

New Collaborative Approaches to IP Protection

Roy Kamphausen

ROY KAMPHAUSEN is a Senior Advisor for Political and Security Affairs at the National Bureau of Asian Research. He can be reached at <rkamphausen@nbr.org>.

EXECUTIVE SUMMARY

This working paper examines new approaches to trade-secret protection and argues that protecting intellectual property (IP) requires more than enhanced corporate protection measures and better government enforcement mechanisms; informal information sharing is a necessary component.

Main Argument

The loss of trade secrets is an especially challenging issue for multinational corporations. Corporations that suffer the theft of trade secrets in foreign markets often have few incentives to pursue legal remedies or might have low expectations that their issues will be redressed. Ultimately, they may simply “eat the losses” from IP theft in ways that neither satisfy company goals nor hold IP thieves accountable. To be sure, corporations could do much more to prepare for challenging new environments and defend against trade-secret theft. Additionally, international trade organizations and agreements also serve useful roles in establishing structures and principles by which countries can establish regimes for protecting intellectual property. But these regimes can be ineffective against persistent entities intent on continuing to steal intellectual property, in particular trade secrets. Thus, changing the behavior of bad actors becomes a paramount consideration, one that requires alternative approaches to the problem of IP theft. Viewing the challenge as a collective-action problem faced by multinational corporations and national governments presents new possibilities to address the issue. Considered in this way, the principal challenge is how to develop a model for the meaningful sharing of information between corporations and governments in a multilateral setting.

Policy Implications

- Corporations and governments need more tools to deter the theft of intellectual property, especially trade secrets.
- A mechanism that provides for information sharing between governments and the private sector on a multilateral basis would complement existing multilateral agreements.
- The Wassenaar Arrangement provides one such model. This model emphasizes standards-based development of a list of bad actors, transparency of operations, voluntary participation, national compliance and enforcement, and threat-focused information sharing.

The May 2013 *Report of the Commission on the Theft of American Intellectual Property* (IP Commission Report) identified challenges to the protection of intellectual property, measured the scale and scope of the problem of the theft of American intellectual property (IP), and focused on the global origins of IP theft, a large portion of which was found to be from China. The IP Commission Report concluded that diminished revenue and reward, as well as decreased incentive to further innovate, were deleterious effects of IP theft that put at risk continued advancements needed to maintain the current period of unprecedented global economic prosperity.

The IP Commission Report concluded with a series of short-, medium-, and long-term policy recommendations that U.S. administrations and the U.S. Congress might undertake to better facilitate the protection of American intellectual property. Included were specific recommendations to bolster the protection of trade secrets and allow for more vigorous legal action in the event of trade-secret theft.¹

This working paper builds on the findings of the IP Commission Report to suggest new multilateral approaches for preventing the theft of intellectual property, in particular trade secrets. To be sure, principal responsibility for the protection of a corporation's trade secrets lies with the corporation itself. Although national implementation of international trading agreements serves important and useful functions, these measures are inadequate by themselves to provide the robust protections required, especially for trade secrets, in large part because they focus on the actions of states and not the perpetrators of theft. The paper argues that considering protection from trade-secret theft as a collective-action problem rather than just a bilateral or multilateral trade-enforcement issue suggests new approaches for finding policy solutions.² Multifaceted problems call for multidimensional responses that emphasize transparency and

¹ Commission on the Theft of American Intellectual Property, "The Report of the Commission on the Theft of American Intellectual Property," National Bureau of Asian Research, May 2013, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf. This source will subsequently be referred to as "The IP Commission Report."

² For the purposes of this paper, a "collective action" problem exists when a certain public good would benefit multiple actors, but no single actor acting alone is able to provide that good. In such cases, the provision of the public good is best achieved through the collaboration of two or more actors. If some actors choose not to participate in the provision of the good, while still benefiting from its provision by others, the "free rider" problem arises.

voluntary participation in which there are proper and agreed roles for the corporate sector, government-to-government channels, and international organizations.

This paper begins with a discussion of the nature of the problem, examines several dimensions of the issue, and then proposes two potential models for consideration. It finds that a government membership structure that focuses on standards-based development of a list of bad actors, demonstrates transparency of operations, allows for voluntary national compliance and enforcement, and provides threat-focused information sharing might yield useful points of comparison and analysis. The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, because it exhibits many of these characteristics, is one specific approach that merits examination and consideration (see **Appendix**).

