Terrorism as an External Threat in Global Value Chains

ABSTRACT

Global terrorism incidents and business-related threats have intensified in scale and scope over the past seventeen years. MNCs are thus exposed to direct and indirect negative impacts on their international activities. Previous research lacks thorough theoretical frameworks to analyze these impacts. The Global Value Chain (GVC) framework offers a perspective that is both comprehensive and quantifiable for the evaluation and expansion of this prior research. The GVC enables us to assess terrorism impacts on international business overall and at each stage of the value chain. On this basis, we develop a 'terrorism resilience theory' (TRT) that can be used in future theoretical and managerial analyses of the response to terrorism risk.

KEYWORDS: global terrorism; global value chain; terrorism risk; terrorism resilience theory; multinational corporations (MNCs); uncertainty; risk.

INTRODUCTION

Seventeen years after the Twin Towers in New York City were hit by two hijacked planes, terrorist attacks worldwide have reached an unprecedented level. Data on terrorist attacks, e.g., tracked by the Global Terrorism Database (GTD), dramatically confirm this notion, identifying more than 10,900 terrorism events worldwide in 2017 alone. In their codebook, the GTD (2018) defines terrorism as "the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation" (p. 10); this definition is also consistently used by most scholars in this field. Since 2001 there has been over a five-fold increase in the annual number of deaths from terrorism, and businesses in 56 countries have been directly affected locally and in their international activities. The rise of what is named 'Islamic State' of Iraq and the Levant (ISIL, or ISIS), with other affiliated or competing terrorist networks, led to attacks including the *Charlie Hebdo* shootings in January 2015 in Paris, the Bangkok bombings of August 2015, multiple attacks in Paris on November 13, 2015, in Brussels on March 22, 2016, in Nice on July 14 and Berlin on December 19, 2016, in Manchester in May and Barcelona in August, 2017. However, not only radical jihadist terrorism is advancing. There are other variants of terrorism, for instance, lone wolf attacks and other ideologically motivated attacks, such as the Charleston Church shooting on June 17, 2015, the Las Vegas shooting on October 1, 2017, or the mosque shootings in New Zealand, on March 15, 2019. These different types of terrorism all are planned and designed to instill fear and have a high social impact (Prieto-Rodríguez, Rodríguez, Salas, & Suarez-Pandiello, 2009). Terrorism counts as one of the main security threats to countries (Hasnat 2015), perhaps the most severe one today. Different types of terrorism also pose different risks for businesses and are very hard to predict and manage. In particular, the exposure of single businesses to terrorism very much depends a variety of factors, such as the company's reputation (high- vs. low-value target), its exposure (attack causes strong vs. weak impact for GVC), and the ease of attacking (soft vs. hard target). What it is in common is that companies have to prepare themselves and deal with terrorism as a potential threat factor.

In the last few decades, the field of international business (IB) research has greatly matured (Rugman, Verbeke, & Nguyen, 2011). However, there are still new challenges that have not been covered sufficiently, from business operating in global value chains to risks ranging from market-based phenomena to systemic features. The following article provides a synopsis of the most relevant advances in the international business (IB) and management literatures regarding the impact of terrorism as an external threat factor on theory and practice. And it suggests a theoretical approach for dealing with the terrorism risks. We focus on the scope and weaknesses of existing analyses and propose that these contributions are in need of a better theoretical framing: we suggest that the Global Value Chain (GVC) approach is a suitable organizing framework, and we develop with it a terrorism resilience theory that sets the scene for future research advances that can help to shape appropriate corporate strategies.

Data published by the National Consortium for the Study of Terrorism and Responses to Terrorism (2018) reveals 108,586 entries when listing terrorist attacks worldwide from September 11, 2001 until December 31, 2017. Breaking this number down, that means an average of 18.2 terrorist attacks per day, or .76 attacks per hour, every single day. When considering what are denominated as 'successful' attacks, which exclude attempts that failed (e.g., a bomb did not detonate as planned), the number remains at 94,756. While not every attack has such a magnitude as the 9/11 attacks, overall the incidents reported in the GTD have significant human, organizational, and financial implications; and their frequency raises the behavioral impact (Rose, 2009). A staggering 8,594 of the attacks were directly targeting businesses. That equals, on average, about 1.44 terrorist attacks each day on businesses that are independent or part of a multinational firm's global value chain (GVC). In other words, on average every day since 9/11, at least one company was the direct victim of a terrorist attack, with related direct and/or indirect effects on other businesses. When looking at the year 2017 alone, the GTD reports 707 attacks on businesses, which is an average of 1.94 terrorist attacks per day targeting a company.

The relevance for management of organizations given the scale, scope, and nature of terrorism today is significant, and the direction is clear; the data are convincing and now, available. Yet, despite regular scholarly contributions, determining how to capture and theorize on this phenomenon has remained a challenge. With this article, we aim to fill this gap and provide a basis for theory-building with respect to strategies for configuring and protecting the GVC. We will start by examining the terrorism literature as it relates to decisions on purchasing, production, sales, human resource management, and risk management, as well as other business activities.

THE GLOBAL TERRORISM LEGACY: BACKGROUND

In the context of 9/11, management literature started to scrutinize terrorism that had become more global (Schneckener, 2002), and awareness of the threat has increased (Czinkota & Ronkainen, 2005; 2009). New technologies and communication possibilities, such as encrypted messaging and video-chats, allow terrorists to connect, recruit, and (inter)act globally. Given these experiences, research has looked at how companies were affected and how they were planning to deal with threats or attacks, including direct and indirect effects. By 2001, terrorist organizations had started to become decentralized, network-focused rather than hierarchical organizations. Their groupings of individuals were now transient (ICAR, 1995) and they had started to organize along a structure and communication framework similar to that of transnational organizations (Suder, 2004). Much of the research-driven thinking was around how to best capture sufficient data to start building up a pool of research contributions that would eventually provide a basis for theory-building and make the needed contribution to mainstream thinking.

