







## 6.1 DISCUSSION GROUP INSIGHTS AND RECOMMENDATIONS

Edward A. Smyth

The panelists on the Countering Common Adversary Weapons Roundtable were Dr. Richard White of the Institute for Defense Analyses; Dr. Eric I. Thorsos of the Applied Physics Laboratory, University of Washington; Mr. Andrew Green of Hazard Management Solutions; and Dr. Stephen McBrien of The MITRE Corporation. Each panelist presented a short briefing to the Symposium.

The participants were tasked to identify and examine three primary issues:

- What are the common adversary weapons to be addressed in 2006 and in the near term (5–8 years in the future)?
- From a technology perspective, where is the United States in terms of our ability to counter these weapons?
- What are the most important challenges, technological and otherwise, in the years ahead?

In addressing these issues, it is important to consider the full range of the elements that comprise the term, unrestricted warfare, as defined by Liang and Xiangsui in their recent book [1]. Clearly, if unrestricted warfare is construed to encompass such diverse areas of conflict as cultural, drug, economic aid, environmental,

---

---

*Colonel Edward (Ted) Smyth, USMC (Ret.) heads the Joint Effects Based Operations Group at The Johns Hopkins University Applied Physics Laboratory. Mr. Smyth has taught quantitative methods, operations research, and systems engineering at many universities, including The University of Virginia, U.S. Naval Academy, The George Washington University, University of Maryland, and The Johns Hopkins University.*

---

---

financial, international law, media, network, psychological, resource, smuggling, technological, and terrorism, then the challenges facing the technology community in countering such a wide array of weapons' choices are immense.

The scale of this challenge is further evidenced by several insights provided by the Symposium's Keynote Speaker, Anthony Zinni. In Zinni's view, the demise of the former Soviet Union has been a spur to globalization, which, in turn, has enabled both potential friends and foes to gain access to the most sophisticated technologies. According to Zinni, this problem is further complicated by the lack of a national strategic vision to counter the threats of today and tomorrow. The challenges faced by the technology community in developing appropriate countermeasures result from the combination of these two factors. A subsequent Symposium speaker, T. X. Hammes, added yet another level of complexity to this problem by challenging the technology community to anticipate future adversary weapons before they actually appear.

---

*"... technology in and of itself will not be sufficient to defeat the movement. Advances in ... strategy and analysis—are essential."*

---

Where then does the technology community begin to address such an immense challenge? The Roundtable panelists began by assessing perhaps the most significant common adversary weapon in use today, the Improvised Explosive Device (IED) and some of its common derivatives. According to data available as of 7 March 2006, since March 2003, more than 40% of the U.S. hostile action fatalities—more than 700 hundred deaths—in the Iraqi theater of operations can be attributed to IEDs. Although data on the number of U.S. wounded attributable to IEDs is not readily available, it is presumed that a similar percentage could be reasonably applied to the nearly 17,000 wounded in action [2]. Such statistics provide ample rationale for the Roundtable's focus on weapons of terror and IEDs in particular.

The panelists agreed that IEDs are clearly weapon systems that warrant immediate attention. They are extremely inexpensive and easy to develop and use. In comparison to major U.S. weapons systems, IEDs can be developed, modified, produced, and employed in days rather than years and at a tiny fraction of the cost of more sophisticated weapon systems. In the hands of Iraqi terrorists, IEDs serve not only to inflict human casualties but to instill fear, shape media coverage and public opinion, and separate U.S. forces from the local population.

---

*“If we are to prove successful in meeting the challenges of unrestricted warfare, the analysis community must develop tools and processes that address more than just physical phenomena. The full range of societal, informational, cultural, and military interactions must be incorporated into future analytical developmental efforts.”*

---

IEDs exist in many forms and variations. They may be timed devices, using either mechanical or electrical timers, or command-detonated weapons that are initiated when a suitable target comes within range. In Iraq, the IED is most commonly used as a roadside bomb, initiated with some form of electronically controlled device. It was noted, however, that IEDs are complex weapons systems that employ simple technology. The IED weapon system consists of not only the device itself but also a fairly sophisticated support infrastructure that provides for identifying suitable targets and target vulnerabilities, producing the device, emplacing the device, and providing requisite command and control for detonation.