The Nature of the Problem

The protection of intellectual property has many dimensions. At the level of the firm, corporations have the principal responsibility for the protection of their own intellectual property. Copyrights need to be protected, trademarks need to be honored, and company trade secrets—including formulas, processes, and outcomes—need to remain anonymous profit producers for their owners. As a February 2014 study points out, corporations have much work to do in understanding the unique nature of their own trade secrets as well as the potential threats to the protection of those trade secrets while framing comprehensive strategies to operate effectively in a variety of scenarios.³

For multinational corporations seeking to operate profitably in foreign markets, the protection of trade secrets becomes an especially important undertaking. Legal protections for trade secrets can be quite limited in some countries, and the robust legal regimes that permit redress for trade-secret theft are often less well-developed in those same countries, thus making the hard task of protecting trade secrets even more challenging. For instance, a report released by the U.S.-China Business Council just after the IP Commission Report was published noted that trade-secret protection was judged as the greatest IP concern to U.S. business in China.⁴

³ “Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats,” CREATE.org, February 2014.

⁴ U.S.-China Business Council, “Recommendations for Strengthening Trade Secret Protection in China,” September 15, 2013.

In nations that have mature legal systems, intellectual property rights (IPR) violations are most often handled by lawsuits brought by private rights holders. In such a plaintiff-based system, IP violations are dealt with singly and consecutively. Eventually, a body of law emerges that has a regularized set of penalties for similar behavior, and over time these punishments serve to deter bad behavior.

However, if protections break down and legal systems fail, trade secrets may be lost without recourse. These losses can have particularly deleterious effects. In extreme cases, corporations may not learn of the loss of proprietary information until the very existence of their own corporation is at stake. In situations that fall short of an existential threat to a corporation, there is often an unwillingness to disclose losses out of concern for the reputational impact on its stock prices and Wall Street valuation. Companies also worry that investors and shareholders could initiate liability or class action lawsuits on the basis of corporate malfeasance, especially in cases where a corporation's competitive advantage is revealed to have been stolen. If a loss does not become public knowledge, a corporation might choose to not disclose it and to instead write the loss off as a "cost of doing business," especially if the corporation worries that disclosing the loss might negatively affect its ability to remain viable in the same national market where the theft occurred.

In cases where multinational corporations do pursue legal remedies, the process still can be fraught with uncertainty. Cases may be barred outright on the basis of lack of standing. Additionally, extralegal obstacles might emerge and market access issues be introduced. If a case is permitted to be lodged, the ability to conduct legal discovery might be limited, or national law may not allow for the confirmation of evidence that might lead to the conviction of guilty parties.⁵ In short, the available legal remedies for globalized trade-secret theft are limited and rarely result in legal satisfaction for the injured party.

At the level of state-to-state relations, the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) was established in 1996 to address many of the challenges faced by corporations in a multilateral setting.

⁵ Commission on the Theft of American Intellectual Property, "IP Commission Report," 39–45.

The TRIPS Agreement includes three main features:

- *Standards.* The agreement sets out the minimum standards of protection to be provided by each member country. Each of the main elements of protection is defined—namely, the subject matter to be protected, the rights to be conferred and permissible exceptions to those rights, and the minimum duration of protection.
- *Enforcement.* The agreement deals with domestic procedures and remedies for the enforcement of IP rights.
- *Dispute settlement.* The agreement makes disputes between WTO members about the TRIPS obligations subject to the WTO's dispute-settlement procedures.⁶

TRIPS represents the highest standard of interstate interactions on the protection of IP rights and is the basis for new 21st-century trade agreements such as the Trans-Pacific Partnership and the Transatlantic Trade and Investment Partnership. Yet the importance of TRIPS notwithstanding, the agreement has several shortcomings:

- The post-TRIPS environment has not seen a robust transfer of technology from more developed countries to lesser-developed countries, at least to the extent envisioned by some lesser-developed countries. In some cases, this has contributed to a perverse logic where the illegal acquisition of trade secrets is perceived as an acceptable course of action to access new technologies.⁷
- Negotiations on trade agreements are secretive and inherently political in nature, including the possibility of trading concessions on the protection of intellectual property.⁸ As a function of the political nature of negotiations and the intensive interactions that characterize them, there are winners and losers in the establishment of the rules. Some individual sectors might have outsized influences on the outcomes. Yet from the perspective of individual countries, protection against the theft of trade secrets supersedes the rules of the TRIPS Agreement.
- Perhaps most importantly, the TRIPS Agreement regulates trade-related activities at the level of government-to-government interaction. However, governments can hardly openly endorse IP theft; in the cases where they do, one can have a high degree of confidence that those same governments would not enter into trade agreements on those activities. Trade-secret theft is a targeted activity against specific corporations, but one that is perpetrated by highly distributed actors, which diminishes the efficacy of national enforcement mechanisms.

