A State Within a State: Schlesinger's 1961 CIA Warning, Covert Power, and Democratic Control

Douglas C. Youvan

doug@youvan.com

www.youvan.ai

January 3, 2026

In June 1961, in the wreckage of the Bay of Pigs, Arthur M. Schlesinger Jr. delivered a blunt diagnosis to President Kennedy: "The contemporary CIA possesses many of the characteristics of a state within a state." The phrase endures because it names a recurring tension in modern governance: how a democracy can field clandestine capability without allowing secrecy to become sovereignty. This paper treats Schlesinger's line not as a slogan but as a diagnostic category. What institutional conditions make an intelligence service drift toward autonomous policy-making? What happens when covert action, liaison networks, and operational tempo outpace the slower disciplines of diplomacy, law, and public accountability? And what forms of oversight actually work when the core activity is designed to resist visibility? Rather than retell a familiar mythology, the paper reconstructs the problem Schlesinger identified: parallel foreign policy, blurred lines between analysis and action, incentive structures that reward operational success over strategic coherence, and the moral hazard of plausible deniability. From there, it evaluates reform proposals—then and now—through a practical lens: mission clarity, legal authority, budget transparency, interagency coordination, congressional supervision, and the cultural psychology of secrecy. The goal is not abolition or sanctification, but democratic control without naivete.

Keywords: CIA, state within a state, Arthur Schlesinger Jr., Bay of Pigs, covert action, clandestine operations, intelligence oversight, democratic accountability, national security state, foreign policy coordination, plausible deniability, executive power, congressional oversight, secrecy and governance, interagency rivalry, institutional incentives, secrecy culture, moral hazard, rule of law, reform proposals.

Outline

1. Introduction: The Phrase That Refuses to Die
1.1 The 1961 moment: Bay of Pigs and institutional shock
1.2 "State within a state" as diagnosis, not slogan
1.3 Scope and method: what this paper will and will not claim

2. What Schlesinger Actually Meant
2.1 Parallel capabilities: political desks, foreign service, paramilitary reach
2.2 Autonomy by accumulation: missions that expand faster than doctrine
2.3 The "rubber stamp" problem: when State becomes downstream
2.4 Early reform instincts: separation of functions and clearer chains of authority

3. Defining "State Within a State" in Institutional Terms
3.1 Parallel diplomacy: liaison networks and unofficial foreign policy
3.2 Parallel military capacity: covert force as a policy instrument
3.3 Parallel bureaucracy: budgets, proprietary assets, and internal logistics
3.4 Parallel legitimacy: secrecy narratives that substitute for public consent

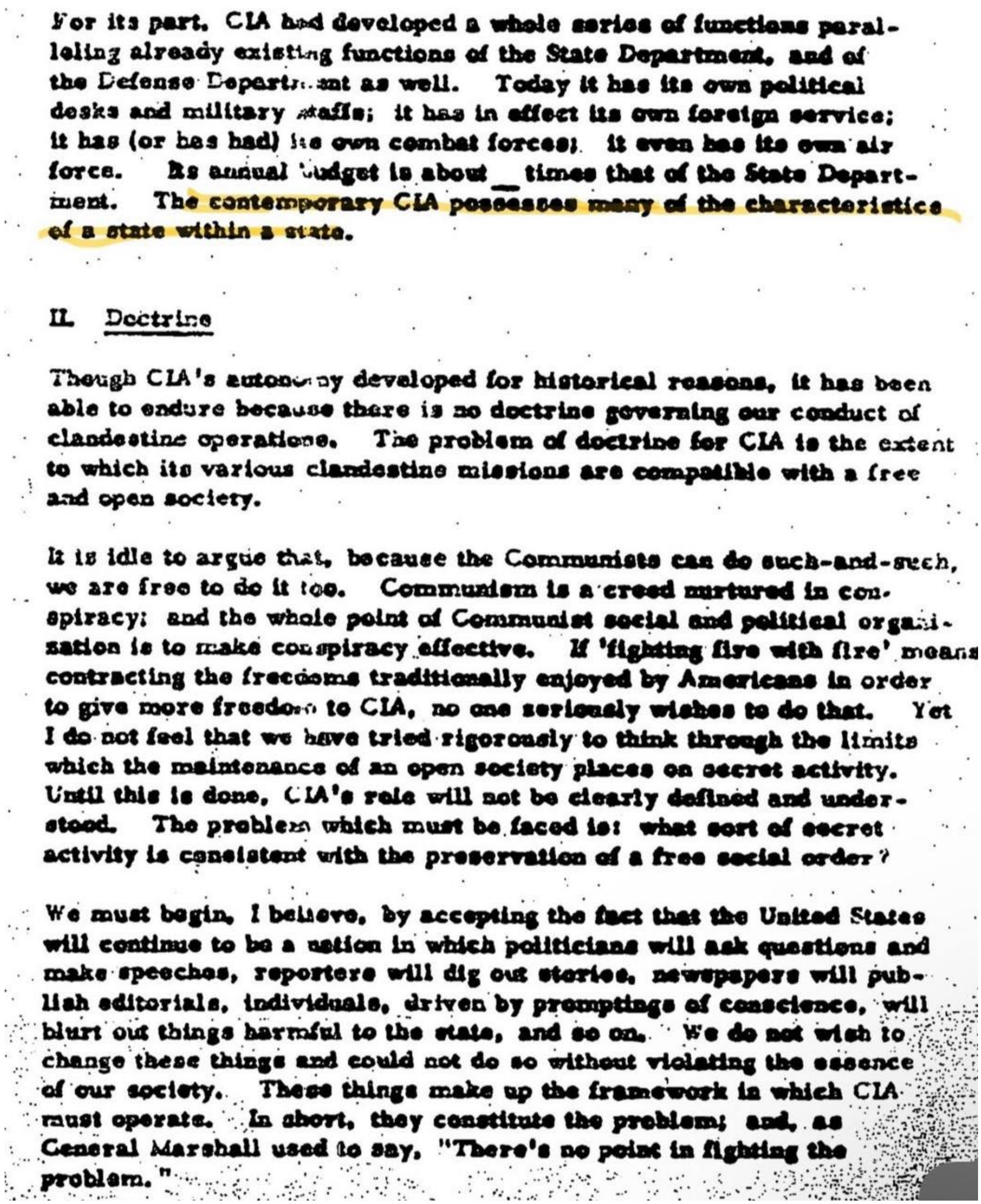
4. Why Covert Institutions Drift Toward Autonomy
4.1 Incentives: operational wins vs. strategic alignment
4.2 Information asymmetry: who knows what, when, and at what granularity
4.3 Speed mismatch: covert tempo vs. deliberative governance
4.4 Secrecy as organizational gravity: classification expanding by default
4.5 Career ecology: prestige, risk, and the romance of clandestinity

5. The Bay of Pigs as a Case Study in Governance Failure
5.1 Planning dynamics: optimistic assumptions and siloed evaluation
5.2 The role of plausible deniability in distorting decision-making
5.3 Civilian leadership failure modes: deference, ambiguity, and crowding out
5.4 After-action lessons: what reforms tried to correct (and what they didn't)

6. Analysis vs. Action: The Structural Tension
6.1 When the same institution collects, analyzes, and executes
6.2 Politicization pathways: serving policy vs. shaping policy
6.3 The epistemic hazard: "classified confidence" as an authority substitute
6.4 Institutional separation: benefits, risks, and historical attempts

7. Oversight in a World Designed to Resist Oversight
7.1 Executive oversight: principals, deputies, and the problem of bandwidth
7.2 Congressional oversight: secrecy constraints and capture risks
7.3 Judicial oversight: limits of adversarial review in national security

1. Introduction: The Phrase That Refuses to Die



For its part, CIA had developed a whole series of functions paralleling already existing functions of the State Department, and of the Defense Department as well. Today it has its own political desks and military staffs; it has in effect its own foreign service; it has (or has had) its own combat forces; it even has its own air force. Its annual budget is about __ times that of the State Department. The contemporary CIA possesses many of the characteristics of a state within a state.

II. Doctrine

Though CIA's autonomy developed for historical reasons, it has been able to endure because there is no doctrine governing our conduct of clandestine operations. The problem of doctrine for CIA is the extent to which its various clandestine missions are compatible with a free and open society.

It is idle to argue that, because the Communists can do such-and-such, we are free to do it too. Communism is a creed nurtured in conspiracy; and the whole point of Communist social and political organization is to make conspiracy effective. If 'fighting fire with fire' means contracting the freedoms traditionally enjoyed by Americans in order to give more freedom to CIA, no one seriously wishes to do that. Yet I do not feel that we have tried rigorously to think through the limits which the maintenance of an open society places on secret activity. Until this is done, CIA's role will not be clearly defined and understood. The problem which must be faced is: what sort of secret activity is consistent with the preservation of a free social order?

We must begin, I believe, by accepting the fact that the United States will continue to be a nation in which politicians will ask questions and make speeches, reporters will dig out stories, newspapers will publish editorials, individuals, driven by promptings of conscience, will blurt out things harmful to the state, and so on. We do not wish to change these things and could not do so without violating the essence of our society. These things make up the framework in which CIA must operate. In short, they constitute the problem; and, as General Marshall used to say, "There's no point in fighting the problem."

Figure 1. Arthur Schlesinger's 1961 Warning to JFK.

The phrase “a state within a state” persists because it names a structural anxiety that never fully expires in a constitutional republic: the fear that a necessary instrument of security can evolve into an instrument of governance that answers primarily to itself. Unlike ordinary bureaucracies, clandestine institutions are built to conceal intentions, methods, budgets, and even chains of responsibility. That concealment can be justified in narrow tactical contexts, but it becomes politically radioactive when secrecy begins to function as a substitute for authorization, and when operational capability becomes a form of policy initiative rather than policy execution. The power of Schlesinger’s line is that it compresses this entire tension into a single diagnosis. It also remains usable across decades because it does not depend on one scandal, one director, or one administration. It points to a repeating pattern: covert organizations grow by accretion of functions; they normalize exceptional authorities; they develop internal cultures of mission-first loyalty; and they can outpace the slower, more transparent institutions meant to define national purpose—diplomacy, law, and public deliberation.

This paper begins with the sober possibility that the phrase is neither a conspiracy trope nor a timeless truth, but a recurrent risk condition: a recognizable configuration of incentives, authorities, and information asymmetries that can arise whenever clandestine capacity expands without matching doctrinal clarity and effective oversight. The point is not to treat the CIA as uniquely malignant, nor to indulge romantic fear of “shadow government,” but to take Schlesinger’s warning seriously as a governance problem: how to preserve the advantages of secrecy without granting secrecy the right to rule.

1.1 The 1961 moment: Bay of Pigs and institutional shock

The Bay of Pigs failure did more than embarrass a new president; it produced an institutional shockwave. It exposed a gap between what elected leadership thought it was approving and what the operational apparatus had built, planned, and psychologically committed itself to delivering. In the aftermath, the usual bureaucratic defenses—“we acted under pressure,” “the intelligence picture was uncertain,” “the adversary responded unexpectedly”—could not fully explain the core issue Kennedy and his inner circle confronted: the operational pipeline had achieved a momentum that constrained political choice. This is one of the most important dynamics in covert action: once a plan exists, once assets are in motion, once a network has been activated, the cost of stopping becomes politically and morally rebranded as weakness, betrayal, or waste. The program itself begins to generate its own necessity.

Schlesinger’s memo arrives inside that moment of disillusionment. It is not a philosophical essay written in calm; it is a governing memo written under pressure, aimed at preventing recurrence. The shock was not merely “the CIA failed.” The shock was the discovery that an intelligence service could become a quasi-independent foreign-policy engine—capable of conceiving, preparing, and pushing action—while the constitutional institutions designed to authorize and coordinate policy struggled to keep pace. In that frame, Bay of Pigs becomes emblematic less because of its tactical mistakes than because it dramatized the deeper problem: clandestine capability is not neutral. It tends to pull decision-making into its orbit, because it offers tools that feel decisive, fast, and deniable—precisely the qualities that tempt leaders during crises.

So the 1961 moment is best understood as a collision between two tempos: the tempo of covert action (fast, compartmented, operationally confident) and the tempo of democratic governance (slow, argumentative, constrained by law and legitimacy). Bay of Pigs forced Kennedy's team to ask whether the nation had accidentally created an institutional structure that could partially escape the normal disciplines of coordination, accountability, and strategic coherence. The question was not, "Do we need intelligence?" but "What is intelligence for, and what must it never become?"

1.2 "State within a state" as diagnosis, not slogan

Used as a slogan, "state within a state" degenerates quickly. It becomes either a rhetorical club—proof of villainy—or a theatrical flourish—proof of sophistication. Either way, it stops doing analytic work. Used as a diagnosis, it becomes precise: it refers to a configuration in which an agency (a) accumulates capacities that replicate core functions of statecraft, (b) operates with weak external constraint because of secrecy and information asymmetry, and (c) develops internal momentum that can initiate or shape policy rather than merely implement it.

In this diagnostic sense, Schlesinger's phrase is not an accusation of treason. It is a warning about institutional architecture. A "state" is not only a set of people; it is a set of powers: diplomacy, force, finance, narrative, and administration. When a clandestine service develops its own "foreign service" (liaison networks and covert channels), its own "military staffs" (planning cells), its own "combat forces" (paramilitary capability), and its own quasi-independent budgetary ecosystem, it begins to resemble a parallel statecraft apparatus—especially if it can act with minimal friction from the institutions nominally responsible for policy. The phrase becomes even sharper when "plausible deniability" enters the picture. Deniability can be used to protect legitimate operations; it can also be used to dissolve responsibility, creating a structure in which power can be exercised without clear ownership.

Calling this a diagnosis also forces an honest concession: the same features that enable "runaway" autonomy also enable legitimate effectiveness. The ability to move quietly, to coordinate internationally, to act rapidly, to protect sources and methods, to operate behind adversary lines—these are not pathologies in themselves. They become pathologies when they are untethered from a coherent doctrine, a clear chain of authority, and enforceable oversight. A diagnostic approach therefore avoids two simplistic errors: demonizing clandestine capacity as inherently illegitimate, or sanctifying it as inherently necessary. It treats the risk as contingent and correctable.

This paper will repeatedly ask a disciplined version of the question: what exactly would have to be true, institutionally, before the “state within a state” label becomes warranted? And conversely, what safeguards and structures meaningfully prevent that drift without hollowing out the intelligence mission?

1.3 Scope and method: what this paper will and will not claim

This paper is a governance analysis anchored in Schlesinger’s 1961 warning, not an attempt to prove a master narrative of secret omnipotence. It will not claim that the CIA “runs America,” that elected officials are mere puppets, or that covert action explains all major events. Such claims are usually unfalsifiable and often function as story comfort rather than analysis. The paper also will not treat the CIA as uniquely prone to these dynamics; any clandestine apparatus—domestic or foreign, intelligence or special operations—can drift toward parallel sovereignty if its authorities expand faster than its constraints.

What the paper will do is narrower and, for that reason, more testable. It will (a) define “state within a state” as a set of institutional properties rather than a mood, (b) use the Bay of Pigs aftermath as a revealing case of misalignment between covert machinery and democratic decision-making, (c) examine structural drivers of autonomy—information asymmetry, tempo mismatch, incentive gradients, bureaucratic empire-building, and classification gravity, and (d) evaluate oversight and reform options in terms of mechanisms rather than intentions.

