Terrorism and the Breakdown of International Order: The Corporate Dimension

by
Patrick James and Jesse Goldstaub

INTRODUCTION

> Terrorists' acts do not normally cause a business to close down operations, although that can happen. But terrorism does contribute to the economic factors that may in fact create the climate for such a decision. As terrorism contributes to a deteriorating economic, political and psychological situation, it influences basic investmant decisions in a very negative manner . . . . Consequently, the company suffers, the affected country suffers even more and the . . . national interest suffers.[1]

During the worst period of terrorist violence in Argentina in the 1970s, the disinvestment and departure of multinational corporations (MNCs), especially North American firms such as ITT, IBM, Coca-Cola, John Deere, Otis Elevator, and Alcan, were directly attributable to the prevalent terrorist tactic of expatriate executive kidnapping.[2] Radical displacements of this nature disrupt coordination of operational management tasks, have an impact upon productivity, and create substantial problems in tactical decision making. Many parallels are being drawn in the counter-terrorism and intelligence communities and the security industry between the situation then and current conditions in Colombia, where the agenda of declared assassination targets for terrorist groups features expatriate and domestic businessmen, as well as police and government officials.

Assassinations of businessmen and other violent acts attract media attention and are difficult to cover up. These events demand action of some sort—or the appearance of action—from the host country government and have a prolonged impact on operations in the host country and its geographic area. As a tactic against soft targets, which include multinational corporations, terrorism achieves large effects at minimum cost to perpetrators. Since mortality during an incident and non-lethal casualties are accorded attention in the media far in excess of their statistical importance, the detonation of one bomb at the offices or in the production facilities of a corporation, the kidnapping of one executive, or an ambush and attack upon an executive, can initiate a reactive chain of corporate security measures. It will not only introduce a climate of fear and apprehension throughout an MNC's overseas operations, but that sense of anxiety and trepidation will permeate the organization, extending to its headquarters thousands of miles away.

The aggregate number of attacks on multinational business and those involving death or injury in comparison to the number of corporate

overseas operations is in itself not large. In relation to the number of vehicular deaths in Canada in any year or the annual homicide rate of a major U.S. city it is not substantial. However, the incidents impart a disproportionately high impact on business. Shock tactics, such as the assassination of an executive, are met with a "gut reaction" and it is possible through these measures to drive foreign executives and their companies from a country.[3]

A brief review of the statistics on terrorist incidents, particularly those against business, is in order. There are at least eight organizations keeping terrorism databases. Because of the disparity in coding procedures between and among official agencies—such as CIA and State Department—and International Terrorist Research Center, Risks International, Intertel and other private firms, only two sources are used here for benchmark data.[4]

In the five-year time-frame from 1983—the year of the terrorist truckbomb attack on U.S. Marine Headquarters at Beirut Airport—through year-end 1987, annual terrorist incidents, according to official figures, rose from 485 to 832 (831 plus one attack that occurred in international waters). Business Risks International (BRI), using coding criteria substantially different from State Department and other U.S. government agencies, reports a total of 3089 terrorist incidents in 1987 (2860 in 1986), with 1868 of them taking place in Latin America. U.S. government figures reflect 108 of 831 incidents as having occurred in Latin America, while 370 transpired in the Middle East. BRI puts 211 incidents in the Middle East/North Africa of their 3089 incident total.[5]

Casualty figures from official sources reflect an increase in dead and wounded from 1904 in 1983 (883 in 1982) to 2905 in 1987. The 81% escalation in wounded for the five years, and an extraordinary 368% rise in Asian incident figures, 1987 over 1983, are attributable to 1987 terrorist bombings in Pakistan, of which 128 are believed to be linked to the Afghan secret police. They caused 1298 casualties (1076 wounded and 222 killed). Assassination continues to grow as an instrument of choice—374 in 1985, 399 in 1986, and 426 in 1987.[6]

State Department indicates 150 arson incidents in 1987, while there were 47 in 1983. Explosive bombings officially reported totaled 473 in 1987 (as against 254 in 1983) out of the year's aggregate incidents. (Incident figures may exceed event totals due to overlapping.) Risks International Division of BRI records 1501 bombings in their 3089 total for 1987 (48.6%). Of that 1501, however, 802, or 53.4%, were directed against business.[7]

Official records, according to conservative State Department coding criteria, specify 204 attacks against business in 1987 (74 in 1983) out of the total 832 incidents this last year (485 in 1983). The recent five-year time-frame thus reflects a 71.5% increase in incidents but a 175.7% rise in business attacks.[8]

Perhaps the most telling statistics (occurring in the BRI reporting structure) are those relating to "facilities attack." These continued to increase from 879 in 1986 to 1087 in 1987. Facilities attack as a category is

characterized as one in which the terrorists are physically present during the incident, as opposed to a remote-control or timed detonation of an explosive or incendiary device. In some cases, the terrorists intentionally remained on the premises and engaged security forces, when they arrived, in fire fights, inflicting considerable casualties by dint of the terrorists' superior weaponry and firepower. The increase in confidence implied by these figures and anecdotal chronologies of events is especially ominous.

Having described the scope of terrorism in quantitative terms, with special reference to MNCs, it is appropriate to set more precise boundaries. This will entail a discussion of terrorism as a concept, thus setting the stage for an analysis of potential responses to the problem.

THE CONCEPT OF TERRORISM

"Terrorism" is a term that has generated a great deal of confusion in recent years. Misunderstanding is widespread. Sometimes the media will treat an act of politically-motivated violence as terrorism, and on other occasions perpetrators will be referred to as "guerrillas."[9] Uncertainty is most apparent in the international community, which has been unable to agree upon a definition. This reflects the efforts of states which support terrorist movements and seek to legitimize terrorist acts.[10] For example, terrorism is regarded in some quarters as essential to the struggle for "national liberation" waged by those under "imperialist oppression." Thus it is important to set the boundaries of an investigation of terrorism quite carefully. From this point onward terrorism will be defined as follows:

> the systematic threat or use of violence by a state or non-state actor, with the intention of inspiring fear, influencing government or corporate policy, undermining public confidence, or promoting unrest, as part of a plan to impose the perspectives held by the terrorists on society.

This definition has two principal advantages. One is that it eschews any reference to guilt or innocence. The other advantage is that the definition incorporates state and non-state actors; it is very difficult to distinguish these entities in the contemporary world of terrorism. For example, if a state supplies dissident foreign nationals with intelligence, weapons and safe houses, are these individuals or groups still independent agents, that is, non-state actors, or should they be regarded as extensions of the state? In either case their activities are appropriate subject matter for an investigation of terrorism.

Some believe that the problem posed by terrorism has been greatly exaggerated, mostly due to the media.[11] It is not difficult to see why this belief has emerged. In a given year, the citizen of a Western country is far more likely to die in an automobile accident than in a terrorist attack, and airline passengers are much more likely to die in a plane crash resulting from human error or equipment failure than because of a hijacking. Why, then, the great concern with terrorism?

There are several reasons why the mere statistical scarcity of events cannot fully convey the dangers posed by international terrorism. One is that its impact is not a direct function of frequency. While the chance of a skyjacking for a given flight in North America is about 1 in 100,000,[12] in 1986 the vacation plans of a great many Canadians changed because of the perceived danger of traveling to Europe. A few highly publicized events can have the effect intended by the terrorists: creation of a climate of fear.

A related problem is the potential of terrorism to damage the modern, interdependent world economy. While the basic motive of terrorism—the use of violence to achieve political ends—has not changed, the tactics are more menacing than ever. Submachine guns and lightweight, high-powered plastic explosives have facilitated killing, and the range of potential victims also has increased. Terrorists, who might once have showed concern that no bystanders be injured or killed, have made it clear through their actions that everyone and everything is a possible target.

Private citizens, such as corporate employees, are especially vulnerable under the current *modus operandi*. MNCs are perceived by terrorists to be mere extensions of their nominal "home" countries. This is not in line with the self-perception of MNCs as transnational, economic actors. The adversaries view the struggle in very different terms as a result. MNCs regard terrorism as a business risk to be insured against; terrorists see MNCs as the global representatives of states with unwanted (that is, capitalist) ideologies. Consequently, terrorist groups increasingly have engaged in "networking," while the collective responses by MNCs and governments have not been impressive to date.

Terrorist networking indeed may be the most significant change over the past few decades. The establishment of links among the many terrorist organizations around the globe constitutes a system of mutual aid used to transmit money, documentation, weapons and training.[13] The factor which has contributed the most to networking has been the aid provided by certain governments. War is more expensive and risky than ever; many states have come to regard terrorism as quite an inexpensive and virtually risk-free alternative method of destabilizing enemies.[14] In an undeclared war by proxy against the West, the USSR (and many of its affiliated states), South Yemen, North Korea, Libya, Syria, Iran and Iraq, among others, provide terrorist allies with support. This assistance includes training, money, weapons, transportation, safe houses and refuge. In most instances these states do not control or direct international terrorism but they assist it quite effectively.[15] Without such aid, it is unlikely that terrorism could have attained its present scale.

Hence, terrorism as a concept should be understood broadly. It is a global political phenomenon involving transnational actors and recognized governments. As will become apparent, responses to international terrorism have not demonstrated a thorough grasp of its essential characteristics.