In Iraq, other adversary weapons that are frequently encountered include suicide bombs and rocket-propelled grenades (RPGs). Like IEDs, suicide bombs exist in several forms, most notably, vehicle bombs, suicide belts, and briefcase bombs. All are relatively inexpensive to construct and use and difficult to detect. RPGs also pose a serious threat because with minimal training, they can be effectively used by an individual against vehicular targets. Recent events indicate that RPGs are becoming

progressively more lethal and must be considered as threats even against armored vehicles.

## CHALLENGES

The Roundtable panelists stated that while developing the means to defeat the weapons and devices themselves is of the utmost priority, such countermeasures cannot be addressed in isolation. Countermeasures must also consider:

- Defeating the device
- Defeating the system
- Defeating the insurgency
- Defeating the movement

In defeating the device and the system, the panelists suggested the need for technology to swiftly and accurately detect bomb factories. Specifically, technology should be developed to provide wide-area coverage for trace detection of explosive chemicals and for efficient monitoring of waste streams such as garbage and sewage. In addition, technology is needed to locate the IED man-in-the-loop and to detect and track large-scale truck bombs. Given the widespread use of roadside IEDs, sensors are needed that can detect changes and disturbances in road and ground surfaces and ground penetration at standoff distances.

Also needed is technology to detect subtle changes in the behavior of the local population that could indicate an imminent major threat weapon event. Some means also should be provided that would allow members of the local population to safely and clandestinely report imminent threat activities. It was further suggested that the United States and its Allies need an intelligence coup similar to that experienced in World War II, when the Allies intercepted and broke the Axis code system. As was the case in World War II, the United States should strive to maintain secrecy about any and all intelligence gains or breakthroughs.

It was noted that technology in and of itself will not be sufficient to defeat the movement. Advances in the other two components of the Symposium triad—strategy and analysis—are essential. It is

also important for the United States to improve its understanding and appreciation of the systemic relationships of the complex 21<sup>st</sup>-century world. We must understand the operational context of this world, including the relationships among its physical, societal, and informational attributes, as well as our own capabilities and vulnerabilities.

## **ADDITIONAL INSIGHTS**

Comments by the participants in the Discussion Group both reinforced the insights offered by the Roundtable panelists and provided their own unique perspective. The group recognized that most of the previously addressed common adversary weapons have multiple purposes and effects. Specifically, these weapons were recognized as primary elements of a larger, terrorist-directed information operation. These weapons have also successfully separated U.S. military forces from the local population, modified U.S. military behavior, and have been partially successful in fomenting civil war.

The participants felt that IEDs, in particular, will remain a significant threat weapon of choice until the Coalition develops successful technological countermeasures. While recognizing the acute need to develop and successfully use such countermeasures, the participants also placed a high priority on developing the means to remedy the economic, societal, and cultural ills of the population that create support for the use of such weapons.

## **SUGGESTED ACTIONS FOR STRATEGY**

The participants agreed that it is essential for the United States to fully understand the cultural, religious, economic, societal, and military motivations of the factions using IEDs. Only then will we be able to take positive steps to effectively separate the insurgents from the population, generate local populace support for both Iraqi and American security forces, overcome past differences, establish a necessary level of mutual trust, and successfully counter IED-type weapons.

The Discussion Group also suggested that U.S. efforts to counter IEDs would be best served by restricting the publication of

revised tactics and countermeasures. A policy such as that recently imposed by the Department of Defense to curtail the distribution of information on counter-IED efforts was considered overdue.

Strategists need to take a much broader view of unrestricted warfare. Although the Discussion Group clearly appreciated why the ongoing conflicts in Southwest Asia received so much attention during the Symposium, strategists were urged to broaden their scope. They should focus not just on the “here and now” of the Arab/Islamic cultures but should consider other potential threats, other cultures, and unrestricted warfare elements other than terrorism. Similarly, the participants believe that the United States must adopt a broader perspective on how we consider and respond to conflicts. All too often, the U.S. response has been dependent on military action and the use of sophisticated military technology. Recent experience indicates that successful conflict resolution may require a different approach.

