The Disclosure Dilemma: Nuclear Intelligence and International Organization

Allison Carnegie and Austin M. Carson*

October 6, 2017

*Allison Carnegie is Assistant Professor, Department of Political Science, Columbia University, New York, NY (Email: allison.carnegie@columbia.edu). Austin M. Carson is Assistant Professor, Department of Political Science, University of Chicago, Chicago, IL (Email: acarson@uchicago.edu). We thank Jeff Colgan, Sarah Daly, Christina Davis, Lindsay Dolan, Page Fortna, Andrew Gelman, Thomas Groll, Alisha Holland, Turkuler Isiksel, Ashley Jester, Leslie Johns, Jeff Kaplow, Andrew Kerner, Chris Kojm, Austin Long, Gwyneth McClendon, John Marshall, Krzysztof Pelc, Maggie Peters, Paul Poast, Carlo Prato, Tonya Putnam, David Steinberg, Joshua Simon, Arthur Spirling, Felicity Vabulas, Jane Vaynman, and Tristan Volpe for helpful comments. We also thank the participants of the APSA 2016 and 2017 and IPES 2015 conferences and seminars at Columbia University, Georgetown University, George Washington University, Harvard University, the University of Chicago, the University of Michigan, and the University of Pennsylvania. We received excellent research assistance from Justin Canfil, Donald Casler, Richard Clark, Andrew Kosenko, Bryan Schonfeld, Laura Sipe, and Joon Yang. We gratefully acknowledge funding from the Columbia Provost’s Grant. All remaining errors are our own.
The Disclosure Dilemma: Nuclear Intelligence and International Organization

Abstract

Scholars have long argued that international institutions solve information problems through increased transparency. This article introduces a distinct information problem that such institutions can address by keeping information secret instead. We argue that states are often tempted to reveal intelligence about other states’ violations of international rules and laws but are deterred by concerns about revealing the sources and methods used to collect such information. Properly equipped international institutions, however, can mitigate these disclosure dilemmas by analyzing and acting on sensitive information while protecting it from wide disclosure. Using new data on intelligence sharing with the International Atomic Energy Agency and a complete set of case study analyses, we demonstrate that reforms that strengthened the Agency’s intelligence safeguarding capabilities led to more frequent intelligence-sharing and resulted in fewer nuclear-related transgressions. Our theory suggests that solving these disclosure dilemmas not only can facilitate compliance with international norms and laws but also can provide informed states with a subtle tool of influence that creates tension with the normative goal of international transparency.

Keywords: global governance, IAEA, intelligence, international organizations, international law, nuclear weapons
Theories of international cooperation have long argued that states follow international rules because non-compliance can prompt naming-and-shaming, damage reputations, and even lead to sanctions or military action. To punish states effectively, however, the international community must first learn about such breaches. Detection is difficult since states tend to hide violations and international institutions are rarely equipped with the authority and resources to intrusively monitor compliance. At the same time, many states invest billions of dollars each year to maintain intelligence services that gather troves of information, some of which pertain to states’ adherence to international treaties, norms, and conventions. States with intelligence could therefore help to fill informational gaps in the international monitoring of compliance behavior, but they often refuse to do so. While states choose not to share information for many reasons, we highlight an especially acute disclosure problem in the security domain: sharing intelligence tends to expose sensitive sources and methods that are necessary to continue to obtain this intelligence.

The challenges of monitoring nuclear proliferation illustrate this logic. In 1978 and 1979, American intelligence discovered progress in Pakistan’s uranium enrichment and plutonium reprocessing efforts. Islamabad’s program posed a threat to both regional stability and the non-proliferation regime, and the U.S. wrestled with how to address it. Washington considered sharing intelligence details that were “of utmost sensitivity” with states like India, Israel, and Taiwan. Doing so would have potentially improved the responsiveness of key international audiences by providing powerful evidence that would be resistant to claims of mistaken or manufactured intelligence. However, sharing this information would also disclose how the U.S. had learned of Pakistan’s program, which “could threaten the effectiveness of [its] efforts” by allowing Pakistan and others to adapt.

1 State to U.S. Embassy in Vienna, “Pakistan Nuclear Program,” Cable 075309, March 26, 1979. National Archives AAD.
We refer to this situation as a “disclosure dilemma,” which arises when states possess private information whose wider dissemination would yield political benefits but would also trigger negative political or operational externalities. Intelligence is one kind of sensitive information that often gives rise to disclosure dilemmas. While its revelation can further a state’s political goals, especially regarding unfriendly actors like adversaries and terror groups, its wider dissemination risks undermining future intelligence collection. These dilemmas arise frequently in international relations. For example, intelligence might reveal the locations of mass graves or identify military orders that implicate war criminals. Sharing it can facilitate the prosecution of war criminals but also risks tipping off intelligence targets. Supplying intelligence might also help peacekeeping missions improve situational awareness and highlight threats to ceasefire agreements, yet again risks revealing the sources used to gather it. Beyond intelligence, states often obtain unique, private information about economic firms operating within their territory. For example, sensitive pricing or cost information might help to resolve a trade dispute, but releasing it may reveal information that jeopardizes a firm’s competitive position.

While such dilemmas often appear intractable, this article argues that international organizations (IOs) can often mitigate them. When IOs are equipped to receive and protect sensitive information, they encourage intelligence sharing by minimizing threats to states’ future intelligence collection. Moreover, IOs can use their technical expertise and monitoring abilities to vet intelligence-based claims, solving persistent credibility problems that occur when states make such allegations unilaterally. The resulting higher quality of information improves international monitoring and enforcement efforts and, as a result, overall compliance with a regime.

We evaluate these claims in the nuclear nonproliferation regime by taking advantage of changes over time in the use of intelligence at the International Atomic Energy Agency (IAEA). In particular, we collected new data on intelligence-sharing from archival documents, interviews with current and former officials, and secondary sources. We then assess changes in intelligence sharing and proliferation patterns through case study analyses using the universe of cases of nuclear proliferation since 1970. We find that these changes elicited more frequent intelligence sharing, improved
monitoring, and boosted compliance with rules barring new nuclear proliferation.

The article makes two main contributions. First, we identify a function for IOs that is broadly applicable and modifies the literature’s central argument that institutions facilitate cooperation by making information widely and equitably available (e.g. Keohane (1984)). The classic view suggests that broad dissemination of compliance-related information to both states and non-state actors fuels political processes that improve compliance. We revise and extend this account, arguing that compliance information which is sensitive requires IOs protect rather than widely disseminate key details provided by states. For non-sensitive information, the conventional wisdom holds. This distinct function has direct implications for the effectiveness of IOs, especially regarding monitoring. Yet it also has other side effects. To solve disclosure dilemmas, institutions must develop an organizational capacity for secrecy. This can conflict with the deepening expectation that global governance institutions act with transparency and accountability. Moreover, addressing disclosure dilemmas can endow intelligence-enabled states with a unique and subtle form of power; after all, they can decide when and how much to share.

The second contribution is to the study of nuclear weapons. Our theory and findings identify an under-studied mechanism by which powerful states and the nuclear non-proliferation regime influence other states’ nuclear ambitions. The IAEA is a under-studied feature of the non-proliferation landscape compared to the causes and consequences of proliferation. Scholarship on the non-proliferation regime tends to analyze the treaty and related norms (Rublee, 2009; Coe and Vaynman, 2015a; Fuhrmann and Lupu, 2016) or highlight the IAEA’s weakness and its role in spreading peaceful nuclear technology used for proliferation (Fuhrmann, 2012; Brown and Kaplow, 2014).

---

4 On reputation, variation in monitoring functions, and the role of non-state actors in driving this compliance, see Milgrom, North et al. (1990a); Mitchell (1998); Dai (2005).
5 E.g. (Lall, 2017).
6 See, for example, calls for transparency in multilateral governance of finance, trade, European integration, and environmental regulation (Blanton, 2007; Ehring, 2008; Gupta, 2008; Koenig-Archibugi, 2004; Tallberg et al., 2013).
7 Fuhrmann and Lupu (2016, 538) conclude that “[a]n important next step in research on the NPT is to understand variation in its effectiveness. To do so, future work should consider how the treaty restrains proliferation” (emphasis in original).
8 Though see Brown (2015).
We provide new insights into variation in the monitoring capabilities of the key IO for nuclear proliferation. Moreover, we embed the IAEA’s intelligence-related practices in larger theoretical debates about global governance institutions and distill generalizable links between disclosure dilemmas, intelligence sharing, and the IAEA’s performance.

**Information, Institutions, and Compliance**

Scholars have long recognized that poor information can prevent states from cooperating. The under-provision and uneven distribution of information can allow defections from agreements to go undetected, breeding fears of exploitation. Improving transparency, however, gives states and other actors the raw material to scrutinize non-compliance and punish it through tit-for-tat retaliation and other forms of punishment. Indeed, the supply of “compliance information to facilitate compliance with international agreements,” has become “a centerpiece of neoliberal institutionalism” (Dai, 2002b, 409).

Yet for a particular kind of information – what we call sensitive information – transparency is not an unmitigated good. We focus on national intelligence, or information gathered through clandestine means about other states’ behavior and intentions. Almost all states gather at least some intelligence through highly systematized bureaucracies on issues of national interest (Andrew, 1979). Doing so draws on human and technical intelligence collection methods, such as spy rings, imagery intelligence (i.e. satellite photography), signals intelligence (i.e. interception of cellular or other communication means), and more obscure tactics (i.e. nuclear radiation emission analysis) (Johnson, 2007; Richelson, 2007). Such intelligence can be highly germane to ques-

---

9 See Keohane (1984); Axelrod and Keohane (1985); Milgrom, North et al. (1990b); Mitchell (1998); Koremenos, Lipson and Snidal (2001); Dai (2002a); Lindley (2004); Carrubba (2005); Voeten (2005); Thompson (2006); Lindley (2007); Guzman (2008).

10 Scholars have also recognized drawbacks to information sharing. On the downsides of exposing multilateral diplomacy, see Stasavage (2004); Hafner-Burton, Steinitz-Threlkeld and Victor (2016). For how multilateral monitoring enables coercion, see Marquardt (2007); Lindley (2007). On the perils of domestic institutional transparency, see Finel and Lord (1999); Florini (2002); Lord (2012); Carson (2016).

tions of (non-)compliance either because such behavior is intentionally targeted as a security or economic threat or as a byproduct of intelligence gathering about other priorities (Chesterman, 2006).

Sharing intelligence can advance a state’s practical, diplomatic, and strategic goals. For instance, publicly releasing intelligence can alter domestic public and legislative opinions to facilitate a political leader’s policy agenda or re-election.\(^ {12} \) Publicly revealing American intelligence about Soviet missiles deployed to Cuba helped build domestic support for President Kennedy’s coercive demands during the Cuban Missile Crisis.\(^ {13} \) More narrowly sharing intelligence with allies can align threat perceptions.\(^ {14} \) The availability of intelligence about other states’ (non-)compliance may influence how the international community reacts to such behavior.\(^ {15} \) Yet sharing intelligence has an important downside well understood by intelligence collection practitioners: endangering the deception necessary for its collection in the first place. Sharing intelligence from signals intercepts can lead a target to change its use of a vulnerable cell phone. Providing imagery might provide current or future targets with tips on how to avoid observation in the future. Sharing intelligence from a human source can lead to that source’s expulsion, imprisonment, or death (Richelson, 1990, 2007; Rolington, 2013).\(^ {16} \)

One alternative is to only share conclusions rather than details of sensitive sources and methods. This introduces a credibility problem. Because intelligence sharers have well-known political interests in the issue at stake, unilateral intelligence claims without details are suspect. The Cuban Missile Crisis illustrates: one key reason sensitive U-2 images were released was to make the American claim about Soviet missiles credible (Brugioni, 1991, 389-391). Alternatively, a state

\(^ {12} \)See Hastedt (2005).
\(^ {13} \)See Brugioni (1991, 428-429).
\(^ {14} \)Aldrich (2000); Brown and Farrington (2017).
\(^ {15} \)E.g. Chesterman (2006); Carnegie and Carson (forthcoming).
\(^ {16} \)Note that this trade-off is not always present as when intelligence targets are unable to adapt even if they are aware of a collection method, or when sources will be exposed for other reasons. The Soviet Union, for example, could not adapt to American stealth technology in the 1980s (Rittenhouse Green and Long, 2016). We return to scope conditions in the penultimate section.
could only reveal sources to trusted allies (Walsh, 2010). Yet this substantially limits the practical and political impact given that most state and non-state audiences remain in the dark; this is especially problematic when the goal is influencing broader multilateral responses.

**IOs and the Disclosure Dilemma**

These dilemmas therefore lead states to typically err on the side of withholding intelligence from international and domestic audiences and preserving informational control.\(^{17}\) One possible way to ease the disclosure dilemma is via international organizations. The intuition is that IOs can receive, analyze, and potentially act on sensitive information. Intelligence can provide the IO with unique information about compliance. This enables more effective monitoring. For the sharing state, the IO offers a narrower disclosure method which can limit damage to sources and methods. Moreover, the IO can validate and supplement suspicions based on intelligence which addresses credibility problems from unilateral claims. In short, IOs can offer states a *via media* between public disclosure and keeping intelligence private.

IOs can serve this purpose under two conditions. First, they must be designed to receive and protect sensitive information. Member-states and the IO itself must create and maintain an organizational capacity to limit the dissemination of information within the IO, preventing unauthorized leaking. This can require a document classification system, physical and cyber security measures for stored data, and rules for how employees can handle such information including penalties for disclosure.\(^{18}\) Second, IOs must have the capacity to credibly review, assess, and act on sensitive information. This requires developing a reputation for technical expertise and unbiased judgment. Without this, IOs will be unable to resolve the credibility problems the intelligence donor itself

---

\(^{17}\)See (Lefebvre, 2003, 523); (Walsh, 2010, 6).

\(^{18}\)On organizational capacity and secrecy, see Geser (1992); Gibson (2014). On the incentives and risks for leaking documents in government institutions, see Pozen (2013); Sagar (2016). Note that IOs may not always succeed in preventing the adaptation that damages intelligence collection if a non-complying state can infer the source of intelligence simply from questions being asked. This and other scope conditions related to information security are discussed below.
faces and will be vulnerable to frivolous and politically motivated assertions.\textsuperscript{19} States that are not privy to the raw intelligence, moreover, will trust conclusions from the IO if the process of vetting is seen as credible. Moreover, having an IO so equipped influences the perception of unilateral intelligence claims: states that refuse to subject their claims to the IO’s scrutiny will appear even more likely to have mistaken or manufactured information.\textsuperscript{20}

To clarify, institutions easing disclosure dilemmas can help through two distinct mechanisms. First, the IO can provide the equivalent of a “second opinion.” Applying technical expertise and its own base of information in a politically unbiased manner allows an IO to screen out inconclusive, mistaken, and manipulated claims. This, in turn, can boost the political impact of intelligence and make state and non-state actors more likely to support preventive or remedial action against a violator. Second, IOs that possess delegated monitoring authority can gather additional information, supplementing intelligence it receives from one or more member-state. This can be crucial because even high-quality intelligence may only suggest suspicious behavior, falling short of conclusive demonstration. An IO that receives intelligence can follow up on these “tips,” asking better questions and scrutinizing hidden or unreported activities.

However, just because states \emph{can} reveal information without jeopardizing their intelligence collection capabilities does not mean they \emph{will}. In particular, states may not wish to share intelligence that negatively implicates close friends or allies. Doing so could threaten cooperation between such states, jeopardize political goals, and weaken states that are important for the informed state’s national security. Moreover, the benefits of multilateral cooperation may be reduced in such cases since states tend to have more influence over their friends, with which they often have extensive trade, financial, and other ties. Our theory thus expects states with information about violations of international norms and laws to reveal intelligence to IOs when: 1) those IOs are equipped to receive it and 2) its intelligence does not implicate the informed state’s friends.

\textsuperscript{19}Others have shown third party mediators, including IOs, can validate information about compliance in conflict settings, though the specific importance of protecting sensitive information has not been developed at length. See, for example, Kydd (2006); Lindley (2007); Mattes and Savun (2010).

\textsuperscript{20}On the role of IOs in validating and legitimizing policy proposals more broadly, see Voeten (2005); Thompson (2006); Chapman (2007).
This view of IOs both revises traditional theories about the function of these institutions. Beginning with Keohane (1984), rational institutionalist theories have developed how IOs can improve the information environment and facilitate state cooperation. A key theme is wide dissemination: Keohane (1984, 94) argues that IOs must guarantee that information “is made available, more or less equally to all members,” while Dai (2002a, 411) describes an IO as serving “as a repository and communicator of information.” We argue that, when sensitive information is important to identifying non-compliance, IOs must instead limit the dissemination of specific details regarding intelligence. In this scenario, IOs preserve the opacity of key details in order to monitor more effectively and make compliance more transparent. The function we develop is therefore a modification, rather than refutation, of the standard account. The net result of integrating intelligence is improved confidence that non-compliance will be identified. Moreover, IOs can serve both functions. The same IO could widely disseminate non-sensitive data about some behavior or events while also protecting confidential details about others.

A Model of Intelligence Disclosures

We develop a simple formal model as a heuristic device to analyze the impediments to information-sharing in the absence of an IO as well as how IOs might ease such dilemmas. The model specifically contrasts institutional solutions to cooperation problems that emerge from non-sensitive and sensitive information. The model makes our assumptions transparent, clarifies how our argument differs from extant scholarship, and allows us to rigorously derive testable implications. This section describes the model in brief; the proofs appear in the supplemental appendix due to space constraints.

The game features three actors: state $E$ (the intelligence holder), state $A$ (the potential rule

---

21 Other cooperation-enhancing functions beyond information provision include serving as forums and facilitating issue linkage (Keohane, 1984) and allowing states to make credible commitments (North and Weingast, 1989; Carnegie, 2015).

22 The IAEA, for example, both releases non-sensitive data on nuclear safety and judiciously protects compliance information that has been submitted confidentially.
violator), and \( I \) (the international community). An IO may also be present, though it is not a strategic actor. The game begins with Nature choosing whether information that is needed to assess \( A \)’s compliance is sensitive or not. If it is not sensitive, it can be gathered by either \( E \) or the IO. If information is sensitive, only \( E \) can gather it, as the IO is not equipped to do so.

\( A \) then chooses whether to violate international law, denoted \( v, \neg v \). The international community does not observe \( A \)’s action while \( E \) detects \( A \)’s action via its strong intelligence capabilities. \( E \) next determines whether to publicly declare that \( A \) violated the law, denoted \( D, \neg D \). If \( E \) decides to do so, it must further choose whether to reveal its sources and methods \( m, \neg m \) to substantiate its claims.\(^{23}\) After observing \( E \)’s actions, \( I \) chooses whether to sanction \( A \) based on its beliefs about whether a violation has occurred. These beliefs are denoted \( p \) if \( E \) has disclosed information (but no sources and methods have been revealed) and \( q \) if no information has been disclosed. Formally, a pure strategy for \( A \) is an element of the tuple \( \{ V, \neg V \} \); a pure strategy for \( E \) is an element of the four-element set \( \{ (D,M),(D,\neg M),D,\neg D \} \); and a pure strategy for \( I \) is an element of the set \( \{ e, \neg e \} \). Our solution concept is (weak) perfect Bayesian equilibrium, and we consider only pure strategies. Such an equilibrium consists of strategies \( \{ \sigma_A, \sigma_E, \sigma_I \} \) and beliefs \( \{ p, q \} \) so that given beliefs, each player’s strategy maximizes her expected payoff, and that the beliefs are computed from strategies according to Bayes’ rule whenever possible.

The actors’ utilities are determined as follows. \( A \) receives both costs and benefits from violating the law, summarized by the term \( v \in [0, 1] \), which indicates whether a violation occurred. \( A \) also loses utility from \( I \)’s enforcement efforts, where \( e \in [0, 1] \) indicates whether enforcement occurs. The term \( \alpha \) captures how much utility \( A \) loses from these efforts, which could reflect \( A \)’s attempts to resist sanctions, its dependence on \( I \) for investment or other resources, etc. If \( E \) reveals sources and methods that show that \( A \) violated the law, \( A \) also loses \( \beta \), because \( I \) knows for sure about \( A \)’s transgression. \( A \) thus suffers a reputational hit that may make \( I \) less willing to cooperate with \( A \) in the future. \( A \)’s utility function is thus \( v - \alpha e \) if sources and methods are not revealed, and

\(^{23}\)Sources and methods cannot be revealed if \( A \) did not violate the law since we assume that \( E \) cannot falsely provide this proof. This assumption could be easily relaxed.
\( v - \alpha e - \beta \) if they are revealed.