Methodologically, the paper relies on a small set of disciplined moves. First, it treats primary documents as anchors for the problem statement, using Schlesinger’s memo as a baseline articulation of the risk as seen from inside the executive branch. Second, it treats history as a set of recurring patterns rather than a single morality play: “what happened” matters, but “what repeats” matters more for governance design. Third, it distinguishes three categories that are often blurred in public debate: intelligence collection and analysis (epistemic work), covert action (instrumental work), and policy (normative and strategic choice). Much of the “state within a state” worry comes from confusing these categories or allowing them to merge without explicit authorization.

Finally, the paper adopts a deliberate restraint: it aims to show how a free society can maintain clandestine tools while refusing clandestine sovereignty. It does not require angelic leaders to work. It assumes ordinary human incentives, institutional self-interest, political pressure, and the constant temptation to solve complex problems with deniable force. If those conditions are permanent, then the only serious question is whether the architecture of oversight, doctrine, and accountability is equally permanent—or whether it remains episodic, activated only after failure. This introduction sets the frame: Schlesinger's phrase refuses to die because the underlying problem keeps being reborn.

2. What Schlesinger Actually Meant

Schlesinger's memo is often invoked as if it were a dramatic denunciation—an early "deep state" manifesto. It isn't. It reads more like a sober internal diagnosis written by someone who accepts the necessity of intelligence but fears what happens when a clandestine instrument begins to behave like a policy engine. The key is to notice how concrete his language is. He does not argue in abstractions about "secrecy" or "power." He itemizes functions—desks, staffs, services, forces, budgets—and then draws a constitutional conclusion: the CIA had begun to resemble a parallel apparatus of statecraft. "State within a state" is therefore shorthand for functional duplication plus weak coordination. It is an organizational warning: the United States had inadvertently created a second foreign-policy machine, with its own channels, incentives, and momentum, operating beside (and sometimes ahead of) the institutions designed to define national purpose.

He also frames the issue as doctrinal. The problem is not simply that covert action exists, but that it exists without an agreed doctrine of limits consistent with a free society. In other words, if clandestine operations are an exceptional tool, there must be an exceptional discipline governing them—clear criteria for when they are used, who authorizes them, who monitors them, how blowback is assessed, and what is off-limits even when it "works." Schlesinger's anxiety is that autonomy had been normalized as routine, and routine autonomy is how parallel sovereignty grows.

2.1 Parallel capabilities: political desks, foreign service, paramilitary reach

Schlesinger's most arresting move is simply to list what the CIA had come to resemble. In his view, the Agency had developed "political desks" and "military staffs" parallel to State and Defense; it had, "in effect," its own "foreign service"; it had its own "combat forces" and even an "air force." The point is not that CIA officers literally replaced ambassadors or fielded conventional divisions. The point is that CIA had assembled the functional equivalents: country-centered planning units, overseas networks and liaison relationships, training and logistics pipelines, and operational assets capable of coercion, sabotage, and paramilitary action.

Why does this matter? Because foreign policy is not just analysis; it is a choreography of commitments, signals, negotiations, and constraints. When an agency can run covert channels that diplomats do not control, it can generate commitments abroad that the formal government later inherits—sometimes without knowing it. Liaison relationships with foreign security services can become a shadow foreign policy of their own: favors, information exchanges, training ties, and shared operations that bind the United States to partners and tactics that may not match declared policy. These relationships can also create a “dual loyalty” trap: field officers may feel responsible to protect the liaison relationship even when it conflicts with the political leadership’s current priorities.

Paramilitary reach intensifies the problem because violence is not just another tool; it is a political act with consequences that radiate outward. Once a clandestine organization can train, arm, transport, and deploy proxies—or run direct action capabilities—it moves from observing the world to reshaping it. That shift is not inherently illegitimate; states sometimes need it. But it changes governance requirements. You do not supervise an organization that can use force the same way you supervise an organization that writes memos. Parallel capability implies parallel risk: parallel diplomacy can create parallel commitments; parallel force can create parallel wars; parallel budgets can create parallel discretion; parallel secrecy can create parallel legitimacy claims (“you can’t understand; it’s classified”).

Schlesinger’s phrase “state within a state” is thus not a metaphysical claim. It is a functional claim: when the CIA possesses enough of the state’s classic instruments—information, influence, force, overseas networks, and resources—it begins to look like a second center of gravity in foreign affairs.

2.2 Autonomy by accumulation: missions that expand faster than doctrine

A second theme in Schlesinger’s memo is that autonomy did not arise from a single coup-like moment. It emerged by accumulation. Agencies rarely announce, “We are now sovereign.” They accumulate new responsibilities because each new responsibility is justified by a real problem. One operation creates a new network; the network creates new opportunities; the opportunities create new missions; the missions create a need for new staff; the staff create a need for new budgets and internal processes; and soon the organization has built an ecosystem that feels “necessary” regardless of whether it remains aligned with national strategy.

This is the logic of mission creep, but in clandestine form it has special accelerants. Secrecy reduces friction. If the details of programs cannot be widely shared, fewer actors can meaningfully object, compare alternatives, or measure costs. Classification also complicates learning: failures can be hidden, and “success” can be asserted without independent verification. In that environment, organizations tend to define success operationally—assets recruited, actions taken, disruptions achieved—rather than strategically—diplomatic outcomes improved, adversary behavior changed in durable ways, long-term legitimacy preserved.

Schlesinger’s point about doctrine is central here. Accumulation is not automatically bad; the world changes. But accumulation without doctrine is dangerous because it produces a capability-supply dynamic: the organization tends to use the tools it has, and the existence of tools becomes an argument for their use. Doctrine is supposed to reverse that polarity. Doctrine says: we are not defined by what we can do; we are defined by what we are authorized to do under explicit limits, for explicitly bounded purposes, with explicit accountability. Without doctrine, "can" slowly masquerades as "should."

Schlesinger's underlying worry is that CIA autonomy had become self-sustaining. Once an organization can plan operations, control channels, allocate funds, and manage proprietary assets, it becomes resilient against external correction. It can outlast administrations because its internal continuity is stronger than political cycles. "Autonomy by accumulation" is the mechanism by which a covert capability becomes a semi-permanent political fact.

2.3 The "rubber stamp" problem: when State becomes downstream

Schlesinger's most politically sensitive claim is not that CIA had power, but that CIA had begun to distort the policy process. He warns that clandestine operations could drive foreign policy while State, formally responsible for diplomacy, became a "rubber stamp." This is a diagnosis of sequencing: policy should set operations, but operations were beginning to set policy.

How does that happen in practice? Often through path dependency. A clandestine initiative begins in a compartmented channel. It produces facts on the ground: assets recruited, local partners promised support, covert commitments made. When the initiative is finally briefed up the chain, the decision is no longer a clean "whether." It becomes a messy "how to manage what is already underway." State then enters not as architect but as negotiator of consequences. Diplomats are asked to rationalize, smooth, or "message" a covert reality that they did not design and may not even agree with. The public line becomes disconnected from the operational line, and the cost is paid in credibility—both with allies and with adversaries.

A second mechanism is asymmetrical information. The CIA may possess granular situational awareness through sources and liaison ties that State lacks. That can create genuine dependency: policymakers may feel they cannot challenge the operational frame because they cannot see the full picture. But it can also create an authority illusion: "They know more; therefore they should decide." That is the exact inversion democratic governance must resist. In a healthy system, better information informs decisions; it does not entitle the holder of information to become the decision-maker.

A third mechanism is the deniability temptation. Covert action offers leaders the chance to "do something" without the costs of open commitment. That can seduce political leadership into treating covert action as a default policy lever. Once that happens, State is inevitably downstream, because diplomacy is a public instrument and covert action is designed to evade public scrutiny. The foreign policy process becomes lopsided: covert instruments dominate because they seem cheaper politically, even if they are expensive strategically.

Schlesinger's "rubber stamp" warning is therefore about institutional dignity and constitutional order. It says: diplomacy cannot be reduced to damage control for clandestine choices. State must not become a communications department for covert action. If it does, the United States ends up with two foreign policies—one stated, one enacted—and that divergence is corrosive over time.

2.4 Early reform instincts: separation of functions and clearer chains of authority

Schlesinger does not merely complain; he proposes structural remedies that reveal what he thought the real disease was. His instincts point in two directions: clarify the chain of authority, and disentangle functions that create self-justifying power loops.

First, clearer chains of authority. If covert operations touch foreign policy, then the institutions responsible for foreign policy must have meaningful clearance authority, not mere consultation. Schlesinger's reforms aim to ensure that clandestine activity does not become a separate lane of policy-making. In practical terms, this means moving from "FYI" briefings to genuine gatekeeping: written approvals, explicit policy alignment checks, and enforceable stop-power held by accountable principals.

Second, separation of functions. Schlesinger suggests reorganizing so that the collection and analysis mission is not structurally fused to the operational mission in a way that allows action to colonize knowledge. When the same institution is responsible for intelligence estimates and for covert action, it faces a temptation: interpret information in ways that support ongoing operations, protect sources, or justify continuation. Even when no one acts in bad faith, the organizational incentives bend toward coherence-with-self. Splitting analysis from operations is a way to preserve epistemic independence—so that intelligence can contradict operational optimism, and so that policymakers can receive assessments not subtly shaped by operational commitments.

There is also a third, quieter instinct in Schlesinger: normalize dissent and reduce the aura of clandestine inevitability. A healthy chain of authority is not only vertical; it is also lateral. It requires structured disagreement—red teams, alternative analyses, and institutional permission to say "no" when momentum is pushing toward "yes." Reform, in this view, is not a one-time reorg chart. It is an institutional constitution: a set of durable procedures that slow the drift toward parallel sovereignty.

Schlesinger's proposals were early, imperfect, and shaped by the moment. But they remain conceptually sharp. They begin with the premise that clandestine power must be governable. If it cannot be governed, it is not an instrument of the republic; it is a rival. The phrase "state within a state" therefore points less to paranoia than to architecture: when functions, secrecy, and incentives align in a certain way, autonomy becomes predictable. Schlesinger's real meaning is a warning about that predictability—and an insistence that the United States can choose design over drift.

3. Defining "State Within a State" in Institutional Terms

If "state within a state" is treated as a mystical accusation, it becomes useless: it floats above evidence, immune to refutation, and easily repurposed as propaganda. To make the phrase analytically meaningful, it must be translated into institutional properties—observable features of organization, authority, and incentive. In this paper, "state within a state" refers to a condition in which a sub-governmental entity acquires enough *state-like* functions, resources, and autonomy that it can (a) initiate or steer consequential policy outcomes, (b) maintain operational continuity independent of political cycles, and (c) defend itself against correction through secrecy, complexity, and dispersed accountability.

This is not a binary label; it is a spectrum condition. Many agencies possess some degree of specialized discretion. The "state within a state" risk emerges when discretion becomes *self-authorizing* in practice—when an institution's internal logic begins to determine what is done, while external institutions become reactive rather than directive. The diagnostic question is therefore not "Does the agency have secrets?" but "Does it possess parallel instruments of statecraft, plus the ability to deploy them with insufficient external friction?" The four components below—parallel diplomacy, parallel military capacity, parallel bureaucracy, and parallel legitimacy—turn the phrase into a working model.

3.1 Parallel diplomacy: liaison networks and unofficial foreign policy

Parallel diplomacy exists when an intelligence service's overseas relationships and channels begin to function as an alternative foreign ministry—sometimes complementary, sometimes competitive, and sometimes contradictory to declared policy. The classic form is liaison: ongoing relationships with foreign intelligence and security services that involve information sharing, training, joint operations, and mutual favors. Liaison is often necessary; it can be one of the fastest ways to understand adversaries and to prevent attacks. But liaison also creates an unofficial foreign policy because relationships generate obligations. A favor extended today becomes a request tomorrow. A joint operation creates shared secrets. Shared secrets create mutual vulnerability. Mutual vulnerability creates pressure to preserve the relationship even when politics shift.

Parallel diplomacy also arises through backchannels—communications that bypass normal diplomatic routing. Backchannels are sometimes legitimate tools of crisis management. The risk appears when backchannels become the *primary* channels, and when they are used not merely to transmit messages but to shape outcomes that the formal diplomatic apparatus has not authorized. In that configuration, the intelligence service is no longer supporting policy; it is running a policy track.

Several institutional mechanisms make parallel diplomacy resilient. First is compartmentation: State may not know the details of liaison arrangements, or may know them only after they have matured. Second is specificity: the intelligence service may hold granular knowledge about local actors, leverage points, and vulnerabilities that diplomats lack, which can tempt policymakers to treat the clandestine channel as the "real" channel. Third is deniability: leaders may prefer unofficial engagement because it reduces public and congressional visibility. Over time, preference becomes habit, and habit becomes structure.

A practical diagnostic indicator is *sequencing*. If diplomatic strategy is being formulated and then intelligence channels are being tasked to support it, the relationship is healthy. If intelligence channels are generating commitments and facts on the ground that diplomacy later must manage, the relationship has inverted. Inversion is the hallmark of parallel diplomacy: State becomes downstream, negotiating the consequences of commitments made elsewhere.

3.2 Parallel military capacity: covert force as a policy instrument

Parallel military capacity exists when an intelligence service can apply organized force—directly or through proxies—in ways that function as a de facto instrument of national policy. This includes paramilitary units, training of partner forces, provision of weapons and logistics, sabotage, and kinetic operations conducted under clandestine authorities rather than conventional military command. The argument for such capacity is straightforward: some problems require tools that are precise, deniable, and adaptable; some environments are politically impossible for overt deployments; and some threats are asymmetric.

The governance risk is that force, once available, becomes policy-shaped rather than policy-serving. Covert force can seem like an elegant shortcut around the slow burdens of diplomacy and public debate. It creates a false economy: low visibility is mistaken for low cost. Yet covert force generates long-tail liabilities—blowback, partner atrocities, escalation spirals, compromised legitimacy, and strategic entanglements that surface later as "unexpected" crises. The more frequently covert force becomes the default response, the more it substitutes for coherent statecraft.

Institutionally, parallel military capacity is marked by three features. First, *deployability*: the organization can plan and execute operations without relying entirely on Defense's command structure. Second, *sustainment*: it can fund, arm, train, and supply activities over time, not merely conduct one-off missions. Third, *policy leverage*: its operational proposals can create pressure on leaders because "the assets are in place," "the window is closing," or "our people will be exposed if we stop." This is a specific kind of momentum: not merely bureaucratic inertia, but a coercive time pressure generated by the existence of clandestine force readiness.

A "state within a state" condition emerges when covert force is effectively insulated from the same clarity of doctrine and chain-of-command discipline expected of overt force. The military has publicly legible doctrines, laws of armed conflict frameworks, command responsibility norms, and formalized oversight. Covert force can blur those lines by operating under different legal authorities, different reporting regimes, and different cultural expectations. When the rule-set is fragmented, accountability diffuses, and policy control weakens.