DEALING WITH TERRORISM

Contemporary terrorism adversely affects individual states, the community of states, and MNCs. All of these targets also may be regarded as potential sources of counter-terrorist measures. It is beyond the scope of this article to deal thoroughly with even a fraction of the many responses that have been advocated for each of these interested parties. However, a survey of a few of the most commonly proposed policy options will support an underlying theme: MNCs should reconsider their options. These range from passive and active defense through reactive measures to proactive policy. It is hypothesized that MNCs will increasingly turn to proactive policies, that is, seizure of the initiative, because they will be driven by circumstances to view them as appropriate.[16] Proactive policies may involve questions of subversion of sovereignty in host countries as well as conflict with home country foreign policy prerogatives and defined interests. This aspect will be dealt with in a pragmatic context later in the discussion. In summarizing state-level performance, it will become apparent that MNCs cannot expect effective responses to terrorism from either individual states or collectivities of states.

No effort will be made to cover exhaustively the strategies and tactics that might be pursued by states or aggregates of states. Instead, a few examples will be used to illustrate an important common trait among all such responses. More specifically, initiatives by individual states or groups of states directed against terrorism will be inhibited by the logic of collective action. Although Olson summarized the paradox of group rationality in a discussion of profit-maximizing firms, the analysis also is relevant to the behavior expected from self-interested governments:

> Just as it was not rational for a particular producer to restrict his output in order that there might be a higher price for the product of his industry, so it would not be rational for him to sacrifice his time and money to support a lobbying organization to obtain government assistance for the industry. In neither case would it be in the interest of the individual producer to assume any of the costs himself.[17]

Since the benefits from combating terrorism are distributed generally—given the transnational nature of the problem—the situation faced by the Western states parallels that of Olson's firms. All of the states would like to see a reduced level of international terrorism. However, there is an incentive to avoid the costs of contributing to the collective good while simultaneously reaping the benefits. Because each state follows a similar line of reasoning, a suboptimal degree of collective action against terrorism may be expected from the relatively large number of states concerned with the problem. Since there is no specific state with a sufficient preponderance of MNCs to provide the collective good on its own, terrorism continues largely unchecked by governments.[18]

Given constraints of space, only a few methods for dealing with terrorism will be discussed. At the state-level, control over media coverage will be appraised. Cooperation among states will be evaluated in terms of basic measures such as the exchange of information. Finally, the options available to MNCs will be considered in light of the likely future profile of state-level action against terrorism.

Governments, scholars and some people within the industry itself have criticized the media for irresponsible reporting and unrealistic portrayal of terrorists. It is asserted, and in some cases demonstrated, that media coverage of terrorist events: (1) legitimizes terrorism by providing the perpetrators with a platform to express their views; (2) leads others to take up terrorism; (3) makes future terrorist incidents more difficult to resolve by excessively detailing both terrorist and counter-terrorist operations; (4) hinders efforts to end an incident quickly; (5) places the lives of hostages and police at greater risk; and (6) spreads fear by magnifying terrorist violence so its impact on the public is disproportionate to actual harm.[19] The media often become more than observers; they participate in terrorist acts by interviewing terrorists and helping them to present viewpoints.

Some have argued that self-restraint should be sufficient, because the media previously have demonstrated self-control:

> In the late 1970s, there was a rash of episodes in which spectators at sporting events jumped out onto the playing field for their fifteen seconds of exposure on national television. After a number of these episodes, some of the networks decided to turn the cameras away. Instead, a reporter would say, 'There's someone running onto the field, but we won't show him to you because if we do, it will encourage other clowns to do the same thing'.[20]

Although U.S. television networks agreed not to show these increasingly mundane events, that is different from getting hundreds of news services to show self-restraint when reporting a hijacking in which terrorists have killed a hostage. Given the desire for higher ratings or for a larger circulation, some media representatives undoubtedly would choose to ignore voluntary restrictions. Of course, there would be no resultant benefit if only some of the media showed self-restraint.

Without self-policing, some government censorship of reporting would be the next logical step. However, that would be very difficult to achieve in virtually all of the countries concerned. Constitutional guarantees of freedom of the press are reasonably pervasive in Western states. The record so far indicates that governments are unwilling to incur the political costs that might result from imposing stringent regulations on media coverage. Once again, the incentive for a government to act alone runs into the problem of collective action. Unless all act together, the impact is minimal.

International cooperation against terrorism started with the League of Nations in 1934. The attempt by that organization to respond reached an impasse over the issue of a suitable definition of terrorism,[21] and this problem continues to plague cooperative efforts. Many African, Asian and Arab states have blocked international conventions on terrorism brought before the U.N. General Assembly, insisting that the causes of terrorism must be understood before it can be eliminated. These states have asserted that "if undesirable acts—which some might describe as terrorism—are undertaken in the name of self-determination or national liberation, then such acts are beyond the scope of condemnation and are legal."[22]

Western states take a different view: the end does not justify the means. Given U.N. inertia on the issue, these governments have started to cooperate through regional agreements. Yet even they have experienced serious obstacles to collective action, resulting from "incompatibilities of legal systems (civil law and common law), from diverging national interests, and from historically-based differences in political outlooks and cultural attitudes (for instance concerning the right of asylum)."[23]

Effective cooperation would require that expertise, intelligence and technology be shared. The participants also would have to arrest, imprison (or extradite) known terrorists operating within their borders. However, because of the reasons just alluded to, these relatively straightforward guidelines have not always been followed.

Stronger measures, such as political and economic sanctions against states which support terrorism, are even more problematic. In addition to differences among individual Western states, there is a systemic problem to consider. Taking effective action against international terrorism is a classic problem of collective action. As noted, benefits are distributed to the group, as a general rule, while the costs of instituting measures are absorbed by individual states. Thus there is an incentive to opt for a "free ride," that is, to have the other members of the group pay for the collective good while still enjoying its provision. The operation of this same logic is evident in the record of NATO, where suboptimal provision levels reflect (at least in part) tendencies toward "free riding."[24]

Further complications await collective action against terrorism, because governments also may believe that privately experienced benefits will accrue from free riding. If Western states do act collectively, those which do not participate may anticipate receiving two kinds of rewards, public and private. The former will be represented by an overall, long-term reduction in the level of international terrorism induced by group-supported countermeasures. The latter set of benefits could be favored treatment from terrorists, who might be inclined to retaliate more (at least in the short-term) against the states involved in collective action.

Individual and collective nation state roles as initiators and aggressive sponsors/supporters of effective counter-terrorist action seem dubious. The lack of governmental resolve or ability to regulate media

coverage, the contention and confusion in the U.N., the legal, cultural, and political disparities among nations, the considerable constraints on wide-spread sharing of intelligence and expertise, and the problem of "free riding" as a disincentive to full participation in political and economic sanctions all point to the fact the prospects for effective action at the state level are not promising. It therefore becomes important to consider the options available to multinational corporations themselves.

The major issues have been spotlighted and viewed from a corporate perspective and from an international relations perspective by Goldstaub:

> A global war is going on and international enterprise is caught in it, not as an innocent bystander but as a participant, a silent and albeit unwilling belligerent, more target than combatant.[25]

This insight far exceeded the prevalent conventional view of passive defense (for example, set barriers to physical access or structural hardening) as a palative and political risk analysis as acceptable intelligence methodology. It assumed that MNCs would be attacked because of a metabolism deriving from successive hardening of symbolic targets—first military, then diplomatic, leaving business as the softest available option. This interpretation is still valid, but it is now evident that the business community is a preferred target because of its inherent attractiveness. That means the "bold steps into uncertain environments"[26] counselled for corporate policy formulators—essentially an active defense with potentially incomplete intelligence resources—no longer are consonant with current realities.

Moreover, the strategic, geopolitical framework for appraising the role of organizational intelligence as an anti-terrorist mechanism for MNCs in conjunction with their nominal countries of domicile (and the Western alliance) presumed more cohesion than actually exists:

> Until the time comes when nation-states, as a geopolitical form, and multinational corporations, as a geoeconomic force, can afford the luxury of sorting it out between themselves, they had better ensure their survival against a common enemy.[27]

The previous work is therefore not complete and requires reassessment in light of contemporary events and altered conditions. Anachronistic mindset and pure conjecture are a recipe for disaster.

OPERATIONAL ASPECTS

It is rather paradoxical that one of the world's largest MNCs may have contributed the start-up money for one of the first multinational terrorist networks. The Peoples' Revolutionary Army (Ejercito Revolutionario del Pueblo - ERP), on June 12, 1974, announced that it had taken $5 million of the $14.2 million ransom paid by Exxon (in 142,000 $100 bills) for Victor Samuelson, manager of the Esso oil refinery in Campagna, Argentina, and provided a "Junta de Coordinacion" with

these funds for the use of Uruguayan, Chilean and Bolivian insurgents. The Junta was established to direct the groups in their "joint struggle" across five Latin American countries.[28] This transnational stage of development for ERP might not have been achieved without the Exxon "contribution."

Multinational enterprise continues to be an eminently popular terrorist target because it has developed a reputation for meeting demands fairly quickly; it has by definition huge resources; it is a vulnerable "soft target"; its very nature is generally suspect, controversial, emotionally charged; and, above all, it is highly symbolic. Naturally, business does everything it can to prevent its victimization being discovered. MNCs will avoid disclosure of kidnap and ransom incidents with the active cooperation of many host country governments which do not want to appear as if they are losing control and also may have a "no ransom" policy.

World total *publicly reported* kidnap ransom demands in 1986, not necessarily the sums that were paid, were less than $2.7 million US.[29] However, larger sums than the total reported in the year are actually paid in single incidents. A representative event was terminated recently. On 8 March 1987, Richard (Rick) Paulson, a 37 year-old Canadian engineer employed by Occidental Petroleum as production engineer in the giant Canno Limon oil field along the Colombian border with Venezuela, was kidnapped by the National Liberation Army (ELN).

