

5 Understanding Impact Scalability, the Dynamic of Reciprocal Threat Perception and their Strategic Implications: The Case for an Actor-Centered Approach to Terrorism Research

I want to close this essay with a few thoughts on the manner in which we conduct research on, and how it affects our perception of, PVMs and terrorism. In an era of possible, even probable, deployment of ABC weapons, the impact of which is in some manner controllable and at the disposal of sub-state actors with known terrorist track records, a stringent appraisal of such PVMs that are potential perpetrators of conventional and, especially, unconventional mass casualty attacks, is vital. Arguably, it constitutes a *sine qua non*.

The urgency of the problem in the near future may increase dramatically, because of the very likely development of the Revolution in Military Affairs (RMA) with respect to dirigible and spatially limitable delivery systems for non-atomic weapons of mass destruction. If we consider strategic scenarios for contemporary states' foreign and security policy, one possibility that cannot escape the detachedly paranoid imagination of the defense analyst is that of the sub-state actor armed with WMD provoking an international crisis by taking the offensive against a state with a scaled, surgical attack with unconventional WMD possibly on behalf, and with the clandestine support, of another state. The likely consequence of such an event is a minor to major destabilization or even disruption of the global strategic security environment.

The potential capability of PVMs to calibrate the impact of an A, B or C attack exacerbates this situation: It would mean that perpetrators of future terrorist acts could scale an attack to their utmost advantage in a precisely calculated way in order to provoke

desired responses from states, to cow governments and to surgically stimulate, aggravate and exploit panic among the population.⁶⁰ The impact scalability of unconventional weapons further refined by the RMA in the field of delivery systems, once their proliferation had begun, would put a powerful “surgical” weapon in reach of PVMs around the globe that is readily translatable into considerable political capital and military leverage. For the stricture and disadvantage to PVMs of indiscriminate destruction caused by ABC weapons systems of the Cold War era would in such a case no longer apply in the way of a self-deterrent. PVMs that could even in a limited way influence the dynamic of reciprocal threat perception to their end – both public fears and the disposition of their members to deploy ABC weapons – through the credible employment of impact scalability, would be in a position to dictate their terms to any government in the world.

The threat emanating from PVMs willing to use WMD is probably even greater now and is, of course, not exclusively subject to influence by the RMA and technology. For today, the disciplining force of the bipolar system, the oppressive awareness, and the brooding reality, of nuclear holocaust lurking around the corner, the “red telephone”-fail-safe mechanisms established following the Cuban missile crisis in the Cold War, are no more. Due to the weight currently attached to the threat scenario in private, public and government circles of sub-state actors seeking to acquire ABC weapons, the actual threat itself may well become a self-fulfilling prophecy according to the dictates of the dynamic of reciprocal threat perception: The more we achieve or manufacture consensus

60 I have excepted radiological dispersion devices from the list because they are weapons of mass disruption rather than weapons of mass destruction and cannot be surgically applied by definition. This is not to suggest that they could not be instrumentalized at all in such a scenario: Their value to the perpetrators could be that of a positively scaled impact. Cf. Michael A. Levi and Henry C. Kelly, “Weapons of Mass Disruption,” *Scientific American*, (November 2002), pp. 59–63.

on being afraid of PVMs possibly deploying WMD – discriminately or indiscriminately – and the more we discuss and disseminate knowledge about this issue in the public domain and the corridors of power, the more we become accessories in the creation of a multilaterally perceived “merit” of the psychological potential of a weapon that can panic entire populations and hold to ransom governments; the more attractive we make the ABC option for terrorists; and the more likely the prospect of an PVM attack involving WMD becomes.

Therefore, an analysis of which PVMs are noted for their predilection toward the use of unconventional weapons, and which are less inclined to use them, is a prerequisite for the establishment of priorities in the combating of terrorism and must serve as a road map for future policy making in the area of national and multilateral counter-terrorism programs. Evidently, if we wish to pinpoint potential perpetrators of terrorist attacks involving ABC weapons, there is no way around actor-centered analysis. This is especially relevant if we accept that the kind of intelligence and threat analysis that helps establish the identity of potential WMD terrorist perpetrators in the present is also critical to the overall effort of thwarting unconventional mass casualty attack in the future.⁶¹

Conversely, generalizing the terrorist threat by abstracting it or quantifying data on PVMs, invites the likelihood of an exponential