## **SUGGESTED ACTIONS FOR ANALYSIS**

As for the analysis community, the Discussion Group believes that our current analytical capabilities remain wedded to a conventional attrition-based set of values. If we are to prove successful in meeting the challenges of unrestricted warfare, the analysis community must develop tools and processes that address more than just physical phenomena. The full range of societal, informational, cultural, and military interactions must be incorporated into future analytical developmental efforts. Specific attention should be focused on developing and achieving consensus on metrics that incorporate these types of factors and that will effectively discriminate between operational and technical options.

The Discussion Group also recommended that the analysis community do a better job of collaborating with key activities in related areas. For example, ongoing research in Tagging, Tracking, Identifying, and Locating (TTIL) capabilities are highly relevant and should be routinely shared with other efforts, such as those involved in IED defeat issues.

## SUGGESTED ACTIONS FOR TECHNOLOGY

On the technology side, the Discussion Group participants endorsed the needs voiced earlier by the Roundtable members. Technology to swiftly and accurately detect bomb factories is an urgent requirement. It should be capable of providing wide-area surveillance coverage using trace detection of explosive chemicals and efficient monitoring of waste streams. In addition, there is a recognized need to develop technology to locate the IED man-in-the-loop in both complex urban environments and in less populated areas. Identifying means to detect and track large-scale truck bombs is also a significant and important challenge. Given the urgency of countering roadside IEDs, there is also a need for technology to detect changes and disturbances in road and ground surfaces and ground penetration at standoff distances.

The Discussion Group also endorsed the need to detect subtle changes in the behavior of the local population that could indicate an imminent major threat weapon event. In addition, members of the local population should have a means for safe, clandestine reporting of imminent threat activities.

## SUMMARY

Both the Roundtable panelists and the Discussion Group participants agreed that the Unrestricted Warfare Symposium was a unique and successful initial effort to explore the challenges of unrestricted warfare from the strategic, analytical, and technological perspectives. It was suggested that future symposia of this type consider expanding the discussion beyond the ongoing hostilities in Southwest Asia to address elements of unrestricted warfare beyond terrorism. If appropriate, future symposia should be classified to enable a broader range of discussion.

## REFERENCES

1. Col. Q. Liang and Col. W. Xiangsui, *Unrestricted Warfare*, Panama City, FL, 2002.
2. "Iraq Index, March 7, 2006," The Brookings Institution, [www.brookings.edu/iraqindex](http://www.brookings.edu/iraqindex).



## 6.2 QUESTIONS AND ANSWERS HIGHLIGHTS

### Transcripts



**Q:** *Grant Hammond, Center for Strategy and Technology at the Air War College – This is a comment, and then I would like whoever on the panel might like to pick it up to have a run at it. As we have discussed this problem of unrestricted warfare the last couple of days, it has been clear that the solution may not be a technological solution, and the moral dimension and human aspects of combating insurgency are obviously critical.*

*That said, the technological aspects of this long war will become greatly complicated over the next few years. It may not be fourth-generation warfare; it may be fifth-generation warfare in which insurgents have access to high tech. The research, technologies, and available capabilities such as directed energy, biotechnology, and nanotechnology, are increasingly civilian designed, commercially available, globally distributed, and outside the purview of governments or the military. The issue of available technology is no longer limited to militarily critical technologies. In an Internet-connected, globalized world you can access much of this technology with a laptop and a credit card—and you can steal both of those. I think we will look back on this era as a relatively simple, low tech one.*

*Is anybody tracking, assessing, or worrying about this much more difficult circumstance in a relatively near-term future in a so-called long war? If we are dealing with unrestricted warfare, I would like to suggest that unrestricted thinking, particularly along these lines, might be in order? Thank you.*


**Mr. Ted Smyth** – I am not sure whether I want to thank you or not with that question. Obviously, we have a challenge. Does anyone on the panel care to offer a comment or two?

The question seems to be this: Is anyone tracking the availability of technologies that could potentially be used against us? I think the answer is yes, probably more than we care to think about. Many analysts worry about the proliferation of all kinds of technologies generated in the civilian community that would be available to potential opponents, and even more are concerned that the civilian community is able to generate ideas and capabilities much faster than DoD can.

It is not a very cheerful thought that it may take us 15 years to develop a system that can combat an alternate system that will be developed and discarded in three weeks. I think wise heads would have to judge whether or not the U.S. military or any military is anxious to incorporate civilian technologies in ways that would allow it to be protected and at the same time used for military operations.

Let me also follow that up in a somewhat related but a somewhat different way. I would hope that someone is tracking these types of challenges. However, I was struck last night by the comments of Steve Flynn, who opened my eyes to the fact that many of the events since 9/11 that we had all assumed were being taken care of—it is not necessarily the case that they are.

I am also recalling the comments of our keynote speaker, General Anthony Zinni, who was frankly lamenting the fact that we do not necessarily have a national strategic vision. When I use the term “national” I am not suggesting just simply a DoD-supported effort, but the entire fabric of the U.S. government as well as the industrial sector itself tracking these issues, thinking about these issues, and hopefully making some progress against some of these issues—and not only today’s concern, IEDs. I can only fanaticize about what our next major weapon du jour might be and what we need to do now to start countering that possibility.

 **Dr. Eric Thorsos** – I couldn’t agree more with the final speaker here—Steve McBrien—that we are not helping ourselves by discussing openly all the things that people are considering and developing. DoD has a huge program underway devoted to trying to counter IEDs, and they probably are addressing many of the

concerns you were raising. It is not a kind of question that is easy to discuss in an open forum.

**Q:** *When I looked at the television coverage of the London bombings, I was impressed by the level of camera or video coverage of much of the city of London. When commentators and news organizations discussed it, they said a similar video monitoring capability in that level of detail existed in the Washington, DC, metro system. How could that video monitoring capability be used to help us in a situation in Baghdad or along those routes that we are traveling all the time with our troops in the field?*

**Mr. Andrew Green** – I will make two points in response to that question, if I may. Clearly, in the case of the London bombings, the pictures from those cameras have only been useful in terms of the prosecution of the case after the event. Sadly, they did not prevent the events taking place in the first place. I think that is the first point to be aware of when we are talking about that use of cameras. Second, you are absolutely right that the application of that sort of technology—not only fixed cameras but cameras mounted on a variety of platforms—clearly is one of the tools that is invaluable in prosecuting this war.

**Q:** *John Leonardis from Northrop Grumman Corporation – Mine is I think a pragmatic question, and I appreciate that we cannot really go into detail in a public forum. I have seen proposals for techniques in jamming or detection in which the asset would be way too expensive to have any merit. Given the constraint that counter-IED solutions have to be cheap, is there a possibility of having a predetonation of these devices? Has thought been given to a standoff procedure of clearing an area and inducing a detonation, that is, treating them basically as landmines?*

**Mr. Andrew Green** – To answer your question directly: yes, it can be done. Whether that is always going to be the best way of dealing with these things is another matter. Someone earlier touched on the point that not only would such a device take out the intended target, it would also cause collateral damage. The political ramifications associated with knowingly initiating devices irrespective of who put them there in the first place is a serious point that would need to be considered.

It would not be the terrorist that is causing that device to function; it would be the government or the coalition forces that was causing it to function. What that does not address is actually detecting them in the first place. To be able to apply some form of predetonation technology, you have to know where they are to apply that technology.

If you are just sweeping an area just to induce detonation, obviously there will be a risk of collateral damage, but that would occur anyway if the device were exploded. By using some of the technologies you are talking about, you are going to be causing not only physical collateral damage, but also fratricide to communications equipment, computers, you name it—everything within that area is also going to be fried at the same time. I suspect that you can assume that any easily described approach as you have described is being investigated because the program is large. My involvement is more toward the long range, and all of these types of things have been considered. Without being particularly privy to the short term, I think the scope of the program suggests that these are being investigated.