3.3 Parallel bureaucracy: budgets, proprietary assets, and internal logistics

A state is not just diplomacy and force; it is also administration. Parallel bureaucracy exists when an agency develops internal resource systems—budgets, proprietary companies, logistics pipelines, contracting ecosystems, facilities, and transport—that make it operationally self-sufficient and politically durable. This is the least cinematic aspect of the "state within a state" idea, but it may be the most decisive. If you want to understand autonomy, follow the money and the supply chain.

Classified budgets create a special kind of insulation. Secrecy can be necessary to protect sources and methods, but it also reduces comparative scrutiny: it becomes hard to ask whether a given program is duplicative, whether its benefits justify its costs, or whether it is quietly expanding beyond intent. Proprietary assets and contractors can amplify this by creating semi-private structures with opaque incentives. Programs can take on an economic life: jobs, contracts, and regional dependencies that generate political constituency, even when the underlying mission is contestable. Autonomy then becomes not merely organizational but political: external actors come to depend on the agency's spending and presence.

Internal logistics further strengthen the parallel bureaucracy. When an agency can move people and equipment, maintain secure communications, sustain overseas infrastructure, and operate proprietary cover mechanisms, it reduces reliance on other departments. Reduced reliance reduces interagency veto power. The more self-sufficient the organization becomes, the more it can act quickly and quietly—and the less it is forced into coordination routines that bring sunlight and friction.

From an institutional standpoint, the "state within a state" condition is strongly correlated with *resource discretion*. The ability to allocate funds and assets with limited external visibility is not merely a budget matter; it is a governance matter. It determines whether the leadership of the agency can, in practice, set priorities without meaningful external contestation. A state-like bureaucracy is one that can finance itself, staff itself, and sustain itself across administrations with minimal reauthorization stress. That durability is valuable for intelligence continuity, but it becomes dangerous when combined with mission creep and weak doctrine.

3.4 Parallel legitimacy: secrecy narratives that substitute for public consent

The deepest dimension of “state within a state” is not operational; it is political. Parallel legitimacy exists when secrecy becomes a substitute for consent—when an institution’s claim to authority rests less on public authorization and more on internal narratives like “trust us,” “you can’t understand,” “it’s too sensitive,” or “questioning harms national security.” These narratives may sometimes be sincerely true at the tactical level. The danger is when they become generalized, turning classification into a kind of epistemic crown: those who know secret things are treated as entitled to decide.

Parallel legitimacy has multiple forms. One is *sacralization of secrecy*: secrecy becomes a moral identity rather than a tool. Another is *threat inflation*: because danger is always imaginable, exceptional measures become normalized. A third is *role confusion*: operational competence is treated as moral authority, and access to classified information is treated as strategic wisdom. A fourth is *accountability inversion*: oversight is framed as interference, and criticism is framed as disloyalty.

This creates a paradox in democratic governance. Intelligence agencies must protect secrets to function. But democracies must preserve the right of legitimate authority to inquire, to constrain, and to refuse. When secrecy narratives harden, the agency becomes politically insulated not only from the public but from the elected branches themselves. The institution begins to occupy an “untouchable” zone in which normal accountability is taboo.

In the “state within a state” spectrum model, parallel legitimacy is what makes the other parallels durable. Parallel diplomacy can be corrected if policymakers insist on coordination. Parallel military capacity can be corrected if legal authorities and reporting are tightened. Parallel bureaucracy can be corrected if budgets and programs face disciplined review. But if secrecy itself has become an unchallengeable source of legitimacy, correction becomes culturally and politically difficult. The agency is no longer merely secret; it is sovereign in the only way that finally matters: it can claim a right to act without being meaningfully questioned.

This is why Schlesinger’s warning still resonates. “State within a state” is not a claim that hidden hands control everything. It is a claim about institutional drift: when parallel instruments of statecraft converge with secrecy-based legitimacy, a republic can quietly acquire a second, partially autonomous operating system. The rest of this paper treats that drift as an engineering problem of governance: identify the mechanisms that create it, and design the counter-mechanisms that prevent it—without pretending that the world allows a naive abandonment of clandestine tools.

4. Why Covert Institutions Drift Toward Autonomy

A covert institution does not have to "go rogue" to drift toward autonomy. Drift is the normal outcome of ordinary organizational forces operating inside an unusual environment: secrecy, urgency, high stakes, and limited external visibility. If you combine (a) tools capable of changing events, (b) information that few can verify, (c) a tempo that outruns oversight, and (d) cultures that treat discretion as virtue, you should expect a predictable tendency: the institution will begin to govern itself. The relevant question is therefore not whether clandestine organizations contain bad actors (they will, as any large institution does), but whether the architecture of incentives and constraints reliably produces alignment with declared policy over long time horizons.

This section treats autonomy drift as an institutional physics problem. The key drivers—operational incentive gradients, information asymmetry, tempo mismatch, classification gravity, and career ecology—do not require conspiracy. They require only competence, pressure, and the human desire to be effective. That is what makes the drift both understandable and dangerous: it can be fueled by good intentions, professional pride, and genuine threat perception.

4.1 Incentives: operational wins vs. strategic alignment

Covert organizations are naturally rewarded for what they can count. Operational outcomes are countable: assets recruited, networks built, missions executed, targets disrupted, adversary plans penetrated, leaders influenced, defections induced. Strategic alignment is harder to count. It involves counterfactuals and long arcs: Did this action improve the diplomatic landscape five years later? Did it reduce hostility or merely defer it? Did it strengthen alliances or quietly corrode trust? Did it deter adversaries or teach them new tactics? Did it protect civilians or generate grievances that become future threats?

When the measurable dominates the meaningful, organizations optimize for the measurable. This is a generic bureaucratic truth, but secrecy intensifies it because measurement itself is partly private. A covert institution can certify its own success in ways external reviewers cannot easily audit. The internal scoreboard becomes the real scoreboard.

This incentive gap produces a classic misalignment: operational wins can be strategically costly. A covert action may neutralize a short-term threat but undermine long-term legitimacy. It may remove one adversary but generate many more. It may strengthen a partner force that later becomes predatory. It may create a "clean" solution for leadership but leave diplomacy with a poisoned residue. In such cases, the covert institution can still experience the outcome as success because its internal metrics reward the action itself, not the strategic consequences diffused across the broader state.

Autonomy drift follows. When an organization believes its operational success is the nation's success, it begins to treat external constraint as obstruction. Coordination becomes a delay mechanism. Diplomatic caution becomes naivete. Oversight becomes political meddling. The institution's self-conception shifts from "instrument" to "guardian." And when an institution sees itself as guardian, it begins to assume it has the right to decide.

4.2 Information asymmetry: who knows what, when, and at what granularity

Covert institutions live inside information asymmetry by design. They collect sensitive information; they protect sources and methods; they compartment operations. This is not a flaw—it is a functional requirement. But it creates a governance hazard: those with information can shape decisions not merely by informing leaders, but by framing reality, controlling what is salient, and managing what remains unseen.

The asymmetry has three dimensions.

First is *timing*. The covert institution often knows earlier: it sees threats, opportunities, vulnerabilities before others do. Early knowledge tends to translate into agenda-setting power. The first frame of a problem often becomes the default frame.

Second is *granularity*. A covert institution may know details that dramatically change how a decision should be made. But granularity can also be weaponized, intentionally or unintentionally. Leaders can be overwhelmed by detail and then defer to those who "really understand." This deferral is rational at the micro-level but corrosive at the macro-level: "they know more" becomes "they should decide."

Third is *verifiability*. Much intelligence cannot be publicly tested. Even within government, it may not be shareable widely. Oversight bodies may be structurally incapable of verifying the operational claim without jeopardizing sources. That creates a special authority effect: classified information becomes a credential that substitutes for evidence. It becomes difficult to disagree without appearing ignorant.

Information asymmetry therefore produces a subtle autonomy mechanism: decision-making migrates toward the locus of knowledge. This can happen even when leaders remain formally in charge. In practice, choices become bounded by what the covert institution presents as possible, urgent, and feasible. The institution gains not only "input" power but "menu" power: it determines what options are on the table.

4.3 Speed mismatch: covert tempo vs. deliberative governance

Democratic governance is slow because it is meant to be slow. It must weigh legal authority, political consequences, moral constraints, alliance commitments, and public legitimacy. It must consult, argue, and document. It must coordinate across institutions that were deliberately designed not to be perfectly efficient, because unchecked efficiency is the pathway to unaccountable power.

Covert operations, by contrast, are rewarded for speed. They exploit fleeting windows. They depend on surprise. They are often opportunistic: assets appear, vulnerabilities open, adversaries move. Delay can kill the operation. So the covert institution develops a tempo optimized for rapid action under uncertainty.

When these tempos collide, the covert tempo tends to win, because crises and opportunities do not wait for committee process. Leaders feel forced into compressed decisions. The institution that can act quickly becomes the institution that defines reality. In effect, tempo becomes authority.

This is one reason Bay of Pigs is archetypal: once a covert operation reaches a certain stage of readiness, leaders are no longer choosing among abstract policy alternatives. They are choosing whether to stop a moving train. Stopping the train requires political and psychological strength; allowing it to proceed feels like "letting the professionals do their job." The speed mismatch turns procedural caution into a kind of betrayal. And that is how autonomy grows: the institution can make itself difficult to stop by constructing situations in which stopping is socially and politically expensive.

Speed mismatch also undermines oversight because oversight requires time to read, question, and compare. If operational tempo routinely compresses decision windows, oversight becomes ceremonial. Briefings happen after the fact. The oversight body hears about the operation when the institution is already committed. This converts oversight into narrative management rather than control.

4.4 Secrecy as organizational gravity: classification expanding by default

Secrecy is not static; it has a natural expansion bias. Classification behaves like organizational gravity: it tends to pull more material into its orbit over time. There are obvious reasons for this. If a piece of information is classified, then anything that reveals it, refers to it, or is connected to it becomes "derivative classification." Operational details connect to other details. Networks connect to other networks. Budgets reveal capabilities. Names reveal cover. Methods reveal vulnerabilities. The logic of protection spreads.

But beyond this technical spread, there is an institutional incentive spread. Classification reduces accountability risk. It lowers external friction. It protects careers. It prevents embarrassment. Even without malicious intent, people classify broadly because the cost of under-classifying can be severe, while the cost of over-classifying is diffuse and rarely punished. This creates a one-way ratchet.

As classification expands, three consequences follow.

First, coordination becomes harder because fewer people can know enough to coordinate meaningfully. That increases the institution's independence: it becomes the only actor that can see the whole picture.

Second, oversight becomes weaker because fewer overseers can access full context, and because the institution can always appeal to source protection as a limit on disclosure.

Third, legitimacy becomes internal: the institution begins to live inside a sealed epistemic environment where its own narratives dominate. If you cannot be contradicted by external evidence, you become less corrigible. Over time, secrecy can reduce an organization's ability to self-correct because dissent is harder to surface and because external critique is structurally excluded.

This is why "classification gravity" is not merely about documents; it is about power. Secrecy expands the institution's discretionary zone. The larger that zone, the easier autonomy becomes.

4.5 Career ecology: prestige, risk, and the romance of clandestinity

Finally, autonomy drift is fueled by the human ecology of clandestine work. Covert institutions do not just recruit skills; they cultivate identities. People who work in secrecy tend to develop a sense of exceptionalism. They know things others do not. They do work others cannot. They take risks others avoid. This can produce admirable courage and discipline. It can also produce insularity and moral licensing.

Prestige plays a role. In any bureaucracy, proximity to action confers status. Those who "run operations" can be seen as more real than those who "write policy" or "do analysis," even when the reverse should sometimes be true. This prestige gradient pulls ambitious careers toward operations and toward the expansion of operational remit. If influence within the institution is gained by running bigger, more daring missions, the institution will tend to generate bigger, more daring missions.

Risk also plays a role. Covert careers are structured around danger—physical danger, political danger, reputational danger. Shared risk produces tight bonds. Tight bonds produce loyalty. Loyalty can become a virtue that competes with legality and policy alignment. The instinct becomes: protect the team, protect the operation, protect the relationship. In that environment, external oversight can be experienced as betrayal rather than governance.

Then there is what might be called the romance of clandestinity: the narrative that secret action is the adult realm of history, where real power operates, while public discourse is theater. This romance is culturally reinforced by media, by internal lore, and by the psychological rewards of belonging to an invisible elite. Once that romance takes hold, democratic constraints can be reframed as childish. A covert institution begins to see itself as the keeper of reality. And when an institution sees itself as the keeper of reality, it becomes tempted to act as the author of reality.

This is not a moral condemnation of individuals. It is an institutional warning about identity formation under secrecy. Any organization that forms strong internal identity while being structurally insulated from external critique will drift toward self-justification. The people inside will increasingly confuse institutional success with national good, and institutional continuity with national security.

Taken together, these five forces explain why Schlesinger's phrase refuses to die. "State within a state" is not a one-time scandal descriptor; it is the predictable endpoint of a system where operational incentives, asymmetric knowledge, accelerated tempo, expanding secrecy, and romanticized identity are not matched by equally robust counter-forces—doctrine, clear authority, enforceable oversight, and cultural humility. The next sections turn from diagnosis to design: what oversight mechanisms and structural reforms can reliably interrupt this drift without disabling the intelligence function that the state still needs.

5. The Bay of Pigs as a Case Study in Governance Failure

Bay of Pigs is often narrated as a fiasco of tactics: the landing site, the intelligence errors, the air cover decisions, the assumption of an uprising that never came. Those details matter, but they can obscure the deeper lesson Schlesinger's warning is pointing toward. Bay of Pigs is a governance failure before it is a battlefield failure. It exposes what happens when covert operations become a semi-autonomous policy engine—when planning momentum outruns political deliberation, when secrecy and compartmentation prevent full adversarial scrutiny, and when civilian leadership experiences a moving covert plan as something they must "manage" rather than something they can still fundamentally refuse.

A governance failure is not simply "the wrong choice." It is a breakdown in the system meant to produce the right kind of choice: the procedures, checks, dissent channels, and interagency coordination that keep an instrument of the state from quietly becoming a driver of state action. Bay of Pigs is therefore useful not as an embarrassment, but as an anatomy lesson. It shows the mechanism by which a covert institution can deliver a plan that is operationally coherent inside its own worldview while being strategically incoherent in the broader national interest.

5.1 Planning dynamics: optimistic assumptions and siloed evaluation

Covert planning has a natural bias toward optimism, and Bay of Pigs displays this bias in its most consequential form. Operational plans require belief. They require a narrative that links means to ends through a chain of assumptions: the adversary will react in a certain way; local forces will behave predictably; secrecy will hold long enough; international response will be manageable; a triggering event will catalyze domestic support. When an organization is structured around action, it becomes psychologically and institutionally invested in its own chain of assumptions. Skepticism threatens momentum. Doubt feels like sabotage.

Siloed evaluation makes this worse. Compartmentation limits how many people can see the whole plan. Even within the same government, different actors are given different slices: some see logistics, some see intelligence, some see political messaging, some see diplomatic risk. The result is a fragmented critique. Each silo can identify issues in its domain, but few can assemble those issues into a decisive judgment about overall viability. The plan can therefore survive because no single critic has the standing or visibility to kill it.

