael S. Goodman and David S. Frey. 2019. "Unforgiven: Russian Intelligence Vengeance as Political Theater and Strategic Messaging." *Intelligence and National Security* 34:561–575.

Gutman-Wei, Rachel. 2022. "What Americans Should Do to Prepare for Russian Cyberattacks." *The Atlantic* .

URL: *https://www.theatlantic.com/technology/archive/2022/02/ukraine-war-russian-hack-cybersecurity/622922/*

Javers, Eamon (Correspondent), Kathy Liu (Producer), Allison Stedman (Editor) and Wally Griffith (Executive Producer). 2023. "How the US caught a Chinese spy." CNBC. Accessed online; October 18, 2023.
URL: *https://www.youtube.com/watch?v=0ydtETPStEI*

Johnson, Loch K. 2009. Sketches for a Theory of Strategic Intelligence. In *Intelligence Theory: Key Questions and Debates*, ed. Mark Phythian Peter Gill, Stephen Marrin. New York, NY: Routledge pp. 33–53.

Jones, Howard. 2008. *The Bay of Pigs*. Oxford University Press.

Kurizaki, Shuhei. 2007. "Efficient Secrecy: Public versus private threats in crisis diplomacy." *American Political Science Review* 101(3):543–558.

Lewis, James Andrew. 2022. "A dangerous moment for Russian cybercrime may get worse." *Barrons* .
URL: *https://web.archive.org/web/20220215151339/https://www.barrons.com/articles/a-dangerous-moment-for-russian-cybercrime-may-get-worse-51644936090*

Olson, James M. 2001. "The Ten Commandments of Counterintelligence: A Never-Ending Necessity." *Studies in Intelligence* Fall-Winter.

Olson, James M. 2019. *To Catch a Spy: The Art of Counterintelligence*. Georgetown University Press.

Poznansky, Michael. 2019. "Feigning Compliance: Covert Action and International Law." *International Studies Quarterly* 63(1):72–84.

Ramsay, Kristopher W. 2004. "Politics at the Water's Edge: Crisis Bargaining and Electoral Competition." *Journal of Conflict Resolution* 48:459–486.

Schelling, Thomas C. 1966. *Arms and Influence*. Yale University Press.

Schultz, Kenneth A. 1998. "Domestic Opposition and Signaling in International Crises." *American Political Science Review* 92:829–844.

Smith, Alastair. 1998. "International Crises and Domestic Politics." *American Political Science Review* 92(3):623–638.

Smoke, Richard. 1977. *War: Controlling Escalation.* Harvard University Press.

Tarar, Ahmer and Bahar Leventoğlu. 2009. "Public Commitment in Crisis Bargaining." *International Studies Quarterly* 53:817–839.

U.S. Department of Justice. 2022. "Chinese government intelligence officer sentenced to 20 years in prison for espionage crimes, attempting to steal trade secrets from Cincinnati company." Office of Public Affairs Press Release. Accessed online; October 22, 2023.

URL: *https://www.justice.gov/opa/pr/chinese-government-intelligence-officer-sentenced-20-years-prison-espionage-crimes-attempting*

Varouhakis, Miron. 2011. "An Institution-Level Theoretical Approach for Counterintelligence." *International Journal of Intelligence and Counterintelligence* 24:494–509.

Wettering, Frederick L. 2000. "Counterintelligence: The Broken Triad." *International Journal of Intelligence and CounterIntelligence* 13(3):265–300.