Improving the Intelligence Community's Contribution to Countering Weapons of Mass Destruction

by Timothy W. Fisher

There is, of course, no such thing as a perfect weapon of mass destruction (WMD) threat assessment.[1] Some of the brightest minds in the intelligence community continuously work WMD issues. The intelligence community, consisting of seventeen organizations from six departments and one independent agency, commits millions of dollars searching for information needed by senior leadership to make the best possible decisions concerning WMD threats to the U.S. Interagency planners rely on the intelligence community's efforts to plan for a potential adversary's use of WMD. According to an analysis by the James Martin Center for Nonproliferation Studies (portrayed in Figure 1, pg. 18), the principal U.S. government agencies involved in nuclear policy making include the White House, nine executive departments and agencies, and over 150 offices within them.[2] If this analysis were expanded to include all four WMD modalities (i.e., chemical, biological, radiological, and nuclear), the number of offices involved would be considerably larger. If it were expanded to include the whole of government (i.e., state, local, and tribal organizations) involved in countering WMD, the list would be well over a 1,000 organizations.

The U. S. has spent billions of dollars on programs to prevent, prepare for, respond to, and recover from a potential WMD attack. Nevertheless, with current and projected limitations on the federal budget, spending on WMD defense programs could likely decline. Hence, the U.S. must carefully prioritize its budget in order to counter WMD. Key to this effort is an effective, integrated WMD threat assessment that includes all the potential WMD actors and modalities, portrays adversarial success for each actor and modality, and identifies critical nodes by looking for threat overlap between or among scenarios.

The concerted efforts of the interagency will be required to ensure that the policies, plans, and activities of the whole of government result in an active, layered, defense in depth to protect

U.S. Army Lieutenant Colonel Timothy W. Fisher is the Chemical, Biological, Radiological, and Nuclear Defense Division Chief for the Army Test and Evaluation Command. He has served in the Office of the Secretary of Defense and the FBI Weapons of Mass Destruction Directorate. He received a M.S. Degree in WMD Studies as a National Defense University Countering WMD Graduate Fellow.

Figure 1. Principal U.S. government agencies involved in nuclear policy

the nation from the threat of WMD. Anything short of high-fidelity integration will result in seams and boundaries between disparate and non-complementary agency plans that could be exploited by a WMD-armed adversary.

Defining WMD

At the root of any successful whole-of-government approach to assessing the WMD threat, there must exist a shared understanding of the term WMD. At present, the definition of the term WMD varies greatly depending on the source.[3] For example, the United Nations defined WMD in 1948 as chemical, biological, radiological, and nuclear weapons or future weapons with similar effects.[4] The Department of Defense defines WMD in terms of the four modalities "chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties..." excluding separable delivery systems.[5] Federal law further expands the definition of WMD by including high explosives.[6] The argument presented in the present study defines WMD as chemical, biological, radiological, and nuclear weapons and includes activities of both state and non-state actors. This delimitation has much to offer, as it includes all traditionally recognized forms of WMD and can be expanded or contracted as technological advancements might indicate without requiring the re-conceptualization of the underlying project.

Defining an "Integrated WMD Threat Assessment"

An "integrated WMD threat assessment" is an intelligence product that incorporates a broad array of information from all available sources into a single picture. It is a compilation of both known and unknown WMD information, showing all the steps necessary for an adversary's employment of WMD against the U.S. or its interests. It cannot end at the point of "known" adversary intelligence, but must continue through successful employment of a WMD. It includes open-source information, classified information, and technical information and fuses this information together to create a comprehensive understanding of the adversary's activities. It includes the people (leadership, technical experts, populations vulnerable to exploitation, and organizations necessary to employ a WMD); infrastructure (medical, industrial, research institutions, communication, transportation, storage, and financial institutions); resources (funding, materials, facilities, precursors, seed stock, process equipment, and delivery systems); and information (internet, academia, libraries, industry, and governmental resources) necessary to create a WMD event. It starts with one actor and shows how that one actor successfully implements a WMD attack. It then adds other actors until all of the actors are included that either have or could produce WMD. The compilation of these pathways will encompass a variety of activities across the globe. This integrated assessment must define what each adversary would target, what modality each is most likely to use against a specific target, and what each might hope to achieve by executing or threatening a WMD attack. Because the assessment portrays success, it does not rely solely on known information. It accounts for looking past the next step and allows those using the assessment to account for an adversary's attempts to surprise the U.S. Collectively, this broad survey of threat information provides an extensive look at the