This is not merely a procedural flaw; it is a structural feature of clandestine work. The same secrecy that protects sources and methods also prevents broad "red teaming." It prevents the kind of full-spectrum adversarial evaluation that open military planning, at its best, demands. In overt military operations, multiple staffs, allied partners, and institutional adversaries can interrogate assumptions. In covert operations, interrogation is often narrow, informal, and dependent on the courage of a few individuals.

Optimism also has a bureaucratic dimension: an operation that feels possible today can justify organizational resources tomorrow. Programs attract budgets, careers, and influence. A plan that "could work" becomes a plan that "should be tried," because trying itself sustains the operational enterprise. The institution becomes incentivized not only to plan well, but to keep planning—because the act of planning is part of its identity and legitimacy.

Bay of Pigs dramatizes the resulting failure mode: a plan that is internally persuasive can be externally disastrous. The system did not sufficiently force the planners to confront a hard question: what if the critical assumptions fail, and what will the United States then do? Governance failure appears when "what then?" is treated as a nuisance rather than as the center of the decision.

5.2 The role of plausible deniability in distorting decision-making

Plausible deniability is often presented as a technical legal-political concept: a way to protect leaders and preserve diplomatic flexibility. In practice, it is also a psychological and institutional solvent. It dissolves responsibility and clarity.

The distortion begins with framing. If an operation must remain deniable, then the overt instruments of statecraft—uniformed military force, open diplomatic signaling, public commitment—are constrained. The operation must be designed to look like something other than what it is. That constraint pushes planners toward indirect methods and fragile narratives. It also pressures leaders into half-commitments: enough support to enable the operation, but not enough visibility to own it. This creates the classic covert dilemma: the operation may require overt-scale resources to succeed, but overt-scale resources break deniability. The result is an underpowered operation—politically constrained from being fully supported, yet expected to achieve strategic outcomes.

Deniability also distorts decision quality by enabling self-deception. Leaders can entertain risky plans because the political downside appears containable: "If it goes wrong, we can deny it." But denial is rarely clean. Adversaries, allies, and publics infer involvement. The denial then becomes an additional liability: it forces the state into a posture of dishonesty or absurdity, undermining credibility when credibility is needed most. Deniability can therefore produce a hidden cost: it turns a failed operation into a credibility wound.

Most importantly, plausible deniability creates accountability diffusion inside the executive. If a plan must be deniable, it is often discussed in euphemisms. Formal documentation may be reduced. Chains of command may be blurred. People may be told enough to act but not enough to be responsible. This ambiguity is not always deliberate; it is a byproduct of secrecy discipline. But it produces a governance hazard: when no one can be clearly said to have authorized the decisive elements, correction becomes difficult and learning becomes shallow.

Bay of Pigs reveals plausible deniability as a structural temptation: it invites leaders to "act without owning." That is precisely the posture a constitutional system must treat with suspicion, because ownership is the foundation of accountability.

5.3 Civilian leadership failure modes: deference, ambiguity, and crowding out

Governance failure is never only the agency's fault. Bay of Pigs also reveals characteristic failure modes of civilian leadership when facing complex covert proposals.

The first is deference. New administrations inherit institutions with deep expertise and long continuity. A president and close aides can feel outmatched by seasoned operators who speak confidently in operational detail. Deference is not irrational; leaders must rely on experts. But deference becomes dangerous when expertise is mistaken for policy authority. "They can do it" silently becomes "they should decide it." In covert contexts, deference is amplified by information asymmetry: leaders may not see the full evidence, but they also cannot easily challenge it, because what they do not know is classified. The result is a subtle surrender of policy control: leadership becomes a consumer of plans rather than an author of strategy.

The second failure mode is ambiguity. Leaders sometimes want the benefits of covert action without the burdens of explicit choice. They may issue guidance that is intentionally vague, preserving flexibility and avoiding recorded commitment. But in practice, ambiguity is interpreted by operators as permission. Vague approval becomes operational green light. Once assets move, ambiguity becomes irreversibility. The plan takes on inertia, and leadership shifts from deciding to managing.

The third failure mode is crowding out. Covert action can dominate attention because it is dramatic, urgent, and action-oriented. Diplomacy is slower, less cinematic, and often ambiguous in its outcomes. In crisis, leaders may gravitate toward the lever that feels decisive. But when covert action crowds out diplomatic strategy, it can invert the relationship between instrument and purpose. Leaders begin to evaluate foreign policy in terms of what covert tools can do, rather than what the nation should seek. The tool becomes the frame.

Bay of Pigs shows how these failure modes can converge: deference to operational confidence, ambiguity in authorization, and the crowding out of diplomacy can produce a decision environment where the covert plan is treated as the default path—even if the strategic rationale is brittle.

A deeper point emerges here: civilian leadership must not only authorize; it must *govern the authorization process*. It must demand doctrine: What is the political end state? What are the assumptions? What are the failure branches? What is the escalation ladder? What will we do if the plan fails? How will we own consequences? If leadership does not enforce these questions, the system will supply action without sufficient strategy.

5.4 After-action lessons: what reforms tried to correct (and what they didn't)

The post–Bay of Pigs reform impulse tried to correct several governance defects: clarify authority, tighten coordination, and reduce unilateral operational momentum. Schlesinger's memo belongs to this impulse. It argues for curbing CIA's parallel statecraft tendencies and reasserting policy primacy—especially through stronger State involvement and clearer limits on clandestine initiatives.

Reforms aimed, implicitly, at four corrections.

First, improve interagency coordination so covert action would not run on a separate track. Second, strengthen accountability so that operations could not proceed on tacit momentum. Third, clarify the boundary between intelligence analysis and operational advocacy, reducing the temptation for an institution to sell its own plans using its epistemic authority. Fourth, create procedural disciplines—clear approvals, oversight routines, written findings—that make covert action harder to "slide into" without explicit ownership.

But the reforms also had limits, some structural and some political.

One limit is that reforms often occur after failure, not before drift. A fiasco creates political energy, but energy fades. As crises change and administrations turn over, urgency dissipates. Institutions then gradually re-accumulate capabilities and discretion because the world continues to supply reasons: new adversaries, new threats, new opportunities.

Another limit is that reforms rarely fully resolve the tempo mismatch. Even with better procedures, covert action will often demand speed. Oversight can be improved, but it is hard to make oversight as fast as operations without making oversight superficial.

A third limit is cultural. Organizational identity—prestige, secrecy romance, mission-first loyalty—cannot be reorganized away by charts. If covert culture rewards daring operations and regards policy constraints as naive, the drift will continue under new names.

A fourth limit is the deniability temptation itself. Leaders across parties and eras are drawn to covert options because they appear to offer control without cost. As long as political systems reward leaders for "doing something" while punishing them for openly owning hard tradeoffs, covert action will remain attractive. That attraction continually pressures the system back toward the same risky posture.

So Bay of Pigs offers a sobering lesson: governance reforms must be designed as *permanent counter-forces*, not episodic reactions. The "state within a state" risk cannot be eliminated by declaring good intentions. It is a dynamic that re-emerges whenever secrecy, speed, and operational capability outrun doctrine, oversight, and civic legitimacy. The after-action history shows that reforms can reduce harm, but they must be sustained institutionally and culturally—or drift resumes, and the next crisis becomes the next anatomy lesson.

6. Analysis vs. Action: The Structural Tension

The most important structural tension in intelligence is not secrecy versus transparency. It is *knowledge versus intervention*. Intelligence, at its best, is an epistemic discipline: it seeks to reduce uncertainty, clarify adversary intentions, and inform decisions. Covert action, by contrast, is an instrumental discipline: it seeks to change the world by manipulating events, influencing actors, or applying force under deniable authority. Both functions can be legitimate. The tension arises when they are fused inside one institution, because the act of intervening changes the incentives and the epistemic posture of the organization that is also supposed to tell the truth.

This is not a moral accusation; it is a systems claim. A single organization that (a) collects information, (b) interprets information, and (c) acts on the basis of that interpretation will predictably develop feedback loops that reward coherence-with-self. Once the organization is operationally committed to a course of action, its knowledge work is no longer neutral. It becomes, even subtly, a support structure for the action. It begins to protect sources, protect assets, protect partners, protect momentum, and protect institutional prestige. The result is an epistemic vulnerability: the same organization tasked with telling leadership what is real is also tasked with making a preferred reality happen.

Schlesinger's concern points directly here. "State within a state" is partly about parallel capabilities, but it is also about the fusion of epistemic authority with operational initiative. When knowledge and action share the same roof, intelligence can become self-justifying power.

6.1 When the same institution collects, analyzes, and executes

The fusion problem can be stated simply: a collector-analyst-operator organization has a built-in conflict of epistemic interest. Not because its people are dishonest, but because its survival and prestige are tied to action. Action requires confidence. Action requires persuasion. Action requires a narrative of feasibility. Those requirements exert pressure on analysis.

Several mechanisms make this pressure predictable.

First, *selection bias in collection*. Collection priorities are not neutral. If an organization is running an operation, it will prioritize collection that protects and advances that operation. That can be prudent—operational security matters—but it also means the organization will see the world through the aperture of its own plans. It will attend to threats to the operation more than to strategic alternatives. It will value intelligence that supports continued action.

Second, *interpretive bias in analysis*. Analysts working near operations (or within an organization culturally dominated by operations) can unconsciously adopt operational frames. They begin to ask: "How do we make this work?" rather than: "Is this the right instrument?" They may downplay inconvenient uncertainties because uncertainty slows action. They may inflate the competence of partner forces because the operation depends on that competence. They may discount political complexities because the operation is primarily engineered around tactical leverage.

Third, *organizational pressure to converge*. Large institutions develop strong norms against internal contradiction, especially under secrecy. Dissent can be seen as disloyal, or worse, as a security risk. The institution wants a unified front, particularly when presenting to leaders. This convergence pressure can flatten nuance and compress uncertainty into confidence.

Fourth, *ownership bias*. If an institution "owns" a plan, it becomes invested in that plan's success. Ownership changes cognition. It is hard for an organization to evaluate impartially a strategy that it has built, resourced, staffed, and psychologically committed itself to delivering.

Even honest people, acting in good faith, can become emotionally and professionally tethered to the operation.

The result is an epistemic danger: the institution's intelligence function can become an internal lubricant for its action function. Intelligence becomes less like a map and more like a steering wheel.

6.2 Politicization pathways: serving policy vs. shaping policy

"Politicization" is often imagined as crude manipulation: leaders demand a certain conclusion, and analysts produce it. That happens, but the more common politicization in fused institutions is subtler. It is the drift from *serving policy* to *shaping policy*.

Serving policy means: provide the best assessment of reality, including uncertainty and dissent, so elected leadership can choose. Shaping policy means: present assessments and options in a way that nudges leadership toward a preferred course—often the course the institution is already positioned to execute.

There are several pathways by which this drift occurs.

One pathway is *option control*. The institution can present a "menu" of options that subtly privileges covert action by making other options appear vague, slow, or unrealistic. Diplomacy becomes "wishful thinking." Sanctions become "symbolic." Military action becomes "too escalatory." Covert action becomes "practical." Leadership then believes it is choosing freely, but the choice architecture has been engineered by the institution's capabilities and preferences.

Another pathway is *framing through threat salience*. Intelligence organizations naturally highlight threats; that is part of their mission. But salience can be tuned. A risk can be presented as urgent and catastrophic, or manageable and long-term. Covert institutions that want authorization may emphasize urgency and narrow windows: "If we don't act now, we lose the chance." This compresses deliberation and shifts leaders toward immediate action.

A third pathway is *confidence management*. The institution can express high confidence in operational feasibility and lower confidence in alternatives. Even without lying, it can distribute certainty asymmetrically. Because leaders under pressure gravitate toward apparent clarity, asymmetric certainty becomes a steering mechanism.

A fourth pathway is *bureaucratic constituency*. Over time, covert programs create internal constituencies—units, careers, budgets—that have a stake in continued activity. These constituencies generate advocacy. Advocacy can seep into intelligence products and briefings as a tone: the operation is depicted as the "serious" option, while restraint is depicted as "doing nothing."

In each pathway, the institution is not overtly partisan. It may not be serving a party or ideology. It is serving itself—its programs, its momentum, its self-conception as the adult in the room. That is a form of politicization because it shifts policy outcomes without democratic visibility. It turns technical authority into political leverage.

6.3 The epistemic hazard: "classified confidence" as an authority substitute

One of the most corrosive dynamics in clandestine governance is what might be called *classified confidence*: the rhetorical power of saying "we know" without allowing others to see how we know. Classified confidence can be legitimate—sources must be protected—but it creates an epistemic hazard. Confidence becomes a substitute for evidence, and access becomes a substitute for argument.

This hazard has three layers.

First, *the aura of secrecy*. When information is classified, it gains an aura of seriousness. Leaders may assume it is more reliable simply because it is restricted. But classification often reflects sensitivity, not truth. A false claim can be classified. A speculative inference can be classified. A politically convenient assertion can be classified. The label "Top Secret" does not confer epistemic validity; it confers restricted circulation.

Second, *the delegation trap*. Because leaders cannot personally verify the underlying intelligence, they delegate epistemic trust to the institution. That delegation is sometimes necessary, but it becomes dangerous when it turns into deference: "I cannot judge, therefore I must accept." In a constitutional system, leaders must be able to question, to demand alternative assessments, and to require explicit uncertainty. Classified confidence can make questioning feel like irresponsibility, especially in crisis.

Third, *the monopoly of interpretation*. If only the institution can see the data, it can also control how the data is interpreted. It can present the strongest case for its preferred action while withholding ambiguous details that might slow or complicate decision. This is not necessarily malicious; it can occur because briefings have limited time and leaders demand clarity. But the consequence is epistemic centralization: the institution becomes not only the collector of facts but the arbiter of what facts mean.

This is how "classified confidence" becomes an authority substitute. The institution does not say, "We rule." It says, "Trust us." And in high-stakes contexts, "trust us" can function like rule. It becomes extremely difficult for other institutions—State, Congress, even the president's broader staff—to resist the gravitational pull of certainty packaged in secrecy.

A disciplined response to this hazard is not to demand impossible transparency. It is to demand structured humility: explicit confidence levels, explicit alternative hypotheses, documented dissent, and independent analytic pathways that are not downstream of operational commitment.

6.4 Institutional separation: benefits, risks, and historical attempts

Given the fusion problem, it is natural that reformers—Schlesinger among them—have periodically proposed separating functions: insulating analysis from operations, or at least creating strong internal firewalls. The argument is that epistemic integrity requires distance from operational advocacy.

The benefits of separation are clear.

First, *analytic independence*. Analysts not embedded in operational chains are more likely to surface inconvenient truths: partner unreliability, adversary resilience, blowback risks, legal fragility, and strategic incoherence.

Second, *policy clarity*. If analysis is structurally independent, leaders can receive assessments that are less entangled with "what we can do" and more focused on "what is true." This restores the proper order: reality first, then instrument choice.

Third, *accountability*. Separation can make it easier to trace responsibility. When analysis and action are fused, failure can be blamed on "intelligence" or "execution" interchangeably, diffusing accountability. Separation forces clarity about whether the error was epistemic or operational.

Fourth, *dissent preservation*. Separation increases the chance that dissent survives long enough to reach decision-makers. Independent analytic units can institutionalize red teaming and alternative assessments.

