Research on Humanities and Social Sciences
ISSN (Paper)2224-5766 ISSN (Online)2225-0484 (Online)
Vol.6, No.16, 2016

Resilience Planning for Terrorism, An Emerging 21st Century Malicious Risk

Dunama Wazis Bsc, Msc
Dako District Abuja

Abstract

In this paper, the development of resilience to terror attacks and there consequences has been presented in terms of use of public-private partnerships in all phases of the incident lifecycle and management protocol following a terror attack. It is clear that the best and most effective strategy for all countries is the recognition and understanding of the changing aspects of new age terrorism. The most important aspects are carrying risk assessment and implementing preventive strategies at national and international level with the help of public-private partnerships or collaboration. This is because it can be recommended that the most effective stage of a terrorist act is the prevention stage since the moment this is crossed then it becomes a disaster. As such, the best way of tackling this emerging 21st century malicious risk is strong prevention strategies involving all the relevant stakeholders on both the international and national level.

Keywords: counterterrorism, resilience planning, impacts of terrorism, terror attacks, 21st century malicious risk, disaster management

Introduction

A number of conventional as well as unconventional malicious 21st century risks have been observed in the two decades. The world has experienced many catastrophic, large-scale disasters as well as events that have had very serious direct as well as in direct consequences on human lives as well as critical infrastructure. Amongst unconventional disasters, acts of terrorism have become one of the major 21st century, important malicious risks. Due to the newly emerging forms of terrorism, it is difficult to give this term a clear definition or continue to use traditionally given ones for it. One of the new definitions given by the Council of Europe has made use of significantly better terminology by considering an act of terrorism to include any offense done by a single person or group of persons that resort to the use of violence or threaten to utilize violence against any nation and its people, existing institutions, issue threats against any specific individual (all being driven by separatist goals and ambitions, extreme ideology notions, fanaticism or illogical and subjective reasons) with the intention of creating an atmosphere of terror among the authorities, targeted individuals or all section of the society in which the targeted individuals or groups or the general population exist (Dumitriu, 2004; OECD, 2003). The 21st century began with several catastrophic, large-scale disasters in the form of terror attacks like those of 11th September 2001 in USA and the Sarin gas incident that took place in Japan. These resulted in countless human fatalities, injuries as well as major damage to critical infrastructure. It is necessary for all the concerns stakeholders will play a part in the development of human resilience of the words the race can impact of nonconventional disasters like terror attacks.

For the last two or three decades, a lot of theoretical as well as practical research and initiatives on the development of resilience in humans has highlighted several informative lessons and best practices which can be used for planning future disaster response and recovery strategies for terror based incidents. As for the existing development theories, resilience in the wake of any disaster usually happens in different forms that include resistance to stress, physical, mental as well as social recovery and positive changes for handling future disasters. Evidence based data from a lot of research indicates that fundamental adaptive systems have a major part to play in the development of resilience in young individuals exposed to different kinds of threats which included attachment, agency, intelligence, behavior regulation systems combined with social interactions within families, with their peers, in educational or community-based systems. Even though human resilience research has brought focus on the adaptive well-being of specific populations of people, there still exist important parallels within resilience theories that span over development and ecological fields of study. The preparedness of a society to respond to any main disaster requires integrating knowledge on human resilience with knowledge obtained in other fields related to the development of resilience. This is inclusive of particular systems, which have major interactions with individuals before the disaster strikes, while it unfolds and attending to its impact in the recovery phase (Masten, and Obradovic, 2008).

The impacts of disasters also have a huge financial cost that is inclusive of the direct costs and indirect costs in terms of economic, infrastructural and environmental losses that resulted. With the continuous rise in terror attacks, there is a need for increased cooperation between the private and public sector on a national as well as international level. Relevant stakeholders such as emergency managers, business continuity specialists, crisis management executives, incident management experts, security staff and policy makers need to work in conjunction with researchers both academic-oriented and industry-based. There is need to implement changes in all steps of the incident lifecycle and management protocol to provide adaptive systems in required fields that can build resilience. If the best practices and recommendations from the lessons learnt are highlighted, then preventive efforts and resilience towards terror attacks can be successful and can be helpful in the recovery phase also. In the last two decades, the nature of terror attacks is shifting from the traditional to more non-conventional types of attacks that require changes in assessment, prevention or mitigation initiatives, preparedness, response measures and recovery efforts (Masten, and Obradovic, 2008; OECD, 2003).

In this paper, the lessons learnt from the ongoing research on development of human resilience and the needed steps for promoting combined resilience-oriented planning towards disaster response as well as recovery processes have been presented from an extensive secondary research.