61 Jean Pascal Zanders, “Assessing the Risk of Chemical and Biological Weapons Proliferation To Terrorists,” *The Nonproliferation Review*, (Fall 1999), pp. 17–34, pp. 26, 30. Although clearly lacking actor-centered analysis as a focus in his investigation, Zanders does review the “social environment and norms” of a PVM, but focuses on the “assimilation model for studying the demand side of the proliferation process in states.” States and sub-state actors usually have different priorities and models generally disregard exceptions to the rule. Both implicit assumptions – that state and sub-state actors are comparable in relation to PVM use of WMD and that PVM behavior per se can be modeled – ignore the established diacritic nature of PVMs at the peril of voiding their very premises. PVMs tend to be unpredictable and hence exceptions to most rules.

trajectory of analytical error. The nomenclature of the generalization of terrorism in the shape of sweeping, impersonal categories is symptomatic of its reductionist mindset (e.g. “the global terrorist network,” “Middle Eastern terrorism,” terrorism as a national-level *risk*, as opposed to a documented *threat* etc.); reductionism, in turn, constitutes an invitation to deterministic thought; and determinism, by virtue of its model-like, teleological nature, is frequently quite removed from the nuts and bolts of reality.

Too often we are removed from the violent field. We need to interact with those who are violent. The best research on small-group political violence is undertaken by researchers who, on some level, interact with the people being researched. Sampling is important. With every research method there is the possibility that respondents will tailor what they say, for a number of reasons... Immersion in the research field and regular interaction with activists often allows one to overcome problems that plague the journalist, as well as the one-shot survey approach.⁶²

It is evident that the consequences deriving from an analytical mistake caused by the exclusion the evident idiosyncratic psychological backdrop of PVM use of terrorist tactics and the diacritic property of PVM decision-making, including the situational specificity of implementing impact scalability, would likely be catastrophic well beyond the benchmark of destructivity established on 11 September 2001 in New York and in Washington D.C. And to be certain of one thing: All attacks carried out on 11 September bear the imprint of the traditional, and not the “New,” terrorism. In terms of the psychological impact and the economic disruption, but not necessarily the volume of casualties caused, 11 September will almost certainly

62 Robert W. White, “Issues in the Study of Political Violence: Understanding the Motives of Participants in Small Group Political Violence,” *Terrorism and Political Violence*, Vol. 12, No. 1 (Spring 2000), pp. 95–108, pp. 100–101.

be overshadowed by a PVM attack with ABC weapons.⁶³ The next attack is a virtual reality.⁶⁴

On a fundamental level, the ability to learn how *to think the way that terrorists do* is the key to any sensible analysis of the terrorist threat. There are no objective indicators in aid of an assessment of the terrorist threat. *Ex post facto* examples too numerous to be listed here illustrate the preeminence of non-linear and non-quantifiable determinants in the decision-making processes of PVMs. Likewise, the accuracy of prognostication is dependant upon the specificity, and not any presumed objective character, of the intelligence and its contextualist interpretation, which, in turn, rests upon a solid understanding of the subjective reality of the actors.

The rationale behind the use of terrorism is conditioned by a multiplicity of influences, some of which are likely not to be factored in by analysts due to lacking information or understanding. Where the determinism germane to game theory and rational choice models will almost certainly fail to adequately capture the peculiar nature of the PVM phenomenon, the situational experience of role-play and other scenario-techniques still have a chance to succeed at producing insight, capturing unpredictable behavior and opening up new perspectives.

An understanding of the PVM mindset is the best source for inferential analysis, which is especially important and practicable, for example, in the devising of guidelines for protective measures and countermeasures. This approach promises to produce the best clues about PVM decision-making processes and the mechanisms

63 Thomas Isler and Martin A. Senn, "Der 11. September war noch eine Form des altmodischen Terrorismus," interview with Walter Laqueur in the *Neue Zürcher Zeitung*, Sunday Paper Edition, 20 October 2002, p. 27.

64 This author understands that his assessment cannot escape being integral to the process of the dynamic of reciprocal threat perception, too, but feels that tabling the issues addressed in this work outweighs other considerations.

at work in the formation of objectives. C.J.M. Drake points to the significance of understanding this key lesson of PVM analysis:

A group's ideology is extremely important in determining target selection. It defines how the groups' members see the world around them. Events and the actions of various people – both potential targets and other actors – are interpreted in terms of the terrorists' cause... When a group takes the decision to use violence, an early step is to determine who or what will be attacked. The ideology of a terrorist group identifies the 'enemies' of the group by providing a measure against which to assess the 'goodness' or 'badness', 'innocence' or 'guilt' of people and institutions.⁶⁵