At the root of any successful whole-of-government approach to assessing the WMD threat, there must exist a shared understanding of the term WMD.

threat that will enable the development of a properly-layered WMD defense. However, this much is clear: The integrated WMD threat assessment thus described is not possible even with the thorough integration of the intelligence community; it requires the integration of the interagency community as well.

Contrary to popular belief, WMD attacks are not easy to perform, and they are not simply random events.

Impediments to Obtaining Accurate WMD Threat Assessments

Contrary to popular belief, WMD attacks are not easy to perform, and they are not simply random events. A WMD attack or even the threat of an attack is the product of an adversary's concerted efforts to achieve specific political objectives. However, because of the near universal condemnation of WMD, it is hardly surprising that states and non-states would go to great lengths to hide their WMD-related efforts. The resulting opacity exponentially increases the magnitude of the challenges associated with producing an accurate WMD threat assessment.

Development of WMD is not the only thing proliferators try to conceal. WMD policies and employment doctrine are also ambiguous. Both doctrine and policy for employing WMD are very closely guarded secrets. Nevertheless, an integrated WMD threat assessment must account for the uncertainties arising from both the knowns and the unknowns of a leader's WMD policy and employment doctrine.

Principles for Formulating an Integrated WMD Threat Assessment

In spite of these not inconsequential challenges, most of the information needed for an integrated WMD threat assessment is already available. The intelligence community has detailed estimates that outline what it believes each WMD adversary is capable of achieving. Because WMD events are low-probability events, adversaries are not likely to attack with WMD or are likely to only attack with toxic industrial chemicals or poisons. This fact constitutes what is called in tactical and operational analyses the "most likely" adversary course of action (COA). Consideration of the "most likely" COA is where most intelligence estimates stop. However, an integrated WMD threat assessment should consider both the "most likely" and the "most dangerous" WMD scenarios—which are not by any means necessarily the same thing. If the integrated WMD threat assessment only shows what is likely to happen, then it will continue to show WMD as very unlikely because that is the most probable scenario. Of course, this is not to suggest that a litany of "the sky is falling" scenarios will serve the national interest. The task is to portray the most dangerous adversary COA without either overinflating or dismissing out of hand the associated WMD risks.

One possible approach would be for interagency players to focus on preventing surprise instead of merely predicting the adversary's most likely activities. Focusing on preventing surprise has the added advantage of accounting for the uncertainty inherent in an adversary's WMD activities, as well as the uncertainty in understanding leadership policy and doctrine for employing WMD. To be useful as a tool for preventing surprise, an integrated WMD threat assessment must look at a broad array of potential actors and WMD modalities.

The easiest method of accounting for incomplete WMD intelligence and unclear understanding of an adversary's WMD policies and doctrine is to template an adversary's success in as many different scenarios as possible. An interagency effort must anticipate

an adversary's success to prevent a surprise WMD event. On this account, one is reminded of the conclusions from the 9-11 Commission. The 9-11 Commission's report stated that one of the biggest mistakes of the intelligence community was a "failure of imagination and a mindset that dismissed possibilities."[7] The model that focuses on both the "most likely" and the "most dangerous" courses of adversary action—a staple for tactical military planning—provides a model for the formation of an integrated WMD threat assessment across the interagency. Often, as interagency organizations build their plans, they spend too much time and lose perspective by fixating on questions of which modality is the most dangerous and which actors are the most capable. What is needed is an integrated WMD threat assessment that accounts for the most likely and most dangerous adversary COAs, regardless of how successful those COAs are assessed to be.