Early research found that it was most suitable to focus on the *impact* of terrorism: impact led the agenda in all analyses. Terrorism had indisputably caused higher costs for business -- domestic and international -- as was noted by Enderwick (2001), Suder (2004, 2006), and summarized by Czinkota, Knight, Liesch, and Steen (2010). A number of examples from the last fifteen years support this: analyses noted, for example, Delta Airlines' terrorism insurance premium that increased from $2 million per year in 2001 to $152 million per year in 2002 (Enderwick 2006, p. 65). The Tunisia hotel attack in Port El Kantaoui in 2015 was estimated to cost the tour operator alone about £32 million[1]. These effects also have in common that companies' global value chains were affected. Another aspect of direct costs is ransom. The GTD lists 56 cases in which ransom has been paid and the amount was reported. In total, these companies were

[1] http://business-reporter.co.uk/2015/08/13/tunisia-terrorist-attack-to-cost-tui-up-to-32-million/

blackmailed to pay more than 234 million USD in ransom[2]. Moreover, the GTD lists 85 incidents with a major monetary damage of more than one million USD. Examples are, for instance, a bomb blast targeted at the BLOM Bank in Lebanon, causing direct costs of 60 million USD; and the detonation of two coordinated bombs exploding simultaneously in a Cumaná supermarket in Colombia. Although nobody was hurt, including nearby stores the damage added up to 73 million USD.

Also, on a macro level, research found that "higher levels of terrorist risks are associated with lower levels of net foreign direct investment positions. On average, a standard deviation increase in the terrorist risk is associated with a fall of about 5% in the net foreign direct investment position as a percentage of GDP" (Abadie & Gardeazabal 2008, p.14). A good example of that are the 2008 attacks in Mumbai that were reported to have had an estimated $100 billion negative impact on India's economy, mainly because key institutions such as stock exchanges and banks, as well as commercial establishments, were closed for several days and business activity dropped for weeks afterward[3]. Also, given India's important participation in international business, especially through outsourced and offshored production and services in the GVC, the impact was broad in scale and scope.

The list of terrorism events presented by Czinkota et al. (2010) has expanded extensively over recent years. It was a simple list of events, dates, and victims in 2010. Today we know that this list needs more fine tuning, through analyses of frequency, numbers, and extent of attacks using corporate and publicly available data. Cross-border business impact and costs have become more calculable - and calculated - due to the availability of statistical data, and advances in analytics (Chen, Chiang, & Storey 2012) and the progress made in the understanding of GVCs and the framework derived from them.

For research, this quantifiability - albeit tragic for the victims - adds possibilities to better analyze, understand, and model terrorism in management, and to factor it into theory-building. Looking back on seventeen years of post-9/11 terrorism research in management, we recognize that at the time of 9/11, not much business-related data was available, and terrorism was often subsumed under political risk (Goerzen,

[2] Given the confidentiality of this topic, especially when insurance is involved, these numbers are by no means representative, they just indicate an minimum estimate.
[3] http://www.asiaecon.org/special_articles/read_sp/12094

Sapp, & Delios, 2010; Oetzel, Bettis, & Zenner, 2001; Alon et al., 2008). Inspired by Enderwick (2001) and Laqueur (1987), Suder (2004) provided a collection of IB analyses with eminent scholars, starting to calculate cost and impact. Importantly, Enderwick (2006) provided estimates stating that "(s)ome 43% of businesses suffering a disaster never recover sufficiently to resume business, and of those that do reopen, less than one-third survive for two years or more." While this analysis covers all kinds of disasters, terrorism was explicitly included (p. 64). Many papers were conceptual to some extent; some papers relied on solid single or multiple case studies, upon the premise that "(s)ound empirical research begins with strong grounding in related literature, identifies a research gap, and proposes research questions that address the gap" (Eisenhardt & Gaerbner 2007, p. 28).

The field of terrorism was rather new to management literature. Global terrorism studies made their appearance in the Academy of International Business's (2007) 'Frontiers Conference', which encompassed, *inter alia*, the discussion of 'the relationship between international trade and investment and terrorism.' It provided a new forum to discuss future terrorism research and revealed and considered the challenges shared by all in obtaining the type of data used in traditional management publications, which was scarce, often highly confidential, and even more often, rather difficult if not dangerous to obtain in-country. Beck (2008) explicitly mentioned terrorism as one of the factors playing a role in his paper on impacts of global power games among business, nation-states, and society, indicating its increasing relevance in management literature. In the same vein, Cheng, Guo, and Skousen (2011) highlight the importance and relevance for terrorism and propose the topic as a worthwhile research field.

Disaster literature was also entering the discussion: Oh and Oetzel (2011) used this to investigate the intensity of terrorism as well as host country governance quality. Boudes and Laroche (2009) analyzed post-crisis reports and mention parallels between reactions to terrorism and other disasters.

While terrorism in the United States has remained relatively limited since the 9/11 attacks that are fading into history, the likelihood of further terrorist attacks is ever-present. And the terrorist attacks typically by individuals on schools in the US (including Columbine in Colorado in 1999, and the Sandy Hook attack in Connecticut in 2016, all the way to Highland Ranch in Colorado in 2019) demonstrate that terrorism remains a serious threat in the US today. It is all but certain that additional terrorist activities will occur and cause significant damage to people and to business in the United States in the future. It is therefore important to come to a better understanding of the subject, from event likelihood to impacts on business, to government policy responses. This paper looks at the impacts of terrorism on international business and possible corporate responses.

PERSPECTIVE: TERRORISM RESEARCH THROUGH THE GVC LENS

Companies have to deal with uncertainty, and terrorism is a crucial factor of such uncertainty (Kobrin, 2017). How to frame the contributions of early terrorism research using mainstream theories and concepts, and how to align best with emerging quantitative data remained unclear. In parallel, global value chain research became part of mainstream research (Beugelsdijk, Pedersen, & Petersen, 2009; Hanson et al., 2005; Buckley, 2011; Gereffi & Lee, 2012, Gereffi, Humphrey, & Sturgeon, 2005; Pananond, 2013; Grosse 2016).