But separation has real risks.

One risk is *stovepiping*. If analysts are too distant from operations, they may lack context and may produce assessments that are academically correct but operationally irrelevant. They may miss tactical realities, misunderstand capabilities, or underestimate the value of human networks.

A second risk is *coordination friction*. In fast-moving crises, separation can slow the flow from knowledge to action. If too rigid, it can create bureaucratic paralysis where no one feels responsible to integrate.

A third risk is *false purity*. Structural separation does not guarantee epistemic integrity if the culture still rewards conformity or if leadership pressures analysts for supportive conclusions. Separation can become symbolic if not matched by norms of dissent and methodological rigor.

Historically, reform attempts often oscillate between fusion for efficiency and separation for integrity. When threats feel acute, governments gravitate toward fusion: integrate collection, analysis, and action to move faster. After scandals or failures, they gravitate toward separation: restore credibility, reduce abuse, reassert oversight. The pattern itself is instructive. It suggests that the underlying tension is permanent: states will always want secret tools, and those tools will always create incentives to treat knowledge as leverage for action.

The governance task, then, is not to imagine a final organizational solution. It is to design a stable equilibrium: enough integration to function, enough separation to preserve truth-telling, and enough oversight to prevent operational momentum from colonizing epistemic authority. If "state within a state" is a drift condition, then institutional separation—partial, disciplined, and culturally enforced—is one of the few durable counter-forces capable of slowing that drift without destroying the intelligence mission.

The next section turns from this internal tension to the external question: how oversight can operate in a domain where secrecy is intrinsic and where "classified confidence" can otherwise become a political trump card.

7. Oversight in a World Designed to Resist Oversight

Oversight is not an accessory to clandestine power; it is the condition that makes clandestine power compatible with constitutional government. Yet the intelligence domain is structurally resistant to oversight for the same reasons it exists: secrecy, compartmentation, speed, and the protection of sources and methods. This creates an enduring paradox. A democratic state must supervise covert action precisely because it is dangerous, but covert action is engineered to minimize visibility precisely because it is vulnerable. In this environment, oversight can easily degrade into ritual: periodic briefings, selective disclosures, after-the-fact reviews, and moral comfort language. Ritual oversight is worse than none, because it creates the appearance of control while allowing drift to continue.

To treat oversight seriously, we must define it operationally. Oversight is not merely "being informed." It is the existence of enforceable mechanisms that can (a) authorize or deny, (b) impose conditions, (c) audit claims against evidence, (d) compel correction, and (e) assign responsibility when harm occurs. The question is not whether oversight bodies exist, but whether they have *bandwidth, access, independence, and leverage* sufficient to constrain a fast-moving, secretive apparatus that can generate its own narratives of necessity.

This section examines five oversight arenas—executive, legislative, judicial, internal watchdogs, and budget transparency—through the lens of their failure modes and design requirements.

The goal is not utopian transparency, but governability: a stable set of controls that can operate under secrecy without becoming captive to secrecy.

7.1 Executive oversight: principals, deputies, and the problem of bandwidth

In theory, executive oversight is the strongest form because the intelligence community ultimately sits under the executive branch. The president, national security advisor, and cabinet-level principals hold formal authority to direct, approve, and terminate covert activity. In practice, executive oversight is limited by bandwidth and by the asymmetry between political time and operational time.

The bandwidth problem is straightforward. Senior leaders have finite attention. They face multiple crises simultaneously. They must manage politics, diplomacy, domestic priorities, and public legitimacy. Covert operations, however, are detailed and continuous. They require monitoring of evolving conditions, operational risk, partner behavior, blowback signals, and mission creep. No president or principal can personally supervise the granular reality of even a handful of major covert programs. Oversight is therefore delegated to deputies, staff, committees, and processes. Delegation is necessary—but it is also the pathway by which autonomy grows, because delegation creates gaps.

Those gaps are filled by the institution itself. The covert organization becomes the persistent actor in the room. It frames the briefings, selects what rises to senior attention, and defines what is "too sensitive" or "too technical" to burden leadership with. Over time, leaders can slide into a posture of episodic authorization rather than ongoing governance. They approve launches and renewals but do not continuously interrogate assumptions and consequences.

Executive oversight also suffers from an incentives mismatch. Political leaders are exposed to public risk: if an operation fails, they own the scandal. That can tempt leaders to preserve deniability and minimize documentation—precisely the opposite of what oversight needs. Conversely, leaders can be tempted to treat covert action as a policy shortcut, authorizing more than they can supervise. Both temptations weaken control.

Effective executive oversight therefore requires durable mechanisms that do not rely on heroic attention. Examples include structured decision gates, written mission definitions, explicit success and failure criteria, mandatory reauthorization intervals with evidence-based review, and systematic red teaming that reports to leadership independently of operational chains. Oversight must be engineered as an operating system, not as a mood.

7.2 Congressional oversight: secrecy constraints and capture risks

Congressional oversight is essential because it represents democratic consent and because it can impose constraints through law, funding, and investigation. But congressional oversight faces a structural dilemma: secrecy both limits what can be shared and creates incentives for selective sharing. Members of Congress and staff often cannot publicly discuss what they learn, which reduces the feedback loop that normally disciplines oversight. The public cannot easily evaluate whether oversight is being conducted seriously. This allows oversight to become performative internally while remaining invisible externally.

Secrecy constraints create practical problems. Briefings may be limited in time, scope, and documentation. Staff clearances and secure facilities restrict who can participate. Compartmentation can prevent a committee from seeing the full operation. Legislators may be informed only in general terms, with details withheld to protect sources. These constraints can be legitimate, but they also create a chronic "trust deficit": oversight becomes dependent on the institution's willingness to disclose.

Capture risks complicate this further. Capture does not necessarily mean corruption. It can be cognitive. Oversight committees that repeatedly receive classified briefings can begin to identify with the institution they oversee. They can internalize threat frames. They can become reluctant to challenge operational claims because they do not want to appear naive or irresponsible. They can also become politically invested in "being in the know," which can shift the oversight posture from adversarial accountability to insider partnership.

There is also an asymmetry of expertise. Covert institutions maintain large cadres of professionals who live inside the technical details. Legislators rotate, staff turnover is high, and expertise is uneven. This makes oversight vulnerable to being guided by the very institution it is supposed to constrain. The institution becomes teacher; the overseer becomes student. That dynamic is not inherently bad, but it is dangerous if the student never graduates into independent judgment.

Serious congressional oversight requires institutional investment: highly trained staff with long tenure, independent analytic capacity, and routine access to program-level evidence—not merely narrative briefings. It also requires mechanisms to reduce capture: structured dissent hearings, independent inspector reports delivered directly to committees, mandatory reporting of significant incidents, and budgetary controls tied to compliance.

7.3 Judicial oversight: limits of adversarial review in national security

Judicial oversight is often invoked as a constitutional safeguard, but in national security it is limited by the nature of the court system. Courts are designed for adversarial review: opposing parties present evidence, cross-examine claims, and allow a judge to weigh arguments. Covert operations often cannot be litigated in that way because evidence cannot be publicly disclosed and because affected parties may not even know they were affected. The secrecy of intelligence creates a scarcity of justiciable cases.

Where courts do operate—often in surveillance contexts—they tend to review applications and procedures rather than the full strategic wisdom of operations. Courts can enforce statutory constraints, demand warrants, and punish clear violations. But they are not well designed to evaluate whether a covert action is strategically wise, politically legitimate, or likely to produce blowback. Even when courts review classified material in camera, their review is limited by what is presented and by their institutional posture of deference to the executive on matters labeled national security.

This creates a governance gap. Many of the most consequential questions—should we run this operation, should we partner with this group, should we pursue this influence program—are not judicially reviewable in any meaningful way. The judiciary is therefore a partial guardrail at best, mainly effective when clear statutory frameworks exist and when oversight is procedural rather than strategic.

The implication is sobering: if a democracy relies on courts as the primary constraint on clandestine power, it will be disappointed. Judicial oversight can be important, but it cannot substitute for robust executive and congressional governance. Courts can stop certain abuses; they cannot by themselves prevent autonomy drift.

7.4 Inspectors general and internal compliance: independence under pressure

Inspectors general (IGs) and internal compliance structures are often the most practical form of oversight because they can access sensitive information, conduct audits, and investigate misconduct without immediately exposing operations. In a world of necessary secrecy, internal watchdogs can function as the "eyes" that external institutions cannot always deploy.

But internal oversight lives under pressure. The IG or compliance office sits inside the same ecosystem it is meant to scrutinize. Its access can be contested. Its findings can be politically inconvenient. Its staff can face career costs. Leadership can subtly retaliate: limiting scope, restricting resources, delaying clearances, or framing the watchdog as "not mission-aligned." Even absent retaliation, internal watchdogs can suffer from cultural isolation: colleagues may view them as disloyal, or as threats to operational success.

Independence is therefore the central design challenge. Effective internal oversight requires statutory protections, guaranteed access to records, stable budgets, and direct reporting lines to both executive leadership and congressional committees. It also requires norms that treat compliance not as obstruction but as a necessary safety system—like engineering redundancy in aviation. A high-risk domain cannot treat its safety engineers as enemies.

Internal compliance also needs methodological strength. Audits should not only look for legal violations; they should evaluate mission creep, governance breakdowns, reporting failures, and the integrity of analytic claims used to justify operations. If internal oversight focuses only on "did we break the law?" it may miss "did we quietly become a parallel policy engine?"

7.5 Budget visibility: black budgets, accountability, and democratic consent

Budget oversight is where democratic governance becomes concrete. Authority over money is the most reliable lever legislatures have, and it is the lever that can constrain autonomy without micromanaging operations. Yet intelligence budgets are often deeply classified. "Black budgets" can protect capabilities, but they also create conditions for discretionary empires: programs can persist with limited scrutiny, costs can expand, and priorities can be set internally rather than democratically.

Budget secrecy produces three risks.

First, *opacity of scale*. If the public cannot know even approximate magnitudes, it cannot meaningfully debate tradeoffs. A democracy that cannot debate tradeoffs cannot provide consent. The result is a legitimacy deficit.

Second, *program persistence*. Classified programs can survive because they are hard to challenge. Oversight bodies may not see full details. External watchdogs cannot evaluate effectiveness. The institution can claim necessity without being forced to demonstrate results.

Third, *incentive distortion*. Budgets shape organizational incentives. If funds flow toward operations and covert tools, those functions gain prestige and power. If analysis and dissent mechanisms are underfunded, the epistemic integrity of the institution declines. Budget is therefore not merely accounting; it is a governance architecture.

The hard truth is that perfect transparency is impossible. But complete opacity is incompatible with democratic consent. The design problem is to create a layered visibility regime: enough public-level information to allow meaningful debate about scale and priorities, enough congressional-level detail to enforce accountability, and enough operational secrecy to protect sources and methods. Without such layering, black budgets become a sovereignty substrate: an autonomous resource base that can sustain parallel capability and resist correction.

In sum, oversight in the intelligence domain must be understood as an engineering problem under constraints. You cannot rely on goodwill, and you cannot rely on episodic outrage. You need redundancy: multiple oversight channels that compensate for each other's weaknesses. Executive oversight must overcome bandwidth through procedure. Congressional oversight must overcome secrecy through expertise and leverage. Judicial oversight must be treated as partial, not primary. Internal watchdogs must be protected to remain independent. Budget visibility must be layered to preserve both security and consent.

If these conditions are not met, the "state within a state" drift becomes not an aberration, but the default outcome of a system built for secrecy without equally durable counterweights built for control.

8. Coordination With Diplomacy and Defense

If "state within a state" is partly the emergence of parallel statecraft, then coordination is the primary antidote. Coordination is not merely about politeness between agencies; it is about preserving constitutional hierarchy. Diplomacy is the state's declared voice. Defense is the state's declared force. Intelligence should support both by providing truth and, when authorized, by enabling narrowly bounded covert tools that serve declared objectives. When coordination fails, the country can drift into a condition where clandestine action becomes a competing instrument of policy rather than a subordinate instrument within policy. The result is not only bureaucratic friction but strategic incoherence: allies receive mixed signals, adversaries exploit contradictions, and the United States accumulates commitments it did not consciously choose.

Coordination is hard because it fights against natural gradients: secrecy encourages compartmentation; operational tempo discourages consultation; agencies compete for influence and budget; and political leaders sometimes encourage competition as a way to generate options. But in the covert domain, competition can be indistinguishable from sovereignty. If two or three separate policy engines are operating simultaneously—State saying one thing, Defense doing another, and covert channels shaping a third track—the nation loses unified intentionality. In foreign affairs, incoherence is not neutral; it is read as deception, weakness, or internal conflict.

8.1 The interagency problem: rivalry, duplication, and mission creep

Interagency problems are often discussed as managerial headaches. In national security, they are existential to governance. Three dynamics dominate: rivalry, duplication, and mission creep.

Rivalry emerges because agencies are not only tools; they are institutions with identities and constituencies. State sees itself as the steward of legitimacy and alliance coherence. Defense sees itself as the steward of deterrence and readiness. Intelligence sees itself as the steward of reality under uncertainty and the provider of "options" when overt action is impossible. Each identity is partly true, but identities become weapons in bureaucratic struggle. When intelligence agencies claim that diplomats are naive or slow, and when diplomats claim covert operators are reckless or destabilizing, the conflict becomes a fight over who gets to define what "seriousness" looks like.

Duplication is the operational manifestation of rivalry. Agencies build overlapping capabilities because they do not fully trust each other, because they want independent channels, or because classification and compartmentation prevent awareness of what already exists. A covert institution may develop influence capabilities that resemble public diplomacy, or paramilitary capacities that resemble special operations. Defense may develop intelligence-like networks. State may develop backchannels that bypass normal diplomatic routing. Duplication is sometimes valuable—redundancy can protect against failure—but in secrecy-heavy domains duplication often becomes unaccountable proliferation. Each duplicative capability becomes a new lever in a bureaucratic contest, and the whole system becomes harder to supervise.

Mission creep is the long-term outcome. Once an agency has a capability, it seeks problems that justify that capability. If CIA has an influence apparatus, it will see influence opportunities. If it has paramilitary reach, it will see kinetic solutions. If it has a liaison ecosystem, it will see joint operations. This does not require cynicism; it is how organizations remain relevant. But in national security, relevance can become policy-making. The agency's capability landscape begins to shape the state's strategy landscape.

The interagency problem becomes acute when coordination structures are weak or episodic. If the only coordination happens in crisis, then routine drift continues unnoticed. Agencies evolve separate mental maps of the world, separate measures of success, and separate relationships abroad. At that point, "coordination" becomes negotiation between semi-autonomous actors rather than direction by a unified state.

8.2 "Covert action" as foreign policy: when instruments become strategies

Covert action becomes foreign policy when it stops being a tool used occasionally to support a broader strategy and becomes the strategy itself. This can happen because covert action offers three seductive features: it feels decisive, it feels flexible, and it feels deniable. Leaders under pressure often want "something that works" without public escalation. Covert action can deliver that feeling. The danger is that feeling becomes habit and then doctrine, even without being named as doctrine.