\( E \) has political considerations which may lead to bias \( b \) against \( A \). This component of \( E \)'s utility is expressed as \(- (e - (v + b))^2\), so that \( E \)'s bias prevents it from desiring perfect enforcement. \( E \) also loses utility from three activities: First, \( E \) pays \( c_M \) for revealing sources and methods due to the damage that doing so causes to future intelligence collection. Additionally, \( E \) pays \( c_L \) from lying due to the risk that domestic or international populations will discover the lie later, expending efforts to cover the lie up, and a potential intrinsic preference for truth-telling.\(^{24}\) Finally, \( E \) pays \( c_D \) if it discloses information. This cost is made a basic transaction cost, and is higher when \( E \) discloses information about its friends. \( E \) prefers not to reveal information about its friends’ misdeeds both to protect them and because it is often less costly to confront an ally privately. As we detail elsewhere, \( E \) often has leverage over allies that it does not have over other states, making alternative routes of enforcement cheaper. While these routes are not explicitly modeled, they are summarized by this cost for simplicity.

Lastly, \( I \) simply wants to enforce the law in an unbiased manner, so that its utility function is \(- (e - v)^2\). These payoffs are depicted in the game tree and are summarized in the table of parameters.

\(^{24}\)We assume that if \( E \) is indifferent between two actions, it tells the truth.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Interpretation</th>
<th>Range/restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>( v )</td>
<td>Indicates whether a violation occurred</td>
<td>( v \in [0, 1] )</td>
</tr>
<tr>
<td>( \alpha )</td>
<td>A’s utility loss from being retaliated against</td>
<td>( \alpha \in \mathbb{R}_+, n &lt; \alpha )</td>
</tr>
<tr>
<td>( \beta )</td>
<td>A’s utility from being caught with evidence</td>
<td>( \beta \in \mathbb{R}_+ )</td>
</tr>
<tr>
<td>( b )</td>
<td>( E )'s &quot;Bias&quot; towards ( A ); higher values denote greater negative bias</td>
<td>( b \in \mathbb{R}_+ )</td>
</tr>
<tr>
<td>( c_L )</td>
<td>( E )'s cost from lying</td>
<td>( c_L \in \mathbb{R}_+ )</td>
</tr>
<tr>
<td>( c_D )</td>
<td>( E )'s transaction cost from disclosing</td>
<td>( c_D \in \mathbb{R}_+ )</td>
</tr>
<tr>
<td>( c_M )</td>
<td>( E )'s cost from revealing sources and methods</td>
<td>( c_M \in \mathbb{R}_+ )</td>
</tr>
<tr>
<td>( p )</td>
<td>Probability that ( I ) assigns to ( A ) having violated, conditional upon being asked to move following ( \neg M )</td>
<td>( p \in [0, 1] )</td>
</tr>
<tr>
<td>( q )</td>
<td>Probability that ( I ) assigns to ( A ) having violated, conditional upon being asked to move following ( \neg D )</td>
<td>( q \in [0, 1] )</td>
</tr>
</tbody>
</table>

We assume that \( c_L > b - \frac{1}{2} \), which ensures that the bias of \( E \) is not too great relative to the truth-telling motive. Intuitively, if \( E \) is too biased against \( A \), it will always accuse \( A \) of violating, and the disclosure dilemma cannot be solved. We also assume that \( -v > 0 \), otherwise \( A \) would never violate the rules. We assume that \( v < \alpha \) to avoid trivialities. Finally, we assume that the value of \( c_D \) is so great that \( E \) never reports a violation by an ally. We thus solve the model for the case of non-allies. We first consider information that is not sensitive, and compare the equilibria in a world without an IO to the equilibria in a world with one. We then examine information that is sensitive, and compare the equilibria in a world without an IO that can protect sources and methods to a world with such an IO.

**Solution: No IO, Info not Sensitive**

The equilibrium here is straight-forward. \( E \) gathers compliance information as long as doing so is not too costly. Since the information is straight-forward, \( E \) does not have to prove its claims. \( I \) can
Figure 1: Game Tree
thus see whether $A$ violated. $A$ then does not violate, and is not punished. If the information is too costly, however, $E$ does not gather compliance information and $A$ may violate, after which $I$ may punish. ***Need to solve this fully***

**Solution: IO, Info not Sensitive**

If the information relative to a dispute is not sensitive, the IO can be empowered to collect it and to thus verify and disseminate compliance determinations (Maggi 1999). In this case, the above game simplifies greatly. $E$ no longer is a strategic player, since the IO simply checks whether a violation occurred or not. $I$ then punishes if one occurred and does not punish otherwise. Thus, $A$ violates only if the benefits of doing so outweigh the drawbacks of the punishment. Since we have assumed that they do not, $A$ does not violate the rules, and the IO maintains international cooperation. ***Solve fully***

**Solution: No IO, Info Sensitive**

Two equilibria exist. In the first, $A$ plays $V$, $E$ selects $D$ and then $\neg M$, and $I$ chooses $e$; it can be checked that this is an equilibrium for any $\{p,q|p \geq \frac{1}{2}, q \geq \frac{1}{2}\}$. This equilibrium is supported by $E$’s off-path actions $D$ and $\neg M$. In the second equilibrium, as long as the assumption about $k$ is satisfied, $A$ plays $\neg V$, $E$ selects $\neg D$ and $I$ chooses $\neg e$. $I$’s beliefs are $p = 1$ and $q = 0$, and the equilibrium is again supported by $E$’s off-path actions $D$ and $\neg M$.

Notice that $E$ does not share its sources and methods in either equilibrium, as the model highlights the key tradeoff that $E$ faces when an IO is not available. In particular, $E$ often cannot credibly convey its information to the international community unless it shares sources and methods details, but it faces a high cost of doing so since this would compromise $E$’s future intelligence collection capabilities. However, as a result, $A$’s violations are commonly unidentified, unpunished, and therefore undeterred.

---

$^25 p = q = 1$ since actions pin down beliefs.
This outcome is conditional on $E$’s bias, however; if $E$ is unbiased, $E$ and $I$’s incentives perfectly align and there is no reason for $I$ to doubt $E$’s claims. However, the less neutral $E$ feels, the more $I$ views $E$’s claims with suspicion because of the potential for politically-motivated allegations. As a result, $I$ often chooses not to punish $A$, making $A$’s initial violation more likely.

**Solution: IO; Info Sensitive**

Sometimes, however, IOs are not able to collect their own information. States often do not want to empower IOs when the information to be collected is sensitive due to sovereignty costs and the financial expenditure needed to do so. In such a scenario, IOs often must rely on states to provide them with information. Thus, suppose that the states play the same game but $E$ has an option of securely providing intelligence – including sources and methods details – to an IO, so that $p = 0$. As we explained previously, many IOs can validate and/or supplement $E$’s intelligence, and then disseminate its overall conclusions to $I$. Further, because the IO is not as biased as $E$ is, $I$ tends to believe the IO’s conclusions.\(^{26}\)

In this case, only one equilibrium exists. In particular, notice that for $p \geq \frac{1}{2}, q \geq \frac{1}{2}$, $E$ is indifferent between $(D, M)$ and $(D, \neg M)$ after a violation. The equilibrium in which $A$ violates the rules becomes a knife-edge case, which we have assumed does not occur since it relies on a player’s exact indifference between two options, which rarely occurs in reality. Further, if we allow for perturbations of the payoffs, the knife-edge equilibrium may not exist at all, and is therefore not robust.\(^{27}\) However, the set of parameters that supports the non-violating equilibrium is not made empty by taking $p$ to 0, so that equilibrium is not eliminated by the parameter change. There is

\(^{26}\)While we do not explicitly model the IO’s independent incentives in an iterated game structure, it would be straight-forward to show that an IO’s concerns about its reputation for honesty motivate it to carry out these functions in an unbiased way. We do not incorporate an IO as an agent in order to focus attention on the strategic choices most relevant to the theory. Further, this formalization makes clear that we do not conceptualize IOs as “biased experts” (Krishna and Morgan, 2001) or “advocates” (Dewatripont and Tirole, 1999) which have incentives to misrepresent their information to the international community. Our conceptualization also differs from “mediators” which typically seek to promote cooperation between two feuding parties, and which face conflicting incentives over whether to report violations of agreements (Kydd, 2006). We discuss this further in the discussion subsequently.

\(^{27}\)Even if we do not assume that the knife-edge case does not exist, if $E$ chooses a different action since it is indifferent, the equilibrium with a violation again disappears.
thus only one equilibrium, and \( A \) never violates the norm with positive probability.

The secure IO therefore encourages \( E \)’s revelation of sources and methods if \( E \) desires to reveal them, i.e. when \( A \) is not a friend. It thus also leads \( I \) to punish \( A \)’s defections, and thus reduces the defections in the first place. These claims lead to two testable hypotheses. First, when an IO can safeguard states’ sources and methods, \( E \) should be more likely to share its intelligence, particularly when it has a political motive to do so.

**Proposition 1.** *The greater the intelligence reception and protection capabilities of an IO, the more intelligence informed states share with it, particularly about states they are not friendly with.*

Moreover, because increased intelligence-sharing allows states to detect noncompliance and agree on collective punishments and/or opprobrium, \( A \) should be more likely to curb violations of international law.\(^{28}\) Again, this is more likely when \( E \) is not friendly with \( A \).

**Proposition 2.** *The greater the intelligence reception and protection capabilities of an IO, the fewer violations of international law occur, particularly for states that are not friendly with informed states.*

Table 1: Summary of Intel Sharing Decisions

<table>
<thead>
<tr>
<th></th>
<th>IO Unable to Protect Intel</th>
<th>IO Able to Protect Intel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel About Friends</td>
<td>Little Sharing</td>
<td>Little Sharing</td>
</tr>
<tr>
<td></td>
<td>Violations Common</td>
<td>Violations Common</td>
</tr>
<tr>
<td>Intel About Non-Friends</td>
<td>Little Sharing</td>
<td>Frequent Sharing</td>
</tr>
<tr>
<td></td>
<td>Violations Common</td>
<td>Violations Uncommon</td>
</tr>
</tbody>
</table>

**Nuclear Intelligence and the IAEA**

We apply the insights of our model to the nuclear domain both for empirical tractability and due to the substantive importance of nuclear nonproliferation. States routinely gather intelligence about

\(^{28}\)The enforcer is necessary to obtain an equilibrium in which \( A \) does not violate, as the intelligence is critical for deterring \( A \)’s violation. Results for these equilibria available from the authors.
others’ nuclear programs that may pose direct or indirect security threats. This can include tracking overt and clandestine nuclear facilities, estimating stockpiled uranium or plutonium useful for weapons purposes, and monitoring trade in sensitive technologies (Richelson, 2007). Such intelligence directly bears on whether a government is in compliance with formal treaty commitments (i.e. the Nuclear Nonproliferation Treaty) and the corresponding norm against new nuclear weapons programs. We define a violation as a non-nuclear state developing nuclear infrastructure and weaponization for military purposes whether for security, prestige, or other motivations (Sagan, 2012).

Nuclear intelligence often creates disclosure dilemmas. On one hand, sharing it can sound alarm bells and facilitate diplomatic, economic, and other forms of pressure that might slow proliferation.29 This is particularly important because the security and symbolic value of nuclear weapons means intelligence holder rarely possess sufficient unilateral leverage to stop a program.30 As one internal report from the intelligence donor we analyze noted, “US leverage over the nuclear programs of Argentina, Brazil, South Africa, Iraq, and Libya is marginal and we have absolutely no influence over the nuclear activities of the East European nations and North Korea.”31 On the other hand, sharing nuclear intelligence risks revealing sensitive sources and methods, endangering future collection opportunities. For example, when Syria learned that its nuclear activities were monitored using satellites, it moved its nuclear site underground.32 Further, sharing intelligence conclusions without providing sources and methods raises new credibility problems. As the controversy over intelligence claims about Iraq in 2002-2003 dramatized, geopolitical and even personal sources of bias can reduce the credibility of unilateral claims by intelligence-holders (Pillar, 2006; Rovner, 2011).

29On risks of sounding the alarm if reversal is unlikely, see (Carnegie and Carson, forthcoming).
30Though see coercion among allies with nuclear ambitions in (Fuhrmann and Kreps, 2010; Miller, 2014; Solingen, 2012; Gerzhoy, 2015).
The IO charged with monitoring nuclear non-proliferation is the IAEA. It has been equipped to receive, protect, and act on intelligence since reforms instituted in 1991 after the discovery of Iraq’s clandestine nuclear program during the Persian Gulf War (Rauf and Kelley, 2015, 16). While the IAEA had the authority to receive intelligence prior to 1991, the agency lacked protections for especially sensitive intelligence information. Member-states and the IAEA adopted reforms that encouraged governments to share information about non-compliance on a confidential basis (Carmody, 1994) and that established “the organizational requirements necessary [for the IAEA] to receive intelligence information” (Dembinski, 1995, 32). These measures included clarification that IAEA staff would sign non-disclosure agreements, limited access to intelligence, procedures to address breaches of confidentiality, and secure cyber and physical infrastructure for sensitive information.

How does this work in practice? Intelligence may be shared via briefings with the Director General – whom powerful, informed states ensure that they trust during the selection process – and a select few staff members. To ensure security, intelligence material might be stored in the Director General’s office or other secure areas and read only by thoroughly vetted staff members. Other shared intelligence is integrated into the IAEA’s Safeguards Division data system. Improvements to the information management system allow the secretariat to limit access to specific details to select staff. These intelligence-related measures benefit from the IAEA’s decades-long experience handling sensitive information collected during its on-site inspections and from member-states declarations about their own infrastructure.

---

33Interview 2. Because our interviewees were promised no attribution, we refer to interview by number. Article VIII of the 1956 IAEA Statute on “Exchange of information” states member-states should “make available such information as would, in the judgment of the member, be helpful to the Agency.” Reflecting the traditional transparency function of the IO, the same article states that the “Agency shall assemble and make available in an accessible form the information made available to it.”

34Interviews 4, 6; (Louka, 2011, 122). Note that we discuss other changes at the IAEA not directly related to intelligence in the Alternative Explanation section.

35Interviews 14 and 42.

36Interview 6.

37Interview 43, 14; an overview of safeguards and confidentiality is (Rockwood, 2007).
IAEA then evaluates intelligence-based claims either through extant expertise and information or through new monitoring activities such as on-site inspections.

Integration of intelligence has, at times, been controversial. By adopting “procedural safeguards that guarantee its objectivity and neutrality when using such information” (Coppen, 2015), the IAEA has sought to reassure member-states that it does not do the bidding of intelligence donors. As a former top IAEA official wrote, “all information provided to the Agency goes through a rigorous process of internal IAEA corroboration” (Heinonen, 2013). Very visible demonstrations of its independence include the IAEA rebuffing offers of intelligence about South Africa and rejecting the quality of shared intelligence during the run-up to the Iraq War in 2003. The multinational staff also helps broaden the credibility of judgments and conclusions reached by the IAEA. States, including those that serve as intelligence donors, recognize the value of the IAEA’s reputation for non-bias.

Empirical Analysis

Hypotheses

Our empirical analysis focuses on U.S. intelligence sharing patterns and IAEA performance before and after intelligence-related reforms. We do this for several reasons. The U.S. has the most sophisticated intelligence collection capabilities of any state and a history of monitoring proliferation. Our interviews suggest that the U.S. has provided more intelligence to the Agency than other states. The importance of U.S. behavior is magnified because other providers (e.g. Britain, 

38 The IAEA rejected offers of intelligence regarding South African dismantlement of its nuclear weapons program in 1994 in part to show “institutional impartiality and integrity” (Brown, 2015, 108). It rejected the validity of intelligence about yellowcake purchases by Iraq from Niger (Interview 10).


40 Brown (2015, 125) state that American leaders, for example, “recognize that the appearance of excessive US influence would compromise the basis for Agency authority with others.”

41 Interview 7.
France, Germany) do not contribute as frequently and share information about similar states in similar circumstances. Moreover, while China and Russia collect intelligence, they do not tend to share it with the IAEA because they do not trust the IAEA to safeguard it despite the protections we detail above. Thus, in practice, the IAEA mainly solves disclosure dilemmas for Western countries. Finally, U.S. archival records regarding intelligence and nuclear proliferation are more accessible and consistent in the period we analyze.

Our theory expects that intelligence sharing with the IAEA is most common when 1) the IAEA is equipped to safeguard sensitive information; and, 2) the discloser has a political incentive to provide such information. The second condition is an important qualifier. As Louka (2011, 121) notes, “states have not been keen on sharing their intelligence information with the IAEA unless it serves the states interests.” We operationalize the first condition by comparing states’ behavior before and after the IAEA’s intelligence-related reforms. We operationalize the second condition by alliance status. We assume that, on the whole, the U.S. prefers to share intelligence about non-allies and withhold for allies both because the threat of a nuclear arsenal in the former is greater and because Washington possesses other tools besides IAEA-enabled multilateral pressure for allies (Miller, 2014; Gerzhoy, 2015). These claims suggest:

**Hypothesis 1a.** The U.S. shared more intelligence with the IAEA about the nuclear activities of its non-allies in the post-1990 period than it did in the previous period.

**Hypothesis 1b.** The U.S. shared the same amount of intelligence with the IAEA about the nuclear activities of its allies in the post-1990 period than it did in the previous period.

Our model also suggests shared intelligence should lead to better monitoring and strengthen the credibility of claims of non-compliance in the eyes of the international community. This, in turn, should strengthen compliance. Since non-allies of the U.S. were more likely to be monitored and caught after 1990, our theory suggests they should be less willing to engage in military programs or

---

42 Interview 2.

43 We emphasize that this does not constitute a natural experiment, since these changes were not made at random (e.g. Carnegie and Samii (2017). We consider alternative explanations subsequently.
activities that could be construed as such. Note that intelligence integration at the IAEA should both identify extant activities more effectively and, *ex ante*, deter new activities in the first place. We should therefore observe:

**Hypothesis 2a.** Non-allies of the U.S. engaged in suspicious nuclear activities less in the post-1990 period than they did in the previous period.

**Hypothesis 2b.** Allies of the U.S. did not engage in suspicious nuclear activities less in the post-1990 period than they did in the previous period.

These hypotheses are summarized in the following table:

<table>
<thead>
<tr>
<th></th>
<th>Pre-Reform</th>
<th>Post-Reform</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Ally</td>
<td>Rare Sharing</td>
<td>Rare Sharing</td>
</tr>
<tr>
<td></td>
<td>Proliferation</td>
<td>Proliferation</td>
</tr>
<tr>
<td>U.S. Non-Ally</td>
<td>Rare Sharing</td>
<td>Frequent Sharing</td>
</tr>
<tr>
<td></td>
<td>Proliferation</td>
<td>Reduced Proliferation</td>
</tr>
</tbody>
</table>

**Case Selection**

We collected new data on intelligence-sharing with the IAEA and its impact on IAEA activities both before and after reforms. One important reason this was feasible is that our hypotheses only require identifying *whether* intelligence was shared rather than the content of that intelligence. To establish the universe of cases, we first identified country-years in which a state pursued a nuclear military capability using data from Bleek (2017). We begin our analysis either once a state began pursuing nuclear weapons or after the codification of the NPT in 1970, whichever came later. A case ends if pursuit of nuclear weapons ends or if a state successfully conducts a publicly acknowledged nuclear weapons test. Note that NPT membership is not a criterion: the

---

44 States may pursue hedging or similar strategies short of full weapons pursuit (Narang, 2016; Volpe, 2017) but the very ambiguity of such efforts often leads to efforts to prevent them.

45 We exclude the original five states with nuclear weapons under the NPT (U.S., China, Russia, Britain, and France).
IAEA often has facility-specific safeguards agreements with non-NPT states which gives the IAEA a routine and sometimes important role.\textsuperscript{46} The resulting list appears in Table 3 below; the exemplar is italicized while the others appear in the Supplemental Appendix due to space constraints.\textsuperscript{47}

<table>
<thead>
<tr>
<th>Table 3: Case Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ally</td>
</tr>
<tr>
<td>South Korea (1970-1981)</td>
</tr>
<tr>
<td>Non-ally</td>
</tr>
<tr>
<td>Brazil (1970-1990)</td>
</tr>
<tr>
<td>India (1970-1974)</td>
</tr>
</tbody>
</table>

For each case, we also coded several variables. First, we assessed whether U.S. intelligence was shared with the IAEA by relying on a combination of memoirs (e.g. ElBaradei (2011)), IAEA public reports on safeguards, secondary accounts of the IAEA (e.g. Brown (2015); Fuhrmann (2012)), secondary accounts of specific states’ programs, and interviews with current and former IAEA and U.S. government officials.\textsuperscript{48} While we record and describe each instance of this sharing in the case studies, our descriptive analysis codes this variable on a scale of 0 to 2 where 0 indicates

\textsuperscript{46}As we describe in the cases, this means the IAEA maintained a normal relationship with well-known non-NPT states at the time like Pakistan, India, Israel, Argentina, and Brazil.

\textsuperscript{47}We omit Yugoslavia due to the absence of declassified information about its program and Ukraine after the end of the Cold War because it inherited a publicly acknowledged nuclear status.