A Practical Approach to Interagency WMD Planning

According to open-source information published by Pro-Con, 21 countries (not counting the U.S.) have known or suspected WMD programs.[8] Figure 2, page 22, is based on the Pro-Con analysis of state WMD programs.

There are 13 known WMD programs in 10 countries, including the eight declared nuclear weapon states and three states that are continuing to destroy their declared chemical weapon stockpiles. The remaining 25 programs in 19 countries are only suspected WMD programs, which illustrates that most countries believed to be pursuing WMD try to keep these programs secret. Thus, not counting U.S. programs, there are 21 countries with 36 known or suspected WMD programs. However, this is only part of the threat.

An integrated WMD threat assessment must account for both state and non-state actors. In 2013, the Director of National Intelligence listed eight terrorist organizations as significant concerns to the U.S. and its interests:

1. Al Qaida in the Arabian Peninsula
2. Al Qaida-inspired home grown violent extremists
3. Core Al Qaida
4. Al Qaida Iraq
5. Al-Shabaab
6. Al-Qa'ida in the Land of the Islamic Maghreb
7. Lashkar-e-Tayibba
8. Hezbollah[10]

There are 13 known WMD programs in 10 countries, including the eight declared nuclear weapon states...

However, the Director of National Intelligence did not list any of these groups as specific WMD concerns—and this in spite of the fact that, in 1998, Osama bin Laden asserted that it was his duty to acquire and employ WMD.[11] It is not definitively known whether the other seven terrorist groups have aggressive WMD programs. Considering the level of effort terrorist groups could go to keep WMD programs secret, it is possible that any of these groups could aspire for, develop, or even employ WMD capabilities without detection by the U.S. and its allies' intelligence organizations. This threat can be expected to continue to increase in the future as chemical and biological technology continues to spread around the globe. This means, all things considered, that all eight terrorist organizations should be accounted for in an integrated WMD

Weapons of Mass Destruction Programs			
	Nuclear	**Biological**	**Chemical**
Known Programs	9	0	4
Known Countries	China France India Israel North Korea Pakistan Russia U.K. U.S.		North Korea (Syria)[1] (U.S.)[2] (Russia)[3]
Suspected Programs	1	8	16
Suspected Countries	Iran	Algeria China Egypt Iran Israel North Korea Russia Syria	Algeria China Egypt India Indonesia Iran Israel Kazakhstan Myanmar Pakistan Saudi Arabia South Africa South Korea Sudan Taiwan Vietnam

[1] Syria's *declared* stockpile has been destroyed. However, reports persist that regime forces continue to employ chlorine gas in contravention of Chemical Weapons Convention obligations.

[2] The U.S. stockpile is currently being eliminated in accordance with obligations under the Chemical Weapons Convention.

[3] The Russian stockpile is currently being eliminated in accordance with obligations under the Chemical Weapons Convention.

Figure 2. Weapons of Mass Destruction Programs[9]

threat assessment.

Based on the definition of WMD presented above, all four of the modalities—chemical, biological, radiological, and nuclear—could be exploited by terrorists. Therefore, the integrated WMD threat assessment must include 24 programs and eight terrorist organizations. Nuclear weapons are a special case. It is acknowledged that most terrorist organizations lack the resources to build a nuclear weapon, and that any nation with a nuclear weapon would be reluctant to share it with terrorists. However, as President Obama has stated, violent extremists with nuclear weapons are among the Nation's greatest threats.[12] Additionally, any intelligence in this area is highly classified. For present purposes, therefore, the intelligence community should assume the most dangerous case and include for all four modalities to illustrate the terrorist WMD threat. Therefore, the new total is 29 WMD actors with 68 potential WMD programs.

The WMD "battlespace" encompasses the entire globe, and WMD proliferators may be expected to seek to develop intricate and obscure proliferation networks in order to avoid detection.