Changes Needed In The Incident Lifecycle and Management Protocol

Anticipation and Assessment Phase Systems:

Terrorism has changed in the last decade even though the old form of terror continues. In order to promote resilience against it, stakeholders need to carry out analysis of the impact and implications of the latest emerging forms of terror attacks in order to be able to do any accurate risk assessment and anticipation studies. Terrorism incidents can be anticipated and assessed by four features that they have in common including the goal, the targets, the identity of those that sponsor it with those that carry it out and last of all the means used to carry out the act itself (OECD, 2002). Using these four features, it has been assessed that many of the recently done terrorism events acts are different from previously done one. One example is the USA 9/11 attacks on the twin towers of the World Trade Centre, which is quite separate from previous terrorist activities like plane hijacks (OECD, 2003; Adey and Anderson, 2012). Resilience can be enhanced by development of private-public anticipation technologies that can be used enacted through laws as legal and used as part of the traditional resilience assessment done in security measures. A good example of this is seen in the implementation of security measure in UK's Civil Contingencies and civil protection laws as well as practices (Adey and Anderson, 2012). In the past, the main aim of terrorism used to be national liberation and it had clear political goals in the country where it took place. The new kind of terrorism that exists today is quite different since the main goal here is continuous opposition of the entire Western system of economics, politics, culture and society. Due to this the new breed of terrorism is global in nature and crosses international boundaries (OECD, 2003; Coaffee, 2009).

The emerging kind of new terror attacks is designed to kill as many civilians as possible with the maximum number of injuries as well as damage to critical infrastructure (Sandler, 2002). The targets include all public places that have high crowd concentrations like metro stations, shopping malls, mass gatherings and large-scale buildings that may house critical infrastructure. Locations that have hazardous installations like nuclear power generation facilities or dams are possible targets since they present massive catastrophic potential. New age terrorism is known to take advantage of the dependence which present day society has on critical infrastructures like electricity, water, transportation, public Health Care Systems, financial hubs and information technology as well as communication media. Terror attacks, which damaged these systems usually, cause significant amount of harm in terms of human lives, damage to critical infrastructure and economic costs. As such the security of such systems has to be accordingly enhanced to provide resilience in the future (Michel - Kerjan, 2003).

Terror groups now operate using organized networks of smaller size that are dispersed but coordinated since they are able to give the advantage of very catastrophic incidents at minimal cost with the global publicity and no public knowledge in case of failure. As such, governments have to make collaborations with the private sector for the development of specified communications strategies that report failed attacks (Comfort, 2002; OECD, 2003; Kapucu, 2006).

The agents of conventional terrorism were well- organized extremist militia groups sponsored by political players. New age terrorism is no longer localized and because of the relative ease in obtaining material or knowledge for creating weapons, terror groups no longer need large amounts of funds, technology or a logistics. Risk assessment for these kinds of disasters also needs to take into account the changes in the ideology spectrum of terrorist groups. In the past, this ideology used to consist of extremist left doctrines or ethnicism while at present it mainly consists of religious fundamentalism and many other types of fanaticism (Weber, McEntire and Robinson, 2002; OECD, 2003; Hoffman, 2001).

The means through which most of all of the recent terrorism incidents were carried out included traditional means like explosives or advanced gunfire but there is now the real threat of the use of non-conventional means like bio agents, chemical weaponry or nuclear agents. The government and public sectors have to ensure that accessibility to such means is a highly secure and limited (Post, Sprinzak and Denny, 2003; OECD, 2003).

Prevention Phase Systems:

Prevention measures to combat terror acts have to be of different types since various organizations may make use of different means to achieve their aims. In a majority of scenarios, the terrorist threat is that the controlled in the early stages prior to the gathering of all the resources required sense in the late stages it becomes a full blown attack that only needs a response and recovery efforts. As such all preventive measures for this kind of malicious risk preventive strategies designed with the aim of preventing terror attacks need the involvement of both the public and private sector. The basic preventive measures have to include addressing the root causes such as ignorance or in certain cases factors like injustice or political exclusion. This has to be followed by systemic and coordinated measures for dismantling the funding and supporting infrastructures of the group, while exercising control over accessibility of critical information or material. Preventive strategies also need to educate vulnerable sections like the youth and discourage their association with terror outfits. Preventive strategies also need to find ways of weakening the support systems of terrorism and imposition of strict sanctions against governments or organizations that act as sponsors of terrorism (OECD, 2003; Paraskevas and Arendell, 2007; Stewart, Kolluru and Smith, 2009).

Improvement in the coordination of surveillance, security alerts and early detection is important as a preventive measure as well as an important factor in preparedness. Since most of the new kind of terrorist acts precede using precursor signals, cooperative and improve collection systems of intelligence and communication of obtained data between international agencies, government says unless the private and public sector are vital. Efficient systems of surveillance before the start of an attack as well as early warning Communications Systems provide a secondary level of mitigation and protection. The lessons learned from previous catastrophic level terror acts have consistently demonstrated that lapses in surveillance and early warning communications need serious improvement through higher levels of coordinated efforts between international, national and local stakeholders and the resources of the private sector enterprises Paraskevas and Arendell, 2007; Stewart, Kolluru and Smith, 2009).