In a healthy system, foreign policy begins with declared ends: alliance commitments, regional stability goals, deterrence posture, human rights priorities, economic strategies, and legal boundaries. Instruments are then selected—diplomatic engagement, sanctions, military posture, intelligence collection, covert support—to serve those ends. When covert action becomes foreign policy, the order reverses: leaders begin to ask what covert tools can do, and then define policy in terms of those tools. The covert instrument becomes the frame through which reality is seen.

This inversion is especially likely when diplomacy appears stalled and overt force appears too costly. Covert action then becomes the "middle way"—a seeming compromise between talk and war. But covert action is not a middle way in consequence; it is a different way whose consequences are often delayed and distributed. It can generate conflict while denying that conflict exists. It can create partner forces with their own agendas. It can produce escalation while masking responsibility. It can also undermine the very diplomatic relationships that a declared policy depends on, because allies eventually recognize that they are being asked to live with consequences they did not consent to.

When covert action becomes strategy, the state risks losing the capacity for honest public justification. Public policy cannot be debated if it cannot be named. That is a democratic injury. It also becomes a strategic injury because adversaries and allies operate in the realm of inference, suspicion, and countermeasures. A state that cannot speak plainly about its aims forces others to guess—and guessing tends toward worst-case interpretation.

8.3 Deconfliction failures: operational success that creates strategic damage

Deconfliction is often treated as a technical matter: avoid fratricide, avoid cross-purposes, avoid operational collisions. In reality, deconfliction is a strategic discipline: ensure that actions taken by one arm of the state do not sabotage the objectives of another arm. The hardest deconfliction failures are not kinetic; they are political.

One class of failure is the "ally shock." A covert operation may be operationally successful—assets recruited, targets disrupted—but it can blindsight allies who have their own domestic politics and legitimacy constraints. An ally forced to deny or distance itself may lose public trust. Or an ally may feel manipulated and reduce cooperation on other priorities. The operational success becomes a diplomatic wound.

Another class is the "adversary learning effect." Covert successes can teach adversaries to harden their systems, restructure networks, and adapt. The short-term win produces long-term resilience on the other side. Meanwhile, the operation's exposure may justify the adversary's own escalation or repression, shifting the moral narrative in their favor. Again, operational success becomes strategic loss.

A third class is "partner blowback." Covert operations often depend on local partners—militias, intelligence services, political factions. Partners are not puppets; they have agendas. A partner may use U.S. support for goals that conflict with U.S. policy, including human rights abuses that later stain U.S. credibility. Even if the initial mission succeeds, the partnership can produce a long tail of moral and political debt. Diplomacy then pays the bill.

A fourth class is internal: covert action can undermine State's negotiating posture. If State is attempting diplomatic engagement while covert operations are simultaneously destabilizing the counterpart, the counterpart may treat diplomacy as bad faith. Negotiations fail not because diplomacy was impossible but because deconfliction was absent. In this sense, covert action can sabotage diplomacy even when both were intended to serve "national interest." The mismatch arises because the system lacked a unified strategy and a disciplined hierarchy of instruments.

These failures share a pattern: the covert organization measures success in terms of what it directly controls, while strategic damage manifests in domains it does not own—alliances, legitimacy, long-term stability. The state experiences a split-brain condition: one part celebrates a win; another part manages a crisis.

8.4 Principles for alignment: primacy of declared policy and unified planning

If coordination is to be more than ritual, it must rest on explicit principles. The goal is not to eliminate covert action, but to ensure it remains subordinate to declared policy and integrated into unified planning.

A first principle is *primacy of declared policy*. Declared policy does not mean publicly broadcasting every detail. It means that the executive branch must have an explicit, accountable statement of ends that governs all instruments, including covert ones. Covert action must be justified as serving those ends, not as creating new ends through momentum.

A second principle is *unified planning with instrument discipline*. Planning should begin with strategic ends and then select instruments in a coherent package: diplomacy, public messaging, sanctions, overt military posture, intelligence, covert options. Covert action should be evaluated not in isolation but as one component of a strategy, with clear assumptions and failure branches. Unified planning also requires that State and Defense have meaningful veto or conditioning power when covert action materially affects their domains. Consultation that cannot stop anything is not consultation; it is notification.

A third principle is *single narrative coherence*. The state must avoid sustaining two contradictory stories: one for public diplomacy and one for covert reality. Total transparency is impossible, but blatant contradiction is corrosive. Alignment requires that covert actions not force diplomats into implausible denials that damage credibility. If an operation cannot be plausibly integrated with the state's broader posture, that is a warning signal that the operation may be strategically incoherent or democratically illegitimate.

A fourth principle is *explicit deconfliction as a standing process*. Deconfliction must be institutionalized, not improvised. That means routine interagency forums with sufficient clearance and authority, documented decisions, and structured dissent. It also means the integration of long-tail consequence analysis: blowback, partner incentives, escalation ladders, and reputational risk. The aim is to prevent the common pattern where operational feasibility dominates the conversation while strategic consequences are treated as someone else's problem.

A fifth principle is *responsibility clarity*. When multiple agencies touch an operation, the system must name accountable owners: who is responsible for legality, for diplomatic impact, for partner behavior monitoring, for success criteria evaluation, for termination decisions. Without named responsibility, coordination becomes a diffusion mechanism, and diffusion is the friend of autonomy.

These principles do not guarantee perfect outcomes. But they alter the default. They make it harder for covert action to become a parallel foreign policy by momentum. They force the state to behave like a single intentional actor rather than a federation of competing instruments. And they embody Schlesinger's deeper warning: in a republic, clandestine capability must never be allowed to substitute for policy. It can serve strategy. It cannot be permitted to become strategy—because when instruments become strategies, the state begins to govern from the shadows, and the constitutional order begins to hollow out from within.

9. Ethics, Blowback, and the Long Tail of Secret Power

Covert power is usually evaluated on short horizons: did the operation succeed, did it disrupt an adversary, did it protect lives, did it avoid escalation, did it stay secret. Ethics operates on longer horizons, because ethical consequences do not stay contained. They migrate. They show up later as hatred, mistrust, retaliation, domestic cynicism, institutional corrosion, and cultural numbness. The central danger of clandestine action is therefore not only that it can be abused, but that it can succeed in ways that quietly bankrupt the moral capital of a society.

This section treats ethics as a strategic variable, not an ornament. In a free society, legitimacy is a form of power. It is the ability to rally allies, persuade publics, and sustain institutions without coercion. Covert action can protect legitimacy when it prevents catastrophe. But it can also erode legitimacy by habituating the state to ends-justify-means thinking, by normalizing secrecy as a substitute for consent, and by building long-tail liabilities that later return as political crises. The "state within a state" worry is not merely constitutional; it is moral. An institution insulated from visibility is also insulated from the ordinary human restraint that visibility supplies.

9.1 Blowback as governance debt: hidden costs paid later

"Blowback" is often treated as an intelligence-world term for unintended consequences that return to harm the initiator. But it can be understood more precisely as *governance debt*. A covert operation can produce immediate benefit by pushing costs into the future and into other domains—diplomacy, domestic politics, alliance cohesion, moral credibility. Like financial debt, governance debt feels useful at the moment of borrowing. It buys time. It creates room to maneuver. It avoids painful public tradeoffs. But it demands payment later, often with interest, and often by people who did not consent to the borrowing.

Covert power accumulates governance debt in predictable ways.

First, by creating *partner dependencies*. Supporting a faction, militia, or foreign service can stabilize a situation quickly, but it also creates long-term entanglement. Partners learn to leverage the relationship. They threaten to defect or expose secrets. They demand continued support. They may use support for agendas the sponsor does not control. What begins as an instrument becomes a relationship that must be serviced.

Second, by generating *narrative liabilities*. When a state acts covertly, it often also lies publicly—sometimes by omission, sometimes by denial. Even if secrecy is justified, the practice of denial can become habitual. When secrets surface, publics feel betrayed. Even citizens who approve of the action can resent the deception. The result is domestic cynicism: a weakening of trust that makes future governance harder.

Third, by shaping *adversary adaptation*. Adversaries learn. Covert operations teach them where they are vulnerable, who can be bribed, what channels are exploited, and what thresholds the state will not cross publicly. The immediate win can accelerate an adversary's hardening and sophistication. Blowback here is not only retaliation; it is the creation of a more capable opponent.

Fourth, by triggering *retaliation dynamics* under ambiguity. Because covert actions are deniable, responses can also be deniable. Escalation becomes a shadow cycle with fewer off-ramps and less public constraint. Ambiguity can prevent de-escalation because parties cannot openly negotiate around actions they cannot admit.

Governance debt becomes dangerous when it is not accounted for. In financial systems, debt is monitored. In covert systems, debt is often hidden by classification and by agency compartmentation. The people who benefit from a covert win may not be the people who pay the blowback bill. That disconnect is the essence of governance debt: externalizing cost across time, across agencies, and across citizens.

9.2 Moral injury and bureaucratic diffusion of responsibility

Moral injury is typically discussed in the context of soldiers and combat: the psychic wound that arises when a person participates in, witnesses, or fails to prevent actions that violate their moral framework. Covert institutions create distinctive conditions for moral injury because they often operate in moral gray zones—where legality is complex, intentions are mixed, and consequences are uncertain. The injury can affect operators, analysts, policymakers, and oversight staff alike. It can also affect a society that learns, later, what was done in its name.

The moral injury risk is amplified by *bureaucratic diffusion of responsibility*. In covert systems, responsibility is often intentionally dispersed. Compartmentation means no one sees the whole. Deniability means authorization is euphemized. Interagency complexity means each actor can claim they only handled a piece: “I just wrote the analysis,” “I just moved the funds,” “I just signed the paperwork,” “I just ran the asset,” “I just briefed the committee.” When harm occurs, the system supplies endless partial truths that prevent full ownership.

Diffusion of responsibility has two corrosive effects.

First, it protects the institution from correction. If no one is clearly accountable, no one can be clearly disciplined, and no one can clearly learn. Mistakes are reclassified as “system failures,” and the system remains intact.

Second, it injures individuals. Humans can tolerate hardship more easily than moral ambiguity. When people participate in actions whose moral weight is unclear and whose ownership is denied, they are left holding a residue of guilt without the dignity of acknowledged responsibility. That is moral injury: not merely “I did a hard thing,” but “I did a hard thing that no one will openly own, and I cannot fully speak about it.”

A free society should treat this as a governance warning, not as a therapy footnote. Systems that routinely diffuse responsibility are the same systems that tend toward autonomy, because diffusion is the enemy of constraint. Responsibility, by contrast, is a brake. When a specific person must sign their name and can later be questioned, caution increases. Diffusion replaces caution with momentum.

9.3 Democratic legitimacy: consent, accountability, and the secrecy paradox

Democratic legitimacy depends on consent, but consent requires knowledge. This creates the secrecy paradox: the state must keep secrets to protect the public, yet the public must have enough knowledge to legitimately authorize the state’s actions. A democracy that cannot authorize cannot truly consent; it merely acquiesces.

The paradox is not solved by demanding that everything be public. That is naive. Some secrets protect lives. Some secrecy is essential for deterrence and for safeguarding sources. But the paradox is also not solved by declaring that secrecy automatically justifies itself. That is how secrecy becomes sovereignty.

Legitimacy in covert action therefore requires a layered structure of consent.

At the public layer, citizens must be able to debate scale and doctrine: what kinds of covert action are permissible, what boundaries exist, what oversight structures function, and what accountability follows failure. Citizens do not need operational details to debate moral and constitutional principles.

At the representative layer, Congress must have real access and real leverage. Oversight that cannot stop programs is not consent; it is theater. Democratic consent is mediated through representatives who can see more than the public can see.

At the executive layer, authorization must be explicit and owned. If leaders want covert power, they must accept the burden of responsibility. Secrecy cannot be used to avoid ownership.

The secrecy paradox becomes acute when covert actions increasingly substitute for overt policy. When major national strategy is conducted in the shadows, democratic legitimacy hollows out. Citizens are asked to "support" policies they cannot see, and the state becomes accustomed to governing without persuasion. That habituation changes culture. It teaches the public that politics is fake and that real power is hidden. Even if the covert actions were originally justified, the long-term effect can be the corrosion of civic trust itself—an internal blowback.

In this sense, "state within a state" is not only a constitutional anxiety about unaccountable agencies. It is an anxiety about the public's relationship to truth. A democracy that cannot tell itself what it is doing becomes vulnerable to cynicism, conspiracy, and political fragmentation. Secrecy can protect the state, but chronic secrecy can also weaken the civic fabric that makes the state worth protecting.

9.4 Boundaries: what a free society should refuse even under threat

The hardest ethical question is not whether covert power should exist, but where it must stop. A free society cannot define itself only by survival. If survival becomes the sole metric, then the society will eventually survive as something else.

Boundaries are therefore not luxuries; they are identity commitments. They answer the question: "What are we, even under threat?" A society that refuses to articulate boundaries will default to the logic of necessity, and necessity is infinitely expandable.

Several boundary principles are especially relevant in the covert domain.

One principle is *non-totalization*: covert action must not become a general-purpose substitute for policy. It must remain exceptional, bounded, and periodically re-justified. If covert action becomes normal governance, democratic life erodes.

A second principle is *non-dehumanization*: operations must not depend on treating entire populations as instruments, collateral, or manipulable masses. Dehumanization is a shortcut to efficiency, but it is also the seed of atrocity and the core driver of moral injury.

A third principle is *non-impunity*: the system must preserve enforceable accountability for violations—legal, ethical, and procedural. A covert institution cannot be permitted to operate as if the law ends where classification begins. If classification becomes impunity, sovereignty has shifted.

A fourth principle is *non-self-authorization*: the agency must not be able to define its own mission boundaries without external contestation. The right to decide the limits of force, influence, and deception belongs to accountable political authority, not to the instrument.

A fifth principle is *non-falsification of civic reality*: a democracy must be extremely cautious about domestic manipulation and propaganda. The temptation to import covert influence techniques back into domestic politics is profound, especially in polarized eras. Once the state begins to treat its own citizens as an influence target, the moral boundary between security and domination collapses.

Finally, there is the principle of *owning consequences*. A free society should refuse actions that it would be unwilling to own if exposed. This is not a call for public disclosure of details; it is a test of moral coherence. If the state cannot, even in principle, justify an action in a future moment of transparency, then the action is likely to be morally or politically corrosive. The refusal to own is often the first sign that the action is not compatible with the society's stated identity.

Ethics, then, is not anti-security. Ethics is the long-term security of legitimacy. Blowback is what happens when governance debt comes due. Moral injury is what happens when responsibility is diffused and truth is compartmented. The secrecy paradox is what happens when a democracy cannot fully authorize what is done in its name. Boundaries are what prevent the survival instinct from devouring the very freedoms the state exists to defend.

This sets up the next move: if covert power has a long tail, then reforms cannot be limited to procedural fixes. They must include explicit doctrines of restraint and alignment—so that secret action remains an instrument of a free society rather than a mechanism by which freedom is quietly replaced by managed reality.