⁶ "Overview: The TRIPS Agreement," World Trade Organization, http://www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

⁷ Carlos M. Correa, *Review of the TRIPS Agreement: Fostering the Transfer of Technology to Developing Countries* (Penang: Third World Network, 2001), <http://www.twinside.org.sg/title2/t&d/tnd13.pdf>.

⁸ Erik Kain "IP Protection Standards in TPP Represent the Downside of the Trans-Pacific Partnership," *Forbes*, January 25, 2012, <http://www.forbes.com/sites/erikkain/2012/01/25/ip-protection-standards-in-tpp-represent-the-dark-side-of-the-trans-pacific-partnership>.

But even if national governments are not the entire solution, it would be foolish to rule out any role for them in protecting against the theft of trade secrets. Governments do indeed have a role, and they would appear to be most effective when acting in concert with the governments of like-minded states.

In view of these challenges facing TRIPS and other international trade agreements, the IP Commission Report sought to sanction the actions of bad actors, rather than add to the many requirements that governments must deal with regarding IP problems. A set of remedies focused on bad actors emphasizes deterring bad behavior (or punishing it, should it occur) rather than putting the onus on governments to preemptively enforce protections of IP rights as part of additional trade agreement requirements: “The Commission regards changing the incentive structure for IP thieves to be a paramount goal in reducing the scale and scope of IP theft. Simply put, the conditions that encourage foreign companies to steal American intellectual property must be changed in large part by making theft unprofitable.”⁹

The IP Commission Report, however, recognized that its recommendations are limited in their applicability; principally, inputs from countries that are trading partners were not incorporated in the description and analysis of the problem of IP theft. The ramifications of poor IP protections, however, are felt by more than just a single country; consequently, solutions are not completely possible if pursued on a purely unilateral basis. Indeed, multilateral approaches are most likely to be successful over time. This working paper picks up where the IP Commission Report leaves off, by taking up the issue of how to multilateralize the protection of intellectual property. The principal challenge in such an approach centers on how to manage the sharing of information in effective and trustworthy ways.

Trade-Secret Theft as a Collective-Action Problem

At a fundamental level, intellectual property enables the pursuit of competitive advantages through the exclusive use of a technology, a process, or information. Those who steal intellectual property seek a shortcut to the process of trial and error, innovation, and effort that led to its development in the first place. Consequently, corporations seek to protect their intellectual property—not just for the theoretical benefits that a well-functioning economic entity might

⁹ Commission on the Theft of American Intellectual Property, “IP Commission Report,” 4.

entail, but also to realize the very practical benefits (namely, profits) that exclusive use of a trade secret might yield. Corporations have a vested interest both in the process of protecting intellectual property and in the financial benefits that its protection entails.

Earlier, this paper assessed the reasons that corporations might not share information about their own loss of trade secrets, including harm to their reputation, shareholder concerns, and diminished market valuation. However, there is an additional challenge that corporations face. The exclusive nature of trade secrets—as a means of gaining competitive advantage and thus something to be kept from competitors—makes assertions about other corporation’s intellectual property a source of potential competitive advantage. Notwithstanding the many disincentives a corporation might have for spreading spurious rumors, it remains the case that the mere hint of impropriety about a competitor—for example, that it has lost its own or is using another corporation’s trade secrets—can yield benefits.

Corporations thus face obstacles to effective information sharing. While they have the information, corporations are constrained in how they use it, and so their efforts to prevent trade-secret theft are inhibited. Consequently, they require the assistance of governments to regularize that process and prevent inequities. Government intervention to prove illegal activity, punish such activity, and deter future bad activity is essential in an effective protection regime against trade-secret theft. Yet government intervention faces its own limitations. It relies on the information that corporations make available to governments, and thus limited or incomplete sharing may restrict their ability to act. Governments also face obstacles in enforcement jurisdiction, not least because their enforcement responses are constrained by national boundaries. In fact, a country’s ability to reach across boundaries to redress bad behavior is quite limited.