One lesson of the attacks of 11 September is the necessity of moving away from making assumptions about PVMs according to the dictates of the policy of the day, or on the basis of the questionable value of statistical evidence on an issue that is intrinsically non-quantifiable. Countermeasures ought to follow understanding established by *qualitative*, as opposed to *quantitative*, research and thus emphasize detailed actor-centered analysis. Terrorism is a "people business," full stop. In its most pronounced form, the argument raised here is to the academic sector what the increasingly urgent call for the augmentation of human intelligence (HUMINT) capabilities is to the world of secret services.⁶⁶

Frequently, government organizations remain unreformed, despite the self-evident fact that a more successful counter-terrorism policy is to a large extent predicated upon realizing the critical-

65 C.J.M Drake, *Terrorists' Target Selection*, (Basingstoke: Macmillan, 1998), p. 23.

66 On the analogous character of the problems faced in academia and intelligence services described in the text, cf. Bruce Berkowitz, "Intelligence and the War on Terrorism," *Orbis*, (Spring 2002), pp. 289–300, pp. 295–297; and Reuel Marc Gerech (writing under the pseudonym of Edward G. Shirley), "Can't Anybody Here Play This Game?," *Atlantic Monthly Online*, (February 1998) available online at www.theatlantic.com/issues/98feb/cia.htm.

ity, and the mastering, of the analytical challenges as determined by an hitherto underrated qualitative research. Reform also hinges upon a sensitization vis-à-vis the inherently questionable value of abstracted risk analyses, and an appreciation of the dangerous margins of error created due to their approximate nature in their function as determinants in the policy-formation processes.

We should first know who (actors, motives and objectives) and what (organizations and capabilities) we are dealing with, before jumping to conclusions, comparing and referencing with a known, but possibly inapplicable, body of knowledge and committing resources to protect and counteract on that basis. Here introduced by way of a consultative theme, albeit sotto voce, is the warning not to make any assumptions about PVMs based on abstractions of terrorism. This is especially important as such assumptions may enter governmental decision-making processes conducted by people with no, or only little, experience with terrorism, which, in turn, may translate into policy directives, gargantuan fiscal commitments and superfluous exertions – and likely in the wrong places at the wrong time.

A case illustrative of government spending on the basis of originally quite pragmatic, but somewhere along the line generalized and abstracted, renditions of a perceived endemic terrorist threat is that of the U.S.' sudden concern with its critical infrastructures. Massive government funds are being mobilized on behalf of Critical Infrastructure Protection (CIP) programs, which have been enacted on the legal basis of the Clinton Administration's Presidential Decision Directive Number 63 (PDD-63), signed in May 1998.

The US federal government is presently confronted with the challenge of having to “minimize, with a limited amount of resources, the expected impact on the nation's critical infrastructure of any future terrorist attack.”⁶⁷ In spite of the wide scope of identi-

67 John Moteff, Claudia Copeland, and John Fischer, “Critical Infrastructures: What Makes an Infrastructure Critical?,” *Report for Congress by the Congressional Research Service*, (Washington, D.C.: The Library of Congress, 30 August 2002), p. 12.

fied critical infrastructures to be protected, the US government's inquiry has noted that "there will be a need to prioritize effort, to allocate limited resources in a way that can minimize the impact of any future terrorist attacks on the nation's infrastructure..."⁶⁸ A report to Congress of August 2002 distinguishes three criteria for determining allocation of federal funds in the spirit of PDD-63:

- Lack of redundancy, criticality of service provided and robustness of a critical infrastructure
- Cross-cutting vulnerabilities and potential solutions in infrastructures
- Identification and determination of the quality of interdependencies between infrastructures

About the last criteria, the authors of the report write: "Identifying and focusing on those assets that connect one infrastructure to another may be a cost-effective way to reduce the overall impact of an attack."⁶⁹ The irony of such a view is that, sensible though it may be with respect to cost-benefit arguments, it implicitly *assumes* that PVMs will also recognize and identify the *same* interdependent infrastructures as priority targets. An error in this assessment would potentially offset any gain – financial and otherwise – in security to critical infrastructures. Significantly, the criteria established by the authors of the reports tasked with measuring the exposure and vulnerability of critical infrastructures exclude the one determining factor that could possibly allow them to assess the actual threat level and, hence, determine the degree and particular means of protection required: the terrorist actor.

A major problem with assessing vulnerabilities is that they seem to proliferate the closer one looks; threats, though dynamic and amorphous, are not as prone to spontaneously reproduce. While the definition of the former is an arbitrary exercise of questionable value and its only test is a terrorist attack, the analysis of latter

68 Ibid., pp. 11–12.

69 Ibid., p. 12.

constitutes a feasible enterprise with a considerable likelihood of situational gains and the possibility of supporting proactive intervention efforts (counter-terrorist operations).⁷⁰

Assessing exposure and vulnerability to terrorist attack without considering the origin of the threat, i.e. the actor, is hence at best a questionable pursuit costly to the taxpayer. A couple of years prior to the publication of this Congressional report, an expert statement to the House of Representatives' Subcommittee on National Security, Veterans Affairs, and International Relations expounded in no uncertain terms:

Making decisions without commonly agreed upon threat and risk assessment carries the chance that important resource allocation decisions will be based on current beliefs and not on a well grounded understanding of the problem at hand. The apparent over reliance on worst-case scenarios shaped primarily by vulnerability assessment rather than an assessment that factors in the technical complexities, *motivations of terrorists and their patterns of behavior* seems to be precisely the sort of approach we should avoid.⁷¹

When reading John Parachini's critical statement, briefly reflect upon the point raised by Martha Crenshaw about how terrorism research may be event-driven and ponder Ehud Sprinzak's skeptical remarks about the "great superterrorism scare."⁷² Can we, therefore, allow "current beliefs" to exacerbate an "event-driven" approach to terrorism research that, in turn, opens up the possibility of an

70 Ian O. Lesser, et al., *Countering the New Terrorism*, foreword by Brian Michael Jenkins, p. x.

71 Statement of John V. Parachini, Senior Associate, Center for Nonproliferation Studies, Monterey Institute of International Studies, Before the House Subcommittee on National Security, Veterans Affairs, and International Relations. *Combating Terrorism: Assessing the Threat*, (20 October 1999), p. 9 (my italics). The full text of the statement is available at the website of the Federation of American Scientists: http://www.fas.org/irp/congress/1999_hr/991020-test2.htm.

72 Martha Crenshaw, op. cit., p. 21; Ehud Sprinzak, op. cit., p. 33.

exponential trajectory of analytical error? Can we afford to finance the protection of all identifiable critical infrastructures against all and sundry, more or less probable, threats emanating from PVMs? Finally, can we allow ourselves to exclude the actor as the central piece of any threat analysis?

The unqualified answer to all these rhetorical questions is: No. In the sense that it has less “ground” to cover than vulnerability and exposure analysis, actor-centered analysis is probably more efficient in the CIP context because it is geared toward the identification of the source of the threat. Common sense suggests that any CIP response must be calibrated in proportion to the effective PVM threat and relative to its target selection criteria. Defending critical infrastructures against all known factors contributing to its vulnerability renders the task of creating adequate protection complex and thereby opens up previously inexistent vulnerabilities. Seen this way, vulnerability analysis-based critical infrastructure protection may be instrumental in creating new vulnerabilities.

Also consider Parachini’s remark on worst-case scenarios derived from vulnerability assessments as a benchmark for protective measures, and juxtapose it with the conception of impact scalability. PVMs might just succeed at destroying or impairing critical infrastructures because they decide *not* to play along with the CIP scenario “scriptwriter,” deriving his assessment from a “vulnerability perspective,” but instead “undercut” the expected intensity of an attack by selecting an atypical, hard target and attacking it with cutting-edge conventional means. Imagine that the critical infrastructure involved is a military installation, for example a silo housing mirrored intercontinental ballistic missiles.

On the general level, the overall objective of methodological advances in the study of terrorism will eventually have to be a consolidation of analytical methods and practices – a convergence of risk analysis and intelligence analysis. Actor-centered analysis, however, must become central to both, for if we desire to both understand the threat and extrapolate the risks emanating from

PVMs, we are compelled to understand their idiosyncratic “logic,” which is inarguably the inferential basis relative to their modi operandi, objectives and motives.

In pursuit of this task, we do not have to reinvent the wheel and may take recourse to the existing methodological wealth: From intelligence analysis practices, such as the Analysis of Competing Hypotheses, to micro-historical approaches, to case studies, to Behavioral Evidence Analysis in the field of criminal investigative psychology. Because any profile of a PVM hinges upon the perspective (i.e. threat perception) we adopt, we must be careful not to portray static images, but rather endeavor to create dynamic motion pictures sustained by a multi-disciplinary feed from monitoring activities in the study and insight gained in the field. Permitting ourselves to better understand the context within which, and out of which, PVMs operate constitutes our best hope of interdicting future attack and damaging PVMs’ personnel base and their capabilities. Learning how the authors of terrorism think and make decisions is our best line of defense against the augmented terrorism of the future.