Marxist terrorist organizations have been waging a prolonged campaign against oil companies and exploration activity in that area. Two employees of contractors working for Occidental Petroleum were abducted by the People's Liberation Army (EPL) on 10 December 1985 and a ransom of several million dollars demanded. Members of the National Liberation Army (ELN) attacked two sections of the Occidental-Shell-Ecopetrol pipeline near the Venezuelan border on 14 July 1986. That incident was the start of a multitude of similar attacks on the pipeline during the year. Occidental has been targeted in particular to show that MNCs are rapacious. In Paulson's case, public works and a $20 million US ransom were demanded. He was released 376 days later, on Friday, 18 March 1988, by the Castro-inspired ELN group near the town of Beleen, 200 kilometers northeast of Bogata.

The final figure reputedly paid for him was $6 million US, which is less than the common $10-$15 million US figures that were extracted during the heyday of Argentinian and Venezuelan terrorist activity in the 1970s. The largest reported ransom paid was $60 million US in 1975 for two brothers, principals of Bunge and Born, the huge grain concern. Some are not so lucky. Clifford Bevins of Goodyear Tire was kidnapped in Guatemala on 7 December 1980. He was killed by Guerrilla Army of the Poor on 13 August 1981. Of two engineers abducted in Colombia in December 1985, one was released unharmed. The body of the other, Edward Sohl of Bechtel, was discovered on 11 August 1986. He is thought to have died the previous May in captivity.

State Department records indicate a rise from 40 kidnappings in 1983 to 53 in 1987. (An aberrative high in their figures of 87 was reported in 1985.) BRI sets the 1987 total at 73. There is little evidence to sustain the view that a company's executives may be targeted because it has kidnap insurance. Kidnappers are concerned with such issues as company size and political significance. They have little worry about companies having sufficient funds to meet the ransom demands.[30]

Multinational companies will budget what they can to harden structurally housing facilities, to train their expatriate executives in defensive driving techniques, to buy them bullet-proof clothing, armor their cars, and pay for all sorts of deterrents to maintain their presence overseas. They can do much less about a psychological chilling effect that has resulted in the no longer effusive self-esteem of expatriate personnel and an erosion of confidence that they will be afforded total protection at the geographic periphery of the organization.[31] Increasingly stringent security measures are required for corporate executives, and common commentary of CEOs relates to their fall from grace, or at least from gracious living, to the erratic and deceptive movements of the perennial fugitive.[32]

It is easy to see how the average, major MNC bill of half-a-million dollars per year for ransom insurance will continue to rise. If terrorist incidents do come to light, they are denied. If they cannot be denied, they are minimized. Although there is no projective validity to the available figures from any source, kidnapping, as noted, has increased by everyone's count. One more trend is apparently being established: the attacks against business persons and facilities overseas, as well as non-business targets, are becoming more punitive and they involve more indiscriminate, nihilistic methods. Higher levels of deaths and injuries have resulted.

Violence against physical facilities has taken place from immediate and stand-off positions. In order to blow things up—and that is a fairly low-risk, favored ploy of terrorists—you have to get reasonably close to them. The exception is the use of stand-off weapons which, for the most part, have limited range (such as field mortars or even the newer generation of shoulder-fired, rocket-propelled grenades or anti-tank ordnance). Physical damage inflicted on business and non-business facilities by terrorists until now has been done with conventional weaponry. The level of sophistication is rising rapidly,[33] as exemplified by the European exploits of the Communist Combatant Cells, Direct Action, and the Red Army Faction. Whether *ad hoc* marriage of convenience or true ideological bond, the joining of Direct Action (France) and the Red Army Faction (West Germany) portends a potential pattern of greater potency and destructive impact. They declared in coming together:

> Attacks on NATO's multinational structures, on its bases, its strategists, its plans and propaganda, were the first major mobilization with a view to the formation of the proletarian political strategy in West Europe . . ..[34]

Losses from damage to facilities are understated if they become public knowledge. In cases where the costs are too large to conceal, claimed losses to insurance companies are overstated (read, monumental). Not exposing insurance information is just common business sense. Lloyds has insured a very broad spectrum of risks and has done so for quite a long time. INA, in 1982-83, began advertizing its coverage of political risks aggressively. Alexander and Alexander does so more directly and with less fanfare. The total number of organizations insuring various aspects of political risk, loosely defined, is not known. The number, size, and identities of their clients are not generally known either. In fact, there is no comprehensive information about any of these factors. Private sector insurance companies intentionally keep confidential the type of insurance written and the financial volume because international business intelligence analysts have a very strong intuitive grasp of potential or at least possible events. They can deduce from the aggregate figures, if they were freely available, what the big players are afraid of and where. It may take very little in an organization with a tense atmosphere to produce anything from extreme reluctance to make entry decisions to a frenzy to find the nearest exit.

In 1986, *publicly reported* damage for the top five terrorist venues was $9,463,000 US (Colombia); $7,221,000 US (Nicaragua); $5,660,000 US (Peru); $5,210,000 (Chile); and $3,456,000 US (El Salvador). However, indirect damages resulting from terrorist activities represented by revenues lost, for example, the export of raw materials or semi-finished products, are substantially higher and can only be roughly estimated. For Colombia, the top terrorism country that year, in-country indirect loss stemming from terrorist bombing in pipelines and pumping facilities diminished petroleum revenues by over $10,000,000 US, as estimated by the Colombian Energy Ministry.[35] As a comparative benchmark, global total *known* property damage for 1986 attributable to terrorist groups did not quite reach $36 million US.[36] The average of all this erratic action on an annual basis is highly misleading, but it is obvious that whether government-sponsored or private sector insurance organizations provide some relief through "risk-reduction" instruments,[37] the growing risks themselves will not be dissipated.

ORGANIZATIONAL IMPACT

Risk perceptions and economic incentives work in opposite directions. Indeed, perceptions of risk held by top-level corporate leaders probably influence decisions more than even the risks themselves, where they can be objectively evaluated.

The tactical objective of terrorists is to violate, by their various activities, the two basic components of MNC operating regimen: (1) not to be forced into a position of unprofitability, and (2) not be to forced into assessing other potential direct investment opportunities in another country (or countries) as a more attractive, politico-economic option. In the same way that terrorism is not a "vocational hazard" of international business, it is not a "cost of doing business." Ransom payments can dissipate previous, hard-won, country subsidiary profits. Property

destruction and attendant losses are not absorbable in many cases. The security costs of multinational firms may double, triple or quadruple in a brief period because of escalating and at times exponentially rising expenditures for new, highly sophisticated equipment, expanded physical security and protective forces, development of systems and procedures, and contract consultative services.

The fear of terrorist attack and corporate expenditures for internal defense, as well as external services, has not as yet generally extended to the area of crisis management. This may in part mirror the business mentality: "Time means money!" Precipitously taking top-level decision makers away from their normal responsibilities is highly disruptive of the regularity which business craves and it is very costly. In the same way, many firms view expenditures and time dedicated to corporate intelligence capability as not sufficiently compensated for by potential results. This may also be said of preparations designed to increase physical security. Nevertheless, the security industry currently accounts for approximately $25-$30 billion US of annual expenditure. Estimates are that by the early 1990s, the figure may be close to $60 billion US. A broad array of goods and services is included, from electronic surveillance countermeasures equipment to defensive driving training.[38]

The instinct of a new security administrator with a law-enforcement background when a significant physical attack occurs might be to resort to reactive protective measures. He or she soon learns to perceive situations within the business frame of reference:[39] what is the probable extent of damage to be absorbed without protective preparations; what will the preparations cost; which is less and what will insurance cost? Many corporations are still inclined to "take the hit" if it may be less expensive financially. The disruption to organizational continuity and the substantial trauma engendered throughout the organization by a major incident has, however, led more and more firms to consider corporate headquarters and local, site-specific crisis management teams as essential.[40]

Administrative overhead also goes with this organizational growth. Above and beyond the structural attributes, MNCs have had to cope with salary negotiations which reflect the peculiar and special hardships of various posts. Assignments are likely to be shorter as transfer from hardship posts becomes normative, with consequent high costs for the firm. An additional, and major, consideration is that of diminished executive productivity under conditions of psychological stress and required security constraints—a "hidden" but very real cost.

Both strategic corporate investment planning and situational decision making clearly have had to comprehend terrorism as a material risk factor in the calculation of potential losses and increased costs which may result from a postulated range of gradients in the terrorist threat (ergo, the concepts of asset protection and risk management). Physical security has now become a preeminent concern of MNCs. The agenda has been reset. Consequently, the organizational intelligence structures of some global enterprises have been considerably revamped so that security-oriented intelligence activity has emerged as a principal force.

Acquisition, evaluation, and acceptance of other information that is really important to long-range planning may have begun to atrophy in comparison.