Given the scope of extant terrorism research, we posit that most studies can be positioned into this GVC framework. Literature increasingly recognizes international production, trade, and investment in global value chains as a measure of engagement in management across borders (Buckley 2011; UNCTAD 2013; Coe & Yeung 2015). Stages of the production process are located across different countries, in a distributed manner, acknowledging MNC activity and the role of GVCs in a vast range of locations (Gereffi, 1999). This is also seen increasingly in the context of emerging market multinationals (Pananond, 2013; 2015; Grosse 2016). GVC research has given us the means, tools, and knowledge to measure linkages and trends that take place within value chains, including input-output- measurements focusing on value-added (Cattaneo, Gereffi, & Startitz, 2010; UNCTAD, 2013; Suder et al., 2014). Each stage of the value-adding process requires components from human resources to financial resources, risk management, and others. Figure 1a illustrates this GVC structure, while Figure 1b shows how terrorism affects business across the GVC. Each stage encompasses potentially multiple countries, regions, locations, teams, and various value-adding processes that differ from one stage to another yet are highly interdependent. The various actors in the chain and its stages may operate in a range of relationships (ownership structures) with the final client, from agent to supplier to subsidiary or joint venture partner. Firms also need to consider how their actions affect their acceptance by local stakeholders (Stevens & Newenham-Kahindi, 2017). That creates a network of international engagement that is interdependent and subject to, *inter alia*, external threats such as terrorism.

--- Please insert Figures 1a and 1b here ---

The GVC framework establishes a lens that allows assessment of the impact of terrorism on international business in a comprehensive, structured, and quantifiable manner. It also helps to evaluate and expand research findings from prior, mainly qualitative research. To evaluate the significance that terrorism represents for theory-building, we posit that the stages of the GVC are particularly useful because of the scale, scope, and interdependence of today's networked global business that they reflect. The use of a GVC framework enables scholars to respond to calls for more attention to terrorism (e.g., Bader & Berg, 2013; Czinkota et al., 2010; Kotabe, 2005; Shrivastava, 2005, Spich & Grosse 2005), and to enhance theory-building and analyses of managerial relevance. To date, the main weakness of research in this field has been that it was phenomenon-driven instead of theory-driven.

Next, we develop our terrorism resilience theory as a basis for future research. We then proceed to demonstrate how existing studies relate to our terrorism resilience theory through the global value chain. This then enables us to show how the GVC framework promotes in-depth study that will allow for future contributions to analyzing terrorism in the international business and management literatures.

As Suder et al. (2014, p. 409) put it, "(t)he rise of GVCs has been considered one of the most important features of rapid economic globalization in recent decades." More (intermediate) products are being produced across different countries before they are exported to other countries for further production, assembly and distribution, accounting for a fragmented value chain across borders. Firms strive to optimize their fit into GVCs and related processes by placing the various stages across different locations to foster efficiency and productivity. GVC-fragmentation and location decisions are made based on factors such as knowledge, resources, value-added, cost and risk (assuming some level of global transferability), and they encompass developing and developed economies.

TERRORISM RESILIENCE THEORY

The idea of a terrorism resilience theory (TRT) follows from the logic that firms today face a rapidly-changing environment with many risks and opportunities that need to be managed successfully. If a company develops a strategy that can make it resilient to the variety of business disruption challenges that confront it in the 21st century, it has a greater chance of survival. Corporate resilience theories or perspectives have appeared in the literature in recent years, generally guiding companies toward risk management strategies to deal with one kind of risk or another (e.g., Sheffi and Rice 2005 regarding business disruption risk; Bishop 2009 regarding corporate fraud and corruption risk; and Gilbert et al. 2012 regarding market shifts and new technology).

Sheffi and Rice (2005) point out that resilience to business disruption can come from two sources. *Redundancy* can be planned into operations, so that any one facility or machine or process may fail, but another alternative is always available and operating or ready to operate. And second, *flexibility* may be built into the firm's value chain, for example by using standardized machines and processes in different facilities, so that the loss of one facility to fire or a strike or other event can be dealt with by moving the firm's production to an alternative facility(ies) where the process is interchangeable. Or if people at the one facility are lost to a strike or any other reason, people from elsewhere can be brought in to operate that facility (as UPS did in a situation mentioned where a local major snowstorm kept workers from their facility at the airport, and UPS flew people in from elsewhere to operate the facility until local roads were cleared and local employees could get to work again, several days later).

TRT posits that terrorism risk constitutes a sufficient environmental threat to business profitability and sometimes even survival that firms need to confront the risk directly and comprehensively. The strategies that may accomplish this resilience are of two types: *business adaptation* (value chain strategy and management) and *business protection* (risk management). That is, to deal with the increasing direct and indirect impacts of terrorist events, companies should evaluate methods for altering their fit into global value chains, and they should explore methods such as insurance contracts and physical protection for their facilities and people.

Business adaptation may be accomplished by literally moving a business activity away from a location that is or is expected to be affected by terrorist attack(s). This may be illustrated by business in many parts of the Middle East, where terrorist attacks are frequent and avoidance of locating business in those places will enable the firm to reduce the risk. Business adaptation may also be accomplished by contracting out with another firm to carry out a business activity that may be subject to terrorist risk. If offshore assembly were being carried out in a country such as Colombia or in the Uighur region of Xinjiang, China, the possibility may exist to contract with an outside firm to do the assembly and then pass on the assembled products to the MNE in question[4]. The company itself can adapt its operations to provide duplicate ('redundant' according to Sheffi & Rice) facilities or by having trained people available to operate any facility in the case when a strike or storm or other event causes the existing people not to be able to operate. And finally, if the company can diversify its suppliers, so that a terrorist attack that causes problems with one supplier can be overcome with products or services from another supplier, this mitigates the terrorist risk. All of these strategies are methods to reduce the impact of terrorist risk by adjusting the business activities of the firm.

Business protection can be achieved with the common risk-management tools of insurance policies, option contracts, and other financial market hedging instruments. For example, the US Government after 9/11 established an insurance program to offer policies covering terrorist risk (the Terrorism Risk Insurance Act[5]). This law essentially acts as a type of reinsurance for commercial property and casualty insurance policies. The program only comes into effect when an act of terrorism is "certified" by the Secretary of the Treasury (in consultation with the Secretary of Homeland Security and the Attorney General) that the act falls under the definition of terrorism and triggers an event dollar threshold.

[4] Although outsourcing the assembly to another firm reduces the MNE's facilities risk, it still leaves the supply chain at risk of disruption by a terrorist act, so this possibility needs to be considered as well.
[5] https://www.treasury.gov/resource-center/fin-mkts/pages/program.aspx

When such an event occurs, the US Government shares the cost of insurance payouts with the insurance companies that offer the coverage (in an 80/20, government/insurer split in the most recent re-authorization of the policy). All property/casualty insurers must offer the coverage, while clients do not have to choose to accept and pay for it.