After accounting for the truly global dimension of the WMD battlespace, the next step is to formulate the integrated threat assessment itself. Consider the 29 actors and 68 WMD programs. In order to achieve success, each of these adversaries must accomplish the following six essential tasks for each of the programs:

1. Decide to pursue WMD to achieve desired goals.
2. Develop policy to achieve goals.
3. Select modality or modalities (biological, chemical, radiological, or nuclear).
4. Acquire WMD (purchase, build, or steal).
5. Threaten employment and/or actual employ WMD.
6. Exploit the threat or actual employment of WMD to achieve desired goals.

...all four of the modalities—chemical, biological, radiological, and nuclear—could be exploited by terrorists.

Preparing a complete assessment of the most likely and most dangerous courses of action for each of the 68 WMD programs results in 136 scenarios. Development of 136 detailed scenarios that include all six steps results in a spider web of activities around the entire globe. Again, the primary reason for completing this many permutations is not because any single scenario is likely to occur, but because only by considering the totality of the problem can interagency planners identify critical nodes and develop an integrated plan of multiple layers of defense. Planners can then identify those points where different scenarios overlap, achieving important synergies of effort.

Next, consider the conventional wisdom that "good guys" have to be right 100 percent of the time, but the "bad guys" have to be right only one time to achieve a successful attack. This theory appropriately applies to a single-layered defense. With only one layer in a defensive plan, the "good guys" do have to be correct 100 percent of the time. However, given the scenario in which there are multiple layers of defense, this is not true. For example, if there are 10 layers in the layered defense and each is only 80 percent likely to successfully prevent an adversary's success, the cumulative chance of success for the entire operation plummets to less than one chance in 10 million. If each

layer was improved to 90 percent success, then the adversary's chances of success are reduced to about one chance in 10 billion. This illustrates two important points: (1) the strategy of a layered defense is essential, and (2) in an environment where a single layer of defense is less than 100 percent successful, an integrated approach that employs overlapping interagency defensive layers will strengthen the less than perfect defense layer within a single agency. This approach will allow each layer to perform at its maximum potential.

The U.S. does not need an impenetrable WMD defense. The U.S. needs enough good layers of defense integrated across the interagency communities to reduce the chances of an adversary's success to negligible levels.

The U.S. does not need an impenetrable WMD defense. The U.S. needs enough good layers of defense integrated across the interagency communities to reduce the chances of an adversary's success to negligible levels.[13] The task of the integrated WMD threat assessment, therefore, would be to consider not only the WMD threat writ large, but also the threats that would impinge upon the success of each defensive layer. For example, each time the adversary is able to completely circumvent a single layer, chances of success steadily improve. Similarly, if an adversary determines his chances are only one in a billion, he may adopt a strategy of flooding the field with millions of inexpensive attempts to penetrate the defense. This is similar to the typical lottery held in many states today. The chance that any single person will win the lottery is one chance in a billion. Nevertheless, the credibility of the lottery hinges on the proposition that someone will eventually win the jackpot.

By taking a layered-defense approach that is coordinated across agencies, potential vulnerabilities become less vulnerable due to defensive checks and balances, enabling success where it may have been threatened in the absence of a layered-defense approach. Consider the U.S. investment in radiological detection. Today, funding provides coverage of all of the most likely routes into the country. By taking a layered-defense approach, providing coverage of 100 percent of the border becomes unnecessary. Likewise, efforts to produce the perfect solution in other areas are not necessary. Using the best technology available today at the critical nodes can achieve more success than the never-ending pursuit of a single, perfect, or comprehensive solution. Rather, an integrated WMD threat assessment that truly accounts for both the most likely and most dangerous COAs will favor adding more defensive layers—and adding them more intelligently—from multiple agencies at critical nodes instead of a perfect solution from a single agency or allied nation. Indeed, the approach advocated here is similar to massing combat power at obstacles in order to achieve success. It emphasizes the comprehensive inclusion of all available tools—technical detection, human intelligence collection, all source analysis, law enforcement, non-proliferation regimes, and other methods of massing counter WMD capabilities at the critical nodes—instead of millions (or billions) of dollars on a single perfect detector that might never meet its desired objective.