The challenges that both corporations and governments face suggest that whatever model is developed to protect intellectual property must have mechanisms for transparent information sharing between governments and corporations. Moreover, to address national boundary questions, the participation of many governments on a multilateral basis becomes essential. Thus, the interactions of corporations and governments can be highly complementary so that the strengths of each compensate for the weaknesses of the other.

Put together, the different dimensions of the challenge of IP theft, particularly of the theft of trade secrets, suggest a common problem that no single actor can resolve. Yet if addressed

properly, a wide range of actors will benefit. In short, the challenge of international trade-secret theft begins to fit the description of a collective-action problem. Governments and corporations acting together can mitigate the shortcomings of each other while contributing to a robust system characterized by transparent information sharing, voluntary participation, and enforcement.

Of course, an additional dimension of the collective-action dilemma, namely the “free rider” problem, can quickly come into play. Corporations cannot be compelled to share their information, and however effective a structure is put in place, it is useless unless aggrieved corporations participate. If a corporation believes that other entities will share information about a potential bad actor and thus excuses itself from sharing that information out of concerns for its own reputation, then the corporation is benefitting from others’ actions without making its own contribution, or “free riding.” It would seem that this challenge is best addressed by rules of voluntary participation—that is, by underscoring to corporations that when information is shared about trade-secret theft, future bad behavior is more likely to be deterred. It may well be that the most effective sharing of information takes place between a corporation and its own national government, which then shares the information with other governments on a non-attribution basis.

Challenges

The foregoing discussion of the dimensions of the problem of IP theft brings up several issues that bear consideration in thinking about potential models for finding a solution. First, how should bad actors be defined? Should there be an objective set of measures—for instance, the number of criminal cases litigated against an individual or corporation, evidence of state sponsorship of theft, or evidence of cross-border targeting of technology or assets? Or should the tests be more subjective, using, for example government analysis of government-procured information? Or is a combination of the two the best approach? The means applied to judge a bad actor have important implications, not least for multinational companies, which worry that insecure supply lines could result in unknown IP theft and jeopardize the parent company. The issue of the difficulty in determining metrics points to the necessity of an information-based and voluntary enforcement solution. In any case, the challenge of defining a bad actor cannot undermine legitimate legal action by private parties and requires that safeguards be put in place to prevent abuse by competitors.

Second, with respect to multinational companies, does the nationality of corporate actors matter? If so, how is the nationality of corporate actors to be determined? In a world of major multinational corporations, globalized supply chains, and highly distributed operations, investment, sales, and profits, establishing the nationality of a corporation is a particularly difficult problem. Corporations have national loyalties, to be sure, but their entities are also fully globalized. This issue points to the need for a solution that focuses more on the activity of a company than on its nationality but that also allows for a distributed means of regulation on the basis of shared information.

A third issue concerns how information can and should be shared and disseminated. Companies are reluctant to share information on trade-secret loss with their own governments, often out of concern that the source information will be adequately protected. Governments likewise worry that information procured by technical means will be leaked, causing embarrassment. Any solution must deal with the issue of information sharing through a process that guarantees the protection of the trade secret.

Fourth, what should be done about the concern that the process of information sharing results in national governments using foreign intelligence to “tip off” their own domestic companies? Any measures for mitigating this risk must rely on standards of transparency and voluntary participation. Or put differently, if information were to be shared openly and transparently within a consortium of government entities, then all could participate in using the information.

Finally, there is the concern that a corporation might be listed as a bad actor on the basis of bad information. The approach described here does not in its incipient form address an appellate process for accused bad actors. However, a solution that requires consensus on the part of the governments that participate, and perhaps that gives the accused entity an opportunity to defend itself before being included on a watch list, would mitigate this concern.

Existing Mechanisms

Two current multilateral arrangements for discussing the protection of trade secrets and other forms of intellectual property include the U.S.-EU IPR discussions and the Japan-EU Dialogue on IPR.