Business protection can also be pursued in the cases of at-risk physical facilities and people by building greater defense against a terrorist attack. This can be done by fortifying buildings, by using protective services from companies such as Kroll or Pinkerton, and by using electronic means to increase surveillance and warn when an attack may be imminent or underway. And certainly in the 21st century this extends to building greater protection into electronic systems of the company, which could be hacked or otherwise harmed or disabled.

Table 1 illustrates the two sides of terrorism resiliency that the theory proposes.

[Table 1 goes here]

Next, we want to incorporate the terrorism resilience theory in the framework of global value chains and explore the possibilities for dealing with terrorism at each stage of the value chain. With this structure of analysis, the challenge of dealing with terrorism can be understood in detail and responses designed appropriately.

Global value chains enable the disaggregation of corporate purchasing, production, and distribution in MNCs; each stage in the global value chain may be exposed to terrorism risk differently. Consequently, we posit that resilience for the company's international activities is a sum of the respective resilience of each stage of the GVC. There are also variations of focus on certain stages related to the firm's internationalization scale and scope, structure, resources and portfolio of activities. As a basis of analysis, Figure 1b above illustrated the GVC along with the ways in which terrorism may impact the value chain. The literature of global terrorism contains findings mainly in three of the stages of the GVC: procurement of inputs, production of products and/or services, and sales. We also note that two of the elements that occur in each stage of the GVC are a focus of existing literature: human resource management (HRM) and risk management. We now assess each one of these current main themes in the literature and outline how they can be positioned in the GVC framework, as well as suggesting how companies can alter their activities to become more resilient to terrorism risk through adaptation and protection strategies.

GVC Stages -- Procurement of Inputs

Procurement deals with the process of acquiring goods and services from providers, i.e., the inter- and intra-company supply chain network. This early step is acutely vulnerable to direct and indirect disruptions by terrorism, e.g., an attack targeted at a supplier or delays in the sourcing due to longer terrorism-induced customs procedures (e.g., Reade, 2009). The vast majority of terrorism-related research regarding procurement investigates and conceptualizes its impact on supply chains. Worldwide logistics networks have been found to be disrupted by even slight incidents, with financial and reputational impacts. Shortages of critical production inputs induce costs (Christopher & Lee, 2003). The impact of interruptions is highlighted through multiple case evidence, including Toyota's near-loss of production after 9/11 (Jain & Grosse, 2009), and vulnerabilities at ports and in maritime operations (Barnes & Oloruntoba, 2005). Most analyses were either conceptual, using various examples as evidence, or case study contributions. The "persuasion with case studies" (Siggelkow, 2007, p. 20), through single cases, or the constructs stemming from multiple case studies and conceptual papers to develop theory inductively, as Eisenhardt and Gaerbner (2007) note, were crucial also in this emerging field of research, when it suffered from data limitations in its infancy. Also, case studies serve in the "theory-building process (which) occurs via recursive cycling among the case data, emerging theory, and later, extant literature," that is "likely to produce theory that is accurate, interesting, and testable" (Eisenhardt & Gaerbner 2007, p. 26).

In one of the first large-scale empirical studies on supply chain vulnerability, Wagner and Bode (2006) confirmed what was, until then, only conceptualized: that the impact on supply chains is either directly (i.e., the firm itself is under attack) or indirectly (i.e., a trading partner is under attack or trading routes are blocked or delayed). Moreover, additional "indirect consequences of terrorism that are not caused by an attack itself but by the reaction of governments and markets" (p. 305), including longer customs declaration and procedures, were found to be relevant issues to investigate.

The macro-perspective, in the context of homeland security, was also investigated with regard to supply chains (e.g., McIntyre & Travis 2006; Spich & Grosse 2005). A diversification or increase of the number of suppliers, especially for critical input goods, or the option of in-house production as a way to minimize supply chain interruptions, was recommended as a solution (McIntyre & Travis 2006, Czinkota et al. 2005). McIntyre & Travis (2006) also recommended shortening of supply chains. Research on response mechanisms might help to build models that focus on keeping the supply chain working, in recognition of the need for redundancies and in sacrifice of economies of scale which would require additional financial resources. The repatriation of supply chains to safe-haven countries "might paradoxically result in an increase in risk in the global economy" due to exclusion of risky countries (p. 138). These studies generally look at means for adjusting the firm's business activities to reduce terrorism risk, rather than at protection methods such as insurance and physical facilities' protection.

GVC Stages -- Production

Management scholars also note that terrorism poses a significant challenge for production, immediately and potentially, with high loss impact in value-added. In the example of 9/11, US production was reported as severely disrupted; overall real GDP shrank in the third quarter (OECD 2002, p. 119). The OECD calculated the production cost under terrorism attacks in various scenarios, amounted to an impact of "three percent of [US] GDP, that is, the equivalent of a small OECD country's GDP" (p. 120). Security measures were found to increase costs of production and doing business; consumer fear resulted in reduced demand and negatively impacted the ranking and value of brands (Suder, 2004 & 2006; Frey et al., 2007). In tourism, the reduced demand from abroad cannot be compensated by domestic demand (Fleischer & Buccola, 2002).

Within this production-related literature, a common thread is that terrorism impacts put lean management into question (e.g., Zsidisin et al., 2005; Sheffi, 2002). However, there appear to be no studies yet that analyze a direct link with a modification of production away from lean to other approaches. We do know though that shortages of critical production inputs require the mitigation of supply chain risk through "end-to-end" visibility (Christopher & Lee, 2003). While this lean production refers more to obtaining inputs into the production process, terrorism risk also suggests the use of redundant production locations, to avoid complete halting of production when a particular facility is harmed.

The production stage is also highly exposed to impacts on resources including, importantly, people, and thus, labor/ HRM which is crucial also from a social and responsible employer perspective. Protection of people with more secure facilities is a logical response, which has not been explored in the literature. Finally, complementing elements of the production stage such as financial resources, technology, and facilities involved, suffer from terrorism exposure and thus may have an indirect effect on this core stage of the GVC.