Creation of an integrated WMD threat assessment provides one additional advantage to the U.S. government. It provides a useful yardstick for measuring the effectiveness of the "active, layered, defense in depth" called for in the WMD strategy.[14] It empowers each agency and department to act within its own

resources and authority while simultaneously illuminating scenarios and critical nodes where improvements can be made, which provides the President and Congress with the ability to see how competing programs within the federal government address specific threats. It also helps identify unnecessary duplication of effort. It avoids trying to determine which adversary actor will succeed first with which of the different modalities, which makes the measure of effectiveness how many scenarios and critical nodes are addressed by agencies and departments across the interagency.

An integrated threat assessment shows how each adversary is most likely to succeed in completing its WMD program, selecting a target, employing the weapon, and exploiting the results of the attack or threat. Because the devil is in the details, this model must be as detailed as possible. If states or terrorists have access to certain materials, facilities, or experts, the integrated WMD threat assessment must include the portions in the template that are known, suspected, and unknown. It must include the entire chain of events from considering the pursuit of WMD, through exploitation of a WMD threat or event. It must be done for all 68 WMD programs and 28 actors with WMD aspirations. Note that this has to be done in spite of the fact that U.S. intelligence is limited and it is ultimately impossible to know with certitude what an adversary's next step will be. This level of detail is important because every situation is different. Fleshing out each potential adversary's different paths will allow the interagency to build a global template of potential paths for WMD. This global template will help account for the fact that the data input to the integrated WMD threat assessment may be either incomplete or inaccurate or both. This template will allow the U.S. to plan for situations for which it may not have all the answers and can only postulate additional WMD-event locations. Only by planning for an adversary's success without perfect intelligence can the U.S. build an adequate defense that is layered across the spectrum of potential adversarial actions.

The next issue is how to build a layered and integrated WMD defensive plan that addresses 136 scenarios. On the surface, this may seem like an almost insurmountable task. However, the solution is to use the 136 scenarios to identify critical nodes. Critical nodes are the points where the 136 scenarios cross paths. A critical node could be, for example, crossing the physical boarder of the U.S. with WMD components or weapons, gaining access to the precursors or seed stock necessary for building chemical or biological weapons, or recruiting technical experts from universities with vulnerable student populations. When considering the activities of 29 actors with a potential of 68 programs, critical nodes can be identified as the spots on the integrated WMD threat assessment where multiple scenarios cross the same point. The more threat scenarios that cross the same point, the more important the critical node becomes. Identifying critical nodes provide a prioritized list of the most important locations for implementing the layered defense. Careful analysis of these critical nodes is important because once the intelligence community correctly identifies these nodes, the entire interagency can—and must—use the same integrated threat assessment to build a layered U.S. defensive plan, which will allow planners to create a layered defense that looks

An integrated threat assessment shows how each adversary is most likely to succeed in completing its WMD program, selecting a target, employing the weapon, and exploiting the results of the attack or threat.

at the entire spectrum of threat activities instead of simply funding the next new idea. Only when the entire interagency uses the same integrated threat assessment can it prevent the exploitation of seams.

Of course, there always exists the potential for a "wild card"—that a country with a known WMD program could simply give a WMD capability to a terrorist organization with instructions to employ the weapon against the U.S. or its interests. To prevent this type of surprise, the intelligence community should supplement the 136 scenarios with additional analysis to show how the most likely proliferation countries might give WMD to specific WMD actors and what guidance these proliferators might give to the actors to achieve mutual goals. Because this is likely to occur where goals overlap, the 136 scenarios already created probably cover these potential activities. For example, if country A chose to give WMD to terrorist B, the most likely targets would be within terrorist B's current operational range and would target locations where terrorist B and country A's interests overlap. The main difference with a "wild card" scenario is the speed with which it could present itself. Therefore, scenarios where terrorist's and WMD state's objectives overlap must include an alternative accelerated timeline in order to account for the "wild card" scenario.