10. Reform Options: From Schlesinger to the Present

Reform in the intelligence domain is often reactive: it follows a fiasco, a scandal, or a declassification shock that makes denial politically impossible. That rhythm is itself a problem. If “state within a state” is a drift condition produced by ordinary institutional forces—secrecy, tempo, information asymmetry, operational incentives—then reform cannot be episodic. It must be constitutional in character: durable counter-forces embedded into doctrine, structure, procedure, budget, and culture. Schlesinger’s 1961 memo is valuable not only because it warned of autonomy, but because it implied a reform philosophy: curb parallel statecraft by tightening the relationship between clandestine instruments and accountable policy authority.

What follows is not a single “fix.” No organizational design eliminates the tension between security and consent. The goal is to change the default trajectory: to make autonomy drift harder, slower, and more visible; to force covert action to remain exceptional and policy-serving; and to preserve the epistemic integrity of intelligence analysis against the gravitational pull of operations. These reforms are best viewed as a bundle. Any single one can be circumvented; together they provide redundancy.

10.1 Clarify doctrine: what covert action is for (and not for)

The most important reform is doctrinal because every other reform depends on it. Without doctrine, oversight becomes a procedural game: did the right boxes get checked? Doctrine tells you what the boxes are for.

A serious covert action doctrine should do at least four things.

First, it should define *ends*. Covert action is not “something we do.” It is a tool used to achieve explicitly defined political objectives. Doctrine should require that every covert program be tied to a declared policy end state that is intelligible to accountable leadership and consistent with the broader strategy of State and Defense.

Second, it should define *use cases*. Covert action is appropriate for certain classes of problems—time-sensitive threat disruption, narrow influence shaping under exceptional constraints, covert support for allies under specific conditions. It is inappropriate as a general substitute for diplomacy, as a default response to complexity, or as a way to avoid political ownership.

Third, it should define *prohibitions*. A doctrine without “never” clauses is not doctrine; it is permission. Prohibitions do not require public disclosure of methods; they require internal commitment that certain tactics are off-limits because they corrode legitimacy, invite blowback, or violate foundational values. The prohibition category should be explicit enough that oversight bodies can evaluate compliance without needing operational minutiae.

Fourth, it should define *termination logic*. Covert programs die badly when they persist by inertia. Doctrine should require explicit success criteria, explicit failure criteria, and explicit sunset conditions. If a program cannot articulate what would make it end—either by success or by unacceptable cost—it will tend to expand and persist, becoming an internal constituency.

Doctrine, in short, reasserts the order: policy defines ends; clandestine tools serve those ends; covert action is exceptional; and "can" never becomes "should" without a disciplined argument.

10.2 Separate functions: analysis, operations, and influence

Schlesinger's instinct toward separating functions remains one of the few reforms that directly targets the epistemic hazard. If analysis and operations are fused, the organization is structurally tempted to sell its own plans using its own knowledge authority. Separation does not guarantee integrity, but it reduces the likelihood that operational momentum colonizes truth-telling.

The separation logic can be implemented at multiple levels.

One level is *structural independence of analytic units*: analysts should have leadership lines that are insulated from operational chains, with explicit protection for dissent and alternative assessments.

A second level is *firewalls for influence operations*. Influence—whether covert propaganda, information operations, or political shaping—poses special legitimacy risks and can easily bleed into domestic politics or alliance trust. Treating influence as just another "operation" is dangerous. Influence functions should be bounded by doctrine, subject to heightened oversight, and evaluated for long-tail legitimacy costs, not merely tactical effect.

A third level is *competitive analysis and red teaming* as an institutional right, not an optional courtesy. Competitive analysis prevents an operationally invested unit from monopolizing the interpretation of intelligence. It forces alternative hypotheses to survive long enough to reach decision-makers.

Separation does carry risks—stovepiping, slower response, coordination friction. But the deeper risk is already present in the fused model: the gradual replacement of truth with institutional coherence. A state that loses epistemic integrity in its intelligence system becomes strategically blind. It will be operationally busy and strategically surprised—precisely the condition in which covert autonomy becomes most tempting.

10.3 Tighten authorization: written findings, time limits, and renewal hurdles

Authorization is where democratic governance becomes concrete. The problem is not that covert action is authorized; it is that authorization can become vague, evergreen, and insulated from evidence. Tightening authorization does not mean micromanaging operations; it means preventing "drift by default."

Three instruments matter here.

First, *written findings with explicit scope*. Authorization should specify the objective, the permitted instruments, the constraints, and the agency responsibilities. Vagueness is the oxygen of mission creep. Written scope is the brake.

Second, *time limits*. Covert action should not be authorized indefinitely. Time limits create a forcing function: leadership must revisit the program with fresh eyes. They also make it harder for programs to persist purely because they have constituencies.

Third, *renewal hurdles tied to evidence*. Renewal should require more than "still necessary." It should require a structured review: what was achieved, what assumptions failed, what blowback emerged, what alternatives exist now, what is the plan for termination. Renewal hurdles do not block urgent action; they prevent indefinite action.

A subtle but important addition is *reversibility planning*. Authorization should include failure-branch planning: what the state will do if the program is exposed, if partners misbehave, if objectives cannot be achieved, or if escalation occurs. Without reversibility planning, leaders authorize optimism without owning consequences.

10.4 Strengthen oversight capacity: staff, expertise, and audit power

Oversight fails not only because of secrecy, but because of weakness. An institution that is out-resourced, out-experienced, and out-informed by the agency it oversees cannot reliably govern it. Oversight must therefore be treated as a capability, not as a moral stance.

Three reforms matter.

First, *professionalize oversight staff*. Congressional and executive oversight bodies need staff with deep domain expertise, long tenure, and secure access. Rotation and amateurism are gifts to secrecy. Oversight cannot be episodic and still be real.

Second, *independent analytic capacity*. Oversight bodies need the ability to evaluate claims without relying entirely on the agency's narrative. That means access to independent analysts, alternative assessments, and external expertise under appropriate security constraints.

Third, *audit power with teeth*. Oversight must be able to demand records, inspect programs, and enforce compliance. If oversight is only briefed, it is downstream. If it can audit, it is upstream. Audit authority should include the power to compel corrective action, not merely to complain.

This is also where oversight redundancy matters: executive oversight, congressional oversight, and inspectors general should receive independent streams of reporting, including dissent and incident reporting, so that the institution cannot manage all oversight through a single curated narrative.

10.5 Budget and proprietary constraints: limiting autonomous resource empires

Budget is the most durable substrate of autonomy. An agency that can finance itself in opaque ways can sustain programs through political cycles and resist correction through classification. If the "state within a state" worry has an economic core, it is here: autonomous resource empires create autonomous policy capacity.

Reform in this category aims not at eliminating secrecy, but at limiting discretionary empires.

One approach is *program-level budget visibility to cleared oversight*, ensuring that oversight committees can see real costs, real contractors, and real growth patterns. If oversight cannot track growth, it cannot govern priorities.

Another is *constraints on proprietary and quasi-private structures*. Proprietary assets and contractor ecosystems can become parallel bureaucracies with their own incentives. They can also create political constituencies that make programs hard to terminate. Constraints might include stricter approval requirements, periodic audits, and limitations on long-term proprietary holdings unless clearly justified.

A third is *budget discipline tied to compliance*. Funding can be conditioned on reporting quality, audit results, and adherence to doctrine. This is one of the few levers that does not require operational micromanagement: it governs the system by governing its resource flows.

Finally, budget reforms should aim to prevent the common pattern where operational functions get lavish funding while analytic integrity and oversight functions are starved. If analysis and dissent are underfunded, operations become the dominant culture, and autonomy drift accelerates.

10.6 Cultural reform: humility, dissent channels, and red-team discipline

Structural reforms can be circumvented if culture remains unchanged. Covert institutions are especially culture-driven because secrecy intensifies identity and loyalty. If the culture treats oversight as interference, treats dissent as disloyalty, and treats operational daring as the highest virtue, then doctrinal and procedural reforms will be treated as obstacles to be navigated rather than as constitutional commitments.

Cultural reform is difficult because it cannot be mandated in a memo. But it can be engineered through norms, incentives, and leadership practices.

Humility must be institutionalized. This means requiring explicit uncertainty expression, rewarding the surfacing of risk rather than punishing it, and treating "we don't know" as a professional statement rather than a failure. Humility is not weakness; it is the epistemic defense against self-justifying action.

Dissent channels must be protected and normalized. People must be able to raise concerns without career suicide. Protected dissent can include formal dissent memoranda, anonymous reporting lines, ombuds structures, and leadership routines that actively solicit contrary views. A covert institution without dissent becomes a closed loop—and closed loops drift.

Red-team discipline must be routine. Red teaming should not be an occasional exercise performed to satisfy oversight. It should be a standing institutional function with independence and authority. Red teams should challenge assumptions, simulate adversary adaptation, analyze blowback, and stress-test the moral and political plausibility of operations if exposed. In a secrecy environment, red teams are one of the few ways to reintroduce adversarial scrutiny.

Finally, cultural reform must include the restoration of “instrument posture.” The institution must see itself as a tool of policy, not as the guardian of national destiny. That posture is fragile in the clandestine world because secrecy produces exceptionalism. Leadership must actively resist that exceptionalism by reaffirming the chain of authority, honoring oversight as part of mission, and disciplining the romance of clandestinity.

Taken together, these reforms form a coherent response to Schlesinger’s warning. Clarify doctrine so covert action remains exceptional and policy-serving. Separate functions to preserve epistemic integrity. Tighten authorization to prevent drift by default. Strengthen oversight capacity so control is real, not ceremonial. Constrain budgets and proprietary empires so resources cannot become autonomous sovereignty. Reform culture so humility and dissent counterbalance the natural self-justification of secrecy.

None of these eliminates risk. But they change what is easiest. Without them, autonomy is easy and correction is hard. With them, autonomy becomes harder and more visible, and the constitutional order gains what it most needs in the shadow domain: governability without naivete.

11. Objections and Replies

Any argument for reform in the covert domain faces a predictable set of objections. Some are made in good faith by professionals who have seen threats up close and who know how fragile operations can be. Others are made as institutional self-defense, because reform threatens autonomy, budgets, prestige, and the romance of clandestine efficacy. The serious task is to answer the best version of these objections without becoming naive about the world. A free society cannot afford either fantasy: neither the fantasy that secrecy is unnecessary, nor the fantasy that secrecy automatically justifies itself.

The underlying claim of this paper has been structural: covert institutions drift toward autonomy because of normal organizational forces operating under secrecy, speed, and information asymmetry. If that claim is right, then objections that treat abuse as merely political miss the deeper point. Likewise, objections that treat oversight as inherently paralyzing mistake governance for interference. The replies below aim to preserve what covert capability is for—protection under constraint—while refusing the idea that constraint is optional.

11.1 "Secrecy is necessary; oversight will paralyze operations"

Secrecy is necessary. The question is not whether secrecy exists, but whether secrecy becomes a zone of impunity. Oversight does not require broadcasting operations; it requires that someone accountable can see enough to authorize, constrain, and audit. The alternative to oversight is not efficiency; it is drift.

The paralysis objection often assumes a false binary: either full operational freedom or public disclosure. Real oversight is neither. It is layered and selective. It is the creation of small, trusted, legally empowered oversight nodes with secure access and disciplined discretion. The goal is not to slow every action; it is to ensure that exceptional powers remain exceptional and policy-serving.

Moreover, the idea that oversight "paralyzes" operations often confuses two different frictions: *tactical friction* and *strategic friction*. Tactical friction can be harmful if it breaks time-sensitive missions. Strategic friction is necessary because it forces justification. A system with zero strategic friction will optimize for action, not for wisdom. Covert institutions naturally seek speed; oversight is the counterweight that ensures speed does not become sovereignty.

A practical reply is to redesign oversight around tempo. Oversight can be structured with pre-approved doctrines, standing rules of engagement for certain categories of action, rapid decision gates for urgent scenarios, and post-action audits that are mandatory and consequential. That approach preserves operational agility while maintaining governance. If the only way an operation can proceed is by avoiding oversight entirely, that is a warning sign about the operation, not about oversight.

11.2 "Covert action is just another tool; abuse is political, not structural"

Covert action *is* a tool. But not all tools have the same governance requirements. A tool that can change governments, kill people, manipulate political outcomes, and create long-tail blowback is categorically different from a routine administrative tool. The structural argument is not that covert action is evil; it is that covert action is *high-leverage under low visibility*, which makes it uniquely prone to self-justifying drift.

Saying “abuse is political” treats the problem as episodic: bad leaders do bad things; good leaders won’t. History does not support that comfort. Even good leaders face incentives to use deniable options to avoid political cost. Even well-intentioned institutions face mission creep. Even careful operators can produce blowback because consequences are complex and delayed. Abuse is not only malice; it is the predictable output of systems that reward action, protect secrecy, and diffuse responsibility.

The real question is not “Are leaders good?” It is “Is the system corrigible?” A structurally governable system can restrain even bad leaders and correct even good-faith errors. A structurally ungovernable system will eventually drift regardless of who holds office, because the underlying forces remain constant.

So the reply is: yes, politics matters, but structure determines whether politics is decisive or cosmetic. In the covert domain, structure is the difference between accountable instrument and parallel sovereignty.

11.3 “Splitting agencies creates stovepipes and slows response”

This objection is real. Separation can create stovepipes. But the argument for separation is not that speed is irrelevant; it is that epistemic integrity is a national security asset. A fused institution that moves fast but gradually loses its capacity to tell the truth is not secure; it is strategically brittle. It becomes vulnerable to self-deception, operational echo chambers, and policy capture by its own momentum.

The reply is to distinguish between *separation of roles* and *severing of collaboration*. Firewalls can exist without isolation. Analysts can be organizationally independent while still embedded in shared information environments. Red teams can operate independently while still having access to operational detail. Influence functions can be bounded and supervised without being disconnected from intelligence collection.

In engineering terms, separation is a safety system. The goal is not to slow everything; it is to prevent runaway feedback loops where the same organization both generates the justification and executes the action. The cost of some friction is the benefit of avoiding catastrophic drift.

Furthermore, the “stovepipe” risk is often overstated in comparison to the “fusion” risk. Stovepipes create coordination problems that are visible and correctable. Fusion creates epistemic problems that are invisible until crisis. A democracy can fix coordination with process improvements. It cannot easily fix a culture of self-justifying secrecy once it becomes normalized.

So the reply is: yes, separation creates costs, but those costs are manageable, and the alternative costs are existential to governability.

11.4 "Public accountability is impossible; citizens can't know enough"

Citizens cannot know operational details. But public accountability is not an all-or-nothing condition. Democracies routinely authorize complex systems they cannot fully understand—central banking, military procurement, nuclear safety—through layered consent: public doctrine, representative oversight, and specialized audit mechanisms. Intelligence can be governed the same way.

The mistake is to equate "citizens can't know everything" with "citizens can know nothing." Citizens can know the categories of permissible action, the existence and powers of oversight institutions, approximate budget scale, the doctrine of limits, and the consequences for abuse. Citizens can also know after-the-fact histories through declassification and independent review. These are meaningful forms of accountability even if they do not include real-time operational transparency.

The deeper issue is legitimacy. In a free society, legitimacy is not only the absence of dissent; it is the presence of a credible consent structure. If citizens are told, in effect, "trust us, you don't get to know," then legitimacy becomes fragile. The state teaches cynicism. People then fill the void with conspiracy, which is not merely a cultural problem but a national security problem. A society that cannot plausibly authorize its own power becomes internally unstable.