GVC Stages -- Sales

Terrorism affects sales directly when clients/ customers are discouraged from visiting points of sale due to terrorist activity. Wernick and von Glinow (2012) revealed that tourists and businesspeople stayed away from hotels perceived to be in high terror-risk locations, as did our earlier example of the Tunisia hotel attack in Port El Kantaoui in 2015. Wagner and Bode (2006) state that disruptions in the supply chain can be detrimental and negatively affect sales volume. When people stay away from locations where terrorist attacks have recently occurred, retail sales suffers, for example in lower Manhattan after 9/11 and in the Paris locations that were attacked in 2015. Retail facilities of various kinds suffer this cost of lost sales whenever a terrorist attack moves people to stay away. Points of sale such as hotels or tourism destinations cannot be substituted with the same services in other locations, but they can be protected with both insurance and physical protection arrangements.

The global shift toward greater purchasing through the internet may help some retailers deal with the terrorism threat. Stores that sell consumer products can sometimes be replaced by on-line sales that are shipped from the producer to the consumer’s home without need for a store or office. Some sales still must be done through physical facilities, such as restaurants and hotels, so these services will continue to be plagued by terrorism risk and providers will need to devise different strategies to mitigate the risk. Overall, the US Census Bureau estimated in 2018 that approximately 10% of US retail sales were carried out through the internet (Census Bureau 2018). And, of course, industrial products often may not be possible to sell through the internet, so their sales facilities will still be subject to terrorism risk. Overall, sales activity can sometimes be moved to locations with less terrorism risk, and other business adaptation strategies are often possible. Business protection is possible through both insurance and facilities' protection strategies.

On the other side of the coin, providers of security and safety equipment should be among the main beneficiaries of terrorist attacks. When organizations recognize the terrorist threat, they tend to purchase more equipment and other sources of protection. Similarly, insurance companies' sales are also positively affected by terrorism when they charge increased insurance premiums – although of course the insurers suffer losses when they pay for damaged or destroyed property and harmed people when terrorist attacks occur. So, while production costs may rise for one set of firms that are exposed to terrorism risk on their production facilities, the revenues of risk-protection firms will rise as a result.

Concerns at every GVC Stage -- Human Resource Management.

Within the GVC, labor is diverse and HRM includes, *inter alia*, a full portfolio of activities comprising hiring and retaining staff, as well as suitable training and compensation (Porter, 1985). This is conducted under various levels of control along the chain of intermediate production, inter- or intra-firm, and under various legislations. Each stage of the chain may encompass direct HRM or that exercised by independent suppliers. Research on this part of the GVC is conducted at the individual level and reveals that managing people under the threat of terrorism always comprises particular skills in dealing with the feelings of human beings, such as stress, anxieties, or sensitivity (Bader & Berg; 2013, Bader, Schuster, & Dickmann, 2019; Paulus & Mühlfeld, 2017; Reade, 2009), and the willingness of staff to work with risk and/or in risk-sensitive locations or organizations. Yet, considering the increasing scale and scope of terrorist activity, and the targeting shift from a few high-visibility political targets to many soft target attacks, there are several open topics that need more scholarly attention - that, again, can be analyzed along the GVC. This also affects global mobility and management of international assignments (McNulty & DeCieri, 2011). First, most studies focus on HRM in crisis areas, yet do not cover research on terrorism impact on individuals who were unprepared and who live in countries that are infrequently exposed to terrorism (such as was expected for the USA, France, Belgium, Germany, and the UK in the early 2000s). Also, most studies focus on expatriates in specific locations rather than as a network that is an instrumental part of a GVC.

In existing studies, we learn unsurprisingly that terrorism is found to have a negative effect on HRM. What and how strong any effect is and how companies manage it, will continue to be a broad field of terrorism research. Bader and Berg (2013) showed the negative effects of terrorism on expatriates and discuss mitigation of effects such as perceived organizational support (POS), which is also addressed in a study by Reade and Lee (2012).

Social network studies on staff inform us, as in Kastenmüller et al. (2011), that people focus more on their personal social networks in the aftermath of terrorist attacks, and that high terrorism threats can impede their willingness for organizational networking. Considering the importance and value of individuals building and maintaining social networks at work, this is alarming for organizations. Social networks are a valuable source of social support (Wang & Nayir, 2006) and of learning in distributed, internationally dispersed organizations. Expatriates ceasing to establish and maintain professional social networks, or performing below their standards, affect the individual and organizational performance. Also, workforce planning and succession (e.g., Liou & Lin, 2008) remains an underdeveloped research theme with the promise of further insights into resilience planning in GVCs.

MNCs not only employ expatriates but also local staff. Lee and Reade (2015) found that sensitivity to ethnic conflict in a societal context is positively related to ethnic homophile perceptions in the workplace. In other words, except when contextually sought for learning to gather competitive advantage, terrorism creates tension and conflicts among the workforce, restricting the international firm to tap into local knowledge and to exert control.

Overall, our resilience theory suggests that MNCs should be looking for ways to reduce the human exposure to terrorism risk by adapting the business activities (e.g., moving facilities to less-risky locations; contracting out to third parties for activities that must be done in risky locations; providing training to employees so they will be less overwhelmed when terrorist acts occur) and/or protecting the people with more secure facilities, guards in the facilities, and even personal protection for executives at risk.

Concerns at Every GVC Stage -- Risk Management

As early as 1993, Harvey published a study on corporate measures to manage terrorist attacks. He stated that, at that time, less than 50% of the companies in his sample had formal programs dictating what to do in the case of an attack. Among better-prepared companies, most budget allocation focused on purchasing security equipment and on “protection of assets, i.e., physical means to reduce access to and increase security of corporate buildings and computers” (Harvey, 1993; p. 470). However, research only slowly picked up on this important notion, and on a more comprehensive approach. Almost twenty years later, Gephart, van Maanen, and Oberlechner (2009) introduced a special issue on risk, still pointing out that “risk is an important but under-investigated feature of organizations in Late Modernity” (p. 141), dedicating a significant part of the issue to terrorism. Managerial impacts remained under-researched at that time; this has only changed over recent years. Another study relevant here, though not exclusively focusing on terrorism, was that by Oetzel and Getz (2011) investigating the role of local stakeholders and the impact of their pressure on MNCs’ response to violent conflict. As one of their results, they find that MNCs’ operations abroad are protected by firm response and preparedness, and that most firms do not (or cannot) leave a host country when violent conflict occurs.