Moreover, business requires the semblance of continuity, stability, and calculations which are both rational and delicate, while "terrorism projects mostly destabilization, discontinuity and extreme emotions."[41] Terrorist intent is to produce a pervasive sense of disorientation and destabilization of the operating environment so that there will no longer be an expectation of getting up in the morning and going about "business as usual" because disruption will become normative. Hence, policy formulation will be engaged in within the constraints of "fuzzy gambling."[42]

PRA AND ORGANIZATIONAL INTELLIGENCE[43]

Until approximately five years ago, political risk assessment (PRA) was a household word in international corporations. This is no longer the case, although the fraternity continues its pursuit of technical excellence as a substitute for realistic appraisal. Part of the mythology created at the zenith of PRA was that the tools of logic and rationality so sacrosanct in business, economic and academic cultures (the philosophy of knowledge) could be adequately focused on political risk and it thus could be "managed."[44]

However, events have proven recurrently that logic is culture-bound and terrorism as a culture has a rationality which is diametrically opposed to that of Western industrial civilization, although terrorists individually and collectively are quite capable of using its technological accouterments. Hence, terrorism as a tactical weapon has the advantage over large-scale conventional warfare of being used in a manner which maximizes the crucial element of surprise—especially time surprise—as a concomitant of its inherent unpredictability and abrupt changes in methods and targets. Given that the intrinsic rationality of terrorism is alien ("crazy") to social sciences practitioners who advise most business and government hierarchies, terrorists are therefore provided with a further conceptual advantage.

PRA has both a structural tunnel vision, that is, *country* risk, and a fascination with technique which make it as vulnerable as the system it was meant to serve. Business, with its functional orientation, remains convinced that inducing a political scientist to engage in periodic speculation will provide sufficient intelligence for staff to run models of potential impact on the proverbial bottom line of marketing, finance, etc. Hard realities dictate that MNCs must think and operate as inherently geo-political entities as well as geo-economic ones within an interactive world system. In sum, nationhood is not the fundamental determinant of status or the capacity to influence outcomes. That capability hinges on information, which is the real power of organizations, indeed, of any organism, almost regardless of size.

The largest MNCs do have intelligence services, which certainly cannot be called "little CIAs." They have had them for some time, and are

not in the immediate process of creating them. However, there are people (some of whom had formerly been in government service) who offer services such as teaching MNCs how to evolve their own intelligence systems. Such systems are not an off-the-shelf item in the way PRA used to be and, in large measure, still is. Previously and presently, an advisory service may provide risk analysis on sixty countries and it does not matter whether the firm is in pharmaceuticals or resource extraction. If they pick Mexico, they receive a standard product and what they make of it is their problem.[45]

The political risk analysis that was practiced in the main had accomplished little more than to unnecessarily constrain the type of intuitive grasp that Chief Executive Officers (CEOs) had of their operating environments and projected an image of omnipotence on the part of political risk analysts and a specious sense of control. PRA is inclined toward computer treatments and exercises such as Bayesian analysis and modified Delphi technique. Those involved in the activity became so good at these conceptual games in the early days that the intelligence community would approach some of the consulting firms doing political risk analysis for major corporations and the corporations that had built in-house capacity to see if they could derive anything out of it.[46] There has been a perceptible shift over the past five to seven years, so that it is now the government which has superior techniques for treating intelligence of this nature and by far a more extensive and integrated network for dedicated collection.

In addition, the institutionalization of internal capacity for political risk analysis in international corporate structures often took the form of hiring a new Ph.D. in political science and parachuting him or her into an old-line corporate international economics division, at which time he or she was promptly frozen out of the flow of information and isolated from the process of high-level decision influencing, thus aborting the original intent. Nevertheless, from being a corporate fad earlier, PRA grew wildly because of the traumatic fall of the Shah in Iran.

Iran was a disaster from the point of view of Western Alliance defense policy, it was a disaster from the point of view of strategic posture, and it was a disaster so far as international business was concerned. It was so much of a "surprise"[47] that even a Swiss financial organization which is reputed to have the best commercial intelligence service in the world was caught off guard. Their intelligence unit is not modeled on a strategic/geopolitical service like the CIA,[48] but their validation of information is much the same. They check the information against other information they are receiving and they assign a measure (uncomplicated, running the gamut of just three levels or categories) to the reliability and credibility of the source. Had they received information from that source before? Had the previous information been reliable? What about the validity of the information currently being provided? Fortunately, they do not generate the same kind of end product that many PRA producers did and still do.[49]

Political risk analysis was excessively concerned at one time with the possibilities or probabilities of an impending change in host country government—that was considered a linchpin. If the government was in danger of changing, that was *bad*. If the incumbent regime stayed on, that was *good*. We now know that it does not matter whether governments change or not. For instance, American multinational corporations continue doing business with the Marxian-oriented governments of Angola[50] and other similar regimes which, for the sake of general consumption at any rate, the U.S. government finds reprehensible, morally repugnant, and an affront to American ideology.

Business has no ideology except survival and profit, as distinct from the ideological biases of its top management as individuals. Viability is a preeminent concern. Since the organization needs information from its environment so that it can remain a potent force, business will get that information in any way it can. If it collects information from open sources, that is all right. If intelligence collection is from individuals, groups, or organizations as primary or secondary sources, the manner of access and the MNC's home country become very important considerations.[51]

The global corporations with well-institutionalized intelligence services have teams that go out and collect information. However, that is not always or not even usually the case. Ideally, everyone who is out at the periphery and those at the headquarters who make visits overseas are part of the intelligence apparatus of an MNC. They have to be. The people who are line operating personnel, from corporate headquarters out to the periphery, are invariably more knowledgeable than the internal staff at the center, where purportedly the thinking is going on. Although many companies have not recognized the value of it, the debriefing process, when people come back from overseas assignment, is more valuable for the intelligence that can be extracted from it than as a mechanism for mitigating the trauma of reentry by the executive and his family to home country environment after a long period abroad. This is finally being realized.

Both corporate and strategic geopolitical intelligence employ many of the same kinds of procedures, although the technical intelligence (techint) capacity of the national intelligence establishment is staggering. There are, to begin with, open information sources being utilized. People do environmental scanning from available data and literature and also talk to reporters, bankers, businessmen with whom they maintain contact, and a broad array of people whom the firm does not pay—all of which is permissible. In addition, favours are done on a reciprocal basis. Other people know things as well and information is traded and exchanged between and among individual intelligence officers. It is being accomplished on an informal basis and has traditionally been done that way. With the levels of risk presently being encountered, however, it is evolving in a more formalized way.[52]

Contracting out for information is expensive. The fees are very high, depending in some cases on how prestigeous the individual who

may be the supplier of concentrated intelligence or infallible judgments had been in former public life. Even in the cases of firms regularly supplying country analysis, the fees may range from a quick overview for $9,500 to a yearly report, with or without supplements, at $50,000. As a consequence of the costs, as well as growing self-confidence, many smaller firms prefer to secure critical information from government and other private sector sources and use their own judgment, based on longitudinal experience in a particular country or area, as to what the potential of the impending situation means for their specific operations.

The management decision in many corporations to forego development of in-house capacity, or to accept or reject expensive external information inputs which do not totally accord with idiosyncratic organizational characteristics, may be made on the basis of considerations other than the magnitude of the direct cost itself. The potential costs of having a proprietary intelligence system, even of the PRA genre, are weighed against the perceived costs of large-scale organizational development and many corporations have opted for the acqusition of externally-generated policy inputs. The deciding factors are not necessarily the size of the fees but anxiety over expected disruption of the organizational structure and the concomitant opportunity costs of preempted top-level management time in the organizational development process (=$). These may be false economies in the longer run because the decision process also conditions perceptions of the necessity for development of a crisis management team or teams.

An alteration has taken place over the past decade in organizational priorities relating to information gathering at the corporate periphery, the amalgamation of this information with other internal and external resources, and the submission to top management of risk or threat assessment profiles. The thrust has lately been on physical and personnel security-related information. The concern over other relatively conventional economic issues such as foreign exchange exposure, repatriation of profits, expropriation, etc., that PRA had been apprehensive about previously, has significantly dissipated. Amelioration of these exposures with commercially available risk-reduction instruments has been rendered routine procedure, and, as a result, there has been a decline in multinational corporations of the PRA emphasis on central analytical staff (the paralysis of analysis).[53] More direct human collection of information is now emphasized.

Of necessity, as do governments, the organization will acquire information from: foreign government officials; professors, both domestic and foreign;[54] perennial host country graduate students, especially in the law schools, and their expatriate counterparts; journalists; and members of identifiable dissident elements within any given society in which it operates. In some cases, it is critical to determine what they are doing or to attempt to make contact with them at the risk of alienating the incumbent authorities. Intelligence is accumulated through "service sector" workers such as maitre d's, bell hops, waiters, taxi drivers, travel agents, airport baggage handlers, doctors, politicians, security forces personnel,

judges, lawyers, accountants, bankers—in short, from anyone and in anyway it can be gotten. A multinational corporation is not a moral paragon, and it does not have to posture the way governments invariably posture. Its basic *raison d'etre* is to survive, and even to prosper, which is why it distrusts governments. It distrusts all governments, even that of its home country.

PHILOSOPHY AND PRACTICE

In order to "destroy capitalist imperialism," terrorists and states that employ terrorism see this activity as a legal and morally acceptable instrument of policy. It must be used to disrupt and ultimately destroy the global market system and the enterprises which are instrinsic to its vitality and viability. Of course, from an ideological perspective, Marxism views capitalism as a self-destructive economic system, especially as related to less-developed countries. Capitalism therefore must be seen as collapsing because of its internal contradictions. Put differently, the Soviets do not have to defend communism (it is, in practice, indefensible); their doctrine says that it is capitalism which must fail. They, and those who subscribe to that philosophy, intend to help it do so.[55] The chaos and dissolution syndrome is accordingly a very attractive one ideologically.