The U.S.-EU IPR discussions take place in the context of the Transatlantic Economic

Council. The Transatlantic IPR Working Group (previously known as the U.S.-EU IPR Working Group) was set up in 2005 and has met periodically thereafter, usually on an annual basis. The working group hosts government-to-government talks and creates avenues for consultations with transatlantic stakeholders from both the business and NGO communities on a wide range of IPR-related issues. It addresses three main areas under the U.S.-EU IPR action strategy: “engagement on IPR issues in third countries, customs cooperation, and public-private partnerships.”¹⁰

Japan-EU discussions take place via the Japan-EU Dialogue on IPR. Similarly, Japan and the United States participate in an IPR dialogue. Both dialogues are managed for Japan by the Intellectual Property Affairs Division of the Economic Affairs Bureau of the Ministry of Foreign Affairs.¹¹

While laudable, these existing efforts appear to suffer from the same problem as trade negotiation-based efforts, namely, that they focus on harmonizing government responses but do not seem organized to specifically address and deter known bad IP actors. The foregoing discussion suggests that there might be new models that focus on deterring and punishing bad actors through a collective-action approach by governments that focuses on standards-based membership, transparency of operations, threat-focused information sharing, and voluntary national compliance and enforcement.

Policy Options

New Model for Consideration

An ideal model would welcome national governments to participate in developing a standards-based list of bad IP actors, drawing on information provided by corporations; would be characterized by transparency of operations; would employ voluntary national compliance and enforcement regimes; and would provide for the sharing of threat-focused information.

¹⁰ U.S. Department of State, “Transatlantic Economic Council: Annexes to the TEC Joint Statement,” November 29, 2011, <http://www.state.gov/p/eur/rls/or/178419.htm#ipr>.

¹¹ Ministry of Foreign Affairs (Japan), “MOFA’s Undertakings to Promote Intellectual Property Rights,” February 2011, http://www.mofa.go.jp/policy/economy/i_property/promote0810.pdf.

A model for cooperation in dealing with trade-secret theft would need to include several requirements:

- It should be led by governments, because of the shortcomings that a corporate-led effort faces with regard to conflicts of interest and inaccessibility of government information.
- It should focus on sharing information broadly—from all sources, including private and public—about known bad actors in IP protection.
- It should leave actions in response to IP theft, including enforcement, to national authorities but allow for common responses (e.g., to cease cooperating with a specific actor).
- It should include mechanisms for corporate inputs and advice, but these are best managed by function or type of company rather than by nationality, thereby somewhat reducing challenges related to competitive advantage.

Such a model presumes high trust between participating governments, anticipating that existing patterns of cooperation are already in place and further suggesting that state-to-state relationships are at least friendly, if not at the level of alliance partners.

Two Existing Models for Consideration

Use existing intelligence-sharing agreements to pass information between counterpart intelligence organizations. Available options include the Five Eyes agreement (between the United States, United Kingdom, Canada, Australia, and New Zealand) and alliance relationships (e.g., with Japan, South Korea, and NATO).¹² It is anticipated that having received information on IP theft, governments would then notify national companies so that they can make informed decisions regarding potential engagement with a bad actor. Existing protocols for sharing information within existing intelligence structures would require adjustment to allow for sharing across structures.

The advantage of this approach is that it utilizes existing high-trust information-sharing networks with proven track records. The disadvantage is that information sharing that is exclusively handled within intelligence circles suffers because it cannot be openly and

¹² Five Eyes is a top secret agreement made in 1946 between the United Kingdom and United States to share signals, or communications, intelligence. It was later extended to cover Canada, Australia, and New Zealand. The agreement allowed for sharing of the most sensitive intelligence information collected by each of the countries and contained an implicit understanding between member states not to “collect” (read “spy”) on each other. For a more detailed discussion of Five Eyes, see the National Archives (United Kingdom), <http://www.nationalarchives.gov.uk/documents/ukusa-highlights-guide.pdf>.

transparently scrutinized. Additionally, this approach does not have a mechanism for incorporating corporate inputs and is limited by its singular focus on national-level actors. This approach would have a much more difficult time developing an appellate procedure, given its reliance on government-classified information. It could also easily be construed as a U.S.-led coalition effort against other states.