[I think this is paragraph really bs, and not related to our argument, and should be dropped. Please let me know if you are willing to drop the paragraph. We need to focus on *business adaptation* and *business protection*, i.e., our TRT.] → Did drop as suggested. You actually need to ask Gabriele if it’s fine to drop, but I think if we just drop it and don’t point it out, she won’t realize it’s gone.

In terms of operational risks, Suder (2004), Suder and Czinkota (2005), and Jain and Grosse (2009) informed that managerial plans with a defined protocol are essential to protect operations. In particular, their work reinforces both a country-level and cross-border dimension to mostly internationally–focused terrorism-related literature, stressing operations-centered resilience planning as contingent on terrorism threat levels. Jain and Grosse (2009), among others, note that MNCs manage operations in light of company-wide risk assessment and with a recognition of interdependencies in the internal marketplace -- if necessary redefining strategy and operations through an adaptive cost-benefit analysis. The magnitude of the shift in risk management can be observed, for instance, by looking at the airline industry. Drakos (2004) illustrated that terrorism increased the idiosyncratic and systematic risks of airlines substantially.

Within the specific case of tourism, Sullivan-Taylor and Wilson (2009) shed light on how managers of firms in UK's travel and leisure industry perceive threats from terrorism and how they handle these risks. Wernick and von Glinow (2012) focused their investigation on the effects of terrorism, as well as potential safety measures. International luxury hotels are a place where representatives of (Western) MNCs typically go in-and-out. Due to their role and the attention that attacks on them create, they are often in the crosshairs of religiously inspired terrorists (Wernick & von Glinow, 2012). In their paper, the procedure and equipment of terrorists, as well as potential responses of MNCs and local anti-terrorist forces were investigated. By proposing mechanisms including "target hardening," e.g., through clandestine security agents, they started to conceptualize how companies prepare for defending assets and resources crucial for operations in the case of an attack, as part of international location-bound strategy. To note that the peripheries of tourism and events venues, e.g., linking to transport, merchandise retail, services, and of corporations, are often difficult to secure and include the soft targets of bystanders and citizens that global terrorism aims for. This adds yet more complexity.

These examples show that terrorism risk management has moved from phenomenon-based to integrative management. After an attack, MNC management scrutinizes GVCs and organizational structures and take coordinated actions. Incidents need to be handled with regard to their short-medium as well as long-term impact, and pre-empted. Also, management may need to handle relations with governments and take care of security roles for infrastructure management (Sheffi, 2002).

Indirect Effects

Indirect effects of terrorism represent a tremendous and much broader challenge for management. For instance, Bader (2015) found out that the satisfaction with an expatriate's compensation does not have a positive effect on his or her work attitude, when the person is sensitive to terrorism. In other words, MNCs cannot just buy their employees' ability and willingness to perform well with money. Yet, perceived organizational support -- i.e., the company credibly showing that it cares for its staff -- does help to improve work attitudes of staff in terrorism-endangered countries. Along these lines, Bader, Berg, and Holtbrügge (2015) investigated the impact of intra-family tensions of expatriates on their performance, and found it to be negative. These findings are important, for including the human factor into terrorism (and thus: man-made) risk management is crucial.

Related to that is the indirect effect of fear. Paulus and Mühlfeld (2017) showed that fear of terrorism negatively influences cross-cultural adjustment of expatriates. The fear of terrorism increases with the objective threat level in the country. In other words, the higher the (potential) threat level in a country, the harder for expatriates to adjust. This effect holds true for adjustment at work as well as outside work. Moreover, terrorism increases the chance of failed international assignments since it leads to perceived constraints at work and in the private domain, when the terrorism level in a country is high. Eventually, this increases the intention to leave the country and, consequently, abort the assignment (Bader, Reade, & Froese, 2017).

CONTRIBUTIONS OF THIS ANALYSIS

The body of literature on terrorism related to business that has emerged in the past seventeen years, i.e., since 9/11, is primarily a range of analyses and conceptualization efforts of a phenomenon that focus on specific issues, rather than a holistic approach (e.g., Bader, Berg, & Holtbrügge, 2015; Bader & Schuster, 2015; Branzei & Abdelnour, 2010; Oetzel & Getz, 2011). A political risk classification used to be reasonable when relatively few companies were exposed to high direct terrorism risk, or to an extreme, hostile business environment accompanied by "instability, information ambiguity, and rapid, discontinuous, violent and simultaneous changes in the environment" (Brown & Eisenhardt, 1997). However, in the past seventeen years, scholars agree, the scale, scope, and impact of terrorism changed to a systemic challenge that has become quantifiable and spans the modern GVC. This places managerial and scholarly discussion, including that on just-in-time and lean production, into a broader, analytical context today.

Our terrorism resilience theory disaggregated through the GVC allows for current scholarly literature on terrorism to be understood comprehensively. It can be integrated by exploring the implications of terrorism as a whole and at every stage of the value-adding process, from purchasing inputs to providing after-sale service. Based on these considerations, the terrorism resilience theory is built to derive appropriate response strategies, including both protection and business adaptation steps. Also, since companies do not carry out all of the stages in the value chain themselves, and strategic management decisions are at the chain's core, this framework helps to model the implications of terrorism strategic decisions in relation with partners, suppliers, and customers, and networks of firms.

For firms that significantly participate in the international aspects of the GVC, we can now theorize about management needs for responding to the threat of global terrorism. The comprehensive management of the MNC is contingent on establishing resilience to terrorism through the entire GVC. In other words, instead of approaching the threat from terrorism in general, impact and risk assessment need to be broken down into GVC stages, which then enable overall risk response strategies. In fact, terrorism can be considered an external environmental threat to the value chain and needs to be managed accordingly.

Adger (2000) argues that resilience can be defined in various ways. For instance, it can be considered "the buffer capacity or the ability of a system to absorb perturbations, or the magnitude of disturbance that can be absorbed before a system changes its structure" (p. 349). However, it can also relate to the speed of recovery after a disturbance. Organizational and disaster research predominantly understand resilience as being influenced by approaches rooted in engineering or ecological sciences, with resilience being a characteristic of a system (Jabbour & Thomas, 2015).