At every turn, planners must not fixate on the integrated WMD threat assessment to the point that it generates "group think." Indeed, there is a danger that analysts could create critical nodes by simply applying the same template to multiple organizations. For instance, recent reports of Ebola outbreaks in Africa could potentially be exploited by every actor seeking a biological weapon capability. In reality, only organizations close to an outbreak with appropriate technical expertise and potential access to research facilities are likely to succeed. For these and many other reasons, each integrated WMD threat assessment must look for the most likely and most dangerous COAs for each individual state and non-state actor as the threat pertains to the U.S. This approach avoids the argument of only addressing one agency's favorite threat or modality. By the same token, the approach suggested herein enables each element of the U.S. interagency to tackle the problem within the context of each agency's respective areas of responsibility and resources.

Conclusion

Because the potential impact of an adversary's use of WMD is so great, the issues are so complex, and so many organizations are involved in the effort, there are no simple solutions. The challenge is compounded by the fact that terrorists and nation states pursuing WMD go to great lengths to hide their efforts. Competing budget priorities, compartmented intelligence information, and concern over encroachments upon civil liberties further complicate the problem.

This much is clear: the U.S. needs a more comprehensive integrated WMD threat assessment in order to account for the uncertainty inherent in tracking adversary efforts to acquire, threaten, or employ WMD. In order to prevent surprise, the intelligence community must prepare a common set of threat scenarios for interagency planners to prepare integrated and layered defenses at critical nodes. Critical nodes are identified by looking at an extensive list of threat scenarios and identifying the locations where multiple scenarios overlap. This method will help to empower interagency planners and enable them to develop an "active, layered, defense in depth."[15] Each agency can analyze its investment strategy to identify the investment level that provides the most capability at critical nodes. It will also enable each agency to avoid the negative effects of diminishing returns on investments focused on achieving a perfect solution at any single node. Only by accepting a common integrated threat assessment can the interagency build multiple, layered defenses without

visible seams that WMD-enabled adversaries can exploit.

The creation of a template with 136 different WMD scenarios is not intended to portray the threat as a high-probability event. It is only intended to provide enough scenarios to allow sufficient planning to prevent surprise. However, in the high-stakes enterprise of counter-WMD planning, avoiding surprise is the single most important key to success. ***IAJ***

NOTES

1 The views expressed herein are those of the author and do not necessarily reflect the official views of the U.S. government or any of its entities.

2 James Martin Center for Nonproliferation Studies, "Principal US Government Agencies Combating Nuclear Proliferation," 2009, <http://cns.miis.edu/stories/090213_wmd _coordinator.htm>, accessed on June 24, 2014, used with permission.

3 W. Seth Carus, "Defining 'Weapons of Mass Destruction,'" Center for the Study of Weapons of Mass Destruction, Occasional Paper #8, revised and updated, National Defense University Press, Washington, January 2012.

4 Ibid.

5 Department of Defense, *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, November 8, 2010, as amended through January 15, 2014, <http://www .dtic.mil/doctrine/dod_dictionary/>, accessed on January 31, 2014.

6 Federal Bureau of Investigation, <http://www.fbi.gov/about-us/investigate /terrorism /wmd/wmd_faqs>, accessed on February 5, 2014.

7 Thomas H Kean (Chair) and Lee W. Hamilton (Vice Chair), "The 9/11 Commission Report," July 22, 2007, p. 336.

8 Based on ProCon.Org, "26 Countries' WMD Programs; A Global History of WMD Use," used with permission, <http://usiraq.procon.org/view.resource.php?resourceID=000678>, accessed on March 23, 2014.

9 Ibid.

10 J. R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," statement for the record, Senate Select Committee on Intelligence, March 12, 2013.

11 Rolf Mowatt-Larsen, "Al Qaeda Weapons of Mass Destruction Threat: Hype or Reality?" 2010, <http://belfercenter.ksg.harvard.edu/publication/19852/al_qaeda_weapons _of_mass_destruction_threat.html>, accessed on February 17, 2014.

12 The White House, National Security Strategy, 2010.

13 This section was inspired by a similar discussion presented by Michael Levi, *On Nuclear Terrorism,* Harvard University Press, Cambridge, MA, May 2009.

14 Department of Defense, "National Military Strategy to Combat Weapons of Mass Destruction," 2006.

15 Ibid.