Enhancement of preventives measures via partnerships between the private-public sectors are a powerful tool that can help in mitigating terrorism risks. At present such initiatives continue to remain underutilized because of the failure of governments to provide effective incentives and resources. The development of science and technology in this field has continued to remain view of the limitations posed on its commercialization. As such the use of research and development for many potential kinds of technology that could prove useful in this area is lagging behind even though it could have been making available significant protection against terrorism's capability for destruction. Certain governments have started the utilize of public-private partnerships that function at the basis of incentives. A very good example is the Canadian government that has provided a lot of resources to the CBRN (Chemical-Biological-Radiological-Nuclear) Research and Technology Initiative that is involved in the scientific and technological development of counter-terrorism programs that help in creating partnerships between the industrial sector, government organizations and the academic field (Norris et al, 2008; OECD, 2003; Paraskevas and Arendell, 2007; Stewart, Kolluru and Smith, 2009).

Preparedness Phase Systems:

Improved levels of the preparedness in terms of better emergency response systems, improved level of public awareness and preparation are known to increase the level of community, social as well as mental resilience and the resilience of critical infrastructures. The reality today is that the interdependence, which most systems have on each other serves in highlighting the risk due to terror attacks. It is the main goals of terror outfits to create a destructive systemic impact, so as to ensure that the attacks has the maximum possible secondary impacts in the context of death, injuries, disruption of utilities and Communications Systems, massive economic costs, societal disruption and in the end political unrest (Boin and McConnell, 2007; OECD, 2003; Coaffee and Wood, 2006). The implication of interdependencies of important systems and critical infrastructure in terms of terrorism is that the failure or disruption of any one particular system for example the information Technology System will automatically ensure damages and costs to all the other systems. Therefore, making efforts for increasing the resilience of potential target systems (especially those that have critical infrastructures) is of vital importance in minimizing the total impacts as well as consequences of a terror attack. The incidence, which took place on 11th September 2001, has given many important lessons in this context. It is the responsibility of governments to improve the identification of the most important networking nodes and operational elements within critical infrastructures and carry out for the development of adequate procedures that can protect or in the very least limit potential damage and disruption. With the systems involved in information and communication infrastructures, it has been seen that the most important interfaces are the ones which provide connections to highly reliability systems like nuclear processing plants, energy generation, air traffic control systems as well as some physical distributing ones like the metro, railway systems, petroleum or gas pipelines and dams or bridges (OECD, 2003; Hellström, 2001; Coaffee, Murakami Wood and Rogers, 2009). Vital nodes can also be recognized in the present day information-dependent systems like the Intelligent Transportation Systems that are fully reliant on the global positioning system or GPS (OECD, 2003; Hellström, 2001).

Response and Recovery Phase Systems:

Depending on the targeted location of a terror attack, the response as well as recovery systems require emergency response services for helping people, the rebuilding of damage infrastructure during the recovery phase and the economic as well as financial crisis management due to the consequence use of such a disaster. Many lessons were learned during the 9/11 attacks of USA. This particular terrorism act was successful in not only inflicting mass fatalities as well as casualties, but the impact on infrastructure as well as economic damage was to a level that has not been recorded in any previous terror based incident in recent times. The destruction of material assets was calculated to be in the range of national accounts as high as $14 billion private sector. $1.5 billion for the state and national level government sector, while it was $0.7 billion at the federal government level. The rescue efforts, cleanup of the debris and associated expenses have been approximated to have been more than $11 billion. The Lower Manhattan area of New York sustained a loss of over 33 of useable office space and a large number of businesses were simply annihilated. More than 200 000 people lost their jobs or had to shift out of New York City for long periods of time until the infrastructure was rebuilt (OECD, 2003; Comfort, 2007; Kapucu, 2008). Several industries were badly affected and the financial markets had to be closed for enough time to sustain serious losses. In the aftermath of this terror attack, the process of rebuilding communication and power connections as well as ensuring the problem free reopening of the financial markets was somewhat facilitated due to the availability of proper financing and gold coordination between the private-public sector collaborations. In the case of developing nations, serious terror attacks cause very long lasting effects since the safety net in the form of proper response and recovery systems is not present (Linnerooth-Bayer and Mechler, 2007).