Our conceptualization of terrorism resilience follows this reasoning and looks at how the GVC system can be altered to protect the MNC, through both adaptation of the GVC and also pursuit of direct protection measures. From a GVC perspective, each stage needs to be considered separately first and then as a part of the total organization. For each stage, there are two general strategic options: re-configure the stage (i.e., improve resilience of the chain by adding flexibility or avoiding exposure) or protect the stage (i.e., improve resilience by imposing protective measures) – or pursue both strategies simultaneously.

In terms of protection, Harvey (1993) was among the first to present measures that could help companies to protect their assets. He found that only a few companies did invest in some kind of counter-terrorism program; the majority spent money on security equipment. Other research reports on the increased use of e.g., metal detectors or concrete barriers (Brandt & Sandler, 2010). While these and other measures might not be capable of preventing the company from being attacked, such target hardening may increase the chance of being spared because other targets are softer and thus easier to hurt. They do not protect the firm from indirect impacts that still affect most MNC activity.

The other option for resilience, re-configuring the GVC or stages, suggests that companies should look to measures for passing terrorism risk management on to others, e.g., contracting value chain activities out to others, or to diversification, or to strategies that re-position the firm in the GVC. Retailers such as Wal-Mart and Home Depot can look for domestic as well as international suppliers to become more resilient. A gasoline station operator could look to move upstream into gasoline transport to avoid over-dependence on physical facilities; while a natural gas production company could look downstream into refining or power production to reduce dependence on locations that are subject to high terror risks.

DIRECTIONS FOR FUTURE RESEARCH

The legacy of 9/11 in the management literature and the parallel advances of GVC literature have provided insights that allow for better framing and theory-building for considering terrorism in management research. And our terrorism resilience theory provides a conceptual framework for seeking responses to terrorism risk. We note that future studies first should distinguish between domestic and transnational terrorism. Even though "… domestic terrorism cannot be treated as an isolated problem" (Enders, Sandler, & Gaibulloev 2011, p. 335), it is not the same as transnational terrorism, and each has different, though often overlapping, consequences. Domestic terrorism is communicated less than transnational terrorism, though it is more frequent (Enders, Sandler, & Gaibulloev, 2011); impacts occur to local and foreign business interests. Distinct, comparative studies between the two kinds of threats and attacks are now needed to strengthen and advance the proposed theory. It is likely that there will be different impacts on the GVC for MNCs versus local firms. The further adaptation of this emerging theory to the interconnectedness of the different stages in GVCs implies the comparison of isolated versus interconnected effects of terrorism in the GVC.

Also, the incremental 'target-softening' direction of terrorism attacks increases the vulnerability of business interests (Brandt & Sandler, 2010; Wernick, 2006). Even if the total number of attacks might remain constant in the future, the relative number of attacks on MNC interests and their qualitative impact are likely to increase. In other words, future research needs to identify where the GVC is weakest/ most exposed and thus most vulnerable to attacks and find solutions. This also includes defense against cyber-terrorism, a topic of increasing relevance for MNCs (Doh, McGuire, & Ozaki, 2015). Much of our resilience theory leads to a choice of diversification of locations and sources of inputs at each stage of the GVC, as well as ownership and control reconfiguration.

Perhaps paradoxically, the presence of powerful MNCs driving globalization has contributed to greater inequality in many countries. In weak states in regions such as the Middle East, Africa, and Latin America one of the responses is criminal and terrorist activity. Perhaps MNCs partially hold the solution to the problem through the way they structure, manage and reward those along their GVCs. Future research could explore this issue – which is one more element of the current debate about costs and benefits of globalization.

Another important observation of our investigation is that research on terrorism in management is almost exclusively cross-sectional. Given inherent early data collection issues, this is understandable. However, in order to gain a deeper understanding of the long-term effects and different effective mechanisms, longitudinal studies are needed. Future research can overcome previous limitations, through the availability and usability of data and new data methods. It may be able to scrutinize the impact of terrorism over a longer period of time with more than one empirical measurement and transform data into the relevant theory-expansion including through text analysis, social media and sentiment analyses, and data analytics (Roche & Blaine, 2014; Chen et al, 2012). Ways to strengthen the proposed theoretical approach are hence manifold.

Finally, with regard to the nature of this topic, most research so far dealt with the downside risks. However, this is only one side of the coin. Despite all the negative developments coming along with increased terrorism, there are also upside benefits. For instance, when companies come up with novel ideas to manage terrorism, they are in a position to do business which their competitors have ceded. Although the harm is tragic, insurance companies and providers of security equipment may also see some sort of upside benefit in that increased terrorism has the potential to boost their business. Therefore, it is worthwhile to further investigate this development and conduct more research in this direction.

MANAGERIAL IMPLICATIONS

Terrorist attacks have increased in frequency and intensity during the early 21st century. Companies involved in GVCs need to understand how terrorism risk may affect their business – from attacks that might affect a production facility or employees of the firm to terrorist activity that might affect suppliers or customers. Our analysis points out the ways in which terrorism affects international business, from purchasing inputs to providing after-sale service. The empirical evidence presented in research thus far relates only to selected stages in the value chain, but the call for company responses goes through all the stages. The terrorism resilience theory developed here emphasizes an integrative approach as the sum of relevant GVC stage protection or reconfiguration. The inputs affected by terrorism – from human resources to physical facilities to reputation – need to be managed differently at different stages of the GVC.

By grouping previous analyses along the GVC framework, we are able to demonstrate to company managers what strategies have been followed and made their way into literature. Based on the GVC stages, strategies to deal with the terrorist events and risks can be identified, and this view emphasizes the need for a strategy to be integrative. The examples discussed above can be understood as applications of our terrorism resilience theory that show direct and indirect terrorism impacts on the GVCs. And these impacts can be mitigated through the methods of resilience. These include both risk protection methods and re-configuration of the value chain, that is, ownership, location and control. For example, when production facilities have been attacked, such as financial offices on 9/11, or oil wells in the Middle East, or a hotel in the Indian example, or a supplier of a high value-added component bombed, a viable strategy is to operate multiple facilities or networks, or to contract out the facilities in question to third parties. Table 2 sketches the kinds of response that serve to protect the company against losses due to terrorist attacks on any aspect of the value chain.