Consider models for voluntary, government-led, multilateral structures that focus on accountability, transparency, and threat-based information sharing. The Wassenaar Arrangement, a successor structure to the Cold War-era Coordinating Committee for Multilateral Export Controls (COCOM), stresses transparency, information sharing, and greater incentives for national responsibility. An approach roughly patterned on this model would emphasize a collegial approach, open membership based on adherence to certain standards, a commitment to information sharing and standard setting, national implementation and action based on shared information, and international enforcement. The arrangement would work to complement existing international agreements and employ moral suasion and public accountability as tools for corrective action.¹³ In a Wassenaar-like arrangement, states would voluntarily come together on the basis on their interest in addressing the problem of trade-secret theft and not via routine alliance protocols. Information about bad actors would be shared with the group and then, on the basis of consensus, compiled into a list of “denied actors” and shared within the group. National governments and corporations alike would make their own decisions about whether or how to interact with the bad actors on the list. Governments would pursue legal and enforcement decisions, while corporations would use the information for the purposes of making business decisions. In this way, a Wassenaar-like approach is successful when companies that steal trade secrets find no place in the world where they can do business because information sharing has resulted in a common awareness of the bad actors.

¹³ To be sure, the Coordinating Committee for Multilateral Export Controls and its successor Wassenaar Arrangement were designed to prevent the transfer by states of munitions and other sensitive materials. As proposed in this paper, a voluntary agreement by member states would seek to prevent the theft of trade secrets by actors. But the principles of open and transparent information sharing and voluntary national-level enforcement appear to have application.

The advantage of a Wassenaar-like arrangement is that it would ensure transparency and high-quality information sharing from both government and private sources. The approach emphasizes voluntary participation, with membership being based on open standards, and information on corporate trade secrets is strictly protected. Such an arrangement would also militate against the perception of a U.S.-led coalition.

Conversely, although pursuing laudable information-sharing goals, a Wassenaar-like approach is not effective if corporations do not share information or if national governments fail to act in their self-interest and enact punitive actions against bad actors. The sharing of government information also potentially taints evidence that might otherwise be used in a court of law, should individual corporations later decide to pursue legal action against a foreign bad actor. Although a consensus-based decision would be required to list a bad actor, one can imagine that a Wassenaar-like approach might result in collusive activities against a corporation for competitive reasons rather than to address trade-secret theft.

Conclusion

This working paper concludes that neither self-generated defensive activities by corporations nor remedies under the WTO's TRIPS Agreement are sufficient by themselves to protect against trade-secret theft. Efforts to address such theft are faced with a collective-action problem, in which individual actors cannot fundamentally change outcomes on their own but can only bring about real change when they operate together. Recognizing this dynamic yields the potential for new ways of thinking about the problem; for when trade-secret theft is understood as more than a bilateral or multilateral trade-enforcement issue, then new approaches to finding policy solutions present themselves. This paper finds that various models of government-to-government information sharing might allow for rapid dissemination of information about trade-secret theft, but that the costs of a government information-based (or intelligence) approach might be too high.

Corporations also have a necessary and important role to play in information sharing. Multidimensional responses that emphasize standards development, consensus of decisions, transparency about operations, and voluntary participation and enforcement can be a useful complement to existing trade-related structures. It is likewise important that there are proper and

agreed-on roles for the corporate sector, government-to-government channels, and international organizations. In short, a Wassenaar-like arrangement for sharing information among all participating states about known perpetrators of IP theft shows good promise for dealing with this challenging issue.

APPENDIX

THE WASSENAAR ARRANGEMENT

The Wassenaar Arrangement (WA), the first global multilateral arrangement on export controls for conventional weapons and sensitive dual-use goods and technologies, received final approval by 33 co-founding countries in July 1996 and began operations in September 1996.

The WA was designed to *promote transparency, exchange of views and information and greater responsibility* in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations. *It complements and reinforces, without duplication, the existing regimes* for non-proliferation of weapons of mass destruction and their delivery systems, by focusing on the threats to international and regional peace and security...

The Participating States seek through their national policies to ensure that transfers of arms and dual-use goods and technologies do not contribute to the development or enhancement of military capabilities that undermine international and regional security and stability and are not diverted to support such capabilities. The Arrangement does not impede bona fide civil transactions and is *not directed against any state or group* of states.... on the *basis of national discretion*. The Wassenaar Arrangement calls for the maintenance of two control lists roughly based on the COCOM accord.

Participating states in Wassenaar: 41 [4 in the Asia-Pacific]: Argentina, *Australia*, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, *Japan*, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, *New Zealand*, Norway, Poland, Portugal, *Republic of Korea*, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom, United State.

Decisions are made by consensus.

The Arrangement is open on a global and non-discriminatory basis to prospective adherents that comply with the agreed criteria.

[Bold and italics represent author's emphasis]