Another vital lesson learned was that many institutions such as banks and securities firms were subjected to this crisis with a background of strong capital bases and a very good liquidity. This factor was instrumental in preventing systemic breakdown. With this fact in mind, it is now widely known that if due to the non-availability of proper insurance to cover the cost of terror events, the government may need to act as the insurers for mega terrorism incidents (OCED, 2003). Furthermore, the government may also need to work extensively on communication management with the general population in order to win their trust after a massive incident related to terror (Longstaff and Yang, 2008).

Conclusion

Terrorism is in all probability going to become the main feature of conflicts as well as disasters in the future. The changing face of new age terrorism, the means it uses as well as the targets have serious implications in terms of causing very high in human suffering as well as economic damage. The most important aspects in handling this emerging 21st century malicious risk is related to improve the insights as well as risk assessment of the threats posed by it. The possible use of bio agents, chemical; warfare and nuclear weapons makes it an accessory to place focus on preventive measures.

References

Adey, P., & Anderson, B. (2012). Anticipating emergencies: Technologies of preparedness and the matter of security. *Security Dialogue, 43*(2), 99-117.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management, 15*(1), 50-59.

Coaffee, J. (2009). Protecting the urban the dangers of planning for terrorism. *Theory, Culture & Society, 26*(7-8), 343-355. doi: 10.1177/0263276409349656

Coaffee, J., Murakami Wood, D., & Rogers, P. (2009). *The Everyday Resilience of the City: how cities respond to terrorism and disaster.* UK: Palgrave Macmillan

Coaffee, J., & Wood, D. M. (2006). Security is coming home: rethinking scale and constructing resilience in the global urban response to terrorist risk. *International Relations, 20*(4), 503-517.

Comfort, L. K. (2002). Managing intergovernmental responses to terrorism and other extreme events. *Publius: The Journal of Federalism, 32*(4), 29-50.

Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review, 67*(s1), 189-197. DOI: 10.1111/j.1540-6210.2007.00827.x

Dumitriu, E. (2004). EU's Definition of Terrorism: The Council Framework Decision on Combating Terrorism. *The German LJ, 5*, 585.

Hellström , T. (2001). *Emerging Technology and Systemic Risk: Three Cases with Management Suggestions*, Contribution to the OECD International Futures Project on Emerging Systemic Risks, OECD, Paris. Retrieved on 21st June, 2015 from: http://www.oecd-ilibrary.org

Hoffman, B. (2001). Change and continuity in terrorism. *Studies in Conflict and Terrorism*, *24*(5), 417-428. DOI:10.1080/105761001750434268

Kapucu, N. (2006). Interagency communication networks during emergencies boundary spanners in multiagency coordination. *The American Review of Public Administration*, *36*(2), 207-225.

Kapucu, N. (2008). Collaborative emergency management: better community organizing, better public preparedness and response. *Disasters, 32*(2), 239-262. DOI: 10.1111/j.1467-7717.2008.01037.x

Linnerooth-Bayer, J., & Mechler, R. (2007). Disaster safety nets for developing countries: extending public–private partnerships. *Environmental Hazards, 7*(1), 54-61.

Longstaff, P. H., & Yang, S. U. (2008). Communication management and trust: their role in building resilience to "surprises" such as natural disasters, pandemic flu, and terrorism. *Ecology and Society, 13*(1), 3.

Masten, A. S., & Obradovic, J. (2008). Disaster preparation and recovery: Lessons from research on resilience in human development. *Ecology and Society, 13*(1), 9.

Michel - Kerjan, E. (2003). New challenges in critical infrastructures: A US perspective. *Journal of Contingencies and Crisis Management, 11*(3), 132-141.

Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *American journal of community psychology, 41*(1-2), 127-150. DOI: 10.1007/s10464-007-9156-6

'*OECD.'* (2003). *Emerging Systemic Risks in the 21st Century: An Agenda for Action.* Retrieved on 21st June, 2015 from: www.oecd.org/futures/globalprospects/37944611.pdf

Paraskevas, A., & Arendell, B. (2007). A strategic framework for terrorism prevention and mitigation in tourism destinations. *Tourism Management*, *28*(6), 1560-1573. doi:10.1016/j.tourman.2007.02.012

Post, J., Sprinzak, E., & Denny, L. (2003). The terrorists in their own words: Interviews with 35 incarcerated Middle Eastern terrorists (This research was conducted with the support of the Smith Richardson Foundation). *Terrorism and political Violence, 15*(1), 171-184. DOI:10.1080/09546550312331293007

Stewart, G. T., Kolluru, R., & Smith, M. (2009). Leveraging public-private partnerships to improve community resilience in times of disaster. *International Journal of Physical Distribution & Logistics Management, 39*(5), 343-364.

Weber, R. T., McEntire, D. A., & Robinson, R. J. (2002). *Public/private Collaboration in Disaster: Implications from the World Trade Center Terrorist Attacks.* Colorado: Natural Hazards Research and Applications Information Center.