\textsuperscript{48}We conducted 33 interviews in total which includes a former Director General of the IAEA, other high level IAEA staff, policy experts in Washington D.C., and both current and former officials in the U.S. We attempted to reach all IAEA officials that we were able to locate contact information for, and interviewed those who would agree to do so. Note that while our data may contain some measurement error due to unreported intelligence sharing, it is unclear whether this would be more likely to occur in earlier or later periods. On the one hand, respondents may have forgotten or lacked knowledge of cases from earlier years, or intelligence sharing may have received less attention in those years. On the other hand, interviewees can speak about earlier periods more freely, and more information from earlier periods has been declassified. Thus, we have no a priori reason to believe that measurement error is unequal over time.
no sharing, 1 indicates few (1-3) instances of sharing, and 2 indicates more than 3 instances of sharing in a given period. To assess our second hypothesis about the impact of shared intelligence on the pace of nuclear development, we focus on uranium enrichment and plutonium reprocessing (ENR) plants either in construction or operation in a country. While only military applications “for explosive purposes” are prohibited, ENR facilities’ purposes are ambiguous. Because of their dual use, other states and the IAEA often find them especially indicative of exploration or pursuit of weapons, especially when clandestine or unreported. Data on ENR facilities is taken from Fuhrmann and Tkach (2015). Whether facilities were influenced by intelligence-sharing was coded by the authors using both primary and secondary sources, as described in the case studies.

Finally, we also code each case for our two independent variables. Our first is an indicator of the time period, before or after the IAEA reforms in 1991. Our second key independent variable is alliance status according to Leeds (2005). Note that we code Israel as a U.S. ally given its long-standing and well-recognized status as such.49 For each case, we also describe the intelligence that the U.S. possessed, to establish that it was capable of sharing with the IAEA.

Aggregate Results

Table 4 provides aggregate findings that strongly support both hypotheses. Overall, U.S. intelligence sharing was much more common after the 1991 reforms and the IAEA’s success in identifying ENR facilities was greater after 1991, conditional on the ally status of the proliferating state. First consider sharing patterns. The provision of intelligence to the IAEA regarding U.S. allies in the pre-reform period was rare, with no evidence of sharing about Israel and South Korea and small amounts regarding Pakistan and Taiwan. In the post-reform period, this pattern continued. We did not find any instances of sharing for these four states. A different pattern is found for non-allies. In the pre-reform period, we found a few instances of intelligence sharing (e.g. Brazil; North Korea). Post-reforms, intelligence was regularly shared for each non-ally case except for Algeria and Libya, for which it increased moderately from the pre-reform period.

49See, for example, Bar-Siman-Tov (1998).
Now consider the impact of intelligence-sharing on suspect nuclear activities. We found no evidence that U.S. intelligence sharing with the IAEA influenced an ally’s decision to pause, expand, or roll back its ENR facilities. In fact, we found that an enabling condition for nuclear progress in U.S. allies like Pakistan and Israel was poor information at the IAEA, a byproduct in part of U.S. refusal to share. Similarly, allies cases from the pre-reform period that feature nuclear reversals (e.g. South Korea; Taiwan) were the result of direct pressure by the U.S. rather than due to IAEA scrutiny. In contrast, we find evidence that nearly all programs in non-ally cases were influenced at least somewhat by intelligence-sharing with the IAEA in the post-reform period. Especially powerful evidence in favor of our theory are examples of facility closures in which unique insights from shared intelligence played a key role in scrutiny by the IAEA. Note that these data do not capture deterrence effects. For countries with known nuclear ambitions, our data will not include facilities that were never built in the first place due to the fear of detection by an intelligence-enabled IAEA. This makes facilities closures a tough test for the theory.

Table 5 lists a subset of ENR facilities located in non-ally countries and closed after 1990. It also describes our estimate of the role of the IAEA and any intelligence it received in decisions to close such facilities. Some facilities in Table 5 illustrate how intelligence can play a unique role for IAEA monitoring. For example, intelligence shared with the IAEA helped identify unreported activity at the Kalaye Electric Company in Iran and, by enabling multilateral pressure, helped lead to that site’s eventual closure. Other facilities show that intelligence may not necessarily play a role even in the post-reform period. For example, trilateral diplomacy among the U.S., U.K., and Libya that excluded the IAEA was critical in Libya’s closure of two facilities in 2002-2003. Our case study narratives address these facilities in more detail. Moreover, a complete table featuring facilities kept open and closed in both allies and non-allies appears in the Supplemental Appendix.

We now turn to case studies which feature more details on intelligence-sharing patterns and the role of the IAEA and intelligence integration in a state’s nuclear progress. Because the case straddles the pre- and post-reform period, we are able to analyze within-case variation in intelligence-sharing and the IAEA’s role regarding North Korea. Doing so allow for more fine-grained infer-
ences about both hypotheses and their causal mechanisms, including the direct effects of IAEA-level reforms, the role of political considerations for the sharing state (i.e. \( E \)), and how making intelligence available can influence the IAEA’s operations. Other cases, including ones featuring outcomes for allies and in other time periods, appear in the Supplemental Appendix.
<table>
<thead>
<tr>
<th>Proliferator</th>
<th>Ally?</th>
<th>Pre-Reform?</th>
<th>Intel Shared</th>
<th># Facilities Slowed</th>
<th>Support for H1?</th>
<th>Support for H2?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algeria</td>
<td>No</td>
<td>Yes</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Argentina</td>
<td>No</td>
<td>Yes</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Brazil</td>
<td>No</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
<td>Mixed</td>
</tr>
<tr>
<td>India</td>
<td>No</td>
<td>No</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Iraq</td>
<td>No</td>
<td>No</td>
<td>2</td>
<td>5</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Iran</td>
<td>No</td>
<td>Yes</td>
<td>2</td>
<td>0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Israel</td>
<td>No</td>
<td>Yes</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Israel</td>
<td>No</td>
<td>Yes</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Libya</td>
<td>No</td>
<td>Yes</td>
<td>2</td>
<td>5</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Libya</td>
<td>No</td>
<td>Yes</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>North Korea</td>
<td>No</td>
<td>Yes</td>
<td>0</td>
<td>0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Pakistan</td>
<td>No</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
<td>Mixed</td>
</tr>
<tr>
<td>Pakistan</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>South Africa</td>
<td>Yes</td>
<td>No</td>
<td>1</td>
<td>1</td>
<td>Yes</td>
<td>Mixed</td>
</tr>
<tr>
<td>South Africa</td>
<td>Yes</td>
<td>No</td>
<td>1</td>
<td>2</td>
<td>Yes</td>
<td>Mixed</td>
</tr>
<tr>
<td>Syria</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
<td>Mixed</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Yes</td>
<td>Yes</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Country</td>
<td>Enrichment/Reprocessing Facility</td>
<td>Intelligence-sharing (H1) and Intelligence impact (H2)</td>
<td>Theory support?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iran</td>
<td>Tehran Nuclear Research Center (Reprocessing)</td>
<td>U.S. intel sharing stepped up in 1992, 1993. IAEA visit in Feb 1992 includes three new sites based on Western intel</td>
<td>Very strong</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plasma Physics Laboratories in Tehran</td>
<td>IAEA site visits and intelligence leads force Iran to move centrifuge research to less well-known location (Kalaye) in mid-1990s</td>
<td>Strong</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tehran Nuclear Research Center (Enrichment)</td>
<td>Unclear if U.S. intel aware of laser work at TNRC before 2003 revelation; U.S. regularly sharing intel in 2000; Iran’s need for larger facility (Lashkar)</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Kalaye Electric Company</td>
<td>U.S. satellite photos reveal site and evidence of Iranian cover up; initial move to Kalaye due to need to avoid IAEA scrutiny at TNRC</td>
<td>Very strong</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lashkar Ab’dad</td>
<td>Western intel supports IAEA inspections of laser enrichment 2003; Iran ends work due to scrutiny; U.S. intel sharing regularly in 2003/2004</td>
<td>Very strong</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iraq</td>
<td>Lab Reprocessing Facility (Radiochem Lab)</td>
<td>Building destroyed in Persian Gulf War; Western intel does help IAEA confirm plutonium separation in subsequent inspections</td>
<td>Weak (US bombing)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rashdiya Building 22</td>
<td>IAEA fails to detect enrichment work at Rashdiya in 1991 visit; intel sharing and defector information eventually help IAEA confirm in mid-1990s</td>
<td>Strong</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Al Tuwaitha Hot Cell</td>
<td>U.S. intel sharing shows cover up near Tuwaitha and enables IAEA follow-up visit that ensures permanent closure</td>
<td>Very strong</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Al Tarmiya</td>
<td>U.S. intel identified Tarmiya as likely facility before war but did not share; overhead photos shared in 1991 help IAEA identify enrichment work here</td>
<td>Very strong</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Al Tuwaitha Chemical Ion Enrichment Facility</td>
<td>See Al Tuwaitha Hot Cell details</td>
<td>Very strong</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Libya</td>
<td>Tajora Enrichment Facility</td>
<td>U.S. gets new intel on Russian scientists and AQ Khan around 1991/1992 IAEA visits in Feb 1992; extent of intel sharing with IAEA unclear but likely</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Al Hashan Enrichment Facility</td>
<td>U.S. intel aware of enrichment work; no evidence of sharing with IAEA; closure related to U.S.-U.K.-Libya diplomatic deal (no IAEA role)</td>
<td>Weak (US-UK diplomacy)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Plutonium Separation Facility at Tajora</td>
<td>Closure related to U.S.-U.K.-Libya diplomatic deal (no IAEA role); U.S. blocks U.K. sharing intel with IAEA DG to protect negotiations</td>
<td>Weak (US-UK diplomacy)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>North Korea</td>
<td>Radio Chemical Laboratory (Yongbyon)</td>
<td>U.S. imagery key to initial IAEA scrutiny; more U.S. intel sharing helps IAEA visits (1992-1993) that lead to diplomatic deal ending Yongbyon work</td>
<td>Very strong</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>South Africa</td>
<td>Valindaba (Laser)</td>
<td>U.S. intel briefing to IAEA assists in verification of dismantlement; IAEA verifies reactor closure</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valindaba Z - Plant</td>
<td>U.S. intel briefing to IAEA assists in verification of dismantlement; IAEA verifies shutdown and reported amounts of LEU</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: This table includes all ENR facilities in Fuhrmann and Tkach (2015) coded as "closed" between 1990 and the present that were not allies of the United States (see ATOP coding explanation above). Sources for "Role of intelligence" column described in Appendix.
Case Study: North Korea, 1970-2006

North Korea’s civilian nuclear program started in the 1950s with support from the Soviet Union, and appears to have accelerated in the late 1970s (Oberdorfer and Carlin, 2013, 196). North Korea focused on plutonium reprocessing, taking advantage of its Soviet-built research reactor to produce spent fuel and later reaching an agreement to build large-scale nuclear power reactors in 1985. Pyongyang also purportedly began testing a nuclear implosion device around 1989 (Wit, Poneman and Gallucci, 2004, 6). Soviet leaders successfully convinced North Korea to join the NPT in 1989 (Oberdorfer and Carlin, 2013, 197) and complete a comprehensive safeguards agreement in 1992. Concerns about a possible weapons program and the IAEA’s detection of discrepancies in North Korea’s safeguards declaration led to multilateral pressure and IAEA special inspections in 1993. North Korea refused the request and withdrew from the NPT. Intense diplomatic negotiations led to an agreement in 1994 which froze North Korea’s reprocessing path and permitted IAEA monitoring in exchange for foreign-supplied light-water nuclear reactors. Disputes over the agreement’s implementation, along with allegations about an undeclared North Korean uranium enrichment program, led to the Agreed Framework’s collapse in 2003 (Chinoy, 2010, 117-126). Despite attempts to revive diplomacy, North Korea conducted a nuclear test in 2006.

The U.S. has monitored North Korea’s program continuously since 1950. Overhead imagery in particular provided dozens of images of North Korea’s nuclear facilities in the late 1960s and early 1970s, tracked the construction of a new large-scale power reactor at Yongbyon in the early 1980s, and revealed the near completion of a reprocessing facility and high explosives testing in the late 1980s (Wit, Poneman and Gallucci, 2004, 1-6). In 1992, U.S. spy satellites discovered attempts to conceal reprocessing-related activities, including tunnels around Yongbyon that were meant to either prevent an attack or avoid detection, as well as workers moving equipment away from the plutonium-reprocessing facility, destruction of walls, and rerouting of pipes (Richelson, 2007). Defectors, too, contributed to the U.S.’s receipt of a “steady trickle” of intelligence (Richelson, 2007).

50\textsuperscript{Note North Korea, the Soviet Union, and the IAEA had a facility-specific safeguards agreement in 1977 for the Soviet-built research reactor (Wit, Poneman and Gallucci, 2004, 13).}
The U.S. and North Korea have been adversaries since the early 1950s. Throughout the Cold War, Pyongyang was an ally and proxy of the Soviet Union and China, and engaged in a number of militarized clashes with the U.S. Following the end of the Cold War, North Korea’s hostility toward South Korea and numerous threats to Japan and the United States helped to continued this trend. Our theory therefore expects the U.S. to have provided intelligence to the IAEA regarding North Korea but only after the IAEA received the ability to protect it in 1991.

**Witholding in the 1980s, Sharing in the 1990s**

Consistent with our theory, the U.S. did not share intelligence with the IAEA regarding known North Korean activities prior to 1991. In fact, we find evidence a key concern was revealing sources and methods. Despite growing concerns in the late 1980s, the U.S. “held much back” and was especially reluctant to release “imagery from newer systems,” though it occasionally provided outdated satellite images of the nuclear facilities (Richelson, 2007, 519). When it did release intelligence about North Korea’s program, it only did so to trusted allies such as South Korea and Japan (Oberdorfer and Carlin, 2013, 198-9).

As our theory predicts, Washington “became more forthcoming” once the IAEA reforms demonstrated its ability to handle clandestine information (Richelson, 2007). In general, the IAEA’s inspections of North Korea’s facilities in 1992-3 were “assisted by intelligence provided by the United States” (Richelson, 2007). Illustrating both the validation and new information mechanisms, the IAEA both vetted intelligence claims by the U.S. and followed up on those leads. Take, for example, the IAEA’s first visit to North Korea. Prior to the trip, the Central Intelligence Agency briefed the IAEA director general and his staff at least three times, primarily regarding unreported reprocessing activities. The third briefing included “a ‘virtual reality’ tour of Yongbyon using advanced computer modeling based on aerial photographs. The highlight of the intelligence tour

---

51 As Richelson (2007, 519) notes, sources and methods concerns have been a consistent challenge in addressing North Korea’s ambitions, even limiting what can be shared in Congressional briefings.
was the reprocessing building” (Oberdorfer and Carlin, 2013, 209). Once on location, the IAEA inspectors drew on these experiences and used sophisticated nuclear detection techniques such as swabbing key areas to obtain material for analysis of nuclear signatures. IAEA samples were analyzed by in-house labs but also an American lab with specialized equipment unavailable elsewhere. Results were then combined by the IAEA to reach a conclusion about the timing and extent of reprocessing.

Identifying unreported reprocessing activities then led to a second phase in which nuclear waste storage sites at Yongbyon became the focus. Washington concluded that “it was worth sharing most of what it knew.” 52 The U.S. began to brief “a small group of IAEA experts” using “spy satellite photos and other highly sensitive intelligence” which had previously been kept off-limits. 53 This revealed North Korean workers constructing a new storage site and actively concealing it from the IAEA (Richelson, 2007). Classified satellite imagery also showed a hidden floor in a nuclear waste facility (Oberdorfer and Carlin, 2013, 214) which, when IAEA inspectors arrived to investigate, “they were told by North Korean officials that there was nothing below the warehouse.” 54 North Korea then refused requests for additional IAEA visits of suspected waste sites.

This led to a third phase in which intelligence was more widely shared with states beyond the IAEA staff. At the request of the IAEA’s director general, Hans Blix, the U.S. released select satellite imagery to a closed IAEA Board of Governors meeting with over a dozen other states. This was a difficult decision as, up until this point, the U.S. had exposed its sources information to “Blix and his staff” but not to board members such as “Libya, Syria, and Algeria.” The debate in Washington over this decision shows the tension between the political benefits of sharing and the risks to intelligence collection. The U.S. State Department supported release of imagery to Board members while intelligence officials resisted due to fears of compromising sources and methods. CIA Director Gates ultimately overruled these concerns and the “the Clinton administration con-

53 Ibid. Smith quotes an anonymous IAEA official as saying “We had never received stuff like this before.”
54 Smith, “High-Tech Hide-and-Seek.”
cluded that the failure to provide adequate imagery might impede the IAEA’s ability to press the North to be more open about its nuclear activities” (Richelson, 2007). Thus, in February 1993 the Board was shown a dozen black-and-white pictures of a waste storage facility under construction. It was “the first time in the history of the IAEA that the Secretariat had shared information supplied by Member State intelligence in a Board setting. Member States had historically been very uneasy about the Agency’s use of any information obtained through national intelligence agencies” (El-Baradei, 2011, 43). The Board approved a resolution demanding the inspections of North Korean waste storage sites (Richelson, 2007, 519-21). Further, “this Board meeting on North Korea thus served as a quiet milestone: in subsequent years, referring to the use of intelligence would become much more routine” (ElBaradei, 2011).

The Agreed Framework Collapse and Post-Test Sharing

This mid-1990s success was followed by setbacks in subsequent years. American intelligence sharing slowed in the early 2000s under the Bush administration. This slowdown is not consistent with the theory. American intelligence agencies concluded in 2002 that North Korea was pursuing a separate, clandestine uranium enrichment path. Rather than share with the IAEA, the U.S. chose to confront North Korea directly and shared intelligence only on a bilateral basis (Chinoy, 2010, 115-8). However, even this “off equilibrium” behavior illustrates a key claim of the theory. Because intelligence on the uranium path was not evaluated by the IAEA or supplemented with new IAEA inspections, U.S. claims were met with widespread skepticism. Russia, for example, complained that the U.S.’s allegations were only “based on one source”55 and not long after “doubts began to surface in the press about whether North Korea was constructing a bricks-and-mortar facility.”56. The IAEA director general himself concluded that these doubts dealt a “blow to the credibility and the competent handling of U.S. intelligence information” about North Korea

---


56See Jeffrey Lewis, “How A.Q. Khan Helped Distort America’s DPRK Policy.” 38North, March 29, 2010. Lewis notes that leaks about this intelligence in 2003 and 2005 suggest that assessments in 2002 about North Korea’s progress in uranium enrichment was exaggerated.
(ElBaradei, 2011, 100).

However, after a period in which the disclosure dilemma was resolved through other means than an IO, the U.S. turned back to the IAEA to address them. One review notes that the IAEA “must have been notified of US intelligence findings” as part of a 2003 finding by the Board of Governors about the North’s non-compliance (Kleiner, 2005). Our interviews also suggest the U.S. resumed its intelligence flow to the IAEA even after the test in 2006. Even after North Korea’s tests, the IAEA remains prepared to resume inspection work on North Korea should a diplomatic deal be reached.57 The U.S. supports this readiness by keeping IAEA staff briefed. As one interviewee noted, safeguards staff remain up to date on select U.S. intelligence so that they are able to engage in inspections with as little as 2-3 weeks notice.58

To summarize, U.S. leaders withheld intelligence prior to 1991 due to fears about sources and methods exposure. Multiple episodes of sharing followed reforms at the IAEA. In 1991, 1992, and 1993, American intelligence helped enable the IAEA to scrutinize the Radio Chemical Laboratory (Yongbyon) and, after red flag were raised, identify deception. These IAEA visits helped prompt the diplomatic negotiations and agreement that ultimately ended work on Yongbyon, though the Isotope Production Laboratory remained operational. This both validated states’ suspicions and enabled the IAEA to gather new information on North Korea in subsequent visits, illustrating both mechanisms we identify. The Agreed Framework ultimately unraveled a decade later, in part due to U.S. accusations about uranium enrichment, unvetted by the IAEA, which were seen as lacking credibility. This period of non-sharing was then followed by its restoration which continued even after the 2006 North Korean nuclear detonation.

57 Interview 2.
58 Interview 9.
Alternative Explanations

What other factors, besides IAEA reforms, might explain changes in intelligence sharing and patterns of nuclear facilities? First, the IAEA’s reforms occurred at the end of the Cold War, raising the possibility that the outcomes we observe are driven by the U.S.’s increased ability to work with other governments and IOs following the demise of the Soviet Union. Perhaps the collapse of the Soviet Union eliminated an obstructionist rival power, allowing the U.S. and Western allies to more effectively inhibit proliferation. However, this is implausible since our interviewees and secondary sources point out that while the U.S. and USSR obstructed multilateral rule enforcement in most areas during the Cold War, they cooperated effectively in the domain of nuclear nonproliferation (Brands, 2007; Gavin, 2010; Popp, 2014).

The two superpowers shared an interest in constraining the number of nuclear powers and, particularly since “states could also substitute nuclear weapons for their patronage and subsequently gain autonomy...[They thus] jointly tr[ied] to stop proliferation” (Coe and Vaynman, 2015b, 983). Indeed, the superpowers pressed other states – and each other – to support the NPT, and cooperated to push recalcitrant states back into compliance (Kroenig, 2014).

Instead, the end of the Cold War likely worked against our findings for two reasons. First, the spread of nuclear weapons during the Cold War was particularly concerning for a country like the United States because of bipolarity. New nuclear arsenals in the hands of leaders sympathetic to the Soviet Union posed a special threat given the zero-sum competition of the Cold War. Incentives to share intelligence were therefore strongest in this environment. The end of the Cold War lessened this imperative, making our results especially striking. Second, intelligence budgets in many of the states with the largest intelligence gathering capacities, including the U.S., fell sharply following the Cold War (Warner, 2014). States were thus less likely to collect useful and unique intelligence relevant to the IAEA’s mission in the post-reform period. Finally, our mechanism-related discriminates between broader Cold War changes and our specific IAEA story. We isolate the specific role

\footnote{Interview 41.}
of IAEA reforms and eased sources and methods concerns in sharing decisions; we also isolate the specific importance of intelligence-based details in enabling IAEA scrutiny of ENR facilities. A Cold War story would link these patterns to new foreign policy goals or geopolitical relationships deriving from the Soviet collapse.

Another important alternative to consider is that other reforms, beyond intelligence, allowed the IAEA to more effectively operate. Three changes around this same time are worth considering: the IAEA’s expanded ability to investigate undeclared sites via the Additional Protocol; new techniques for identifying non-compliance like environmental sampling; and a greater willingness to conduct inspections with minimal or no advance notification. These changes, while important, do not account for our specific results. First, the set of states that have signed and implemented the Additional Protocol during the period we investigate radically differs from the set of states that appear to have been influenced by intelligence-sharing. For example, Iraq did not sign the Additional Protocol until 2008, Iran and North Korea have not signed it, and Libya did not sign it until 2004. Second, while tactics like environmental sampling have given the IAEA greater detection powers, knowledge about and access to clandestine sites has largely depended on shared intelligence. The IAEA relies on intelligence to identify potentially useful sites from which to take samples meaning the independent effect of such tools is unclear (Rockwood, 2007). Finally, the IAEA has rarely invoked its special inspection power; it is an option that is largely ‘on the books’ and therefore was unlikely to drive proliferation decisions (Heinonen, 2010).

A third possibility is that changes in intelligence-related technology might explain the patterns we observe. Perhaps the U.S. obtained a qualitative improvement in the ability to clandestinely detect nuclear activities in the post-1990 period and simply shared more often as a result. This explanation does not appear to account for our results. Most intelligence that was shared after 1990 was from “legacy” systems like satellites. While novel technologies always help states gain new insights, it cannot account for the specific pattern we observe. If anything, changes in technology likely cause us to underreport the effect of the IAEA’s reforms. These same advances have made

---

60 However, Iran informally implemented it for awhile.
some techniques available commercially; thus, the comparative advantage in states’ intelligence has arguably shrunk making expanded intelligence sharing a surprising result (Chesterman, 2005).

**Conclusion**

This article identifies a widely applicable information problem in international relations and argues that institutions can mitigate the dilemmas that arise from sensitive information. States with intelligence on rule-violating behavior are often deterred from sharing it by the threat of damage to future collection. We argue that properly equipped IOs can receive, protect, and act on such intelligence. This both improves the effectiveness of the IO’s performance and better protects the intelligence donor’s sources and methods. Our formalization contrasts this function with a traditional “transparency” function and derives two empirical propositions which we evaluated in the nuclear proliferation domain. Drawing on archival materials, interviews, and secondary sources, we present data on intelligence sharing patterns and the impact on sensitive nuclear fuel cycle technology useful in nuclear weapons development. Our findings provide strong support for the theory, showing that reforms at the IAEA prompted more frequent intelligence sharing and more effective scrutiny of proliferation efforts. We therefore identify a novel institutional function for IOs that differs significantly from the classic view of IOs as information clearinghouses.

The article has theoretical and normative implications. First, the process by which IOs help address disclosure dilemmas – by developing the capacity for concealing sensitive information – stands in contrast to the norm of international transparency. Indeed, advocates of this norm argue that it can enhance the legitimacy of international institutions (Grant and Keohane, 2005), which is especially important in an era in which these organizations often face intense scrutiny and populist scorn even in established Western democracies.\(^{61}\) If institutions move to increasingly integrate sensitive information, we will likely see more and more efforts to build barriers to access to elicit the trust of states. However, this will come at the cost of democratic accountability.

Our disaggregation of the information functions IOs can serve helps better prepare scholars and practitioners to understand the challenges, limits, and complications of efforts to make international institutions more accountable.

Our findings also shed new light on power in IOs and the role of information. Information can serve as a source of power in international relations. While extant literature tends to argue that power comes from holding key positions within IOs, funding these bodies, and engaging in bribery, we show that another, more subtle, form of influence is held by states with the capacity to collect intelligence. Because intelligence donors choose whether to share their information, they hold a form of influence about which states are scrutinized, caught, and punished. Even when an IO – such as the IAEA – carefully protects its neutrality, the political agenda is inevitably influenced by integrating intelligence. Thus, the benefits derived from membership in IOs are not evenly distributed among member-states; those with intelligence are able to share this information selectively to further political priorities. States without information but with informed allies also benefit because their violations likely escape this additional level of scrutiny.

The concepts and theory developed here are relevant to other issue areas as well. The Organization for the Prohibition of Chemical Weapons maintains “rigid confidentiality” of sensitive information about chemical industries. The International Monetary Fund’s Financial Sector Assessment Program uses a three-tiered document classification system to protect states’ financial sector health. The 1989 Montreal Protocol regulating emission of chlorofluorocarbons obscures commercially valuable information. The World Trade Organization has adopted reforms to protect trade secrets and other firm-level data from wider public exposure during trade disputes. These suggest the broad relevance of different kinds of sensitive information to issues of compliance and the promise of future research on these institutions. To be clear, our theory does not apply to all

---

62 E.g. (Stone, 2011; ?).
63 See, for example, Tallberg (2003); Broz and Hawes (2006); Dreher, Nunnenkamp and Thiele (2008).
64 See, respectively, Article VIII of the Chemical Weapons Convention; the Articles of Agreement of the International Monetary Fund, Article V, Section 2(B), “Confidentiality Protocol - Protection Of Sensitive Information In The Financial Sector Assessment Program”; (Chayes and Chayes, 1995, 165); (Grando, 2009, 276).
transnational cooperation problems or IOs. Institutions that serve primarily as clubs of like-minded states may have no need for sensitive information; IOs that rely on information that is not sensitive or is widely known may also lack this need. Moreover, many IOs exist that could solve disclosure dilemmas, but currently do not, either because states have not properly equipped the IO to do so, or for other political reasons.

The article also raises important theoretical questions for future research. First, under what conditions do states allow IOs to develop the capability to handle intelligence? In the nuclear domain, the Gulf War was an exceptional event which revealed the inner-workings of a clandestine nuclear program that had eluded IAEA scrutiny. This dramatized the shortcomings of business as usual and prompted intelligence and other reforms. Other IOs suggest this same pattern: integration of intelligence into UN peacekeeping missions was prompted by the failure to prevent a massacre at Srebrenica (Rijsdijk, 2011) while innovation in the OPCW’s integration of intelligence occurred in reaction to chemical weapons usage in Syria. A related issue for future research regards accumulated effects over time. How do institutions that receive intelligence maintain their perception of neutrality over time? The case of the IAEA suggests institutions must work hard to avoid politicization by applying maximum technical expertise, rejecting information that is unsound, and avoiding over-reliance on a single intelligence donor. Finally, future work might directly test the impact of sensitive information reforms on public and elite opinions about global governance. Tracking the changes in perceptions of neutrality is a promising direction for future work. Future research might also investigate the impact of broader changes to the information environment – such as new technologies and social media – on the importance of sensitive information and the risks of leaks of sensitive information at IOs.

---


66(ElBaradei, 2011, 62-3); Interviews 1, 45.
References


Coppen, Tom. 2015. “Developing IAEA Safeguards: An Institutional Perspective on the State-
level Concept.” Journal of Conflict and Security Law p. krv004.


Leeds, Brett Ashley. 2005. “Alliance treaty obligations and provisions (atop).” *Houston: Rice University, Department of Political Science*.


The Disclosure Dilemma:
Nuclear Intelligence and International Organization

Appendix of Supporting Information
(Not for publication)
Solving the game explained in the main text:

- In any subgame perfect equilibrium (implying in any PBE), after the history \((V,D,M)\), \(I\) must play \(e\).

- Letting \(p, q\) denote the probabilities that \(I\) assigns to being at the left node in the relevant information sets (i.e. the probability that \(A\) violated), we have: 
  \[
  \sigma_I(q) = \begin{cases} 
  e & \text{if } q \geq \frac{1}{2} \\
  -e & \text{if } q < \frac{1}{2}
  \end{cases}
  \]

  Therefore, at the very beginning, \(A\) should best respond by:
  \[
  \sigma_A = \begin{cases} 
  \text{either } V \text{ or } \neg V \text{ for } p \geq \frac{1}{2}, q \geq \frac{1}{2} \\
  V \text{ or } \neg V \text{ for } p < \frac{1}{2}, q \geq \frac{1}{2}
  \end{cases}
  \]

  Where:
  \[
  S_1 = \{k,b,p\mid p < \frac{1}{2}, q \geq \frac{1}{2}, \sigma_E(V) = (D, \neg M), \sigma_E(\neg V) = \neg D\} 
  \] (1)
\[ S_3 = \{k, b, \rho | p < \frac{1}{2}, q \geq \frac{1}{2}, \sigma_E(V) = \neg D, \sigma_E(\neg V) = \neg D\} \] (2)

\[ S_4 = \{k, b, \rho | p < \frac{1}{2}, q \geq \frac{1}{2}, \sigma_E(V) = \neg D, \sigma_E(\neg V) = (D, \neg M)\} \] (3)

\[ S_5 = \{k, b, \rho | p < \frac{1}{2}, q \geq \frac{1}{2}, \sigma_E(V) = (D, M), \sigma_E(\neg V) = \neg D\} \] (4)

\[ S_6 = \{k, b, \rho | p < \frac{1}{2}, q \geq \frac{1}{2}, \sigma_E(V) = (D, M), \sigma_E(\neg V) = (D, \neg M)\} \] (5)

\[ S_7 = \{k, b, \rho | p \geq \frac{1}{2}, q < \frac{1}{2}, \sigma_E(V) = (D, \neg M), \sigma_E(\neg V) = \neg D\} \] (6)

\[ S_8 = \{k, b, \rho | p \geq \frac{1}{2}, q < \frac{1}{2}, \sigma_E(V) = (D, \neg M), \sigma_E(\neg V) = (D, \neg M)\} \] (7)

These sets of parameters are chosen such that they are nonempty,\(^1\) and for those parameters, \(E\) acts as described. One additional logical possibility is the set of parameters \(S_1 = \{k, b, \rho | \sigma_E(V) = (D, \neg M), \sigma_E(\neg V) = (D, \neg M)\}\), and similarly there are the sets \(S_9\) and \(S_{10}\), but it turns out that there are no parameters that satisfy the constraints, so these sets is empty and thus are excluded from consideration.

Thus, without an IO we have the following equilibria:

**Proposition 1.** There exists a perfect Bayesian equilibrium where \(A\) violates with probability one.

*Proof.* We exhibit the full strategy specification; the fact that this is an equilibrium can be checked by direct computation. In this equilibrium \(A\) plays though action \(V\), \(E\) plays the actions \(D\) and then \(\neg M\), and \(I\) plays \(e\); it can be checked that this is an equilibrium for any \(\{p, q | p \geq \frac{1}{2}, q \geq \frac{1}{2}\}\). (In fact of course, we have \(p = q = 1\) since actions pin down beliefs). This equilibrium is supported by off-path actions \(D\) and \(\neg M\) for \(E\). \(\Box\)

**Proposition 2.** Suppose that assumption 1 is satisfied. Then there exists a perfect Bayesian equilibrium where \(A\) does not violate with probability one.

*Proof.* In this equilibrium \(A\) plays the action \(\neg V\), \(E\) plays \(\neg D\) and \(I\) plays \(\neg e\). Beliefs of \(I\) are \(p = 1, q = 0\); this equilibrium is supported by off-path actions \(D\) and \(\neg M\) for \(E\). \(\Box\)

---

\(^1\)Computations checked with Mathematica.
When we include an IO, letting $\rho = 0$, for $p \geq \frac{1}{2}, q \geq \frac{1}{2}$, $E$ is indifferent between $(D,M)$ and $(D, \neg M)$ after a violation. The previous equilibrium with a violation still survives if $E$ chooses the same action. However, if $E$ chooses a different action, since it’s indifferent, the equilibrium with a violation disappears. Importantly, the set of parameters that supports the nonviolating equilibrium ($S_7$ in the parlance above) is not made empty by taking $\rho$ to 0, so that equilibrium is not eliminated.
Additional Case Studies

We included one exemplar case study in the main text: North Korea. This section features case studies of the remaining thirteen cases that meet our selection criteria for the universe of cases, listed alphabetically.

Algeria 1983-1991

Algeria began the construction of its hot cell facility at Ain Oussera in 1986, and it became operational in 1992. It can separate plutonium on a small scale, and is a part of the El Salam nuclear reactor. The facility was intended to be used for military purposes, as a surface-to-air missile battery was found nearby. Algeria received help in producing plutonium from China and Argentina, and received the nuclear reactor from China. It also bought 150 tons of uranium concentrate from Niger.

Though Algeria’s nuclear ambitions began in 1983, in 1988, the U.S. “received clear intelligence data...indicating that China was helping Algeria build a nuclear reactor that many Administration officials suspect is intended for nuclear weapons research and production.” Then in 1991, U.S. satellites detected the construction of a new nuclear reactor – Es Salam in the Ain Oussera nuclear site – which it concluded may have been for military purposes. An NSC report details the U.S.’s worry, stating that the, “cooling towers of the reactor appear adequate to support operation of a substantially large reactor, possibly up to 50 MWT,” and that the “heavy-walled facility that appears suited to provide options for a future reprocessing capability, waste storage, or research applications” was also of concern.” While intelligence officials could not “conclude that the [Algerian Government] has decided to pursue a military nuclear program...the State Department wanted the IAEA to inspect the Algerian facilities to answer questions about the reactor’s power level and the size of the cooling tower.”

Algeria was not a U.S. ally, so we expect that the U.S. shared intelligence about Algeria beginning in 1991, but not prior. Indeed, prior to 1991, the U.S. “did nothing with the data,” and we do not find any instances of intelligence-sharing with the IAEA during this time.

In 1991, the U.S. strongly pressured the IAEA to offer to visit Algeria’s facility before it was completed, to submit to safeguards, and to join the NPT. One of our interviewees stated that the U.S. shared intelligence with the IAEA, which was especially likely given this close cooperation.

---

2See “Algeria Special Weapons.” The Nuclear Information Project. FAS.
6“Memorandum for Mr. William F. Sittmann the White House. Subject: Algerian Nuclear Program. United States Department of State.
7Interview 38. News of the Es Salam reactor was leaked to The Washington Times in April 1991, so some of this information was in the public domain, and the U.S. may not have had to share it. The National Security Archive (2007).
This intelligence seems to have helped to shut Algeria’s program down. The year after this close cooperation, Algeria accepted IAEA safeguards and then ratified the NPT in 1995. Algeria also decided not to construct any new plants after 1992.\(^8\) As one report noted, statements to U.S. diplomats by Algeria and China committing to seek IAEA safeguards “have, in large part, alleviated our concern about the proliferation implications of the reactor under construction,”\(^9\) especially since Algeria “had no clear motive” to continue with its program.\(^10\) However, though Algeria has cooperated with the IAEA, not all concerns have been allayed (Albright and Hinderstein, 2001).

**Argentina 1978-1990**

Argentina pursued nuclear weapons beginning in 1978, and its government stated that it intended to both build these weapons and to share them with other states. It began construction of the Ezeiza SF Reprocessing Facility in 1968, which was closed in 1973. Construction was started on it’s second facility – Ezeiza II – in 1978, but it was never operational, and the construction of the Pilcaniyeu Enrichment Facility I began in 1979 and was shuttered in 1994. Argentina’s program was placed in civilian hands after its authoritarian government lost power in the early 1980s, and the country renounced its weapons in 1990.

The U.S. had unique information about Argentina’s program, as national intelligence agencies focused their efforts on Argentina due to its “significant nuclear activities” and the fact that it was “resisting the additional protocol” (Ogilvie-White, 2014, 339). The U.S. concluded in 1974 that it would obtain a nuclear weapons capability by the early 1980s.\(^11\) However, the U.S. did not have complete information about the program, as “Argentina had thrown off Western intelligence agencies by encouraging them to look for a nonexistent plutonium production reactor” rather than the gases diffusion uranium enrichment plant that was announced in 1983, but had been under construction since 1978 (Pilcaniyeu Enrichment Facility I).

In this entire period, Argentina was not an ally of the U.S. Since the program also was terminated just prior to 1991, we do not expect to see any instances of intelligence sharing. Indeed, we find no intelligence-sharing with the IAEA.\(^12\) Instead, the U.S. relied on bilateral pressure, though its effectiveness was limited during this period, as it caused “strong, nationalistic opposition”\(^13\) and “backfired and led to an even greater expansion in Argentine nuclear capacities.”\(^14\)

We also do not expect intelligence-sharing with the IAEA to have limited Argentina’s activities. This seems to be the case, since Argentina abandoned its program due to domestic changes

---

\(^8\)See, for example, (Albright and Hinderstein, 2001; Pelopidas, 2013; Feldman, 1997; **Algeria - France: Civil Nuclear Energy Deal**, 2008).


\(^10\)See Albright and Hinderstein (2001, 46).

\(^11\)While Argentina stepped up its efforts in the early 80s, it stated in 1985 that it would not develop the weapons and stopped its program in 1990. See Montgomery and Mount (2014).

\(^12\)See Pelopidas (2013); Merke (2016); **U.S. Concerned Over Nuclear Weapons More Than Human Rights in Argentina** (2003); Redick, Carasales and Wrobel (1995); Leventhal (1992); Hymans (2001); Karp and Carasales (2000); Paul (2000); Carasales (1999); Sagan (2012, 2011).

\(^13\)See National Intelligence Council (1982, 22).

that were unrelated to the IAEA’s activities (Hymans, 2001, 155). Argentina gave up its program “when a civilian government succeeded the military Junta, an agreement with Brazil was reached, and Argentina gave in to US pressure.” Further, the IAEA played little role in Argentina’s decision to get rid of its program since Argentina would not allow the IAEA to inspect most of its facilities, and refused to sign the NPT until 1995. It’s initial Ezeiza reprocessing facility was closed after a lack of success – it only extracted less than 1kg of plutonium – rather than any outside influence. Its second reprocessing facility (Ezeiza II) was also closed, but not because of the IAEA’s involvement; instead, this was due to “economic constraints, and political pressure from the US.”

**Brazil 1970-1990**

Brazil initially explored developing technology potentially useful for nuclear weapons as early as the 1950s, prior to the NPT. Its civilian nuclear power program, however, began in earnest in reaction to the oil crisis and strong economic growth in the 1970s. The centerpiece of Brazil’s civilian program was an agreement with West Germany, signed in 1975, for the construction of eight power plants under IAEA safeguards. Brasilia received technology transfers from West Germany under this agreement, such as the proprietary “jet nozzle” enrichment technique. Yet the joint effort was ultimately disappointing for Brasilia; West Germany refused to transfer more reliable and scalable technologies and a financial crisis in Brazil greatly slowed the construction of the power plants.

This led Brazil to pivot in 1979 to a secret, parallel military program for indigenous development of both reprocessing and uranium enrichment. Each of the three branches of the military operated research and development in the nuclear field in the 1980s, independent of the civilian program under Nuclebras. Important enrichment/reprocessing facilities that were part of this parallel program include laser isotope and gas centrifuge enrichment at the Air Force’s Aerospace Technical Center and the Navy’s reprocessing experiments at the Institute for Energy and Nuclear Research (IPEN) site. Technical achievements by the late 1980s included the ability to convert yellow cake into uranium hexafluoride for use in enrichment and the Navy’s success in ultracentrifuge enrichment techniques. This parallel program was terminated, however, in 1990 as a result of Argentine-Brazilian agreement on the renunciation of nuclear explosive technology and safeguards on their facilities.

---

16 See Green, Jim. “Case Studies: Civil Nuclear Programs and Weapons Proliferation.”
18 Patti (2012) notes that at the time it was “largest technology transfer agreement from an industrialized to an industrializing country ever signed.”
19 Patti, “Origins and Evolution.”
20 The Furhmann nuclear latency data lists IPEN Reprocessing beginning in 1960 but this is most likely the date of the IPEN site’s operation rather than reprocessing experimentation per se. The facility is listed as shutting down in 1989. Enrichment activity at the Aerospace Technical Center is listed as starting in 1975 and ends in 1989.
21 Interview 44.
22 Patti, “Origins and Evolution.”
While Brazil did not sign the NPT until its 1990 renunciation, it possessed a relatively close practical relationship with the IAEA. Each of its foreign-sourced reactor agreements, with the United States and West Germany, included provisions for safeguards by the IAEA.\(^23\) Brazil was also active in the IAEA itself, even seeking the chair of the Board of Governors in the early 1980s.\(^24\) However, as with other governments, Brazil’s clandestine parallel program was not subject to IAEA safeguards. As one review notes, the facility-specific agreements Brazil and Argentina had with the IAEA “dealt with specific cases of co-operation and did not cover the nuclear materials involved in each country’s autonomous programmes.”\(^25\) Regarding its ally status, Brazil did not have a formal alliance with the United States during this period.\(^26\)

Declassified intelligence documents show that the U.S. carefully tracked Brazilian nuclear developments, especially after its pivot towards unsafeguarded, military-led research in the 1980s. This produced specific insights into reprocessing and enrichment research activities. A 1983 Special National Intelligence Estimate did not conclude Brazil had decided to develop an explosive device but sounded the alarm that its parallel military programs were an indication of nuclear hedging. It specifically notes “various sources” confirming unsafeguarded uranium enrichment and a “well placed Brazilian source” that stated Brazil was planning to fund a natural uranium fueled reactor that could supply reprocessing experiments.\(^27\) Alarm bells were clearer in intelligence reporting later in 1980s. A similar assessment in 1985 noted that “each of the Brazilian military services has its own nuclear research and development projects” which spanned “a wide range of nuclear technology and facilities that, if completed and operated successfully, conceivably could give Brazil the capability to develop a nuclear device by 1990.”\(^28\) While portions of the document remain redacted, it also notes indications of early nuclear explosive design research (i.e. spherical configurations).\(^29\) A 1986 intelligence memo specifically notes clandestine sites and activities. The Brazilian Air Force’s Aerospace Technical Center is described as having “made some progress in laser isotope uranium enrichment and composite materials for gas centrifuges” while the Navy’s operations at the IPEN site featured “projects in uranium enrichment and suspected experiments in reprocessing.”\(^30\) While sources are not noted, it includes information on technical details such as Brazil’s “work[s] on uranium enrichment via laser isotope separation and ultracentrifuge.”


\(^{26}\)Note that while ATOP codes Brazil as a non-ally, the Correlates of War dataset codes it as an ally. However, coding Brazil as an ally would not change our results since either way we expect little intelligence sharing prior to 1991.

\(^{27}\)SNIE 93-83, October 1983, cited above.


\(^{29}\)Ibid., p. 6.

\(^{30}\)CIA Directorate of Intelligence Memorandum, “President Sarney and Brazil’s Nuclear Policy.” September 8, 1986. CIA FOIA collection, Document CIA-RDP86T01017R000201360001-8.
Since Brazil’s nuclear activities ceased prior to 1991, our theory does not expect the U.S. to have shared intelligence with the IAEA regarding declared or undeclared sites. Our interviews and secondary literature indicate very few, if any, instances of sharing with the IAEA. Most interviewees reported no knowledge of instances when the IAEA was given intelligence-based information by the U.S. or West German governments, including during the crucial period from 1979 to 1989.\(^{31}\) Secondary histories record no instances of intelligence sharing with the IAEA.\(^{32}\) One of our interviewees with extensive expertise on Brazil’s nuclear program stated that they believed that “at least West German and US intelligence service (maybe also French) informed IAEA about the Brazilian nuclear projects” at some point during the 1980s.\(^{33}\) Overall, we assess that such intelligence sharing was rare.

Our theory also suggests that an absence of intelligence contributed to poor information at the IAEA which, in turn, helped enable Brazil to make progress in its development of the nuclear fuel cycle and military applications. Reporting on the IAEA-Brazil relationship in the late 1980s suggests that the IAEA was privately quite frustrated by its absence of information about Brazil and the progress Brazil was able to make with its parallel military projects. For example, a 1989 report notes that poor information supply regarding Brazil was a recurring problem for the IAEA (“[d]ocuments show that the IAEA has taken both Germany and Brazil to task for failure to report technology transfers as required”) in part due to foot-dragging by Brazil that hindered the quality of IAEA inspections.\(^{34}\) Another report from the same period quotes West German intelligence that Brazil’s parallel military programs were “off-limits to foreign inspection” and that “the IAEA itself has complained secretly about this, despite public statements to the contrary.”\(^{35}\) These kinds of gaps in self-reporting to the IAEA were filled by intelligence sharing after 1990; Brazil appears to be a case where the the IAEA was left in the dark.

The IAEA’s poor information was a manifestation of the general Brazilian approach of autonomy and resistance to outside scrutiny.\(^{36}\) Brazil pointedly did not sign the NPT until 1998. It was determined to continue its program despite interference, stating that “[o]ur nuclear program will continue, at least to the extent it depends on us, against all internal and external pressures.” (US Embassy in Brazil, 1973, 1-2). Despite achieving enrichment capabilities and other milestones noted above, Brazil ultimately wound its program down due to domestic reasons and bilateral negotiations with Argentina. Thus, while Brazil never completed work toward a nuclear explosive nor tested a weapon, its progress in the key decade of the 1980s was enabled by lackluster safe-

---

\(^{31}\) Interviews 46, 47, 48, 49, 50.

\(^{32}\) See, for example, \(\text{Needell, 2015; Leventhal, 1992; Sotomayor, 2013; de Santana Carvalho, 2006; Argüello, 2011; Pelopidas, 2013; Povinec et al., 2008; Paul, 2000; Sagan, 2012, 2011; Barletta, 1997; Siler, 1992; Doyle, 2011.}\)

\(^{33}\) Interview 44. A second interviewee (38) also reported that Brazil was the basis of intelligence sharing but timing and details were not provided.

\(^{34}\) Citing a nonproliferation official from another western government,” Hibbs also reports that “IAEA inspectors in Brazil have been intimidated by local officials and have been denied full access to nuclear facilities under IAEA safeguards.” Mark Hibbs, “West Germany to Investigate Charges of Brazilian Technology Diversions,” Nuclear Fuel, 4 September 1989.


\(^{36}\) As one American intelligence report notes, “Brazil strongly resists what it perceives as foreign efforts to limit its access to new equipment and technologies.” SNIE 93-83, October 1983, cited above.
guards and poor information at the IAEA, despite the presence of good intelligence in the hands of countries like the United States.

**India 1970-1974**

India began its nuclear weapons program in earnest in 1954 and publicly tested a nuclear device in 1974. While a weaponized nuclear test did not take place until 1998, the “peaceful nuclear explosion” in 1974 ended the first phase of its program and established India’s mastery of the fundamentals for a nuclear weapon (Perkovich, 2001, 189). While some details about 1974 test are not known, the period from 1970 to 1974 was a critical phase when India achieved milestones in research and development for an explosive device and decided to undertake it.37

U.S. intelligence monitoring India’s program produced considerable detail during this period. This was despite the fact that India’s explosive device research was highly secretive and featured great efforts to minimize the personnel working on the project and knowledge about decision-making (Perkovich, 2001, 172). American intelligence relied on “a combination of open sources, diplomatic reporting, communications intelligence, and satellite photography” (Richelson, 2007, 225). Specific reports in 1972, for example, included details about quantities of spent fuel available for use in testing from sites like the Trombay research reactor, test site preparations, and hints of a secret parallel program visible reported through diplomatic channels.38 Analysis specifically anticipated any test would be characterized as a peaceful explosion but suspected New Delhi’s program was pursued with military purposes in mind.39 Yet because the Nixon administration put a “relatively modest priority to relevant intelligence collection activities” about India’s program, the value of intelligence information “fell off” during the “20 months before the test.”40

India was not a U.S. ally throughout this period. The early 1970s featured a particularly “frosty” relationship due to the American “tilt” toward Pakistan in 1971, Kissinger’s visit to China around this time, and symbolized by India’s 1971 friendship treaty with the Soviet Union (Perkovich, 2001, 162-166). Thus, Washington did not have political reasons for withholding intelligence. Moreover, while India was not in the NPT, it had facility-specific agreements with the IAEA to safeguard two of its key facilities. Thus, the IAEA had a role in monitoring India’s program as early as 1971.41

Because the case occurred long before the IAEA was willing to and capable of accepting intel-

---


38 See documents 4, 3, and 5, respectively, in National Security Archive EBB 367.

39 See, for example, the prediction in 1972 that “[t]he Indian government would probably identify the devices, if tested, as peaceful nuclear explosives.” Memorandum From the Director of the Bureau of Intelligence and Research (Cline) to Director of Central Intelligence Helms, February 23, 1972. FRUS 1969?1976, Vol E-7, Document 228.


ligence, however, we expect few instances of sharing with the IAEA. Indeed, as anticipated by the theory, our interviews indicate that no intelligence was shared with the IAEA about India’s efforts in the early 1970s or later. Archival records and secondary histories from the early 1970s support this conclusion. Declassified U.S. documents reflecting warnings in 1972 of a possible test show that private bilateral intelligence sharing between the U.S., Canada, and the United Kingdom were ongoing but no indications of inclusion of the IAEA. The only mention of the IAEA’s possible role at the time was as a venue where American and other leaders could shape perceptions of the legitimacy of “peaceful nuclear explosions” to deter India from using this excuse to test.

Moreover, our theory would expect that an ill-equipped IAEA would be unable to slow India’s program and that India’s program overall could not be stopped or reversed. American intelligence analysis specifically noted the possibility that IAEA safeguards could obstruct India’s progress but that the Agency was unlikely to have the ability, in practice, to do so. In terms of specific ENR facilities, the two research centers that were under construction or operational during this time – the Bhabha Atomic Research Center (at Trombay) and the Power Reactor Fuel Reprocessing (PREFR) Bhabha Atomic Research Centre – remained in operation and remain so at present. Finally, India took no steps toward renouncing its “peaceful” program in the 1980s, refused to sign the NPT, and went on to publicly test a weapon in 1998.

Iraq 1975-1991

Iraq created the Iraqi Atomic Energy Commission in 1959. Beginning in 1976, Iraq invested heavily in its nuclear program, which Saddam Hussein believed could help him consolidate power and would provide a strategic asset in the region. The program was monitored by several countries, such as Israel. Yet this information was not shared with the IAEA; instead, Israel bombed the Iraqi nuclear reactor at Osirak in 1981. The Israeli government stated, “for a long time we have been watching with growing concern the construction of the atomic reactor...From sources whose reliability is beyond any doubt, we learn that this reactor, despite its camouflage, is designed to produce atomic bombs.” In response to the bombing, Iraq’s program became more covert, as at least six clandestine weapons labs were established (Richelson, 2007, 323). The U.S. used its satellite capability to evaluate the extent of the damage from Israel’s bombing. The U.S. used “diplomatic reporting, human intelligence, and communications intelligence” to determine that the bombing caused “a significant setback to the Iraqi nuclear program.” It assessed in a lengthy 1983 report that Iraq would not be able to obtain a weapon prior to the 1990s without foreign help. In 1986 the U.S. learned of a Chinese assessment of Iraq’s ability to build another reactor as well. In 1988 the CIA also noted that Iraq viewed a nuclear capability as essential to its security.

42Interview 38 and interview 7.
44“We could also maintain our efforts in the IAEA to gain broader international acceptance of the view that the technology of peaceful and military explosions could not be distinguished.” Memorandum of Conversation between British Foreign Office and State Department, “Indian Nuclear Developments,” 21 September 1972.
45See discussion of safeguards and U.S.- and Canadian-supplied reactors in Memorandum From the Director of the Bureau of Intelligence and Research (Cline) to Director of Central Intelligence Helms (cited above).
Iraq was an adversary during this period, but we do not expect much intelligence sharing with the IAEA until the post-reform period. Indeed, none of this intelligence was shared with the IAEA, as “prior to the Gulf War, no information was ever provided to the agency about illegal activities taking place at undeclared facilities in Iraq” (Zifferero, 1993, 8). El Baradei also notes that the IAEA received no intelligence during this time, as did our interviewees. Harrer (2014) states that during this period “the IAEA made an effort to learn what the intelligence communities (Israel, US, and UK) really knew about the INP and how they had learned it. The results were meager.”

Following the war, the IAEA conducted extensive inspections of Iraq’s facilities. However, the initial inspection team “had very limited help from the U.S. intelligence community” (Richelson, 2007, 450). During these inspections, the international community learned that it had missed a lot of Iraq’s capabilities prior to the war. Dismayed by its failure to detect so much of Iraq’s progress, “new approaches to intelligence, a very delicate area given the apolitical posture of the Agency, had to be adopted” (Harrer, 2014). The IAEA thus underwent major reforms to improve its effectiveness by developing procedures to accept and use national intelligence. Indeed, “Starting in 1991 after the discovery of a large clandestine nuclear weapon development programme in Iraq, the IAEA began to accept intelligence or third party information to facilitate safeguards implementation” (Rauf and Kelley, 2015). The primary goal of the reform was to encourage the early provision of design information: “On 26 February 1992, the Board of Governors adopted a recommendation by the Director General related to the early provision of design information. In so doing, the Board established that... such information shall be provided ‘as early as possible before nuclear material is introduced into a new facility’, should be interpreted as requiring the provision of design information as soon as the decision to construct, to authorize construction or to modify a facility has been taken and, on an iterative basis, as the designs are developed.” However, the Board also considered “proposals on the reporting and verification of the export, import and production of nuclear material and of sensitive equipment and non-nuclear material.” Member states were subsequently informed that they could, on a voluntary basis, provide confidential information to the IAEA related to the transfer or production of nuclear material in another state. Thus, “the Agency announced in its February 1992 Press Release that the Board of Governors now considered itself authorized to receive information from outside sources” (Carmody, 1994). In essence, the 1992 reforms made possible the transmission of confidential information to the IAEA by a relevant third-party. In 1993, the IAEA made the voluntary reporting scheme official: “The scheme established in 1993 for the voluntary reporting by States of nuclear material not otherwise required to be reported to the IAEA under safeguards agreements, and of exports and imports of specified

---

See ElBaradei (2011, 10). Interview 38.

The one potential exception was that just prior to the Gulf War in 1989 or 1990, the IAEA may have received intelligence from the U.S., though it did not use it, according to Interview 2.

Interestingly, the U.S.’s failure to detect Iraq’s nuclear program stemmed in part from its revelation of sources and methods while sharing intelligence with Iraq during the war. Iraq learned the U.S.’s capabilities and altered its activities to avoid detection (Richelson, 2007).

Interview 2.

Rockwood (2013)

equipment and non-nuclear material. States choosing to participate in the scheme do so through the exchange of letters with the IAEA” (IAEA Safeguards Glossary: 2001 Edition, 2001, 9). “The program to reform safeguards aims at improving the IAEA’s ability to detect undeclared nuclear activities. It focuses on the activation of the special inspection rights and, simultaneously the development of additional information sources....The IAEA has created the organizational requirements necessary to receive intelligence information (Dembinski, 1995, 32).

These reforms represented a major innovation that led to a new era of intelligence sharing. Indeed, our interviewees called 1991 “a turning point,” indicating that it “prompted shifts at the IAEA to using other sources of info, and also led to efforts to create a kind of obligation for states to provide intel if they have it,” which was reinforced by a UNSC resolution....Generally information on clandestine programs was recognized as a gap that needed to be filled.”^52 Another interviewee indicated that after the reforms began, “routine contacts started with Iraq...The IAEA began to openly use intel, rather than the very occasional and closely held pre-1991 stuff.” While pre-1991 sharing was “ad hoc,”^53, the IAEA received considerable intelligence in the following period.

Indeed, beginning in 1991, states started sharing their information with the IAEA, and satellite images provided by the U.S. were “particularly helpful” (Albright, 1998, 43). Chittaranjan (1999, 417) notes that “Iraq soon realised that UNSCOM and the IAEA Action Team inspections were going to be far more intrusive than the traditional IAEA safeguards inspections had been as the post-war inspectors had access to intelligence information from IAEA member states (mainly the USA) and overhead photos which were particularly helpful in their initial inspection efforts.” One of our interviewees explained, “Routine contacts started with Iraq. Before IAEAs Iraq team would go into Iraq, there would be an intel briefing. Info was only shared with the team (and probably some specific info that was only shared with a subset of the team)...It was actionable information to follow up on while in the country. The IAEA team was extremely careful with the information, and the intel proved extremely helpful. The IAEA built a lot of trust in this experience.^54

Indeed, the IAEA itself noted that a key to its efforts in Iraq was “the provision of intelligence information” by member states (Richelson, 2007, 451) including a “Western intelligence service [that] had suggested that [Tarmiya] might have housed centrifuges,” and “significant intelligence from the United States, including a fact revealed by satellite images—which immediately after the inspection at Tuwaitha, the Iraqis had uncovered and removed disc-shaped objects that had been buried outside of Tuwaitha” (Richelson, 2007, 451-2). Further, the IAEA inspection team “arrived in Baghdad on Saturday, June 22, armed with intelligence provided, via the United States, from two Iraqi engineers who had fled west and were familiar with Iraq’s nuclear weapons program. In addition, the team knew that U.S. intelligence had been able to track suspicious objects from Tarmiya to the Abu Ghraib military barracks” (Richelson, 2007, 452). After it became clear that Iraq had removed evidence, the U.S. also supplied satellite photos “to be clear that the failure to find anything there was due to Iraqi duplicity not Iraqi compliance” (Richelson, 2007, 452). On June 28th, the team attempted to inspect Falluja “based on a tip from the CIA,” complete with satellite photos and “other intelligence” (Richelson, 2007, 452). Indeed the IAEA noted that it was only able to identify “the essential components of the clandestine program” due to its members’

^52Interview 4.

^53Interview 3.

^54Interview 3. Interview 12 also notes that Russia provided information.
“provision of intelligence information” (Richelson, 2007, 461).

More specifically, during the IAEA’s first inspection of Iraq in May, it was “aided by intelligence input from IAEA member states...that indicated the existence of an underground plutonium production facility comprising a nuclear reactor and, possibly, an associated chemical separation (reprocessing) plant” (Zifferero, 1993, 9). The inspectors were also provided with intelligence information on Tarmiya before the first inspection mission (Harrer, 2014). Afterward, “intelligence had been coming in about sites where sensitive items were said to be located” (Harrer, 2014). “U.S. satellite imagery showed, inter alia, overloaded trucks which were leaving very heavy prints in the sand....[and] satellite photos, which seemed to indicate that Baghdad was concealing nuclear bomb development equipment” (Harrer, 2014). Next, prior to the IAEA’s second inspection of Iraq in June, an intelligence agency had shared reconnaissance photographs with the IAEA showing a surge of Iraqi activity immediately after the departure of the first inspection team, in an area just outside the Tuwaitha site” (ElBaradei, 2011, 20), along with other “overhead photos, and photos of Tarmiya” (Albright, 1998, 46). Then, during the IAEA’s sixth inspection of Iraq in September, it chose sites to visit based “on information received from intelligence sources” (Thorne, 1992, 21). Hans Blix stated that the sixth inspection had been successful because “information secured by member states had been available” (Harrer, 2014). Further, the ninth IAEA inspection returned to Rashdiya due to intelligence showing that “centrifuge equipment had been moved from Rashdiya and that one of its site directors had been Obeidi” (Harrer, 2014).

This intelligence sharing led to the curbing of Iraq’s nuclear activities during the post-reform period. Two facilities – Al Tuwaitha Laser and Al Tuwaitha Centrifuge – ended operations in 1987. Since this was before the IAEA had reformed, we do not expect intelligence to the IAEA to have played much of a role. Indeed, the laser isotope separation program was shut down because Iraq was unable to make progress on it and chose to deemphasize it, and Iraq’s manufacturing ability was too rudimentary to ensure the quality of the centrifuge machines.55

However, for the remaining five facilities that ended operations in 1991 – Al Tuwaitha Chemical Ion Enrichment Facility, Al Tuwaitha Hot Cell, Al Tarmiya (north of Baghdad), Laboratory Reprocessing Facility (Radiochemistry Laboratory), and Rashdiya Building 22 – intelligence played a large role. Indeed, while the Lab Reprocessing Facility was bombed by the U.S., American intelligence helped the IAEA to confirm plutonium separation in subsequent inspections. Further, while the IAEA failed to detect enrichment work at Rishdiya Building 22, intelligence sharing (and defector information) helped the IAEA to confirm it in the mid 1990s. At Al Tarmiya, the U.S. intelligence identified it as a likely facility before the war but did not share until afterward, when it provided overhead photos to the IAEA that identified enrichment work there. Finally, consider Iraq’s Al Tuwaitha facility (both the Hot Cell and Chemical Ion Enrichment Facility), which was bombed in 1981 by Israel and again during the 1990 war, and then was rebuilt to host experiments in reprocessing and storage of parts for uranium enrichment. Between the first and second IAEA visits in 1991, member-states including the United States shared intelligence with the IAEA’s Iraq Action Team that showed Iraqi personnel hastily covering up and removing discs suspected of use in uranium enrichment (ElBaradei, 2011, 20). The IAEA was unaware of clandestine nuclear activity at Tuwaitha before the war in part because of a lack of overhead satellite imagery which was not not shared by those with such intelligence.56 Moreover, significant work at Tuwaitha was

55See “Iraq Nuclear Chronology.” NTI.

56David Albright, Corey Gay, and Khidhir Hamza, “Development of the Al-Tuwaitha Site: What If the Public or
unknown even after its bombing in 1990 and after Iraq’s more complete declaration in 1991. Intelligence shared by the U.S. with the IAEA was critical in identifying and coercing a complete dismantling of the facility. As one expert that worked with the Iraq Action Team describes, “Iraq soon realized that UNSCOM and the IAEA Action Team inspections were going to be far more intrusive than the traditional IAEA safeguards inspections had been. The post-war inspectors had access to intelligence information from IAEA member states, mainly the United States, and overhead photos were particularly helpful in their initial inspection efforts” that focused on Tuwaitha (Albright, 1998, 48).

Note that the dramatic controversy about intelligence regarding Iraq’s nuclear and other weapons of mass destruction in 2002-3 fall outside the scope of our study. We follow others in coding the end of Iraq’s nuclear program as 1991. The public presentation of nuclear intelligence in Secretary of State Colin Powell’s famous presentation before the UN Security Council is an example of states publicizing intelligence including some source and method details.

Yet, this intelligence was not vetted and, in two cases, actively rejected by the IAEA. This absence of vetting, combined with a well-known U.S. political interest in removing Saddam Hussein, led many leaders believed that the intelligence was cherry-picked.

**Iran 1974-1979, 1984-present**

Iran created its Atomic Energy Organization in 1974 with the goal of building 20 nuclear power plants, uranium enrichment facilities, and a reprocessing plant. West Germany, France, and the United States agreed to construct several of the nuclear power plants, though only two reactors were contracted from Germany. However, after the Shah was deposed, the program was thought to be “un-Islamic” and was terminated in 1979. In 1984, Iran’s interest in nuclear power was renewed, and in 1994 Iran secured Russia, which helped with constructing the reactor, training scientists, and supplying nuclear fuel. Exiled Iranians then revealed the presence of secret nuclear infrastructure to the IAEA in 2002 (Nassauer, 2005). In 2005 the IAEA Board of Governors stated that Iran was non-compliant with its Safeguards Agreement and the Security Council passed 7 resolutions requesting Iran to cease its activities. Numerous attempts have been made to negotiate with Iran, the IAEA had Overhead Imagery?” April 26, 1999.

---

57See discussion in (Bleek, 2017, 27).

58See Aid (2010, 245)’s discussion of how the intelligence made public in that presentation “closed off the last low-level sources of SIGINT that were then available to NSA about what was going on inside Iraq.”

59the IAEA received the raw intelligence allegedly demonstrating Iraq’s attempt to buy uranium from Niger on the day of Colin Powell’s speech to the United Nations and determined in a few hours that the evidence was fake, complete with falsified signatures, inaccurate information, and logical inconsistencies. The head of the IAEA, Mohamed ElBaradei, reported to the Security Council that the documents were “not authentic” (ElBaradei, 2011, 62-3). Similarly, the IAEA investigated U.S. claims that Iraq had attempted to import aluminum tubes for uranium enrichment. After a thorough investigation including in-country inspections, the IAEA concluded that “Iraq’s efforts to import these aluminum tubes were not likely to have been related to the manufacture of centrifuges.”

60As ElBaradei (2011, 3) notes, “to the inspection community, [Powell’s] presentation was primarily an accumulation of conjecture, an alignment of unverified data interpreted according to a worst-case scenario.” After choosing to bypass the IAEA, French president Chirac explained to the IAEA head that, “You know why you don’t get the information...It is because they don’t have any” (ElBaradei, 2011, 66).
and the Joint Comprehensive Plan of Action – which provides sanctions relief in exchange for restrictions on Iran’s nuclear capacity – was agreed to by the P5+1 and Iran in 2015.

While the U.S. and Iran were allies until 1979, they are no longer allies as of 1980. The U.S. thus had an interest in sharing intelligence about Iran’s program in order to shape international opinion about Iran and coordinate an international response. We thus expect the U.S. to share its intelligence beginning in 1991, and not to do so beforehand.

Unfortunately, it is difficult to assess how much intelligence U.S. leaders possessed regarding Iran’s nuclear activities prior to 1990. Recently declassified documents do suggest that the U.S. was concerned that Iran would pursue nuclear weapons during the 1970s, though it is unclear how much information the U.S. had because “to a great extent the intelligence side of the story remains an unknown.”

After the overthrow of the Shah, we find some hints of intelligence concern by the mid-1980s. For example, U.S. intelligence analysis stressed the risks of “new life” that had been breathed into Tehran’s “ambitious nuclear development program.” Even as Iran suffered from shortages of manpower and resources, the memo notes detection of Iranian efforts to recruit nuclear scientists and obtain training in foreign countries like Turkey and Argentina. Another memo from one year prior notes plans for “developing nuclear fuel cycle to support a nuclear research and power reactor program” but concludes Iran would be unable to obtain enriched uranium abroad and that “we have no evidence of an Iranian nuclear weapons program.” Intelligence-related material from the late 1980s remains classified.

Following the Gulf War in 1990, the U.S. collected intelligence using satellites, human intelligence, and intelligence from allies, though as of 2005 the U.S. did not have enough information to “permit solid conclusions about that country’s weapons program (Richelson, 2007, 506-7). The year 2004 brought a cascade of information. U.S. satellite imagery revealed “that Iran was burying the Natanz facility ‘presumably to hide and harden it against a military attack,’” and showed two underground structures that could potentially hold centrifuges (Richelson, 2007, 512).

Secondary literature and our interviews have no indication that intelligence-based suspicions about Iran were shared with the IAEA prior to 1991. Beginning around 1992, however, the U.S. began to regularly share intelligence with the IAEA. Changes at the IAEA had an impact on this sharing. One interviewee noted that the more assertive U.S. approach was in reaction to “an early IAEA Board decision that ‘invited’ this kind of information, [as] information on clandestine programs was recognized as a gap that need[ed] to be filled.” While the U.S. “passed intelligence to the IAEA’s inspectors in Vienna” starting in 1992 (Richelson, 2007, 506), this sharing continued through the 1990s and into the 2000s. For example, “The IAEA acquired a new non-compliance

---


65 Ibid.


67 See (Gaietta, 2016); Interview 10.

68 Interview 4.

69 Interview 38 also notes that intelligence sharing began in the early 1990s.
file in 2002, after the United States reportedly briefed the Secretariat on Iran’s clandestine nuclear activities” (Findlay, 2015). In 2003-4, the IAEA followed up on tips from the U.S., going to “a dozen sites” that had been part of a list of facilities to visit. At one point, the U.S. maintained “an active CIA person in the U.S. mission to Geneva that was a liaison with the IAEA to share information,” so that the IAEA “received more and more intelligence” over time.

The United States was far from alone. Other countries shared what they knew as well, leading to a “diversity of information” “from a variety of countries.” As Shea (N.d.) notes, the case for Iran has been “based largely but not solely on national intelligence information provided by more than 10 IAEA member states.” Indeed, almost all of our interviewees highlighted the extensive information shared during this time between the U.S. and the IAEA in particular, as “Iran...in the 1990s and 2000s featured very heavy collaboration between the U.S. intelligence community and IAEA country teams....It was also shared by UK, Germany, and France.” Iran thus represents a “high-profile case where the IAEA is using a lot of third-party information to develop a complete picture of a country’s nuclear program.” As such, Iran is the latest step in a “slow-motion revolution that has been underway at the Vienna agency since the end of the 1991 Persian Gulf War.”

One specific episode highlights the risks of exposing sources and methods in sharing intelligence and the valuable role the IAEA played in authenticating intelligence and overcoming perceptions of bias. In 2004, U.S. representatives stated that they had information from a laptop computer showing that Iran had nuclear weaponization studies that pertained to uranium conversion, high explosives testing, and the alteration of a missile reentry vehicle to carry a nuclear warhead (EIBaradei, 2011). The documents included over a thousand pages of descriptions of experiments and computer simulations. However, “American officials, citing the need to protect their source, have largely refused to provide details of the origins of the laptop computer.” Instead, “IAEA inspectors could neither keep the documents nor examine the laptop” (Brown, 2015, 145-6). Many consequently doubted the U.S.’s claims; for example, a senior European diplomat stated, “I can fabricate that data...It looks beautiful, but it is open to doubt.” As a result, the U.S. asked the IAEA to independently authenticate that the documents were not fraudulent. The IAEA complied, and “nuclear analysts at the international agency studied the laptop documents and found them to be credible evidence of Iranian strides.” The intelligence also prompted further IAEA scrutiny of a possible military dimension to Iran’s activities; its later public reports compared the laptop documentation with other intelligence and IAEA-gathered information to reach a conclusion of

---

70Interview 10.
71Interview 10.
72Interview 3.
73Interview 1.
74Interview 3.
75Interview 10.
78Ibid.
“serious concern.”

One body of evidence about the value of shared intelligence for the IAEA’s work is its own public reports which, since 2007, have regularly referred to the contribution of information provided by member-states. For example, one report explains that some intelligence it received “included procurement information, information on international travel by individuals said to have been involved in the alleged activities, financial records, documents reflecting health and safety arrangements, and other documents demonstrating manufacturing techniques for certain high explosive components” which “reinforces and tends to corroborate” IAEA-gathered information but also “relates to activities substantially beyond those identified in that documentation.”

The IAEA itself was forthcoming about its use of intelligence and the important role it played. For example, it noted in 2004 that it had been given the help of member states, and requested further intelligence submissions, stating, “The Agency has received some information from other States that may be helpful in resolving some contamination questions, and will equally continue to request those States to make every effort to assist the Agency in resolving this matter” GOV/2004/34. It also noted, “With the support of relevant Member States, the Agency has attempted to reconcile the deliveries of key equipment with information provided by Iran in connection with its AVLIS and MLIS programmes.”

In 2008, the IAEA stated, “Since the Director General’s last report, the Agency has continued to assess the information previously provided to it, both by Iran (including INFCIRCs/737 and 739) and by Member States,” and discusses “a computer image provided by other Member States showing a schematic layout of the contents of the inner cone of a re-entry vehicle. This layout has been assessed by the Agency as quite likely to be able to accommodate a nuclear device. The Agency showed Iran certain documentation which the Agency had been given by other Member States, purportedly originating from Iran, including a flowsheet of bench scale conversion.”

In 2009, the reports refer to, “the extensive information given to the Agency by a number of Member States detailing the design of the facility, which was consistent with the design as verified by the Agency during the DIV,”

along with “member States which have provided documentation to the Agency.”

A 2015 report cites a 2012 report when discussing “the existence of two “workshops” that were seen in videos provided by a Member State (Rauf and Kelley, 2015), and many subsequent reports refer to “information, which comes from a wide variety of independent sources, including from a number of Member States” “indicating that Iran has carried out activities that are relevant to the development of a nuclear explosive device, which “is

---

79 Conclusions were “based on more than 1,000 pages of information shared with the agency by US intelligence in 2005” but the IAEA “supplemented the laptop information with data from 10 member states, interviews on three continents, and its own investigations in Iran, Libya, Pakistan, and Russia.” Scott Peterson, “Iran nuclear report: Why it may not be a game-changer after all,” The Christian Science Monitor, November 9, 2011.


81 See GOV/2004/11.

82 See GOV/2008/59.

83 See GOV/2008/4.

84 See GOV/2009/74.

assessed by the Agency to be, overall, credible.” Subsequent reports then highlight that “information provided to the Agency by Member States indicates that Iran constructed a large explosives containment vessel in which to conduct hydrodynamic experiments; such experiments would be strong indicators of possible nuclear weapon development.” The IAEA explains how it used this information in a 2009 report: “Although the Agency has limited means to authenticate independently the documentation that forms the basis of the alleged studies, the information is being critically assessed, in accordance with the Agency’s practices, by corroborating it, inter alia, with other information available to the Agency from other sources and from its own findings.”

A specific episode is valuable for showcasing two issues: 1) the importance of the IAEA’s technical expertise and perception of unbiased analysis, and; 2) the way submissions by states supplies the IAEA with unique material that can address proliferation suspicions. In the late 2000s, the Agency vetted evidence that appeared to show Iranian involvement in weapons-related procurement. In this case, member-states submitted physical material from a procurement network that Iran allegedly participated in during the 1990s. The IAEA states, “On 21 May 2005, the Agency received from another Member State a number of centrifuge components, environmental sampling of which was thought might provide information on the origin of the LEU and HEU particle contamination found at various locations in Iran.” Further, “The analysis of the environmental samples collected at a location in another Member State where, according to Iran, the centrifuge components had been stored by the procurement network in the mid-1990s prior to their shipment to Iran, did not indicate any traces of nuclear material. The Agency’s assessment of these purchases, and the quantities delivered, is continuing with the assistance of Member States.” In its 2006 report, the agency states, “With the assistance of some Member States, the Agency is carrying out investigations on information and documentation which may have been provided to Iran by foreign intermediaries.” Further, “The Agency is aware that the intermediaries had this document, as well as other similar documents, which it has seen in other Member States.” In 2007, the IAEA report says, “The Agency has received additional information from the country from which the components originated.” Moreover, it states, “Based on interviews with Libyan officials and supply network members and information from other sources, the Agency has concluded that most of the items related to the 1993 offer had originally been ordered by the Libyan Arab Jamahiriya

86 See GOV/2012/55, GOV/2012/37, GOV/2012/23, and GOV/2012/9.
87 See GOV/2013/40, GOV/2013/27, GOV/2013.6.
88 See GOV/2009/55.
89 Note that the U.S. role in supplying the material in this episode remains unclear, but our interviews revealed that the US, Israel, and NATO “were all looking at the same information [and] shared with the IAEA” during this time. Interview 8.
91 See para. 11 of GOV/2005/67
92 GOV/2005/87.
94 See GOV/2006/27.
but were in fact delivered to Iran in the period 1994-1996.\footnote{See GOV/2007/58.}

Our theory predicts that this intelligence-sharing should have increased the IAEA’s effectiveness and led Iran to curb its proliferation activities, and we find this to be the case. Consider Iran’s clandestine gas centrifuge research at the Kalaye Electric Company site. Kalaye was Iran’s research and development center for centrifuge-based enrichment from the late 1990s until 2003. In 2003, “intelligence information alerted [the IAEA] to the Kalaye Electric Company, a workshop on the southern outskirts of Tehran where the Iranians had tested a small number of centrifuges” (ElBaradei, 2011, 116). Evidence of Iranian removal of sensitive documents and technology ahead of an IAEA inspection required sophisticated data; thus, during an intelligence briefing to IAEA officials, one account describes how American representatives shared their “most sensitive information” about Iran, which included “classified satellite photos showing that trucks and bulldozers had been at work at Kalaye in April and May, weeks before the IAEA inspectors were permitted into the main building. Tons of dirt were dug up around the building and removed. At the same time, truckloads of concrete rubble, presumably from the destruction of old walls and floors, were hauled off” (Frantz and Collins, 2007). Similarly, El Baradei notes, “The Agency received information that radiation detectors had been procured for use at this location. Satellite photos showed that at some point after August 2003, the site had been razed, its buildings torn down, and the grounds cleared, suggesting an effort at concealment” (ElBaradei, 2011, 127). This change allowed the IAEA to credibly claim to Iran that it knew of cover-up activities. As Frantz and Collins (2007) note, “[w]ithout its own intelligence arm and with limited access to commercial satellite photography, the IAEA depended on the American information as part of its larger inspection strategy in Iran. In the case of Kalaye, the photos confirmed the IAEA’s suspicions that Iran had tried to remove evidence of enrichment activities from the site.” Once on-site the IAEA detected remodeling work and took environmental samples which helped to demonstrate Iran’s dishonesty about enrichment at Kalaye (Gaietta, 2016, 91), and it was shut down in 2003.

Further, while the Natanz Fuel Enrichment Plant (FEP), the Fordow Uranium Enrichment Facility (Qom-FEEP), and the Karaj Agricultural and Medical Center (sometimes called Ramandeh) remain operational, and Molybdunum, Iodine and Xenon Radioisotope Production (MIX) Facility was constructed but is not operating, several other sites have been shut down at least in part due to intelligence that the U.S. shared with the IAEA. The Tehran Nuclear Research Center (Reprocessing) was shut down in 1993 after U.S. intelligence sharing stepped up in 1992 and 1993. This led to an IAEA visit, and the Agency visited three new sites in Feb 1992 based on Western intelligence. Similarly, the Plasma Physics Laboratories in Tehran was visited by the IAEA, and the U.S.’s intelligence forced Iran to move its centrifuges to less well-known location (Kalaye) in the mid-1990s. This site was shut down in 1997. The U.S. regularly shared intel in the late 1990s and 2000 about the Tehran Nuclear Research Center (Enrichment), but it is unclear if the U.S. was aware of its laser work before the 2003 revelation, and Iran shut it down in 2000 in part due to its need for a larger facility. Finally, Western intelligence supported the IAEA’s inspections of laser enrichment at Lashkar Ab’ad around 2003 and shared intelligence regularly between 2003-2004. Iran then ended its work there in 2003 due to the IAEA’s scrutiny.
Israel 1970-present

Israel’s nuclear program began in the early 1950s when it courted European partners to obtain nuclear materials for a clandestine nuclear facility at the Negev Nuclear Research Center near Dimona (Cohen, 1998, 58-65). By 1966, Israel could separate plutonium and had completed weapon designs research and testing of delivery means (Cohen, 1998, 231-3), and therefore possessed a small number of improvised nuclear devices during the 1967 Six Day War. Israel further refined its nuclear capability in the 1970s, reportedly experimenting with laser enrichment techniques, developing more advanced two-stage thermonuclear designs, improving the sophistication of its missile delivery systems, and possibly jointly testing a weapon with South Africa in 1979 (Cohen, 2013, 82-3). Very little information exists on Israel’s nuclear infrastructure and weapons developments in the 1990s and after.

As a non-NPT signatory, Israel’s nuclear infrastructure and materials were not regularly or extensively evaluated by the IAEA, though Israel has a facility-specific agreement with the institution for its Soreq Nuclear Research Centre – the site of a research reactor and, allegedly, weapons design and fabrication activities. Other sites, most importantly Dimona, are not under safeguards.

While the depth of cooperation waxed and waned, the United States has been a mainstay ally of Israel throughout the period under analysis. As early as the Kennedy Administration, Washington expressed its assurance of safeguarding the security and independence of Israel (Cohen, 1998, 169). We thus do not expect the U.S. to have provided intelligence about Israel’s nuclear progress to the IAEA, even once the institution had the ability to protect this information.

American intelligence has carefully followed Israel’s program both prior to and after its weaponization. Between 1958-1960, the U.S. learned through human intelligence that Israel was clandestinely constructing a reactor to manufacture fissile material. Communications intelligence and the U-2 spy plane also supplied information about the Negev site, revealing the presence of construction workers, heavy machinery, cement pouring, and other information. The U.S. uncovered more in subsequent years from its Corona satellite and human sources, and by 1967 it had many indications that Israel was making a bomb. In 1974 the U.S. believed “that Israel already ha[d] produced nuclear weapons” (Richelson, 2007), and in 1976 the CIA estimated that Israel had 10-20 operational nuclear warheads. Human intelligence led the U.S. to obtain additional pictures and information about Dimona in 1986, alerting it to Israel’s ability to produce thermonuclear weapons. Information regarding U.S. intelligence on Israel in the 1990s and beyond is unavailable, though Washington almost certainly continued to monitor nuclear developments.

We found no instances of intelligence sharing with the IAEA from our interviews, archival materials, or secondary sources. In fact, a former IAEA official specifically told us that the U.S. shared “absolutely no intelligence” with the IAEA about Israel. Another stated that the IAEA never inspected the Dimona reactor, and the U.S. never shared intelligence with the Agency and generally sheltered Israel from its scrutiny. A third interviewee stressed that since Israel’s nuclear activity represented less of a threat to the U.S. than other states’ programs – because of

---

98 Secondary sources include ElBaradei (1992); Bahgat (2008); Quester (1983); Cohen and Frankel (1987); Baumgart and Müller (2004); Cohen and Burr (2006); Feldman (1997).
99 Interview 38.
100 Interview 37.
the two states’ close relationship – the U.S. shared little with the IAEA.\textsuperscript{101} These statements are consistent with public reports that this intelligence was even withheld from “normal circulation” within the U.S. government due to its extreme sensitivity.\textsuperscript{102}

This intelligence pattern is also consistent with the U.S.’s broader goal of hiding Israel’s nuclear program.\textsuperscript{103} Rather than coerce Israel to put its nuclear infrastructure under safeguards and roll back its weaponization, the U.S. tried to obscure the status of Israel’s program and avoid public scrutiny. In the late 1960’s, Washington sought to create “circumstances in which Israel would not ‘announce’ a nuclear capability and would maintain secrecy” through “private, bilateral assurances that Israel would not deploy or test nuclear explosive devices.”\textsuperscript{104} Moreover, “Nixon probably guaranteed that the United States would not pressure Israel to roll back its program and join the NPT if it kept a low profile; this entailed a non-testing and non-declaring guarantee.”\textsuperscript{105} Washington even temporarily boycotted the IAEA after Israel came under fire for a counter proliferation strike against Iraq in the 1980s.\textsuperscript{106}

Without scrutiny by foreign partners and the IAEA in particular, Israel’s nuclear program progressed rapidly, and all four facilities – the Negev Nuclear Research Center, Dimona Machon 8; Negev Nuclear Research Center, Dimona Machon 9; Negev Nuclear Research Center, Dimona Machon 2; and Nahal Soreq – remain operational. Cohen (1998, 227-8) specifically notes that the IAEA’s absence facilitated Israel’s progress, stating: “Dimona has never been controlled by anything like the safeguards of the International Atomic Energy Agency (IAEA). All Israel has had to deal with are the United States’ visits to Dimona, whose ground rules it controlled and which ended with the Nixon-Meir amimut deal in 1969.” Moreover, the potential problems created by IAEA scrutiny were qualitatively different than bilateral arrangements because, in practice, manipulation and control are very different under “a bilateral arrangement conducted under tight Israeli control of the ground rules” versus “under an IAEA full-scope safeguards agreement” (Cohen, 1998, 302). Indeed, Henry Kissinger concluded that the U.S. should not “deprive Israel of the option to put together an operational nuclear capacity,”\textsuperscript{107} and could not do so bilaterally, stating that the U.S. “cannot–and may not want to try–[to] control the state of Israel’s nuclear program” (Cohen, 2013, 18).

\textsuperscript{101} Interview 40.


\textsuperscript{103} Cohen (2013, 48-9) describes the U.S. as a “co-custodian” of Israeli nuclear ambiguity and notes that “the United States has used its own influence to persuade others, Western and non-Western states alike, that the world can live with an Israeli bomb that is kept invisible.”

\textsuperscript{104} See Davies (1969).

\textsuperscript{105} See Rabinowitz and Miller (2015).

\textsuperscript{106} The precipitating event was a draft resolution in 1981 sponsored by Arab states which “called for a ban on technical assistance from IAEA resources to Israel, gave twelve months’ notice of a vote on Israel’s suspension from the agency, and further called upon the membership to cease trade with Israel in nuclear materials capable of weapons use” (Imber, 1989, 77).

\textsuperscript{107} Cited in Cohen (2013, 17).
Libya 1970-2003

Libya began pursuing nuclear weapons in 1970 – just after the 1969 rise of Muammar Gaddafi – claiming that the program was for civilian purposes. It began to train nuclear scientists, create a nuclear research reactor, buy nuclear weapons from other states and technology from the network created by A.Q. Khan, and sought uranium enrichment technology. The program was terminated in December 2003 (Solingen, 2009, 213-214).

The U.S. appears to have begun closely monitoring the program in the early 1980s. For example, a 1983 intelligence report noted Libya’s uranium stockpiling and attempts at cooperation with other states to further its program, though it believed the program remained rudimentary. The U.S. continued to collect extensive information using satellite, communications, and human intelligence, detecting the components of the program and the personnel. Fuhrmann (2012, 336).

In 2001, the U.S. found that Libya sought dual-use technologies, and in 2002 the U.S. thought that Libya could produce a nuclear weapon by 2007, though the latter estimate exaggerated the trajectory of Tripoli’s program (Montgomery and Mount, 2014). However, the U.S. and partners like the U.K. did possess detailed intelligence about Libya’s activities, and Libya “saw how much [the U.S. knew] about what they were doing” in the nuclear arena.

Libya was not an ally of the U.S. Our theory expects little intelligence sharing with the IAEA until 1991. This is the basic pattern that we observe. Regarding the pre-1991 period, secondary sources do not find instances of sharing and Fuhrmann (2012, 232) specifically notes that “despite the fact that many of the transgressions discussed above occurred at a safeguarded facility, they were never detected by the IAEA.” After the 1991 reforms, we do find indications of shared intelligence. The IAEA did not detect Libya’s program and so was reliant on shared information (Busch and Pilat, 2013, 463). One interviewee noted instances of intelligence sharing in the mid-1990s, and another highlighted intelligence given to the Agency in 2002 to alert them about centrifuges traveling to Libya. The IAEA itself reported that in 2008, “through clandestine intermediaries, Libya also received UF6 from another country: two small cylinders in September 2000 and a large cylinder in February 2001.” Details on this transaction, the Agency noted, came “from other Member States.”

One important period after 1990 apparently featured the U.S. withholding intelligence despite the IAEA’s readiness to evaluate. In 2002, the U.S. held back intelligence to protect negotiations with Libya. The Al Hashan Facility closed in 2002 and the Plutonium Separation Facility at Tajura Nuclear Research Center closed in 2003 due to a diplomatic deal between the U.S., UK and Libya in which the IAEA played no role. U.S. intelligence was aware of enrichment work at the Al Hashan Enrichment Facility, and the UK had intelligence about the plutonium separation.


110 See also Sinai (1997).

111 Interview 38.

112 Interview 6.

113 In one account, British personnel attempted to share intelligence related to closed diplomatic talks but the U.S. intervened to stop it (ElBaradei, 2011, 148).
experiments. Yet the U.S. did not share at the time and blocked the UK from sharing its intelligence with the IAEA Director General. However, the IAEA was angry when it learned of this, and El Baradei states that he informed the U.S. that it had violated the NPT by refusing to alert the IAEA when it first learned of Libya’s violation (ElBaradei, 2011, 150). He even threatened to resign when the U.S. (and the UK) were about to export Libyan equipment when a deal was reached. On the one hand, this is an episode in which our theory would expect intelligence to be shared. On the other hand, it demonstrates how by 2002 the IAEA had come to expect intelligence sharing because it had become routine.

What about Libya’s pace of nuclear progress? Overall, poor resources and other management problems were a consistent drag on Libyan nuclear activities (Braut-Hegghammer, 2016, 169-217). Moreover, the IAEA played a minimal role in the diplomacy that ended Libya’s program and shuttered two of its facilities. Yet we do find some evidence that Libya’s proliferation pace was slowed in the early 1990’s by the IAEA’s scrutiny which was likely the result tips from American intelligence-sharing. The U.S. received intelligence about possible involvement of Russian scientists in Libya in the 1991-1992 period. Around the same time, the IAEA conducted its first visit to the Tajoura Enrichment Facility and the director general interviewed top officials in Tripoli. This included specific inquiries about former Soviet scientists, which Gaddafi and others denied playing a significant role. This facility – used for gas centrifuge enrichment R & D – was closed in 1992. While we have not confirmed the links between intelligence, the IAEA visit, and the facility closure, the confluence of events is suggestive of an important role in the early 1990s period.

Pakistan 1972-1998

Pakistan’s defeat in a 1971 war with India and an Indian “peaceful nuclear explosion” in 1974 prompted its interest in nuclear weapons. Pakistan initially pursued a plutonium reprocessing route but was stymied by the international nonproliferation regime (Khan, 2012, 11). Its efforts to develop uranium enrichment were more successful, bolstered considerably by the theft of enrichment design information by the eventual head of their program, A.Q. Khan. Using an elaborate procurement network that circumvented export controls on sensitive technology, Khan’s efforts led to breakthroughs in the development of highly-enriched uranium by the mid-1980s. Most observers believe that Pakistan had the ability to create an improvised device by 1987 or 1988; its public detonation of a nuclear device did not occur until 1998.

Despite refusing to join the NPT, the IAEA played a continuous though circumscribed role in monitoring Pakistan’s nuclear infrastructure. Pakistan had facility-specific safeguards agreements with the IAEA at several sites. The IAEA therefore had active legal authority to monitor activity at five facilities during the Cold War, including the Canadian-supplied KANUPP heavy water reactor, American-supplied research reactors, and a reprocessing facility at Chasma that was originally to

---

114. Blix was received by Libya’s Colonel Muammar Qadhafi and other Libyan officials... Contrary to recent reports that Libya is hiring ex-Soviet personnel to boost its clandestine nuclear effort, Libyan officials asserted that, because Soviet funds and equipment were drying up, experts already in Libya under a longstanding cooperation program are now drifting away. Of the approximately 100 Soviet nuclear experts in Libya before the collapse of the USSR, most at the Tajura Nuclear Research Center, all but 20-30 have left the country, the Libyans asserted.” Mark Hibbs, “IAEA Explores Iran’s Intentions, Minus Evidence of Weapons Drive,” Nucleonics Week, February 13, 1992.
be built with the French.\textsuperscript{115} At present, eight Pakistani nuclear facilities are under IAEA safeguards. Other sites important to Pakistan’s nuclear weapons program, most notably the uranium enrichment facility at Kahuta, were built without foreign help and have never been under IAEA safeguards.

Pakistan’s relationship with the United States changed significantly over time. On paper, the two countries had a formalized 1959 defensive security pact, leading us to expect little intelligence sharing. In practice, their relations ebbed and flowed considerably. In some periods, such as the early 1970s and throughout the 1980s, Washington considered Pakistan an important, even vital, friend. During these times, the U.S. provided huge amounts of military and economic aid to Islamabad and, during the 1980s publicly misled Congress and the public about the extent of Pakistan’s nuclear progress to avoid sanctions. In other periods, such as the latter 1970s and the 1990s, Washington and Islamabad were “disenchanted” partners, with Pakistan heavily scrutinized for its nuclear ambitions and, later, its support for the Taliban and terrorism (Kux, 2001). These ebbs included American termination of military and economic aid which, in 1990, “effectively ruptured the bilateral security relationship that had flourished during the 1980s” (Kux, 2001, 311). Though we therefore code Pakistan as an ally, our coding cannot capture these nuances in the countries’ bilateral relationship, which we note here because they help to understand the intelligence-sharing that occurred during this period.

American intelligence services closely monitored Pakistan’s nuclear program from the start. (Richelson, 2007)’s account and a review of declassified American documents provide numerous specific details about clandestine Pakistani nuclear activity from intelligence sources. These include:

- Intelligence about a Pakistani purchase of uranium from Niger for use in its Karachi nuclear power plant (KANUPP) in 1976 (Richelson, 2007, 6642).

- Intelligence about an unreported and UNSafeguarded lab-scale reprocessing facility at Pakistan Institute of Nuclear Science and Technology (PINSTECH) in 1978 (Richelson, 2007, 6689).

- Intelligence from a foreign government indicating Pakistani test site readiness and possible test preparation in 1979 (Richelson, 2007, 6711).

- Intelligence in 1982 on clandestine Pakistani procurement of uranium enrichment described in a memo from the secretary of state to President Ronald Reagan. Secretary George Shultz states he is “absolutely confident that our intelligence is genuine and accurate.”\textsuperscript{116}

- An intelligence summary with a laundry list of specific data points on facilities, including clandestine enrichment at Kahuta, UF6 production at Dera Ghazi Khan, fuel rod production at Chasma, near completion of the New Labs small-scale reprocessing, and continued


\textsuperscript{116}Shultz to President, ”How do we make use of the Zia visit to protect our strategic interests,” November 26, 1982, National Security Archive, EBB 377, Doc 16.

- Intelligence in 1985 or 1986 from a human source in China reporting Chinese-Pakistani cooperation on bomb development, including details like work on a trigger mechanism (Richelson, 2007, 6778).

- Intelligence of uranium enrichment to 93.5 per cent despite Pakistani private guarantees of keeping only low-enriched uranium in 1986 (Richelson, 2007, 6757).

By the late 1980s, the U.S. had “built up a detailed dossier on the Pakistani program, through satellite images of PINSTECH, Kahuta, and continuing construction at Chasma and other facilities; communications interprets of talkative Pakistani scientists and military officials; and probably a few well-placed human sources in Pakistan and China” (Richelson, 2007, 344). Thus, American intelligence gathering had an incomplete but considerable window into all aspects of Pakistan’s nuclear weapons program in the 1970s and 1980s including their plutonium reprocessing facilities, uranium enrichment infrastructure, procurement efforts for both of uranium and enrichment technology, and weaponization activities. Though details after 1990 are not available to the same extent, there is clear indication of continued intelligence monitoring. After India’s test in 1998, the U.S. determined that Pakistan would soon test as well. It monitored Pakistani test-related activities by satellite and other means. After the test, the U.S. used imagery satellites to takes pictures of the test sites, communications intelligence, and seismic signals to collect information about the test and to verify Pakistan’s claims (Richelson, 2007, 440-1).

Regarding intelligence sharing with the IAEA, we find support for the theory’s predictions. We identified one instance of intelligence sharing during the pre-1991 period which, on the whole, serves as an exception to the rule because of the centrality of sources and methods concerns and ad hoc method of sharing. During periods of strong U.S.-Pakistan relations, moreover, we find clear evidence of active efforts by the United States to avoid public and multilateral scrutiny of Pakistani nuclear progress.

Overall we found very few instances of intelligence sharing with the IAEA despite the overwhelming evidence of Pakistani nuclear weapons development. As one interviewee told us, intelligence sharing during the 1970s and 1980s was “not routine and was very closely held at the secretariat.”\footnote{Interview 3.} One history of the relationship describes that the U.S. did not share what it knew. For example, in the mid-1980s, the U.S. “refused to share with the IAEA the information that China had provided help in weapons design and highly enriched uranium to Pakistan” (Mallard, 2014, 272). However, we identified one episode of intelligence sharing with the IAEA regarding Pakistan described in archival documents. In 1978 and 1979, American leaders wrestled with how to handle increasingly clear indications of progress on enrichment and reprocessing by Islamabad. As Washington debated who to inform and how to do so, revelation of sources and methods was an important concern. Several sharing options were considered but rejected due to sources and methods problems. One proposal for sharing information with India, for example, was rejected. As one cable mentions, “We fully understand your concerns about sharing with the Indians our concerns
about Pakistan’s nuclear intentions.”

A 1978 cable describes the “Pakistan Proliferation Problem” and notes that sharing the basis for U.S. concern with states like Israel, India, and Taiwan is unwise because “they could threaten the effectiveness of our efforts by informing the [Government of Pakistan].” In the end, sharing intelligence – but only with the IAEA’s director general and on an informal, ad hoc basis – was chosen. Even the authorization for this verbal briefing “[stressed] that information is of utmost sensitivity and for personal information of Director General Eklund only.”

A cable reporting the results of the meeting, led by Gerard Smith and Robert Gallucci, notes that they had “emphasized the extreme sensitivity of the information [the U.S.] was providing.” After Gallucci provided “some evidence,” the Director General asked whether he could share this information, he was told “no.”

In the 1980s, the Soviet invasion of Afghanistan led the Carter and Reagan administrations to explicitly reduce the importance of slowing Pakistan’s proliferation progress. Indeed, Washington began sheltering Islamabad from scrutiny in ways similar to Israel. The United States thus turned a “blind eye” to the problem both bilaterally and abroad: “since December 1979,” one former official commented, “two successive administrations all evinced a fundamentally permissive attitude toward Pakistan’s acquisition of nuclear weapons” (Smith and Cobban, 1988, 59). The link to Afghanistan is clear from archival material. A memo from the out-going Carter White House in January 1980, for example, describes a conversation with top Chinese officials in which the Americans state that “[o]ur big problem with Pakistan was their attempts to get a nuclear program. Although we still object to their doing so, we will now set that aside for the time being and concentrate on strengthening Pakistan against potential Soviet action.”

A memo on Pakistan’s nuclear program in 1986 notes sheds light on how the partnership on Afghanistan influenced the way the Reagan White House handled its nuclear suspicions. The director of the Arms Control and Disarmament Agency counters suggestions of more aggressively using intelligence and coercion to halt Pakistani developments. Noting that “[i]ncreasing pressure on Pakistan has risks,” Kenneth Adelman argues that “if the issue were forced publicly, Zia might reduce assistance to the Afghan rebels to show his independence from US pressures.” In one meeting, Pakistan’s President Zia explicitly invoked the precedent of Israel to suggest the U.S. could ignore signs of clandestine nuclear activity and maintain generous military aid programs given the close partnership underway in Afghanistan. While not specifically referencing intelligence sharing with the IAEA, Wash-

---


120 Pakistan Proliferation Problem,” State to US Embassy United Kingdom, Cable 292469, November 18, 1978. Wilson Center Digital Archive

121 State to US Embassy in Vienna, “Pakistan Nuclear Program,” Cable 075309, March 26, 1979. National Archives AAD.


125 Shultz to President, ”How do we make use of the Zia visit to protect our strategic interests,” November 26, 1982,
ington’s broader strategy of minimizing public pressure on Pakistan is consistent with declining to share intelligence with the IAEA during the 1980s. The same logic led the Reagan White House to shift emphasis in its private bilateral talks to avoiding a Pakistani nuclear test rather than halting or rolling back their nuclear progress capabilities (Rabinowitz, 2014).

While many factors contributed to Pakistan’s success in developing the nuclear fuel cycle and in weaponization, the absence of effective IAEA monitoring was an important enabling condition. As George Perkovich notes, the threat from India in Pakistan’s eyes rendered dissuasion ineffective meaning that “the only viable nonproliferation strategy was to block it physically from acquiring the capability to make them.” Again and again in the 1970s and 1980s, Pakistan was one step ahead of the non-proliferation regime in general, including the IAEA. Perkovich concludes that “Pakistan benefited enormously by not being a party to the NPT,” because “there were not fullscope safeguards in Pakistan, there was nothing like the Additional Protocol and teams of IAEA inspectors roaming around possibly to discover illicit imports.”

While many factors contributed to Pakistan’s success in developing the nuclear fuel cycle and in weaponization, the absence of effective IAEA monitoring was an important enabling condition. As George Perkovich notes, the threat from India in Pakistan’s eyes rendered dissuasion ineffective meaning that “the only viable nonproliferation strategy was to block it physically from acquiring the capability to make them.” Again and again in the 1970s and 1980s, Pakistan was one step ahead of the non-proliferation regime in general, including the IAEA. Perkovich concludes that “Pakistan benefited enormously by not being a party to the NPT,” because “there were not fullscope safeguards in Pakistan, there was nothing like the Additional Protocol and teams of IAEA inspectors roaming around possibly to discover illicit imports.”

The potential effectiveness of the IAEA in preventing Pakistani progress, if enabled by sophisticated and precise information, is illustrated by an interesting 1981 episode. By 1980, Pakistan had developed the indigenous capability to fuel its KANUPP reactor, a facility covered by an IAEA safeguards agreement. In 1981, the IAEA learned of possible diversion of spent fuel from KANUPP which might allow clandestine reprocessing. The source of information was not intelligence; rather, “concern was triggered by some sources in Pakistan who let it be known to us that the number of fresh fuel bundles could not be verified.” After an IAEA visit, the Director General declared that indigenous fueling meant that the IAEA could no longer verify that material had not been diverted. Pakistan eventually agreed to more intrusive safeguards on the KANUPP facility which, in part, slowed the development of their reprocessing track and elevated the importance of the uranium enrichment program. This was the conclusion of the American intelligence community: the refusal of foreign suppliers and the IAEA’s scrutiny had foreclosed reprocessing in the early 1980s, but uranium enrichment centered at Kahuta remained a major vulnerability.


South Africa began weapons exploring nuclear weapons in 1969, and its uranium enrichment project was announced in 1970. South Africa investigated the separation of lithium isotopes in 1973. In 1974, the Prime Minister then approved the development of nuclear weapons and it began work on a pilot enrichment plant. The country may have conducted a joint test with Israel in the Atlantic Ocean in 1979. South Africa completed a second device in 1982, and then added four

---


127 Lynne Reaves, “The Delicate Negotiations Between IAEA and Pakistan.” Nucleonics Week, November 12, 1981.

The program was shrouded in secrecy until it began to be dismantled in 1989 and was publicly disclosed in 1993 during the transition away from apartheid (Baeckmann, Dillon and Perricos, 1995).

The U.S.'s Corona and Gambit satellites photographed South Africa’s Pelindaba Nuclear Research Center in 1968-9, and continued to do so for decades. In 1976, these satellite missions, combined with aerial missions, revealed evidence of a nuclear test site, leading analysts to be “90 percent certain” that South Africa was preparing a nuclear test (Richelson, 2007, 279). In 1977 the U.S. concluded that South Africa had enough highly enriched uranium for several devices, and “that summer (1977), Soviet intelligence detected test preparations and, in early August, alerted the United States. U.S. intelligence quickly confirmed the existence of the test site (Albright, 1994, 41). The U.S. continued monitoring the site through imagery, human, and signals intelligence. After the Vela satellite detected a double light flash consistent with a nuclear test, the U.S. sought to determine whether a test had in fact occurred, and who was to blame, and collected extensive intelligence to this effect (Richelson, 2007, 286-9). In 1984 the U.S. determined that South Africa had enough uranium for 2-4 devices. South Africa agreed to sign the NPT and allow the IAEA to inspect its facilities in 1991, but considerable skepticism existed that it had been totally honest about its program. The U.S. attempted to answer these outstanding questions through a variety of intelligence collection techniques, though it did not obtain the entire picture (Richelson, 2007, 292-6).

South Africa was not a U.S. ally and thus had “few means of pressuring the South Africans away from pursuing nuclear weapons.” We thus do not expect intelligence sharing until 1991. Indeed, despite the extensive U.S. information about South Africa’s program, it did not seem to share their knowledge with the IAEA before the institution reformed. Our interviewees explained that Russia provided intelligence to the U.S. rather than to the IAEA, and the U.S. did not share this with the Agency. Instead of enlisting the IAEA’s help, “the Western nations pressed South Africa not to test” (Albright, 1994, 41). Even after South Africa began to dismantle its program in 1989, it did so “without the presence of the IAEA” (Heinonen, N.d., 171). Rather than share with the Agency, the U.S. revealed its intelligence to France and Britain, whom it trusted, to convince them to pressure South Africa not to test. However, they believed that there was “no credible threat from the West which would be sufficient to deter the South African government from carrying out a test” (Richelson, 2007, 280-2).

However, starting in 1991, states began to share their intelligence about South Africa’s program with the IAEA, which greatly assisted the Agency. For example, “When the IAEA began its inspections in 1991, South Africa was not obligated to reveal the existence of the critical facility or the other buildings in the valley...The IAEA, however, had learned of Building 5000 from Western intelligence, and asked for and was granted permission to inspect it” (Albright, 1994).

129 See Montgomery and Mount (2014).
130 See Burr and Richelson (2013).
131 Russia did not share it either. Interviews 12 and 38. We also found no instances of sharing in secondary sources such as Baeckmann, Dillon and Perricos (1995); de Villiers, Jardine and Reiss (1993); van Wyk (2015); van Wyk and van Wyk (2015); Harris, Hatang and Liberman (2004); Van Wyk (2012).
132 Further, the U.S. did not share bilaterally, as the U.S. and other states engaged in “parallel efforts” to collect intelligence (Richelson, 2007, 377).
Moreover, during this period, the IAEA “received U.S. briefings on most aspects of the weapon program.”\textsuperscript{133} Additionally, “information from IAEA Member States was used to confirm that all relevant facilities/locations had been inspected.”

National intelligence also assisted the Agency in its efforts in 1992 and later “to confirm the statements made by the South African authorities, and to set up a baseline to monitor that the program or its parts were not re-constituted.” To do so, “the IAEA had extensive discussions and briefings by former staff personnel to understand the country’s nuclear program from a ‘cradle to grave’ approach. Such information received was reconciled with other information received by IAEA from other member states” (Heinonen, N.d.).\textsuperscript{134} Then in 1993, the State Department notes that the IAEA “conducted over 20 inspection missions, examined many thousands of records [deleted] and received US briefings on most aspects of the weapons program [deleted]” (Richelson, 2007, 397).\textsuperscript{135}

Though South Africa’s dismantlement of its program would likely have occurred without the U.S.’s intelligence provision, this information helped the IAEA greatly and allowed it to conclude that the program had been totally terminated and to fully document the “timing and scope” of the program. Further, the Agency was able to determine that seeming discrepancies in the balance of uranium-235 associated with the Valindaba Y Plant – the most important nuclear facility – was consistent with what had been declared (Baeckmann, Dillon and Perricos, 1995). It also found that no sensitive components remained. Moreover, the amounts of LEU that South Africa had reported that were associated with the Valindaba Z Plant were also found to be consistent with the IAEA’s findings (Baeckmann, Dillon and Perricos, 1995). This information reassured the U.S. and others that South Africa had dismantled its program.

**South Korea 1970-1981**

South Korea began pursuing nuclear weapons in 1969 and started to construct a nuclear power plant in 1970 due to changes in the international security landscape, with the goal of building a bomb by 1977. It then tried to buy a pilot reprocessing plant from France. After U.S. pressure, it ratified the NPT in 1975 and dropped its program in 1981, though many believe that it continued to pursue them in later years.\textsuperscript{136}

U.S. president Ford first obtained intelligence about South Korea’s nuclear program in 1974. Analysts believed South Korea could obtain nuclear weapons by 1980. They were aware that South Korea was attempting to obtain a chemical separation plant from France, as well. In 1975, the U.S.

\textsuperscript{133}“South Africa: Nuclear Case Closed?” United States Department of State. December 13, 1993. Indeed, the U.S. cooperated frequently with the IAEA, as it also learned details about South Africa’s program as a result of the IAEA’s inspections after South Africa submitted to safeguards in 1991 (Richelson, 2007, 398-400).

\textsuperscript{134}Our interviewees corroborated these statements, as interviews 38 and 39 both said there was intelligence sharing, and interview 38 noted that it took place after 1992.

\textsuperscript{135}This is consistent with the account received in interview 5, who noted that the U.S. intelligence community representative briefed the IAEA multiple times about every facility. Note that direct assistance from the U.S. in analyzing enrichment plant records from South Africa was rejected by the IAEA since the Agency was “concerned for its institutional impartiality and integrity.” “South Africa: Nuclear Case Closed?” United States Department of State. December 13, 1993.

\textsuperscript{136}South Korea revealed covert nuclear experiments to the IAEA in 2004.
concluded that South Korea was trying to produce nuclear weapons.\(^{137}\)

South Korea was a key ally, so we do not expect to find much intelligence sharing in either period. In fact, we find no instances of intelligence sharing with the IAEA from our interviews, archival materials, or secondary sources,\(^{138}\) and indeed, find references to the U.S. keeping its information from the IAEA. For example, Kang et al. (2005, 47) reports that South Korea engaged in plutonium separation that was legal as long as it declared it to the IAEA. However, South Korea did not do so for many years, and neither did the U.S. Kang et al. (2005, 47) explains, “As to why the United States did not report the activity to the IAEA, it appears that in the 1980s U.S. national intelligence on these matters was shared with the IAEA only on a case-by-case basis.” Further, Hersman and Peters (2006, 549) notes that the IAEA “took.....nearly four years to learn of South Korea’s secret program,” so the U.S. clearly did not reveal it during that time.

Our theory also does not expect intelligence from the U.S. to the IAEA to have much impact on South Korea’s proliferation. In fact, while the U.S. was successful in rolling back South Korea’s program, it was largely due to bilateral U.S. efforts, and not multilateral efforts. Instead, the U.S. applied quiet, bilateral pressure on South Korea by threatening to cut its military assistance, Export-Import Bank loans, nuclear cooperation, technology sharing, financing, and security guarantees.\(^{139}\) The U.S. also tried to “inhibit ROK access to sensitive technology and equipment,...press the ROK to ratify the NPT, [and] improve our surveillance of ROK nuclear facilities.”\(^{140}\) Reagan also offered security guarantees and economic assistance in exchange for its compliance.\(^{141}\) Indeed, “under U.S. pressure, in January 1976 it suspended negotiations for a reprocessing facility; in December 1976 it suspended the whole formal program to develop nuclear weapons technology that it had inaugurated only two years earlier.”\(^{142}\) The U.S.’s status as an ally thus allowed it to use its leverage to prevent further proliferation.

**Syria 2000-2007**

Syria began to develop a plant to recover uranium in 1996 which became operational in 2001. It had one operational reactor that was built by China, though it continued to seek additional nuclear technology. Based on reports of contacts with North Korea soon after Bashar al Assad’s assumption of power, Syria’s nuclear weapons exploration is typically dated in 2000.\(^{143}\) Construction of a likely nuclear reactor at Al-Kibar began in 2001 or 2002, a site which Israel bombed in 2007. Following Bleek (2017), we use 2007 as the end of Syria’s program but, as discussed below, a resumed program is possible and IAEA interest in monitoring continues. Syria originally signed the NPT in 1969 and agreed to comprehensive safeguards with the IAEA in 1992.


\(^{138}\)See, for example, Pelopidas (2013); Heo (2008); Kim and Lie (2007); Ahn and Cho (2014); Moon and Lee (2009); Kang et al. (2005); Siler (1992); Paul (2000).

\(^{139}\)See Miller (2013); CIA (1978).

\(^{140}\)See National Security Council (1975, 3-5).

\(^{141}\)See Miller (2013).

\(^{142}\)See CIA (1978, 1).

\(^{143}\)See discussion in (Bleek, 2017, 29).
Prior to Israel’s 2007 bombing of the Al-Kibar facility, there was little concern about nuclear ambitions in Syria in public sources. However, the U.S. intelligence community watched Syria closely in part due to its chemical weapons program and other weapons pursuits. The U.S. had confirmed in 2004 that A.Q. Khan had offered nuclear technology to Syria, and noted that additional assistance could have been provided as well. 144 Regarding the Al-Kibar site, after receiving intelligence from Israel, the CIA determined that Syria was still pursuing the weapons but was likely not able to afford to develop an indigenous nuclear program, and instead was receiving assistance from North Korea. The intelligence included photographs and videos of the nuclear complex taken prior to the bombing. 145 Intelligence details made public in 2008 suggest U.S. intelligence may have detected work at Al Kibar nuclear site as early as 2001. 146

Syria is not a U.S. ally and its exploration and pursuit of weapons from 2000-2007 post-date IAEA reforms. Our theory therefore expects the U.S. to have shared intelligence with the IAEA regarding details about clandestine activities. Overall, we find mixed support for our two hypotheses. Some intelligence was clearly withheld, in particular regarding Al-Kibar. However, we do find evidence of more robust intelligence-sharing after the bombing regarding the Al-Kibar site and other possible sites in Syria’s nuclear program. Moreover, while military action was central to Syria’s loss of nuclear infrastructure, we find evidence that intelligence-enabled IAEA scrutiny has made resumption of Syrian exploration more difficult.

was shared about Syria’s program, though some intelligence was shared with a delay and other information was withheld altogether.

First, consider the facility Israel bombed in 2007 and intelligence that was not shared. In 2007, after Israel bombed the al-Kibar site, El Baradei notes, “I spoke out strongly, noting that any country with information indicating that the bombed facility was nuclear was under a legal obligation to report it to the IAEA. But no one came forward with such a report” (ElBaradei, 2011, 229). Instead, U.S. intelligence was shared after a delay of six months after the strike (Fuhrmann, 2012, 220). 147 As the former director general’s memoirs note, “An intelligence agency brought satellite images for the Agency to see, purportedly of Dair Alzour, which they said had been taken over a span of two years. The images helped clarify the design of the building that was alleged to have housed the reactor. Another intelligence agency provided additional photos, purportedly taken in the vicinity of the building, including inside” (ElBaradei, 2011, 232-3). 148 The IAEA referenced this intelligence in its safeguards assessment, stating that, “The information provided by some Member States to the Agency includes satellite imagery of the Dair Alzour site and the three other locations.” 149 According to one account, the IAEA’s interpretation of the Al-Kibar’s


147 El Baradei notes, “The US was obligated to share this information with the Agency, not to wait until Israel went and bombed the facility” (ElBaradei, 2011, 232).

148 “Israel, for its part, refused to provide the Agency with any information in their possession as to why they had bombed the facility” (ElBaradei, 2011, 234).

149 GOV/2008/60.
likely nuclear role was based on evidence from national intelligence.\textsuperscript{150} Regarding the Al-Kibar site, then, American intelligence was withheld until after the military strike but later shared, playing a key role in the IAEA's assessment after the fact.

Support for the theory comes from reports that additional intelligence was shared with the IAEA beyond Al-Kibar regarding other sites and nuclear-related purchases. This appears to be acknowledged by the IAEA itself, as its report on Syria notes information from member-states about “three other locations” (see previous paragraph). Moreover, El Baradei’s memoir notes that the IAEA received “satellite photos that showed equipment being moved from the destroyed site to other locations, so it was important to verify the nature of these three other sites” (ElBaradei, 2011, 232-3). A journalist account from 2009 specifically noted that “The IAEA has obtained some information from the US and Israel on other potential sites that might have a nuclear purpose in Syria, sources said.”\textsuperscript{151} Beyond these three sites, reporting from after 2007 also noted intelligence sharing about procurement. As one account notes, “The IAEA has obtained some intelligence-related information from member states that strongly suggests Syria had carried out foreign procurement activities since the late 1990s to support a reactor construction project, sources close to the IAEA said.\textsuperscript{152}

Assessing the impact of intelligence-sharing and the IAEA on Syrian progress is difficult. The bombing by Israel in 2007 was an obvious setback through a distinct mechanism. Moreover, it is unclear whether any substantive impact on Syria’s ability to pursue nuclear ambitions resulted from the IAEA’s use of intelligence to assess Al-Kibar’s true nature after its destruction. Most plausible is that intelligence shared with the IAEA about other sites and Syrian procurement activities will help deter Syria from rejuvenating its program should its civil war end. The IAEA is better equipped to monitor other sites and request access under the terms of Syria’s comprehensive safeguards agreement. It is also positioned to more easily track efforts to procure equipment.


Taiwan began a nuclear program in 1967 because China had obtained nuclear weapons. However, it claimed that its program was for peaceful purposes, and signed the NPT in 1968. The military-run Institute for Nuclear Energy Reaction began to work on the Taiwan Research Reactor in 1969 that it had purchased from Canada, and began to operate it in 1973, producing less than 10 kg of weapon grade plutonium each year. Taiwan also commenced work on a plutonium chemistry laboratory, a reprocessing facility, and a plant to make uranium fuel in 1969. Taiwan also attempted to buy

\textsuperscript{150}Interview 2. As another account summarizes, “the Agency had received information alleging that the installation destroyed at Dair Alzour was a nuclear reactor. This was just over a month after the United States provided the Agency with information it believed indicated that the installation was a nuclear reactor, but nine months after the attack itself. According to this information the reactor was not yet operational and no nuclear material had been introduced into it. Satellite imagery was provided by at least two intelligence agencies. One of these agencies revealed the presence of an individual who appeared to be a North Korean whom Agency personnel recognized from their dealings with the DPRK” (Findlay, 2015, 79).

\textsuperscript{151}Hibbs, Mark. “IAEA not Prepared to Request Syria Host Special Inspection.” Nuclear Fuel. August 24, 2009. See also description of intelligence shared with the IAEA that “flagged three additional suspect sites” in (Ogilvie-White, 2014).

a large reprocessing plant but was unable to do so. After dismantling its reprocessing facilities in 1977, it began building hot cell facilities in 1987.

The U.S. monitored Taiwan’s activities beginning in 1965 through its Corona satellite and embassies. In 1966 it learned of Taiwan’s intentions to develop a nuclear program from a history professor in Taiwan. In 1973 Taiwanese officials told the U.S. about its intention to develop a hot lab, and in 1974 the U.S. concluded that Taiwan was moving “toward development of nuclear weapons” (Richelson, 2007, 270). In 1975, the U.S. knew that five reactors were operating, and that Taiwan was either constructing or planning to construct four nuclear power plants. In 1987, the U.S. learned through human intelligence a variety of additional details about the program, which it used to confront Taiwan in 1988. Indeed, the U.S. had placed a CIA agent – Col. Chang Hsien-yi – as deputy director within the INER, and he was able to pass thousands of pages of information about Taiwan’s program to the U.S. In general, the U.S. had a good deal of information because “the ROC was relatively transparent both to U.S. and international authorities. Both foreign government officials, e.g., West German diplomats, and elements of the ROC elite were willing to pass on significant intelligence about Taiwan’s nuclear plans.”

Taiwan was a key U.S. ally and we thus do not expect much intelligence sharing with the IAEA. We find that, during this time, there were limited, targeted instances of sharing with the institution, though these occurred only after a great deal of hand-wringing about potentially revealing sources and methods. Indeed, intelligence sharing about Taiwan “was not routine and very closely held at the secretariat.” No instances of sharing occurred during the early years of the program. Despite the U.S.’s knowledge of Taiwan’s development, Hersman and Peters (2006, 549) notes that it took the IAEA “nine years to discover Taiwan’s initial nuclear program.” Since the Agency was unaware of the program, the U.S. clearly had not shared what it knew. In 1977 an instance of sharing did occur, however, which was reflected in a memo that proposed that IAEA experts and U.S. experts exchange information to verify whether Taiwan was hiding nuclear capabilities or intentions. One other instance of sharing may have occurred in 1988. Gregorian et al. (2005, 2) explains, “Indeed, in 1987, shortly before Chiang’s death, INER suddenly and quietly began building a multiple hot cell facility in violation of its 1976 commitments. The United States discovered it in 1988 after receiving a tip from a Taiwanese defector. Although no plutonium had yet been separated at the facility, U.S. intelligence officials estimated that Taiwan was within a year or two of developing a nuclear bomb.” Further, “the U.S. and IAEA were working together,” so it seems likely that information was shared with the Agency. This is also supported by Albright and Gay (1998b), which says that the U.S. and IAEA shared information to deter Taiwan.

Our theory also predicts that intelligence-sharing with the IAEA would play little role in pre-

---


155 Interview 3.

156 Also no instances of sharing were mentioned in our archival materials, interviews, or secondary sources such as (Hsu, 2015; US Opposed Taiwanese Bomb during 1970s, 2007; Albright and Gay, 1998a).

157 To: Secretary of State, From Embassy Tokyo, October 1, 1977. “ROC/IAEA Safeguards.” Department of State. P.2. This information matches our information from interviews, such as interview 39.
venting proliferation in this case. Indeed, the U.S. did not need broad international support, as the main driver of Taiwan’s abandonment of its program was direct U.S. pressure, which led Taiwan to get rid of its reprocessing facilities (INER Reprocessing Facility I and II) in 1977, as well as its hot cell facility and reactor in 1988. Starting in 1966, the U.S. insisted that any reactors be put under safeguards, and convinced Taiwan not to purchase a reprocessing facility. While the IAEA did inspect the facilities in the 1970s, it played “a low-profile role in Taiwan’s nuclear industry” and had a “problematic relationship with Taiwan.” Even though it had full safeguards on the INER reactor and also had a surveillance system, it could not account for ten spent fuel rods in 1976. The U.S. therefore conducted its own inspections as well, and was able to pressure Taiwan to get rid of the program by threatening to stop the construction of its three nuclear power plants, and suspending a variety of other contacts such as foreign aid and trade. In particular, “The United States increased public and private pressure on Taiwan to end all nuclear weapons-related activities. Washington threatened to cut off all fuel supplies, demanded the return of all plutonium of U.S. origin, and hinted that Taipei’s actions threatened to weaken the U.S. security guarantee and could result in a freezing of weapons sales to the island.” Taiwan was “generally responsive, of course, was not only that it was a U.S. ally, it was a relatively dependently one. Not surprisingly, Washington had substantially greater capability to discourage the nuclear ambitions of a dependent ally than it had to check those of a strong adversary.” INER Reprocessing Facility III is operational but is for civilian purposes and is subject to the IAEA Additional Protocol.

---


<table>
<thead>
<tr>
<th>Country</th>
<th>Facility Name</th>
<th>Construction</th>
<th>Operation</th>
<th>Intelligence Sharing</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algeria</td>
<td>Nineteen Pilot Fuel Enrichment Plants (PFEP)</td>
<td>1967-1990</td>
<td>Closed by 1999</td>
<td>U.S. pressure</td>
<td>Shut down due to U.S. pressure</td>
</tr>
<tr>
<td>Brazil</td>
<td>Nuclear Fuel Enrichment Facility (NEF)</td>
<td>1967-1990</td>
<td>Closed by 1999</td>
<td>U.S. pressure</td>
<td>Shut down due to U.S. pressure</td>
</tr>
<tr>
<td>Iraq</td>
<td>Atomic Energy Research Center (AERC)</td>
<td>1960-1990</td>
<td>Closed by 1999</td>
<td>U.S. pressure</td>
<td>Shut down due to U.S. pressure</td>
</tr>
<tr>
<td>India</td>
<td>Bhabha Atomic Research Center (BARC)</td>
<td>1967-1990</td>
<td>Closed by 1999</td>
<td>U.S. pressure</td>
<td>Shut down due to U.S. pressure</td>
</tr>
<tr>
<td>Israel</td>
<td>Negev Nuclear Research Center (NNRC)</td>
<td>1960-1990</td>
<td>Closed by 1999</td>
<td>U.S. pressure</td>
<td>Shut down due to U.S. pressure</td>
</tr>
<tr>
<td>South Korea</td>
<td>KAERI (Korea Atomic Energy Research Institute)</td>
<td>1967-1990</td>
<td>Closed by 1999</td>
<td>U.S. pressure</td>
<td>Shut down due to U.S. pressure</td>
</tr>
<tr>
<td>North Korea</td>
<td>SPPR (Scientists and Proliferation Prevention Research)</td>
<td>1967-1990</td>
<td>Closed by 1999</td>
<td>U.S. pressure</td>
<td>Shut down due to U.S. pressure</td>
</tr>
</tbody>
</table>

Note: ENEA facilities are labeled as "closed" or not according to Pileggi and Trush (2015). Sources for the role of intelligence are described in case studies in the main text and the Supplemental Appendix. The facilities listed before the double horizontal line are those that we expect to potentially close or roll back according to the theory since the country is a non-ally and the facility was open during the post-reform period. Our theory expects that intelligence sharing occurred for country-facilities in the top box, and that this led the program to slow down, since these countries are non-allies and the facilities closed after 1990. Further, we see facilities of allies being closed as a result of direct pressure, and facilities of non-allies prior to the reform remaining open.
References


CIA. 1978. “South Korea: Nuclear Developments and Strategic Decision-making.” National For-


Ogilvie-White, Tanya. 2014. “The IAEA and the International Politics of Nuclear Intelligence.”
Richelson, Jeffrey. 2007. Spying on the bomb: American nuclear intelligence from Nazi Germany to Iran and North Korea. WW Norton & Company.
URL: https://www.iaea.org/About/Policy/GC/GC36/GC36Documents/English/gc36-1017_en.pdf

40
URL: http://nsarchive.gwu.edu/nukevault/ebb221/