Thus, in addition to domestic groups or indigenous factions that might want to punish a host-country government, the MNC, or both, global corporations must assess a strategic war. It is being waged by forces which will aid and abet any group, any movement, which, for whatever reason, appears to be helpful in accomplishing their strategic ends: to force Western industrial countries to pull back from areas of the world in which they have been largely preeminent or at least extremely influential in the past. At the heart of the matter is access to world resources and the cohesion of the Western Alliance. Strategic materials are acquired, because of the predisposition in most industrial nations for free-enterprise capitalism or some variant thereof, through corporate enterprise and not in the main by direct bilateral government arrangements. This places MNCs at the strategic nexus of the covert conflict.

A form of withdrawal is to be seen cumulatively on the part of oil companies. They are, much less than before, owners of things in the ground. In the international arena they are becoming essentially intermediaries, which means that they have engaged in risk avoidance. Because they recognize that the oil business is neither quick nor portable so they have decided to provide certain services. This reduces their vulnerability in terms of having to possess fixed assets and resources in a specific high-risk area, factors they must deal with. The oil business is resource-based and location-specific; the product does not exist in other places and cannot expediently be created. Many other resource-based companies have recognized the same thing. In a large number of situations were manufacturing companies are affected, there are few if any expatriate executives in the host countries. Their operations are being run by host country or third country nationals.

Terrorist states also will initiate actions of their own—through surrogates when possible—in furtherance of their objectives if and when they can do so with reasonably low risks and the convenience and the safety of vociferous disavowal. Most attacks by terrorists are carefully planned, researched, and executed. Such preparation is done within a generic and often subjective frame of reference. The act itself is not a spur-of-the-moment reaction to events, although immediate circumstances could well trigger a well-prepared terrorist strike.

Hence, the ties between MNCs and the governments and armed forces of their home countries (especially the United States) and their allies may be seized upon as a legitimation for attack. Such was the case in: the Brussels bombings of Litton, Honeywell, Motorola and other NATO-related defense contractors; the killing of Gen. Rene Audran, Director of International Affairs, Arms Sales Division, French Defense Ministry, on 25 January 1985; the murder on 9 July 1986 of Dr. Karl-Heinz Beckurts by the Red Army Faction with a remote controlled bomb for his role in the nuclear industry and research into the Strategic Defense Initiative (SDI); the murder of French industrialist Georges Besse in November 1986; or the assassination on 20 March 1987 of Air Force Gen. Licio Georgieri, who promoted an Italian role in Star Wars. If these connections are not used as a pretext, then something else will be because terrorists are embarked upon a delineable course of high-casualty attacks against soft targets.

This is not to suggest that terrorists have won or will win, or that multinational corporations are irrevocably hostage to a hostile operating environment which will force them from a state of siege, both physically and psychologically, into abject unprofitability while bankrupting industrial societies and plunging them into ruin. Nor is a Fortress Europe and/or North America postulated, with total havoc being wrought upon sophisticated and vulnerable societies by internal elements and foreign agents in their midst. However, the momentum of events has already radically distorted the global operations of both governments and MNCs which are potential targets, not to mention the effect that the fear of terrorism has had on the public. In addition, the prospects for stable economic progress in the developing world have assuredly been damaged by the mounting violence.

There is not an unlimited elasticity to the capacity of even the very richest MNCs to absorb the costs of doing business in high-risk environments and treat them as normal operating expenses. Ultimately, sustaining large losses from repeated ransom payments or prolonged payment of ransom insurance premiums and high volumes of security expenditures, among other exposures, means that the amounts, in time, become too large to just 'write off.' Initial cost estimates for structural hardening and construction of new secure diplomatic installations submitted by the U.S. State Department were $3.3 billion.[56] Current estimates amount to $4.2 billion.[57] There are many MNCs with levels of global presence at least equal to the U.S. Government. In addition to physical hardening of structures, another passive defense option is

making targets unattractive because attackers cannot get close enough to them with standoff weapons or cannot penetrate them to kill personnel or do extensive damage to sensitive equipment.

Money and communications organizations—VISA, for instance—have attempted to harden themselves procedurally against intrusion into their computer networks by restructuring the networks. They understand that their crucial vulnerability to being attacked is not merely physical but extends especially to the integrity of their networks, to the introduction, say, of a one-in-three margin of error in the internal logic for billing procedures or the ability to transfer funds internationally or internally.

It is known from many incidents in Europe that terrorist groups are technically adroit and have attempted to intervene in communications and computational networks as well as attack the infrastructure. The Committee for the Liquidation of Deterrence of Computers (CLODC) viewed computers as the chosen instrument of those in power because they are employed to classify, control, and repress. This opinion was contained in a statement issued to the French press after they bombed Ministry of Transportation Computers. The Angry Brigade attempted to bomb London police computers; more than twenty computer centers were bombed in Italy by terrorists;[58] the computer center of the West German firm that produces transport vehicles for Pershing II missiles was bombed by the Rote Zellen terrorist group; Philips Data System's computer in Toulouse, France, was bombed by Action Group 27-28 March.

By early 1985 alone, reported attacks on more than fifty computer facilities had occurred in the West with over 40% taking place in the United States.[59] Once again, there are no really valid and reliable numbers on computer attacks or disasters because businesses and governments do everything they possibly can to obscure their individual and collective vulnerability and victimization and rightly so.

It is estimated that of the businesses which have had a computer disaster, whatever the cause, between 85.6% and 93% are no longer in business after five years.[60] Obviously, some organizations are very large and in order to constitute a disaster an event would also have to be quite large in its impact if not scale. Military computer equipment was destroyed at the Sperry plant in Eagan, Michigan, by saboteurs; a person or persons unknown erased 27 computer tapes at a plant in Oak Ridge, Tennessee, which belonged to the Y-12 nuclear weapons parts operation; the IBM offices in Harriman, New York, were bombed by the United Freedom Front. For smaller operations, such as the First Data Corporation of Waltham, Massachusetts, the suspicious fire at its computer center, which forced it to withdraw service for a week to 500 time-sharing clients, hurt badly.

Intrusion into computer networks has become chronic, though in many instances more as a result of weaknesses in the security system than the criminality, predilection for gratuitous mayhem, or political malice

of the hackers. Targets run the gamut from major universities to publishing houses to the military.[61] The recent NASA incident points up the vulnerability of critical networks to high-tech terrorism.[62]

INTELLIGENCE AND ACTION

Terrorist tactics range from the use of destructive brute force to highly sophisticated disruption, with the attendant potential for future evolution of actions against larger social aggregates. This is implied by the availability of weapons, methods and techniques which may be developing at a faster pace than governments or corporations can develop and emplace countermeasures. There is every incentive to "out-invent" terrorists because a reactive anti-terrorist posture still leaves the initiative in the hands of terrorists and terrorist states. They will use it. They are dedicated to attack and will not desist. Low-intensity, unconventional, covert conflict has high yields for them. In the same way that terrorists wage a war of nerves, of symbolism and psychology, of attrition and forced options, they should be granted no quarter and no respite. A proactive counter-terrorist attitude mandates that pressure should be relentless and increasing. Costs in dollars and lives are going to be high, but more likely lower in the long-run with seizure of the initiative.

The multi-faceted campaign to be pursued by nation states encompasses a variety of economic instruments and diplomatic/political levers. It should also include the possibility of paramilitary as well as military operations. This last option must be judiciously employed. However, for reasons explored in the earlier part of the article, truly concerted action on the part of nation states will probably remain at a suboptimal level. It should be pointed out that while cooperation between and among countries, their law enforcement and intelligence agencies, proceeds apace, so does cooperation between and among terrorist organizations. They are well into the most productive segment of their learning curve, and there is no scarcity of professional terrorist pedagogues.

The corporate community is well aware of its vulnerability in this environment. They are quite perceptibly making haste to respond. The current pervasive need for both corporate anti- and counter-terrorist intelligence points up the fact that there is no singular solution offering protection for MNCs, and the most frustrating aspect of the situation is that for some time, as a top security chief put it, they have not been able to "subscribe to a single, accurate, reliable public or private source of constant and routine information to warn" them.[63] Global enterprises are not at all passive, but the costs of being discovered at aggressive action relating to terrorism are far greater than for a company being caught attempting to acquire some proprietary technological secrets.

Should multinational corporations use direct tactics (rather than a government doing so), they would find themselves *persona non grata* in most countries in the world—at least in the Third World. Corporations, under international law, do not have the status or prerogatives of a nation state. Diplomatic representatives are protected persons; corporate

executives are not. Under certain circumstances, nations may use unilateral force to gain redress or even preempt the actions of another; corporations may not legally do so. The corporation and the CEO might also be subject to prosecution in its home country. It is not that the capacity to act does not exist, nor, for that matter, that the will to act does not exist. They can hire expertise if they do not want to act themselves, but they are not foolish. It is the ultimate stake which must be assessed. They understand the risks, and those risks, unless it is a life or death situation for the corporation, are simply too large under the contemporary international legal regimen.

The precarious position of corporate entities in the world system is a direct function of the fact that nation states are still the principal elements of an international framework. Nation states have arrogated power to themselves in the same way that kings and other players in the feudal system pre-dating the evolution of an international system did. They have also decided that the rules of the game (laws) are to apply so as to maintain their position and privilege, which they construe as a right, in the same way as kings had legitimized and enforced their status. It is more possible to believe in the divine right of nations that it is possible to believe in the divine right of kings. But it is possible, indeed, realistically necessary, to believe in power. Power has its privileges, usually constrained somewhat by territoriality. However, it is the system which defines legality, morality and ethics, and not necessarily in a purely rational or equitable manner.

Non-state actors such as organized religion, from the Roman Catholic to the Unification churches, have a corporate structure, as do other non-state entities. The PLO has a reputed treasury (the Palestine National Fund) of over $5 billion US, invests in Western Europe and the U.S. through "shell" companies in Luxembourg and Lichtenstein, 'washes' Saudi Arabian and Kuwaiti petrodollars through accounts in Switzerland, West Germany and Latin America, and amasses its wealth by some fair means and some very foul ones indeed. Its revenues pay for administration, purchase of supplies, social services and retirement benefits.[64] International labour unions have similar concerns—outside of fielding paramilitary forces and purchasing sophisticated arms—even in the bad old days of the Teamsters' and Longshoremen's unions.

The head of the PLO, however, can stride into the United Nations General Assembly with a loaded sidearm, declare his, and his organization's, intention to use lethal armed force in pursuit of their objectives and be greeted by thunderous ovation and the conferral of tacit legality for such acts. No labour leader, church leader, or corporate CEO would be treated thusly, overtly or covertly. It would be an occasion for shock, dismay, consternation, and vilification, not jubilation and adoration.

Those fixated on the nation state, therefore, are bound to see MNCs as non-state actors having only privileges accorded at the discretion of the principal players in the international system and not as forces in a world system with objectives whose legitimacy nation states need not

ratify because they are effective anyway. They are bound to ask: "Who gave them the right to defend themselves?" The answer must perforce be that MNCs have as much a natural right to self-defense, including preemption, as nations who created themselves and a self-serving system.

There is also a perception that seizure of the initiative, that is, a proactive posture, must be defined as if it were a sovereign prerogative. Both for national governments and for multinational corporations, proactive counter-terrorism does *not* mean the use of armed and/or lethal force. That view and the imposed definition which supports it are formal, arbitrary and incorrect. Semantic arguments as to what constitutes passive or active defense and reactive or proactive measures are sterile and counterproductive exercises. There is no desire or intent to engage in such activity here or anywhere else. However, operational examples are appropriate and in order.

The emplacement of fixed warning or physical restraint devices, such as chain link fences, vehicular barriers, alarm systems and similar devices are passive defenses, which, like structural hardening of facilities, may not necessarily require or even have human monitoring as a complement. Active defense includes: K-9 presence; mobile human monitoring of site perimeters by vehicular or foot patrol; the installation and operation of electronic surveillance countermeasures, personal identification security systems, and physical computer security defenses, such as restricted access to sensitive areas. In the event there is the potential for sophisticated attack and a considerable level of technical expertise has been demonstrated by terrorists or others, internal and external computational/communications interfaces (critical nodes) protection which seeks to defend the integrity of systems logic would be considered an active defense.

Many defense mechanisms, such as pre-departure briefing, would also be viewed as reactive in a practical setting and the situational response, in the specific locale and under the prevailing corporate security conditions, would define how it might be construed. Some industries and economic sectors—for example, oil or resource exploration and extraction—have vulnerabilities which are recurrent and global, given their particular activity; other corporation are faced with more site-specific threats. Assuming relatively little previous coverage, the hiring of a host country security force or contracting with domestic security force companies, a booming business in many high-risk countries, would be reactive in the face of threat advisories, as would requests for coverage from local host country police. These may also be construed as active defense.

More patently reactive postures are withdrawal of expatriate managers and staff, closure of operations, the institution of crisis management teams (also, in some contexts, active defense) for the country operation, the area, division, or corporate-wide. The initiation or expansion of cooperation with the host country government security apparatus could likewise be perceived as either active defense or reactive, depending upon whether it was generated by preventive concern or prompted by an actual incident. The offer of rewards for information

resulting in the capture and conviction of terrorists, linked in some way to their ransom demands, would be reactive or perhaps proactive.

Proactive options include, but are not limited to:

— Recruitment and maintenance of cadres of expert advisors and trainers skilled in the political and security aspects of unconventional conflict;

— Training of in-house special operations (counter-terrorism) forces, when permissible by the host country;

— A policy, in high-risk venues, of misinformation, disinformation and deception;[65]

— Psychological warfare campaigns against terrorist elements, expecially when host country penetration of a group can be achieved after surveillance, or "turning" of an apprehended member, or enlistment of an authentic, willing defector;

— Intervention and interference with terrorist group infrastructure, communications and intelligence flow, where and when they can be identified;

— Payment of gratuities for information and assistance from various host country sources, which in many countries is the only way to get anything done, even of a pedestrian nature.

It must be stated here in the strongest terms that these and other measures are not being counselled *per se*. Nevertheless, realistically they are or can be employed and, except for the aberrant recourse to paramilitary forces or assassination, governments and other non-state entities utilize these options as part of an available spectrum of measures. Low-intensity warfare does not mean that armed or lethal force is a mandatory element or that it is the only alternative for counter-terrorism. One of the most potentially effective mechanisms, in fact, is a non-violent one: propaganda, which is not a dirty word, and use of the media.

"Terrorist groups have shown great skill in dealing with the media" and their outrages are "likely to attract considerable press and television attention,"[66] regardless of what any government does. However, MNCs in host country settings have a prototype model to examine which should have been better used for longitudinal proactive effect instead of having been an exemplar of reactive posture. A brief summary of that event is instructive. The Argimiro Gabaldon Revolutionary Command presented documents to the Venezuelan press following the kidnapping in February 1976 of the Owens-Illinois subsidiary President, William Niehous.[67] They made it mandatory, as part of their many demands, that a manifesto be issued by the company as one of the basic conditions for his release. The Venezuelan Government blacked out domestic media coverage but the firm complied and on 6 April 1976 a half-page proclamation, "To the People of Venezuela" was published in the *New York Times* (p. 59, col. 1), *The Times* (London) and *Le Monde*.

The purported "proofs" presented to the domestic media of terrorist allegations that Owens-Illinois was guilty of political interference

and economic administrative meddling involving acts of bribery and embezzlement were really rather mundane and not very incriminating at all. In fact, of the 22 photographs of company telexes, memorandums and business reports, some had been unsophisticatedly falsified. The terrorists' use of the media was countered by Owens-Illinois and the Niehous family. *El Nacional* (Venezuela) printed five pieces in 1976 airing their views: 13 March, p. D16; 17 March, pp. 14-16; 25 March, p. D20; 30 March, pp. D13 and D16; and 7 April, p. A1. The seizure of the initiative was designed to undercut the terrorists' position and public image.

If only a portion of the monies MNCs paid since then in ransom and security-related expenditures had been spent on continuing radio and television campaigns (far more effective than newspapers in host countries with low literacy levels), to undermine the appeal, the legitimacy, veracity and validity of terrorist claims and allegations, there is reason to believe that terrorists' play to public support and the vindication of their acts by the invariable projection of a 'Robin Hood' image would be appreciably weaker. Rather than deny them publicity as a means of depriving terrorists of their visibility, recognition, and implied legitimacy, even respectability, it may well be more appropriate to turn the tables on them and give them all the bad publicity they deserve, cumulatively building a sense of mass repugnance for their brutality, amorality, cynicism, hypocrisy and implacable hatred.

Proactive options of an unarmed, non-lethal nature do exist for governments and corporations, but they will not instantaneously and conveniently destroy terrorism nor many terrorist groups. Hence, the battle with terrorism will be a fact of life, and death, for some time into the future. It is, and will be, a source of constant concern to those nations who prize freedom and refuse to acquiesce to political gangsterism. It is, and will be, a continuing threat to the operations of international business. The initial issue, therefore, is the primary requirement for an adequate corporate intelligence function for their tactical defense and for policy formulation and strategic planning purposes in a global geopolitical context. There is a further need for proactive counter-terrorist assets, informational and operational.

As the present mode of the inter*national* institutions would have it, and in recognition of the at times convoluted and questionable legal, moral and ethical dissonances involving nations and non-state actors, the risks of engaging in some types of activities are obviously substantial. However, risks are what business is used to and the possibility of catastrophic events, as well as their prevention or mitigation, are what geopolitics are all about. Passive as well as active anti- and counter-terrorism options must be explored because the opposition is playing for keeps; this is not a computer simulation.

CONCLUSIONS

A research agenda on terrorism and MNCs should establish clearly the geopolitical context of multinational corporate activities, the nature

of MNCs as non-state actors in global affairs and the commensurate status of terrorism as a non-state and/or state activity, with both dynamics having interactive tactical and strategic properties. Exploring a broad range of potential proactive options could result in additional operational tools for corporations dealing with a high-risk global environment and induce as well substantial revision of organizational self-image and corporate planning and policy practices. Strategic and intelligence considerations more appropriate to the practical essence of MNCs would be duly recognized as a consequence.

The development of a conceptual framework comprehending the dynamics of MNC/geopolitical interaction and examination of its policy implications should be conducted as part of an ongoing consultative process with an extensive range of academically-based as well as operational sources in the linked fields of specialization. However, there is no body of literature to provide policy guidance on the interactive linkage of intelligence-terrorism-covert conflict-global corporate operations-security studies because the articulated concept has not been advanced before. What currently exists is a spectrum of compartmentalized literatures, some large, some small, with, in most cases, little attempt to relate concerns which are operationally as well as conceptually entwined in the real world.

The scientific method and academic discipline are highly distortive mechanisms. This derives in major part from the extremely strong cultural proclivity, conditioned as Western industrial societies are to the philosophy of knowledge, to set up artificial boundaries in the way that information is classified, coded, and stored. This tendency also modifies and constrains perception and learning processes. Because Western societies are not prepared to accept a philosophy of action as "frame-of-appreciation,"[68] they reject terrorist perspectives as logically alien and irrational, a mistake that can be fatal. An important priority of subsequent work, therefore, should be a baseline bibliography that provides the means for addressing resources in an operationally interrelated way rather than according to currently favoured conventional, compartmentalized frames-of-reference. This will facilitate the rigorous evaluation of policy in the new era of active posture by MNCs towards global terrorism.

International relations specialists still have not been willing to come to terms with the realities of MNCs as non-state actors on the global stage whose objectives and behaviour are every bit as significant as that of nation states. As a result, their analysis proceeds along traditional lines of defining "national interests" as the basic dynamic of global interaction. The first priority is to acknowledge that international business is not a little like war, it *is* war, and thereby makes global enterprise vulnerable to all the risks of geopolitical conflict and paramilitary engagement faced by nation states, without the prerogative for the forceful means of conflict resolution available to national entities.[69] Until there is greater formal recognition of the role non-state actors play in the global system, and a corresponding accommodation by nation states to

this power, the world legal framework will not appreciably alter. Its apparent and growing perversities will remain characteristic of an increasingly anachronistic system. For a time, at any rate, intermediation by global corporations in their operating environment will be through the mechanisms of business diplomacy and risk assessment intelligence, geared to specific organizational needs.

Endnotes

1. Unofficial record, Overseas Security Advisory Council (23 January 1986), p. 4. Status report to Secretary of State Shultz by Joseph R. Rosetti, Director of Security, IBM Corporation.
2. In these experiences, corporate and regional offices were removed to neighboring countries (Rio de Janiero and Sao Paulo, Brazil), back to the United States (Coral Gables, Florida), or completely overseas (Madrid, Spain). There are additional economic and political aspects to the decision to leave in many cases, as well as the specific sensitivity of individual enterprises to terrorist activity and the threat of terrorism.
3. Within a matter of 10 days after the ambush of John Swint, the Ford parts' subsidiary General Manager in Argentina, 25 executives of the company and their families left the country. Staff. U.S. House of Representatives. Committee on Internal Security. "Study on Terrorism". Washington, D.C., 1974 (Committee print, pp. 14-15).
4. Each of them is familiar to me and deemed technically reliable (co-author Jesse Goldstaub).
5. Data from Office of the Ambassador-at-Large for Counter-terrorism, U.S. State Department, and Director of Research, Risks International, February 1988. Comprehensive figures are framed on a calendar year basis and revisions proceed well into the early part of the new year.
6. Business Risks International coding criteria.
7. Figures released to JG by BRI in March 1988.
8. As noted, because of the capability of recording multiple victims and/or installations attacked, yearly total attack (event) figures marginally exceed incident totals. However, comparisons within any classification remain completely valid.
9. Benjamin Netanyahu, ed., *Terrorism: How the West Can Win* (New York: Farrar, Straus and Giroux, 1986), p. 3.
10. John W. Amos II and Russell H.S. Stolfi, "Controlling International Terrorism: Alternatives Palatable and Unpalatable," *Annals of the American Academy of Political and Social Sciences,* 463 (1982), p. 71.
11. Paul Wilkinson, *Political Terrorism* (London: Macmillan Press, 1974), p. 144; and, especially, Alex Peter Schmid and Janny de Graaf, *Violence as Communication: Insurgent Terrorism and the Western News Media* (Beverly Hills: Sage, 1982).
12. W.M. Landes, "An Economic Study of U.S. Aircraft Hijackings, 1961-1976," *Journal of Law and Economics,* 21 (1978), p. 26.
13. For an extensive study of networking, see Clair Sterling, *The Terror Network* (New York: Berkeley Books, 1981).

14. Paul Wilkinson, *Political Terrorism,* p. 145.
15. Christopher Dobson and Ronald Payne, *Counterattack: The West's Battle Against the Terrorists* (New York: Facts on File, Inc., 1982), p. xiii.
16. It could be suggested that an empirical basis should be specified for this hypothesis about MNCs. However, as will become apparent, the argument to follow focuses on the rational expectations and potential responses of corporate entities. Since terrorism is unlikely to be checked effectively by Western governments, its attendant costs are expected to increase and create the need for alternative measures. Thus the hypothesis about a more active posture by MNCs has a primarily logical, as opposed to empirical, basis.
17. Mancur Olson, *The Logic of Collective Action* (Cambridge: Harvard University Press, 1965), p. 11.
18. Consider Japan or the United States as potential unilateral actors. Benefits produced are distributed to all of the Western states in the form of a safer operating environment for MNCs. The concentration of MNCs identified with these states may not necessarily increase over time because of the rise of newly industrializing country (NIC) enterprises and continued impetus towards joint ventures, which beclouds the true "home" country. Thus, the incentive to "go it alone" is, if anything, likely to decrease.
19. Grant Wardlaw, *Political Terrorism: Theory, Tactics, and Countermeasures* (London: Cambridge University Press, 1982), p. 77; and John O'Sullivan, "Deny Them Publicity," in Netanyahu, *Terrorism*, p. 121.
20. Charles Krauthammer, "Terrorism and the Media: A Symposium," in Netanyahu, *Terrorism* p. 238.
21. Grant Wardlaw, *Political Terrorism,* p. 105.
22. Grant Wardlaw, *Political Terrorism,* p. 110.
23. Frank Brenchley, "The Terrorist Menace," *Conflict Bulletin* (1985), p. 4.
24. Mancur Olson and Richard Zeckhauser, "An Economic Theory of Alliances," *Review of Economics and Statistics,* 48 (1966), pp. 266-279.
25. Jesse Goldstaub, "Intelligence and Analysis for Global Enterprise," Jerusalem: The Hebrew University School of Business Administration, 1984, Part VI, p. 21.
26. Jesse Goldstaub, "Intelligence and Analysis . . .," Part VI, p. 26.
27. Jesse Goldstaub, "Terrorism Against Multinational Corporations: The Role of 'Company' Intelligence," Washington, D.C.: The Johns Hopkins University, School of Advanced International Studies, 1986, p. 83.
28. Charles H. Russell, James R. Schenkel, and James A. Miller, "Urban Guerrillas in Argentina: A Select Bibliography," *Latin American Research Review,* 9 (Fall 1974), p. 89.
29. Risks International, "Terrorism in 1986," Alexandria, VA, May 1987, p. 1.
30. In the event becoming a kidnap victim cannot be avoided, the company nearly always pays. It cannot afford not to. You can ask a man to die for his country but not his company. Ransom insurance is available from Lloyds, Federal Insurance, American International Group and a number of other private carriers.
31. E.J. Dionne, Jr., "Americans in Europe Lie Low," *New York Times,* 28 April 1986, pp. A1 and A7. This sense of trepidation is often referred to in corporate and diplomatic jargon as the "comfort level." Terrorists have been targeting business leaders and corporate officers in Europe for years, and successfully at that.
32. Agis Salpukas, "Working Abroad in Terror's Shadow," *New York Times,* 13 April 1986, pp. 1F and 8F.
33. Technological advances in weaponry of all sorts are as much an active interest of terrorists and their various sponsors as of governments and their military establishments. There is an open international market for hardware of unlimited variety and buyers are not always required to prove their legitimacy or respectability, just their solvency.
34. Verbatum quote from pact jointly signed by Direct Action and the Red Army Faction dated 15 January 1985, directive, p. 4. Professional killers planted by East European

and Arab Secret Services are thought to be implicated in attacks on NATO. What surprised the authorities was the ideological coherence, international coordination, and unrestricted commitment to violence of these new actions. The terrorism of the 1970s appeared to be directed at producing social destablization in each individual country in which attacks occurred. Current terrorist group activity in West Europe seems aimed at undermining the entire notion of collective defense with the U.S.

35. Risks International, "Terrorism in 1986," p. 4.
36. Risks International, "Terrorism in 1986," p. 1.
37. Risk-reduction instruments include insurance coverage for not only kidnap and ransom but for currency inconvertibility, expropriation, political violence (war, revolution, insurrection and civil strife). Terrorism is included in this latter context as well as in business income coverage (BIC), wherein attack damage to the facilities of the insured company and damage to facilities other than that of the insured—such as critical physical infrastructure in the host country—results in interruption or cessation of income flow. The Overseas Private Investment Corporation (OPIC) in the U.S., the world's second largest government-sponsored political risk insurance organization, offers the broadest coverage spectrum; Japan's Export Insurance Division (EID) of the Ministry of International Trade (MITI) is the largest entity, but extends narrower coverage. There are similar counterpart units in Germany, France, and the UK. A smaller Canadian unit, Export Development Corporation, also created under government auspices, allows political risk insurance to be acquired either complimentary to loan transactions or independently for other than direct investment projects. They do in-house country risk analyses, but subscribe as well to the popular commercial service of Frost and Sullivan. Multilateral Investment Guarantee Association (MIGA) at World Bank is another small facility for some types of risk coverage.
38. Pre-entry/pre-departure and on-site/in-country briefings are provided by firms such as Control Risks, Ackerman and Palumbo, Parvis Co., and the Fairfax Group. Anti-terrorist training is offered by a burgeoning number of private sector consultancy organizations. Paladin Security (London, England) is an illustrative example of the services package. The course covers five days of intensive training and is residential. Its objective is to develop psychological resilience to crisis, preparing the course participant to deal with threats to personal security posed by terrorist activity and other forms of violence. The training encompasses: close quarter fighting; weapons familiarity; knowledge of terrorist methods and their motives; escape and evasion; coping with captivity; dealing with assailants, intruders, and captors; and preventive measures.
39. The ability of an intelligence officer to relate to the consumers of his product, and share their frame of reference and liguistic terminology, may be *the* crucial element in his personal acceptability to the line command structure, as well as the acceptability of the information and analyses produced. I am indebted to Maj. Gen. Aharon Yariv, former Chief of Israeli Military Intelligence, for these and many other insights. The rapidity of metamorphoses in corporate security administration has been confirmed by the heads of two units involved with private sector security at U.S. State Department, and Lawrence Sulc, The Hale Foundation (JG).
40. The release of U.S. State Department, "Crisis Management Guidelines," Washington, D.C.: Bureau of Diplomatic Security, Overseas Security Advisory Council (OSAC), December 1986, resulted in massive corporate oversubscription. Private sector mentors in the art of establishing, training and maintaining crisis management teams are available; one of the most notable being Control Risks, which uses simulation exercises as a training medium. Some firms will negotiate hostage situations for their corporate clients.
41. Ehud Sprinzak, commentary in SRI International, *International Terrorism: The Threat to Industry*, conference report, January 1986, proprietary edition, p. 52.
42. See Yehezkel Dror, "Policy Gambling: A Preliminary Exploration," *Policy Studies Journal*, 12 no. 1 (1983), pp. 9-13; and Dror, Workshop in Advanced Policy Analysis: Policy Making as Fuzzy Gambling. APSA Short Course (notes), Washington, D.C., 29 August 1984.
43. When alluding to organizational intelligence, we are not dealing with industrial espionage, that is, getting someone else's trade secrets. That transpires recurrently, of

course; the most celebrated case recently having been the Japanese attempt at securing IBM technology information. They made the worst possible mistake. They got caught. Perhaps the worst mistake so far as U.S. or Canadian entities are concerned, is having it known, not getting caught. This is so because of the legal, nor moral, strictures that surround the business intelligence function.

44. E.g., David A. Jodice, comp., *Political Risk Assessment: An Annotated Bibliography* (Westport, Connecticut: Greenwood Press, 1985), initial overview section, extolling the virtues of econometric-type modeling and its purportedly predictive elegance. A somewhat more common sense tack is taken in David M. Raddock, ed., *Assessing Political Risk: A Guide for International Businessmen* (Totawa, New Jersey: Rowman and Littlefield, 1986). Compare Thomas L. Brewer, ed., *Political Risks in International Business: New Directions for Research, Management and Public Policy* (New York: Praeger, 1985). *Euromoney* has been doing ongoing country risk analysis since the early 1980s.
45. Coverage beyond the standard subscription analysis is available from some organizations but is always costly.
46. See Richards J. Heuer, Jr., ed., *Quantitative Approaches to Political Intelligence: The CIA Experience* (Boulder: Westview, 1978).
47. For a penetrating analysis of why the Iranian episode was supposedly so much of a surprise, see Michael Handel, "Avoiding Surprise: The Role of Closed Concepts," in Roy Godson, ed., *Intelligence Requirements for the 1980s: Analysis and Estimates,* Vol. 2. (Washington, D.C.: National Strategy Information Center, 1980), pp. 95-98.
48. Those who would like to be instant intelligence aficionados might deal with the Bowen Collection (now approximately 6,000 items) as a starter kit. Marjorie W. Cline, *et al.,* eds., *Scholar's Guide to Intelligence Literature* (Lanham, Maryland: University Press of America, 1983).
49. In some PRA approaches, a multiplicity of concerns are almost forcibly quantified, weighted and homogenized, resulting in a number, a change in which is deemed to be significant. Business Environment Risk Information is still wed to this methodology based on a modified Delphi technique employing expert consultants. Experts, however, are not without their shortcomings nor can a great deal of confidence be accorded any procedure incorporating their inputs. For the most part, the index number meant little and was considered by CEOs with line-management mindset and very limited patience for what they viewed as pseudo-scientific nonsense, not to be worth their time. Such PRA products are now used in the same way that external inputs from other subscription advisory firms are used, as a confirmation mechanism for more acceptable individual consultation with security intelligence agencies of the national government.
50. It is interesting that Chevron facilities were bombed by anti-communist Angolan rebels on 25 March 1986.
51. If the collector is a Swiss, for instance, that is not a problem. If the collection agent is an American, such inhibitions as the Foreign Corrupt Practices Act may impinge on the process. For this and other operational reasons, which cannot be openly explored, MNCs, especially those U.S.-based, will not acknowledged the existence of their intelligence services.
52. Overseas Security Advisory Council (OSAC), U.S. State Department, was originally chartered in December 1964 and began operation in 1985. Its mandate renewal in December 1986 expanded the scope of services. This joint venture with the U.S. private sector is a formal link for sharing current information on mutual security problems. 750 firms are now on OSAC's mailing list. A worldwide computerized electronic bulletin board is scheduled to come on-line in Summer 1988 to provide up-to-the-minute threat alerts. Direct consultations have been expanded as well through the mechanism of mini-council in major overseas centers.
53. Refer to J. Quincy Hunsicker, "The Malaise of Strategic Planning," *Management Review,* 69 (March 1980), pp. 9-14.
54. The intrinsic symbiosis between intelligence and academia is depicted in Ray S. Cline, *Secrets, Spies and Scholars: Blueprint of the Essential CIA* (Washington, D.C.: Acropolis Books, 1976); and, more recently, in Robin W. Winks, *Cloak and Gown* (New York: William Morrow, 1987).

55. For the operational role of the USSR in the global network, one of the clearest pieces of documentation is Ray S. Cline and Yonah Alexander, *Terrorism: The Soviet Connection* (New York: Crane-Russak, 1984). The network encompasses many strange bedfellows, however. C.f. Thomas L. Friedman, "Loose-Linked Network of Terror: Separate Acts, Ideological Bonds, *New York Times,* 28 April 1986, pp. A1 and A6. This world-wide network is interlocked because of its collective animosity to the West and its intent; and it is effective even without de facto coordination from a central source or ad hoc cooperative ventures by sponsoring terrorist states or major groups being assumed.
56. Dan Oberdorfer, "Security Fears Spur Embassy-Building Program," *Washington Post,* 2 March 1985, p. 11.
57. The Advisory Panel on Overseas Security (the Inman Commission) estimated in 1986 that improvement for State Department security at overseas installations would cost $4.2 billion over 5 years.
58. The attack on Italy's Motor Vehicle Ministry computers was so disabling that it took two years for the Government to reconstruct its records.
59. Augusti Bequai, "High-Tech Terrorism and Computer Security," *Washington Times,* 18 February 1985, p. 3D.
60. Donn B. Parker, "The Threat to Information Systems" in *International Terrorism: The Threat to Industry,* SRI International Conference Report, January 1986, proprietary edition, p. 66.
61. The Pentagon's computers were entered and a portion of the data stored there erased by a ninth-grade student hacker with a $250 Atari-400. Augusti Bequai, *loc. cit.*
62. NASA's global network was broken into using a 'trojan horse' program. At least twenty of the computers in the 1600 computer network were regularly intruded into between May and September 1987, its users' electronic mail read, daily space shuttle program updates obtained, and NASA memos on how to deal with the media perused. The West German hackers, members of a Hamburg youth computer club, could have paralyzed the entire network but did not, being satisfied to show the "unbelievable weaknesses" of the flawed security system, which allowed them to obtain information on space shuttle projects and rocket failures. Both ARD Television and *der Stern* reported similar coverage and it was then picked up by Associated Press and Reuter, appearing in *Globe and Mail* (Toronto), 16 Sept. 1987, pp. 1-2.
63. Warren H. Metzner, Corporate Security Manager, EXXON, commenting in SRI International Conference Report, "State Sponsored Terrorism: The Threat and Possible Countermeasures," Washington, D.C., 1985, p. 85.
64. See the very thorough coverage of PLO structure and resources in James Adams, *The Financing of Terror* (New York: Simon & Shuster, 1986); and Thomas Naylor, *Hot Money and the Politics of Debt* (Toronto: McClelland and Stewart, 1987), especially pp. 245 ff.
65. One day action against terrorists may have to be justified on the basis of undisclosed intelligence documentation. Since truth is largely a matter of perception, being perceived as credible is a critical asset. Credibility must therefore be protected in order to successfully carry out a counter-terrorist action without disclosure and compromise of sources and methods (S&M) of intelligence. Hence, deliberate deceptions may in the long run do more damage to the originator than the target.
66. Deputy U.S. Secretary of State John C. Whitehead, address before the Brookings Institution, Washington, D.C., 10 December 1986.
67. A report of his three-year ordeal and June 1979 rescue: William Niehous, "How to Survive as Hostage," in *Diplomats and Terrorists: What Works, What Doesn't* (Washington, D.C.: Institute for the Study of Diplomacy, Georgetown University School of Foreign Service, 1982) pp. 33-36.
68. This astute and useful concept was coined by Yehezkel Dror in " 'Gambling with History,' However Unpleasant, is Normal to the Human Condition," *Technological Forecasting and Social Change,* 29 (Feb. 1986), p. 78.
69. Article 51 of the U.N. Charter explicitly allows the right of self-defense to nation states.