--- Please insert Table 2 here ---

CONCLUSION

This article recognizes the increase in the number of terrorist attacks, its soft targeting trend that includes an increasing range of business targets, the variety of locations and targets, the extent of direct impact and in particular, potentially long-term indirect cost and opportunity impacts of terrorism. Our contribution provides structure to the prior literature and shows its relevance in an emerging field. It fills a research gap by providing a framework that allows effective investigation of global terrorism through the GVC by using the terrorism resilience theory. Each location that is part of a GVC has its (potential) terrorism vulnerability. However, the locations of an MNCs' value chain stages are interconnected and thus vulnerability in one location may affect other locations as well. Because the environment in each location may be unique, an MNC might opt for tighter or looser control as a response to the vulnerability. Most importantly, the managerial capacity to drive optimization, productivity, efficiencies, and performance along the GVC is crucial to manage terrorism risk. In other words, while one needs to consider the MNC and its GVC as a whole when looking at the impact of terrorism, its management is necessary in each stage.

Options for resilience to terrorism include the diversification or increase of suppliers, shortening of supply chains, protection materials and contracts, and strategic decisions about GVC re-configuration. This may include the re-evaluation of lean manufacturing, human resource management adaptation, the use of data analytics to measure terrorism trends versus vulnerability, the flexible protection of assets and resources, with suitable preparedness, response and community engagement, protocols, security infrastructures, i.e., GVC protection.

For example, a useful strategy for a given MNC's manufacturing facility is that it could be fitted with greater physical security and greater insurance. A company's financial center operations (and people) can operate with back-up, its dependence on a single supplier or a single location for high value-added inputs at any stage of the GVC can be diversified, its control over brand-related decisions tightened, its marketing and customer services trained to pre-empt and deal with impact, people protected with physical protection, insurance, and by moving them to locations in which suitable learning and training is provided, no matter the country, and networks are robust to support them. All of these strategies demonstrate the TRT's emphasis on strategic business adaptation across borders.

REFERENCES

Academy of International Business. 2007. Conflict, Security and Political Risk: International Business in a Challenging Environment. *Fifth Annual AIB Conference on Emerging Research Frontiers in International Business*, Florida.

Abadie, A., & Gardeazabal, J. 2008. Terrorism and the world economy. *European Economic Review*, 52(1): 1–27.

Adger, N. W. 2000. Social and ecological resilience: are they related? *Progress in Human Geography*, 24(3): 347–364.

Alon, Ilon, Rajesh Gurumoorthy, Matthew C. Mitchell, and Teresa Steen. 2008. "Managing Micropolitical Risk: A Cross-Sector Examination", *Thunderbird International Business Review*. Vol. 48, No. 5. pp. 623-642.

Bader, A. K., Reade, C., & Froese, F. J. (2017). Terrorism and expatriate withdrawal cognitions: the differential role of perceived work and non-work constraints. *International Journal of Human Resource Management*, Online First.

Bader, B. 2015. The Power of Support in High-risk Countries: Compensation and Social Support as Antecedents of Expatriate Work Attitudes. *International Journal of Human Resource Management*, 26(13): 1712–1736.

Bader, B., & Berg, N. 2013. An Empirical Investigation of Terrorism-Induced Stress on Expatriate Attitudes and Performance. *Journal of International Management*, 19(3): 163 – 175.

Bader, B., Berg, N., & Holtbrügge, D. 2015. Expatriate performance in terrorism-endangered countries: The role of family and organizational support. *International Business Review*, 24(5): 849-860.

Bader, B., & Schuster, T. 2015. Expatriate Social Networks in Terrorism-Endangered Countries: An Empirical Analysis in Afghanistan, India, Pakistan, and Saudi Arabia. *Journal of International Management*, 21(1): 63–77.

Bader, B., Schuster, T., & Dickmann, M. (2019). Managing people in hostile environments: lessons learned and new grounds in HR research. *International Journal of Human Resource Management*, Online First.

Barnes, P., & Oloruntoba, R. 2005. Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. *Journal of International Management*, 11(4): 519–540.

Beck, U. 2008. Reframing Power in the Globalized World. *Organization Studies*, 29(5): 793–804.

Beugelsdijk, S., Pedersen, T., & Petersen, B. (2009). Is there a trend towards global value chain specialization? - An examination of cross border sales of US foreign affiliates. *Journal of International Management*, 15(2), 126–141.

Bishop, Toby, 2009. *Corporate Resilience: Managing the Growing Risk of Fraud and Corruption*. New York, Wiley.

Boudes, T., & Laroche, H. 2009. Taking off the Heat: Narrative Sensemaking in Post-crisis Inquiry Reports. *Organization Studies*, 30(4): 377–396.

Brandt, P. T., & Sandler, T. 2010. What Do Transnational Terrorists Target? Has It Changed? Are We Safer? *Journal of Conflict Resolution*, 54(2): 214–236.

Branzei, O., & Abdelnour, S. 2010. Another day, another dollar: Enterprise resilience under terrorism in developing countries. *Journal of International Business Studies*, 41(5): 804–825.

Brown, S. & Eisenhardt, K. 1997. The art of continuous change: Linking complexity theory and time-paced evolution in relentlessly shifting organizations, Administrative Science Quarterly, 42, 1–34.

Buckley, P. 2011. “International Integration and Coordination in the Global Factory”, *Management International Review*. 51:269–283

Cattaneo, O., Gereffi, G., & Startitz, C. (2010). Global Value Chains in a Postcrisis World: A Development Perspective. Washington, D.C.

Chen, H., Chiang, R. & Storey, V. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, 36(4), 1165-1188.

Cheng, J. L. C., Guo, W., & Skousen, B. 2011. Advancing New Theory Development in the Field of International Management: Contributing Factors, Investigative Approach, and Proposed Topics. *Management International Review, 51*(6), 787–802.

Christopher, M. and Lee, H. 2003. “Mitigating supply chain risk through improved confidence”, *International Journal of Physical Distribution & Logistics Management*, 34(5): 388-96.

Coe, N. M., and Yeung, H. W. C. 2015. Global production networks: Theorizing economic development in an interconnected world. Oxford: Oxford University Press.

Cuervo-Cazurrra, A., Mudambi, R. & Pedersen, T. (2017). Globalization: Rising skepticism. *Global Strategy Journal*, 7(2): 155–158.

Czinkota, M. R., Knight, G. A., