Strategy Research Project

Improving Information Sharing to Support US National Interests

by

Colonel James C. Royse
United States Army

United States Army War College
Class of 2014

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-04-2014	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Improving Information Sharing to Support US National Interests

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel James C. Royse
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Douglas Mastriano
Department of Military Strategy Planning and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,719

14. ABSTRACT

Existing national and DoD classified military information (CMI) foreign disclosure policy does not effectively support U.S. security interests. The US National Security Strategy promotes US security interests through partner capacity, emphasizing at-risk states. Diplomatic and military elements of national power require support from the information element. Foreign disclosure policy can be changed to support better alignment of US interests and partner nation action. Principal-agent theory offers a way to frame foreign disclosure policy changes by applying a metric of improved interest alignment gained through reduced information asymmetry. A more effective national policy reflects the information environment, leverages technology to support foreign disclosure, and leverages CMI disclosure as a means of reducing information asymmetry to improve partner state interest alignment with U.S. security interests. The proposed information sharing policy enables the information element of national power to support U.S. interests in at-risk states in the context of a multi-polar international order.

15. SUBJECT TERMS
Foreign Disclosure, Classified Military Information, Principal-Agent Theory, Information Element National Power

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	31	

USAWC STRATEGY RESEARCH PROJECT

Improving Information Sharing to Support US National Interests

by

Colonel James C. Royse
United States Army

Colonel Douglas Mastriano
Department of Military Strategy Planning and Operations
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Improving Information Sharing to Support US National Interests
Report Date:	15 April 2014
Page Count:	31
Word Count:	5,719
Key Terms:	Foreign Disclosure, Classified Military Information, Principal-Agent Theory, Information Element National Power
Classification:	Unclassified

Existing national and DoD classified military information (CMI) foreign disclosure policy does not effectively support U.S. security interests. The US National Security Strategy promotes US security interests through partner capacity, emphasizing at-risk states. Diplomatic and military elements of national power require support from the information element. Foreign disclosure policy can be changed to support better alignment of US interests and partner nation action. Principal-agent theory offers a way to frame foreign disclosure policy changes by applying a metric of improved interest alignment gained through reduced information asymmetry. A more effective national policy reflects the information environment, leverages technology to support foreign disclosure, and leverages CMI disclosure as a means of reducing information asymmetry to improve partner state interest alignment with U.S. security interests. The proposed information sharing policy enables the information element of national power to support U.S. interests in at-risk states in the context of a multi-polar international order.

Improving Information Sharing to Support US National Interests

> When you cut through the noise, what's really at stake is how we remain true to who we are in a world that is remaking itself at dizzying speed.
>
> —President Barack H. Obama[1]

The U.S*. National Security Strategy* (NSS) seeks to extend influence to more countries and capitals to build new partnerships. However, U.S. foreign disclosure policy is poorly crafted to support the NSS. To rectify this, a review and update of the national information and intelligence sharing policy is necessary to align it with U.S. interests in the confines of the global environment.

The NSS pursues U.S. security interests by investing in the capacity of strong and capable partners. Emphasis is on states entering post-conflict stabilization, states at risk for instability, and states with potential for future conflict.[2] The use of U.S. national power to develop partners in rebuilding states, failed states, or failing states recognizes the fundamental multipolar international order where regional powers have the capacity to exert greater influence over regional problems. This approach envisions leveraging regional power to provide stability and security via partnerships with at-risk states.

In his introduction to the NSS, President Obama specified his vision to extend influence "to more countries and capitals," "build new and deeper partnerships in every region, and strengthen international standards and institutions."[3] To achieve this end, government policies must be complementary to maximize the potential to advance U.S. interests for all of these conditions. A relevant U.S. information and intelligence sharing policy is integral to enabling the information element of national power in support of U.S.

interests. An effective information sharing policy must be designed to enable U.S. interests in at-risk states in the context of a multipolar international order.

Existing foreign disclosure policy does not efficiently support U.S. interests to foster security, pursue sustainable and responsible security systems in at-risk states, or even support conflict prevention. Existing information sharing policy is predicated on a monopoly or at least a high degree of control over intelligence information when dealing with at-risk states. Some changes to foreign disclosure policy can be made to improve alignment of at-risk partner nation actions with U.S. interests. We can leverage principal-agent theory to provide a way to evaluate changes in information sharing policy by applying an objective metric of improved interest alignment gained through reduced information asymmetry. Principal-agent theory provides a rational actor model of asymmetric relationships in which the principal provides incentives to an agent to act in the principal's best interests, even if the actions are not in the agent's interests. It assumes that principles and agents act based on different information and that principals lack information about the agent's choices until the principal can observe the outcomes of those choices.[4]

This paper will express the strategic imperative to share information and intelligence by highlighting relevant U.S. interests. The NSS provides the basis for this and can also illuminate other national security information sharing dependencies. Second, it will examine the policy that underpins the contribution of the information element of national power to national interests. Third, it will offer an appreciation of the stale nature of U.S. policy through a review of how the global context has changed over time. This will demonstrate the need to adapt policy to support the modern reality

envisioned in the NSS. Finally, in light of the modern context it provides a description of principal-agent theory fundamentals and their international relations utility as a means to frame a more effective information sharing policy. To maintain a consistent and narrow focus, the scope here is limited to information and intelligence sharing policy as functions of the information element of national power in support of the military element of national power. A focus on classified military information (CMI) allows a complete review from policy to strategy to implementation with pragmatic recommendations for policy improvement.

The Strategic Imperative to Share Information

Both the NSS and DoD strategy rely directly on sharing information and intelligence with foreign partners for successful implementation. The NSS addresses this broadly as it highlights how the President envisions advancing U.S. interests abroad. This mandate is more explicit in DoD strategy documents where intelligence sharing is highlighted as an important tool for building partnerships with foreign entities. The U.S. has begun to focus on the necessity of information sharing in both the National Security Strategy and defense strategy.

The NSS focuses on functions dependent on information sharing while also focusing on partnering with countries where there is a high risk for compromise of sensitive U.S. information or intelligence. In President Obama's introductory letter to the 2012 NSS he described the following vision for advancing U.S. interests:

> We must also build and integrate the capabilities that can advance our interests, and the interests we share with other countries and peoples. Our Armed Forces will always be a cornerstone of our security, but they must be complemented. Our security also depends upon diplomats who can act in every corner of the world, from grand capitals to dangerous outposts; development experts who can strengthen governance and support human dignity; and intelligence and law enforcement that can

> unravel plots, strengthen justice systems, and work seamlessly with other countries.[5]

His closing thought in this vision focused on intelligence and law enforcement working seamlessly with other countries to build and integrate these capabilities in order to advance U.S. interests.

Both of these functions are dependent on shared information to perform effectively. To build a relationship that helps a country to thwart terrorist attacks or that brings transnational criminal members to justice requires the U.S. to share as much as possible. This in turn will build partner nation confidence that the U.S. can be relied upon to provide further information in a timely manner to prevent attacks.

Sharing such information with reliable partner nations is easy to conceive. Those international relationships have developed trust over time, but what about giving the same consideration to unstable countries with fledgling, untested, and possibly corrupt governments? It is precisely these at risk states that the National Security Strategy says the U.S. will promote as strong and capable partners. In this, the NSS emphasis is on states entering post-conflict stabilization, states at risk for instability, or states with potential for future conflict.[6] These three types of states might also be called rebuilding states, failed states, or failing states. All can be described as at-risk. Rebuilding states such as Iraq, Afghanistan, Sri Lanka, or Libya each enjoy varying degrees of stability and divergent levels of security and law enforcement institutions. U.S. interests with each also vary, but none are long term treaty allies. Yet countries in this category have potential to seek the kind of strong and capable U.S. partner relationship the NSS aspires to develop. Yet, the NSS does not specify that sharing intelligence or information with at-risk states is explicitly required to achieve U.S. interests. It is a

matter of policy interpretation to determine what elements of national power should be applied in each case.

Defense strategy also employs information and intelligence sharing as an option for U.S. Combatant Command (CCMD) campaign plans. The DoD issues the Guidance for the Employment of the Force (GEF) bi-annually to CCMDs to convey strategic priorities in a consolidated document. It synchronizes the overarching planning for the DoD ways and means that will be used to achieve the ends described in higher strategy documents like the National Security Strategy. The GEF directs planning for DoD ways through CCMD campaign plans and contingency plans. It directs DoD means by promulgating the global posture and global force management.[7] The GEF is a detailed DoD strategy that broadly guides CCMD planning.

U.S. Combatant Commanders (CCDRs) develop Theater Campaign Plans (TCPs) that operationalize their strategy. The TCP includes a Theater Security Cooperation Plan (TSCP), which describes how the CCDR uses security cooperation to support the TCP strategy during Phase 0 (shaping) / steady state operations.[8] The TSCP is integral to how the CCDR influences countries on strengthening security institutions. *Intelligence and information sharing* is one of the eight security cooperation focus areas directed as ways that CCDRs may implement a cohesive strategy to contribute to achievement of TCP objectives. The option to share intelligence and information is part of a range of TSCP security activity options available to CCDRs.

With this view, DoD allows the sharing of intelligence and information as part of a comprehensive plan to influence countries, build partnerships, and strengthen security institutions. This does not imply that this tool is meant to be used in isolation from other

security cooperation activities, but rather that it is an enabler to other security cooperation activities. For example, to conduct the security cooperation activity of assurance and regional confidence building relies on building trust to assure partner nations and improve their commitment to peace and security.[9] Sharing information and intelligence is a straightforward way to enable this activity.

US Information Sharing Policy

The national and DoD policies governing the sharing of intelligence with foreign partners are laid out in a series of well integrated policies and directives. The national policy uses an interagency solution which incorporates a thorough membership across the executive branch of government to determine whether to share classified military information (CMI) with prospective partners. The DoD directive ensures tight compliance with the national policy. The following review of the authorities, criteria, process, and oversight function provides the factual basis necessary to later recommend changes. The description of when each policy or directive was issued or last updated is also critical to inform the objective analysis to follow regarding the suitability of this set of policies to the contemporary global context.

National Policy

Both national security and national defense strategy rely on sharing intelligence and information to pursue national interests. Disclosure of classified military information (CMI) is governed by two national level policy documents. National Security Decision Memorandum 119 (NSDM 119) directs the U.S. Secretaries of Defense and State to control the release of CMI in consultation with the “Chairman of the Atomic Energy Commission, the Director of Central Intelligence, and the heads of other departments and agencies.”[10] National Disclosure Policy-1 (NDP-1) is the short title for “National

Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations". It is the interagency document that implements NSDM 119. NDP-1 is a classified document tightly controlled by the Office of the Director for International Security Programs, Office of the Deputy Under Secretary of Defense Technology Security Policy and National Disclosure Policy (ODUSD/TSP&NDP). It is issued only to personnel who are designated disclosure authorities with a need to know.[11]

NSDM 119 was signed on July 20, 1971 by National Security Advisor Henry A. Kissinger. NSDM 119 defines U.S. CMI as:

> information which (a) is under the control or jurisdiction of the Department of Defense, its departments or agencies, or is of primary interest to them; (b) may be embodied in written, oral or other form; and (c) requires protection in the interest of national defense and security in one of the three classification categories -- TOP SECRET, SECRET or CONFIDENTIAL -- as described in Executive Order 10501, as amended.

NSDM 119 established the U.S. government policy with four basic tenets. First, it designates CMI as a national security asset to conserve and protect. Second, it allows CMI to be disclosed to foreign governments and international organizations only where there is a "clearly defined advantage to the United States."[12] Third, it sets out that disclosures be consistent with U.S. "foreign policy objectives and military security requirements and limited to the purpose of the disclosure."[13] Finally, it mandates that disclosures only be allowed when the recipient will "substantially" protect the CMI in the same manner that the U.S. would.[14]

NDP-1 is dated October 1, 1988, a reprint of a September 9, 1981 version, and has updates through February 18, 1999.[15] In addition to specifying categories of CMI, designating disclosure authority to specific officials, NDP-1 establishes five disclosure

criteria in order to ensure the policy is properly administered.[16] The disclosure criteria in NDP-1 restate the four tenets of NSDM 119 to prescribe five discreet considerations of: consistency with U.S. foreign policy objectives for the recipient, consistency and no risk of jeopardy to U.S. military and national security objectives, recipient assurance of security and control of the information in the same manner the U.S. would, U.S. benefits from the exchange at least equivalent to the value of the information, and the disclosure's limitation to information necessary to achieve its purpose. The national policy for determining when CMI can be shared with partner nations and institutions to influence countries, build or strengthen partnerships, and strengthen security institutions is based on the five criteria above, developed in 1971 and codified for implementation in 1981 with minor changes added through early 1999. The criteria and the context of their development provide the basis for examining their suitability in the contemporary geopolitical context.

DoD Direction

DoD direction for sharing CMI is promulgated in DoD Directive 5230.11, under the subject "Disclosure of Classified Military Information to Foreign Governments and International Organizations."[17] DoD Directive 5230.11 was issued on June 16, 1992. It specifies the applicability and scope of the directive; reiterates the policy governed by NDP-1; and assigns responsibilities to DoD Under Secretary and Assistant Secretary level officials, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Defense Intelligence Agency Director, the Director National Security Agency/ Central Security Service, and the DoD General Counsel.[18] It then establishes procedures for international agreements for disclosure of CMI; disclosure during meetings, symposia, and conferences; disclosures to foreign visitors, liaison officers,

and exchange personnel; disclosure related to sales, lease, loans, or grants of classified items; foreign test and evaluations; foreign participation in DoD component classified training; requests for classified documents; foreign access to information when participating in U.S. procurement programs; and operation of the National Military Information Disclosure Policy Committee (NDPC).[19] It is the function of the NDPC to make determinations about exceptions to disclosure of CMI under SECDEF authority using the criteria and conditions established by U.S. policy.[20]

The NDPC also provides guidance on the administration of NDP-1. The members of the NDPC include representatives of the Secretaries of State and Defense; the Secretaries of the Army, Navy, and Air Force; and the CJCS who also represent the Combatant Commands and Specified Commands. These general members are joined by twelve special members. General members vote on all issues and special members vote on issues directly of interest to their organization. Other than the Secretary of Energy, the Director of National Intelligence, and the Director of Central Intelligence, the special members are all represent either DoD Assistant or Under Secretaries or Directors of Combat Support Agencies.[21] The NDPC members represent senior and experienced officials at very high levels within DoD and the executive branch.

DoD direction for foreign disclosure of CMI thoroughly captures the national policy from NDP-1 and NSDM 119, and was given in mid-1992. It establishes processes for common interactions requiring disclosure of CMI to foreign governments and their representatives. It organizes a responsible and complete membership for oversight and implementation of foreign disclosure of CMI. These factors are essential for further discussion of review and update of intelligence sharing policy.

The Global Context Then and Now

Four contextual factors govern foreign disclosure policy suitability based upon a changing global environment and security relationships. The U.S. position as a producer in the global intelligence "marketplace" offers a further area for comparison. Finally, as an enabling capability for that intelligence marketplace, the technology for exchanging information and intelligence is an important factor to consider.

The International Order and U.S. Global Role

From the 1971 formulation of NSDM 119 to the 1992 issuance of the corresponding DoD directive, through the most recent updates of NDP-1 in the late 1990s, the timeline tracing the development of U.S. foreign disclosure policy is long. This forty year old governing policy at the heart of how the U.S. decides when to share CMI begs the question on if it retains its relevance after a period of changes in the international order. The international order in 1971 was bipolar in the framework of the Cold War where the U.S. and NATO led the capitalist West against the communist Soviet Eastern Bloc. The U.S. role as Western leader in this international order was an extension of U.S. containment policy, formulated after World War II to stop the spread of communism.[22] As the cold war ended in 1989, the global order shifted to one of hegemonic U.S. global leadership.[23] The next major adjustment to foreign disclosure policy came during this period when DoD updated its directive in 1992. However, this reflected internal DoD changes rather than adaptations to the international order.

However, the rise of transnational violent extremist organizations was the next major shift in the international order. It really occurred through the 1990s, but is commonly indexed to the September 11, 2001 Al Qaeda attacks against the United States. The "post 9-11" international order is significant due to the transnational and

transient nature of the terrorist threat and the reactions of countries who found themselves targets of terrorists.[24] The U.S. global policeman role became more focused in purpose on the defeat the global terrorist menace and their ilk. As the U.S. took on long and costly wars in Afghanistan and Iraq, the global order began to shift again to a more multipolar order with the U.S. retaining a superlative role as a global military and economic power even while encouraging and cautioning the rise of regional powers that challenged U.S. interests. This modern multipolar environment in 2014 is distinct from the preceding epoch in the international order.

U.S. Alliances and Partnerships

In 1971, the U.S. lead role in NATO, the war in Vietnam, and alliances in the Pacific with Japan, South Korea, and the Philippines were all extensions of the U.S. role to lead opposition to communist expansion. The significant forward presence of over 750,000 armed forces deployed around the world demonstrated its resolve to lead the West.[25] The arms race that accompanied the U.S. role in the bipolar international order drove a stable context for military partnerships and the presence of large numbers of troops in Europe and Asia.[26] These durable alliances and international institutions remain in 2014. NATO's composition expanded after the fall of the iron curtain but remains in a collective security treaty.

As the cold war ended the U.S. began to operationalize the role of global policeman by responding to conflicts at the lead of coalitions to maintain peace, stability, and regional security in places like Kuwait, Bosnia, Somalia, and Rwanda. These coalitions often included international partners as opposed to formal allies. This blending of national power capabilities into coalitions was also used in response to the September 11, 2001 Al Qaeda attacks with the formulation of the Global

Counterterrorism Forum (GCTF), an international diplomatic response to the transnational threat.[27]

U.S. Market Share of Intelligence

In 1971 the U.S. enjoyed a monopoly position in the West for access to sensitive technical intelligence capabilities. With the closest U.S. allies working and sharing in complementary fashion, Western intelligence capabilities represented a distinct advantage in international relations and an advantage over their communist rivals. This was little changed by the late 1980's when NDP-1 received its last major revision. The U.S. no longer has a monopoly on intelligence although it maintains a quantity and quality edge. In a multipolar global order, the U.S. remains the dominant purveyor of information, but is no longer an exclusive one.

Information that was once exclusively government controlled became available to a larger number of governments and commercially accessible. Satellite imagery is an example of a type of intelligence information which has undergone this kind of demystification and growth of access.[28] A policy which demands securing the information the U.S. produces could simply lead to a missed opportunity to secure a customer in the growing global intelligence "marketplace" today. This contrasts boldly with the nature of the environment in 1971 when the choice was between western allies or communist ones to join the community of technical intelligence consumers. Today it is a question of funds. A country can buy it or build their own.

Access, Reliability, Speed, and Risk: the Role of Information Technology

The greatest change in the global intelligence market is the relative affordability of the technology to either hire or own the means of production. The barriers to entry are low and the knowledge and skill necessary to launch technical collection platforms

are readily obtained.[29] In addition to this, the global information environment has expanded in speed, access, and reliability since the foreign disclosure policy was approved in 1971. Satellite photos taken commercially in France or California are routinely transmitted anywhere in the world over the internet in mere seconds. Governments can share raw data and finished intelligence in the same way, reducing the influence of any single player in the intelligence discipline. The influence or leverage available when foreign disclosure policy was formulated is vastly different in 2014.

Reframing Information Sharing Policy

Principal-agent theory began as a way to describe economic situations, usually employer incentives to employees used in developing employment contracts.[30] However, it is applicable to any situation in which one party (the principal) wishes to motivate another (the agent) to act on its behalf.[31] Principle-agent theory explains rational behavior based on four main concepts.[32] The first concept, agency cost, is the difference between how well the agent acts in the best interests of the principal versus how the principal would have acted in his or her own interests. The alignment of incentives from the principal to the agent is meant to improve the degree to which an agent will act in the best interest of the principal.[33] Moral hazard is the second principal-agent concept, occurring when an incentive encourages the agent to act against the best interests of the principal.[34] Interest asymmetry is the third concept and it occurs when either agency cost is too high or competing incentives create a moral hazard causing the agent to act in their own interests. Finally, information asymmetry describes a condition in which the agent operates based on different information than the principal and modifies their actions to not act in the principal's best interests.[35] When the principal has better information than the agent, the principal can reduce information asymmetry

by sharing the information with the agent and improving interest alignment. This is the crux of intelligence sharing in international relations when two states or institutions share a common challenge.

Principal-agent theory is applicable to international relationships such as those described in the NSS where the U.S. desires to partner with other nations and regional institutions to advance U.S. security interests. From the U.S. perspective the agent is the foreign country or regional security institution and the U.S. is the principal. This does not obviate the fact that the opposite is true. It is always the case in principal-agent theory that there is logically a reverse principal-agent relationship, even if a minor one where the incentives may be different but the relationship is mirrored. For the purpose of this analysis the focus is on the primary principal-agent relationship between the U.S. and the worst case of an at-risk state.

The magnitude of agency cost for the U.S. is determined by the degree that the U.S. would use its national power to influence. For example when NATO carried out combat operations against Libya, there was little risk of a direct attack on the U.S. homeland.[36] This represents a low agency cost. There is a higher agency cost when Mexico secures its Southern border from illegal immigration that might include transnational threats to the U.S. attempting to transit to the U.S.[37] In these two simplified examples it is clear that agency cost is a useful way to describe U.S. security interests using principal-agent theory.

The impact of moral hazard applies to U.S. international relations in situations when the ally or partner has a competing external incentive or internal incentive to act in contravention of U.S. interests. An act such as Turkey's denial of U.S. access to deploy

forces through Turkey into Northern Iraq in 2003 is an example of this.[38] The moral hazard of new and untested partners has similar potential to undermine U.S. interests even when preliminary indications are otherwise favorable.

Interest asymmetry captures the reasoning in both previous examples for the agent state or institution to assert its interests ahead of or incongruent with U.S. interests. Interest asymmetry is a constant in international relations where the notion of enduring interests is superior to that of enduring partnerships. The need to understand domestic and international political influences on the agent state is critical to developing good U.S. policies for each partner. The broader category of interest asymmetry is helpful for developing policy approaches to reduce both agency cost and moral hazard.

The final principal agent concept, information asymmetry, describes the international system natural state of affairs. Rarely do any two states or institutions decide policy or take action based on the same set of information about a problem they face. States and security institutions are often surprised or perplexed by the actions or reactions of others in global affairs. The U.S. uses foreign disclosure policy to mitigate risks to national security and regional interests by providing sensitive information to agent states and security institutions. This policy reduces information asymmetry with the closest U.S. partners and allies, many of whom share a high degree of interest alignment with the U.S. already. The concept of information asymmetry with at-risk partner nations or agents evokes an important question about the value of using information, specifically intelligence in the form of CMI, to cause an at-risk agent state to increase interest alignment with the U.S.

Adapting Information Sharing Policy to Improve NSS Effectiveness

Principal-agent theory is an acceptable basis for describing international security relationships. It also allows categorization within a rational actor model. Given this utility, principal-agent theory can also be used to posit improvements to international relations policies. Principal-agent theory can frame a recommendation to improve information sharing policy. The start point for this framework is the concept of information asymmetry and its inverse relationship to interest alignment. The recommendation below is limited to the discussion of changes to NSDM 119. The other instruments of CMI foreign disclosure policy and practice flow from the tenets of this policy and would require commensurate change to reflect the adapted national policy.

Principal-agent theory suggests no specific concern with the first tenet of NSDM 119 as CMI should remain a national security asset to conserve and protect. However, the policy must recognize that where CMI competes with similar sources of intelligence, the U.S. should consider protecting only the capability that exceeds the quality of commercial or governmental competitors. This will allow the U.S. to leverage available information in exchange for enhanced international principal-agent relationships. For example, as higher resolution commercial satellite imagery becomes widely available, the U.S. should use its ability to produce similar products to advantage security partnerships as a matter of policy rather than exception.

Principal-agent theory suggests that disclosing CMI only when the U.S. will gain a clearly defined advantage is short-sighted. If reduction of information asymmetry can be expected to improve interest alignment then the potential advantage to the U.S. would be defined in how the partner nation chooses to adjust its interests in light of reduced information asymmetry. The advantage to the U.S. could well be indirect and

may not manifest in an immediate measurable advantage. This suggests retaining a degree of caution in the development of the detailed policy solution, but the reality of competition in the modern information environment means that the U.S. cannot rely on withholding CMI to coerce or compel potential partner nations.

If the U.S. insists on retaining sensitive information then it should be no surprise when a partner nation, particularly an at-risk one, chooses not to share the U.S. burden of military risk. Sharing CMI with states that already closely align with U.S. security interests does little to leverage the information element of power to strengthen relationships with international partners. This practice reinforces already strong relationships. However, it is the at-risk category of potential partner states where the greatest opportunity to improve U.S. security interests lies. By garnering support to U.S. security interests closest to the global problems confronted by at-risk states the U.S. NSS seeks to reduce direct U.S. military power requirements by enabling partners to maintain security. Foreign disclosure policy framed using principal-agent theory more effectively supports this strategy.

The NSDM 119 notion that foreign disclosure could be simultaneously consistent with military security requirements and foreign policy objectives is anchored in the context of the Cold War. The 2010 NSS sets a strategy to partner with at-risk states to allow regional partners to confront emerging and lingering security challenges with no direct U.S. intervention. This aspect of the foreign disclosure policy should be reframed to disconnect the implied direct relationship between military security and foreign policy objectives.

The final tenet remains reasonable that disclosures only be allowed when the recipient will “substantially” protect CMI in the manner the U.S. would. This is more a question of acceptable protocols than one of suitable circumstances to share CMI to further national interests. The use of information sharing technology in a manner which limits risk of compromise by partner states is technically feasible and should be used to maximize the opportunity to improve interest alignment by sharing CMI when possible. Biometric identity verification technologies and thin client work stations are an example of measures that can reduce the burden on partner nations to duplicate expensive U.S. security protocols. Further research on CMI protection methods is warranted in the spirit of leveraging information sharing to support a foreign disclosure policy based on a principal-agent framework.

A CMI foreign disclosure policy update should be grounded in a principal-agent framework. It should reflect the increasingly multipolar international order in which the U.S. is a leading nation. It also should be enabled by modern information technology. Updated CMI foreign disclosure criteria should adopt four tenets. First CMI foreign disclosure policy should designate CMI as a national security asset to conserve, protect, and leverage in developing aligned national interests with foreign governments and security institutions. Second, it should allow CMI to be disclosed to foreign governments and international organizations where the security interests can reasonably be expected to become more aligned with U.S. security interests as a result of the disclosure. The more the foreign government or international organization demonstrates the will to share U.S. security risk, the greater the level of CMI disclosure should be. Third, disclosures should be consistent with U.S. foreign policy objectives. Finally, disclosures

should be allowed any time the recipient can meet minimum identity verification standards for trusted agents. This adaptation reflects a policy that would allow the U.S. to maximize the disclosure of CMI where possible in order to leverage the information element of national power to enable the other elements of national power. It would build trust in at-risk states and allow the U.S. to rely on a growing number of partners to respond to future security challenges. It would be a policy that allows the U.S. to keep up with the dizzying rate of change in the world while remaining true to who we are.

Conclusion

The NSS and supporting DoD strategies envision U.S. engagement with at-risk states to pursue U.S. regional stability and security interests. The inherently governmental elements of national power, diplomatic and military, are well suited to lead engagement with at-risk states. The other elements of national power, information and economic, are not exclusively governmental and must be influenced by government policy to support national security interests. Information as an element of national power includes aspects that are more exclusively governmental, such as intelligence. The need to support U.S. interests with the information element of power in at-risk states is a particular challenge. Instability and potential links to U.S. adversaries among emerging partner nations in these categories confound sharing in favor of protecting U.S. sensitive information and intelligence.

National CMI foreign disclosure policy was formulated during the Cold War when the information environment for intelligence was essentially bipolar with a Western and communist Eastern Bloc competing as ideological intelligence monopolies. The U.S. undertook little post-cold war adaptation to national foreign disclosure policy or supporting DoD policy and implementation directives. However, the need to meet global

security challenges with at-risk partners demands a review of the national level policy. The degree of exclusive government control and the nature of the information environment are dynamic and increasingly less government dominated. Proliferation of technology, reduced barriers to entry, and access to the global information marketplace through the internet have all contributed to a reduced reliance on governments to develop and distribute information, even information once exclusively controlled by government intelligence agencies.

The view that the information environment offers a choice between sharing or protecting intelligence ignores the broader environment in which the partner nation is not exclusively reliant on U.S. sharing to access information. The U.S. does not have a monopoly on information or intelligence. In a multipolar global order, the U.S. is a dominant purveyor of information, but must recognize it is not an exclusive one, nor even a choice among two major alliances as was more the case during the cold war.

These strategic conditions can be reframed using the basic concepts of principal-agent theory and a better contextual appreciation of the emerging international order within the rapidly changing information environment to develop an improved national policy. A more effective national information sharing policy reflects the information environment, leverages technology to support foreign disclosure, and leverages CMI disclosure as a means of reducing information asymmetry to improve partner state interest alignment with U.S. security interests. With this refined foreign disclosure policy, the U.S. can extend influence to more countries and capitals to build new partnerships that help meet growing security challenges closer to the problem and with more of the risk shouldered by partners, thus freeing the U.S. to engage decisively on the most

critical security challenges. The proposed information sharing policy empowers the information element of national power to support U.S. interests in at-risk states in the context of a multi-polar international order.

Endnotes

[1] Barack H. Obama, "Remarks by the President on Review of Signals Intelligence," January 17, 2014, http://www.whitehouse.gov/photos-and-video/video/2014/01/17/president-obama-speaks-us-intelligence-programs#transcript (accessed March 22, 2014).

[2] Barack H. Obama, *National Security Strategy* (Washington, DC: U.S. Department of Defense, May 2010), 26-27, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed September 11, 2013).

[3] Ibid., cover letter, 2.

[4] Gary J. Miller, "The Political Evolution of Principal-Agent Models," *Annual Review of Political Science* 8 (March 2005): 203-206, http://faculty.washington.edu/jwilker/571/571readings/Miller.pdf (accessed February 15, 2014).

[5] Obama, *National Security Strategy*, cover letter, 2-3.

[6] Ibid., 26-27.

[7] U.S. Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication 5-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), II-3 - II-4.

[8] U.S. Army War College, Department of Military Planning Strategy and Operations, *Campaign Planning Handbook* (Carlisle Barracks, PA: U.S. Army War College, Academic Year 2014), 53-56.

[9] Ibid., 56.

[10] Henry A. Kissinger, "National Security Decision Memorandum 119," July 20, 1971, 3, http://www.nixonlibrary.gov/virtuallibrary/documents/nsdm/nsdm_119.pdf (accessed February 14, 2014).

[11] U.S. Department of Defense, *Disclosure of Classified Military Information to Foreign Governments and International Organizations,* Department of Defense Directive 5230.11 (Washington, DC: U.S. Department of Defense), 1, http://www.dtic.mil/dtic/pdf/customer/STINFOdata/DoDD_523011.pdf (accessed February 14, 2014).

[12] Kissinger, "National Security Decision Memorandum 119," 2.

[13] Ibid.

[14] Ibid.

[15] U.S. Department of Defense, Office of the Deputy Under Secretary of Defense (Technology Security Policy & National Disclosure Policy), *International Programs Security Handbook* (Washington, DC: U.S. Department of Defense, June 2009), HH-2, https://acc.dau.mil/adl/en-US/470589/file/60184/Intl%20Programs%20Security%20Handbook%20June%202009.pdf (accessed February 14, 2014).

[16] Ibid., 3-8.

[17] U.S. Department of Defense, *Disclosure of Classified Military Information to Foreign Governments and International Organizations,* 1.

[18] Ibid., 1-7.

[19] Ibid., 7-14.

[20] U.S. Department of Defense, Office of the Deputy Under Secretary of Defense (Technology Security Policy & National Disclosure Policy), *International Programs Security Handbook*, 3-13.

[21] The special members of the National Military Information Disclosure Policy Committee are: The Secretary of Energy, The Director of National Intelligence, The Director of Central Intelligence, The Under Secretary of Defense for Policy, The Under Secretary of Defense for Acquisition, Technology and Logistics, The Under Secretary of Defense for Intelligence, The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, The Assistant to the Secretary of Defense (Nuclear, Chemical and Biological Defense Programs), The Director, Defense Intelligence Agency, The Director, Missile Defense Agency, The Director, National Geospatial-Intelligence Agency, and The Director, National Security Agency as described in: Ibid., 3-14 - 15.

[22] George Kennan, "The Long Telegram," February 22, 1946, http://www2.gwu.edu/~nsarchiv/coldwar/documents/episode-1/kennan.htm (accessed September 12, 2013).

[23] Quintard Taylor, Jr., "United States History: Timeline: Cold War," http://faculty.washington.edu/qtaylor/a_us_history/cold_war_timeline.htm (accessed March 22, 2014).

[24] Andrea Lynne Drabot, *Transatlantic Intelligence Sharing and the Fight against Terrorism*, Masters Thesis (Chapel Hill: University of North Carolina, 2013), 1-36.

[25] Tim Kane, "Global U.S. Troop Deployment, 1950-2003," October 27, 2004, http://www.heritage.org/research/reports/2004/10/global-us-troop-deployment-1950-2003 (accessed April 2, 2014).

[26] Henry A. Kissinger, *Diplomacy* (New York: Simon & Schuster, 1994), 703-732.

[27] U.S. Department of State Office of the Coordinator for Counterterrorism, “Global Counterterrorism Co-Chairs’ Fact Sheet,” http://www.state.gov/j/ct/rls/other/gctf/173355.htm (accessed April 2, 2014).

[28] Ann M. Florini and Yahya Dehqanzada,”Commercial Satellite Imagery Comes of Age,” *Issues in Science and Technology* 16, no.1 (Fall 1999): 45-52.

[29] James Clay Moltz, “Asia’s Space Race,” *Nature* 480, no. 7376 (December 8, 2011): 171-173.

[30] Joseph G. Haubrich, “Risk Aversion, Performance Pay, and the Principal-Agent Problem,” 1-3, Working Paper, http://www.clevelandfed.org/Research/Workpaper/1991/wp9118.pdf?WT.oss=Risk%20Aversion,%20Performance%20Pay,%20and%20the%20Principal-Agent%20Problem&WT.oss_r=93 (accessed February 15, 20140.

[31] Financial Times Lexicon, “Definition of Principal/Agent Problem,” http://lexicon.ft.com/term?term=principal/agent-problem (accessed February 15, 2014).

[32] Miller, “The Political Evolution of Principal-Agent Models,” 205-224.

[33] Financial Times Lexicon, “Definition of Principal/Agent Problem.”

[34] Financial Times Lexicon, “Definition of Moral Hazard,” http://lexicon.ft.com/Term?term=moral-hazard (accessed February 15, 2014).

[35] Financial Times Lexicon, “Definition of Principal/Agent Problem”; For an in depth review of Principal-Agent Theory in International Relations, see Darren G. Hawkins et al., *Delegation and Agency in International Organizations* (New York: Cambridge University Press, 2006).

[36] Ellen Hallams and Benjamin Schreer, “Towards a ‘Post-American Alliance? NATO burden sharing after Libya,” *International Affairs* 88, no. 2 (March 2012): 313-327.

[37] Mark Joyce, “Mexico’s Security Crisis and Implications for US Policy,” *The RUSI Journal* 154, no.1 (February 2009): 66-70.

[38] Meltem Müftüler-Bac, "Turkey and the United States: The Impact of the War in Iraq," *International Journal* 61, no. 1 (Winter 2005, 2006): 61-81.