So the reply is: full public knowledge is impossible, but meaningful public legitimacy is still necessary—and it can be achieved through layered doctrine, real representative oversight, and credible after-action transparency.

11.5 "Reform invites adversaries; transparency is weakness"

There is a difference between transparency of tactics and transparency of governance. Reform does not require revealing sources and methods. It requires strengthening doctrine, authorization discipline, oversight capability, and accountability. That kind of transparency—governance transparency—can be a strength because it increases institutional credibility at home and abroad.

Adversaries benefit when democracies hollow out their legitimacy. They exploit scandals. They amplify cynicism. They portray democratic states as hypocritical. If reforms reduce abuses, clarify boundaries, and strengthen accountability, they deny adversaries that propaganda fuel. In that sense, reform is a resilience strategy.

The "transparency is weakness" argument also overlooks a strategic truth: secrecy without discipline often produces operational mistakes that become public anyway. Exposure is not rare.

Leaks happen. Investigations happen. Regime changes happen. Archives open. The question is not whether actions will remain hidden forever, but whether the state's actions can be defended when they are eventually scrutinized. A governance system that assumes permanent secrecy is a governance system built on fantasy.

Finally, reform can improve operational effectiveness. Clear doctrine reduces mission confusion. Better oversight can reduce reckless operations that generate blowback. Stronger analysis protects against self-deception. In other words, disciplined governance is not only morally preferable; it can be strategically superior.

So the reply is: transparency of governance is not weakness; it is strength. It signals that clandestine power remains an instrument of a free society, not a rival to it.

In sum, the objections are not trivial, but they often smuggle in a deeper claim: that clandestine power is too important to be governed. That claim is exactly what Schlesinger feared. A democracy can keep secrets and still govern itself. The alternative is not safety; it is drift—toward parallel sovereignty, toward legitimacy erosion, and toward the long-tail blowback that arrives when secret power is allowed to become normal power.

12. Conclusion: Democratic Control Without Naivete

A free society does not get to choose between danger and safety. It chooses between different kinds of danger: the danger of external threats, and the danger of becoming internally unfree while trying to defeat those threats. The intelligence state exists because the world contains adversaries, uncertainty, and time pressure. The temptation is to treat these facts as a blanket permission slip: secrecy must expand, oversight must defer, and exceptional tools must become normal governance. That temptation is understandable. It is also the pathway by which constitutional systems hollow out. The problem is not that covert institutions exist, but that their structural features—secrecy, speed, information asymmetry, operational incentives—predictably generate autonomy drift unless deliberately counterbalanced.

The mature posture is therefore "democratic control without naivete." Not romantic trust, and not paranoid rejection; not denial of threats, and not surrender to secrecy as sovereignty. The core claim of this paper is that the "state within a state" diagnosis remains relevant because it describes a recurring dynamic, not a one-time scandal. Drift toward parallel sovereignty is not primarily a conspiracy; it is an institutional physics problem. If you want to preserve freedom while retaining clandestine capability, you must build brakes that work at the speed of secrecy.

12.1 Restating the thesis: the drift toward parallel sovereignty is predictable

The phrase "state within a state" is often used as a slogan, sometimes irresponsibly. But it can be made precise as a diagnosis: a covert institution acquires parallel statecraft functions—diplomatic channels, military-like capacity, bureaucratic resource autonomy, and secrecy-based legitimacy—sufficient to shape policy outcomes with insufficient external friction. When those parallels converge, the institution becomes capable of operating as a partially autonomous policy engine, even if no one inside intends to usurp authority.

That drift is predictable because it arises from stable forces:

- Incentives reward operational wins more than strategic coherence.
- Information asymmetry gives those with secrets agenda-setting power.
- Speed mismatch forces leaders into compressed decisions that become momentum.
- Classification expands by default, shrinking the space where oversight can operate.
- Career ecology and clandestine identity encourage exceptionalism and internal loyalty.

These forces do not vanish with good leadership. They reappear in every era. The republic's question is therefore not "Can we trust them?" but "Is the system designed to remain governable under secrecy?" Where governability is weak, autonomy drift becomes the default output, and "state within a state" stops being rhetoric and becomes structural reality.

12.2 What is gained by reform: legitimacy, coherence, and fewer strategic self-wounds

Reform is often framed as a constraint—something that makes the intelligence apparatus less effective. That frame is incomplete. Reform is also a way to make national security less self-defeating.

The first gain is **legitimacy**. In the long run, legitimacy is a strategic asset. It sustains alliances, supports deterrence, and preserves domestic trust. When citizens believe the state is governable—even in secrecy—civic consent becomes more resilient. When allies believe U.S. policy is coherent and accountable, cooperation becomes easier. When adversaries cannot reliably portray U.S. actions as hypocrisy and impunity, propaganda loses fuel.

The second gain is **coherence**. Unified strategy requires that diplomacy, defense, intelligence, and covert action operate under a single set of ends. Reform strengthens that hierarchy. It reduces the split-brain condition in which an operational "win" produces a diplomatic crisis, or an influence success produces an alliance fracture. Coherence is not merely aesthetic; it is what prevents the state from fighting itself.

The third gain is **fewer strategic self-wounds**—fewer Bay-of-Pigs patterns, fewer blowback debts, fewer covert commitments that later become public scandals. Many national security failures are not failures of courage but failures of governability: action outruns wisdom; secrecy outruns consent; momentum outruns doctrine. Reforms that clarify doctrine, tighten authorization, and strengthen oversight reduce the likelihood that the United States will harm its own strategic position through clandestine overreach.

Finally, reform improves **epistemic integrity**. When analysis is protected from operational self-justification, leaders receive better maps. Better maps do not guarantee better choices, but they reduce the chance that the nation will act on confidence masquerading as evidence.

12.3 What is risked: slower tempo, fewer deniable options, more visible tradeoffs

Reform is not free. Honest governance requires acknowledging what is risked.

First, reform can produce **slower tempo**. Decision gates, renewal hurdles, red teams, and audit processes introduce friction. In some cases, that friction can cause missed opportunities. But the mature question is not whether opportunities are missed; it is whether the opportunities would have been worth the long-tail costs. In the covert domain, speed is both capability and temptation.

Second, reform can yield **fewer deniable options**. If oversight and doctrine are tightened, some operations will not be authorized. Leaders will lose certain tools that are politically convenient precisely because they are deniable. This can feel like weakness, but it is often the restoration of constitutional ownership: if the state is unwilling to own an action, perhaps it should not take it.

Third, reform makes **tradeoffs more visible**. Leaders and institutions will be forced to confront costs that secrecy often hides: budget magnitude, partner dependencies, legitimacy damage, blowback risk, moral injury. Visibility is uncomfortable. But discomfort is part of democratic maturity. A society that cannot tolerate visible tradeoffs will always be tempted to govern through secrecy, and secrecy will always be tempted to become sovereignty.

These risks are real, but they are also the point. A constitutional system is designed to be cautious with force and deception. If reform makes it harder to act secretly, that is not necessarily failure; it may be success—forcing the state to reserve clandestine tools for genuinely necessary cases and to pursue overt, accountable policy wherever possible.

12.4 Forward work: disciplined References and comparative reform matrix

The forward work is practical. This paper's argument becomes more useful if it is anchored in disciplined sources and translated into a decision framework that policymakers and citizens can actually use.

First, the **Reference section** should be compiled with care: primary historical documents (including Schlesinger's memo context), reputable histories of intelligence reforms, legal frameworks governing covert action and oversight, and scholarly work on secrecy, bureaucratic incentives, and democratic legitimacy. The Reference discipline matters because the topic attracts myth-making. The point is not to debunk everything; it is to separate documented mechanisms from rhetorical fog.

Second, a **comparative reform matrix** can operationalize the reform bundle. Such a matrix would list reform options (doctrine, separation, authorization tightening, oversight capacity, budget constraints, cultural reforms) against evaluation criteria: operational agility, blowback risk reduction, legitimacy protection, oversight feasibility, and resistance to capture. It would also include known failure modes and mitigation strategies. The goal is to move from "we should reform" to "here is what reform changes, what it costs, and how to implement it without breaking necessary capability."

If the phrase "state within a state" is to be more than an alarm bell, it must become a design prompt. The republic cannot abolish secrecy, and it cannot wish away adversaries. But it can refuse the quiet surrender of constitutional control. Democratic control without naivete means building systems where clandestine power remains a tool—powerful, sometimes necessary, always dangerous, and never allowed to become its own source of authority.

References

R1 Primary documents: Schlesinger memo, related JFK-era records

- Schlesinger, Arthur M., Jr. "CIA Reorganization." Memorandum for President John F. Kennedy, June 30, 1961. John F. Kennedy Presidential Library and Museum, National Security File, Departments and Agencies, Central Intelligence Agency (declassified).
- National Archives and Records Administration. "CIA Reorganization" (Schlesinger memorandum). President John F. Kennedy Assassination Records Collection (JFK Records), Document ID 32273831 (declassified).
- Kirkpatrick, Lyman B. "Inspector General's Survey of the Cuban Operation." Memorandum for the Director of Central Intelligence, December 1, 1961. Central Intelligence Agency (declassified).
- United States Department of State. *Foreign Relations of the United States, 1961–1963, Volume X: Cuba, January 1961–September 1962.* Washington, DC: U.S. Government Printing Office, 1997. (Includes U.S. documentary record surrounding Bay of Pigs review and governance issues.)
- New York Times. "C.I.A.: Maker of Policy, or Tool? Agency Raises Questions Around World; Survey Discloses Strict Controls But Reputation of Agency Is Found to Make It a Burden on U.S. Action." April 25, 1966.
- Schlesinger, Arthur M., Jr. *A Thousand Days: John F. Kennedy in the White House.* Boston: Houghton Mifflin, 1965.

R2 Bay of Pigs histories and declassified after-action materials

- Central Intelligence Agency. *Official History of the Bay of Pigs Operation, Volume I: Air Operations, March 1960–April 1961.* Washington, DC: CIA History Staff, 1984 (declassified).
- Central Intelligence Agency. *Official History of the Bay of Pigs Operation, Volume II, Part I: Participation in the Conduct of Foreign Policy—Guatemala.* Washington, DC: CIA History Staff, 1984 (declassified).
- Kornbluh, Peter, ed. *Bay of Pigs Declassified: The Secret CIA Report on the Invasion of Cuba.* New York: The New Press, 1998.
- Wyden, Peter. *Bay of Pigs: The Untold Story.* New York: Simon & Schuster, 1979.

- Higgins, Trumbull. *The Perfect Failure: Kennedy, Eisenhower, and the CIA at the Bay of Pigs.* New York: W. W. Norton, 1987.
- Gleijeses, Piero. "Ships in the Night: The CIA, the White House and the Bay of Pigs." *Journal of Latin American Studies* 27, no. 1 (1995): 1–42.

R3 Intelligence oversight scholarship and legal frameworks

- United States. *National Security Act of 1947.* Pub. L. No. 80-253, 61 Stat. 495 (1947).
- United States. *Central Intelligence Agency Act of 1949.* Pub. L. No. 81-110, 63 Stat. 208 (1949).
- United States. *Foreign Intelligence Surveillance Act of 1978.* Pub. L. No. 95-511, 92 Stat. 1783 (1978).
- United States. *Intelligence Oversight Act of 1980* (enacted via Intelligence Authorization legislation). Pub. L. No. 96-450, 94 Stat. 1975 (1980).
- United States. *Foreign Assistance Act of 1974* (Hughes–Ryan Amendment, covert-action reporting requirement). Pub. L. No. 93-559, 88 Stat. 1795 (1974).
- United States. 50 U.S.C. § 3093, "Presidential approval and reporting of covert actions" (as amended; current U.S. Code section governing covert-action findings and reporting).
- Reagan, Ronald. *Executive Order 12333: United States Intelligence Activities.* 46 Fed. Reg. 59941 (Dec. 4, 1981), as amended (notably Exec. Order 13470, 73 Fed. Reg. 45325 (July 30, 2008)).
- U.S. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Final Report* (the "Church Committee" report). 6 vols. Washington, DC: U.S. Government Printing Office, 1976.
- U.S. Senate. Select Committee on Intelligence. *Committee Study of the Central Intelligence Agency's Detention and Interrogation Program: Executive Summary and Findings and Conclusions.* Washington, DC: U.S. Government Printing Office, 2014.
- U.S. Commission on Protecting and Reducing Government Secrecy. *Report of the Commission on Protecting and Reducing Government Secrecy.* S. Doc. 105-2. Washington, DC: U.S. Government Printing Office, 1997.
- Snider, L. Britt. *The Agency and the Hill: CIA's Relationship with Congress, 1946–2004.* Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2008.

- Congressional Research Service. *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions in Brief.* (CRS report; updated periodically; cite the specific version/date used in final drafting.)

R4 Civil-military relations and executive power literature

- Huntington, Samuel P. *The Soldier and the State: The Theory and Politics of Civil–Military Relations.* Cambridge, MA: Harvard University Press, 1957.
- Feaver, Peter D. *Armed Servants: Agency, Oversight, and Civil–Military Relations.* Cambridge, MA: Harvard University Press, 2003.
- Schlesinger, Arthur M., Jr. *The Imperial Presidency.* Boston: Houghton Mifflin, 1973.
- Neustadt, Richard E. *Presidential Power and the Modern Presidents: The Politics of Leadership from Roosevelt to Reagan.* New York: Free Press, 1990 (rev. ed.).
- Schwarz, Frederick A. O., Jr., and Aziz Z. Huq. *Unchecked and Unbalanced: Presidential Power in a Time of Terror.* New York: The New Press, 2018.

R5 Ethics of secrecy, democratic theory, and accountability design

- Bok, Sissela. *Secrets: On the Ethics of Concealment and Revelation.* New York: Pantheon Books, 1982.
- Sagar, Rahul. *Secrets and Leaks: The Dilemma of State Secrecy.* Princeton, NJ: Princeton University Press, 2013.
- Thompson, Dennis F. *Democratic Secrecy.* Princeton, NJ: Princeton University Press, 1999.
- Pozen, David E. "Deep Secrecy." *Stanford Law Review* 62, no. 2 (2010): 257–339.
- Fenster, Mark. *The Transparency Fix: Secrets, Leaks, and Uncontrollable Government Information.* Stanford, CA: Stanford University Press, 2017.
- Moynihan, Daniel Patrick. *Secrecy: The American Experience.* New Haven, CT: Yale University Press, 1998.
- Johnson, Loch K. *A Season of Inquiry: The Senate Intelligence Investigation.* Lexington: University Press of Kentucky, 1985.

- Johnson, Loch K. *National Security Intelligence: Secret Operations in an Open World.* Cambridge: Polity Press, 2012.
- Zegart, Amy B. *Spying Blind: The CIA, the FBI, and the Origins of 9/11.* Princeton, NJ: Princeton University Press, 2007.

The author has published over 4,700 AI-assisted papers at: https://www.researchgate.net/profile/Douglas-Youvan/research . Google Scholar has indexed these preprints, and if you want a particular reference, the AI mode of a Google search (Gemini) has efficiently catalogued these preprints.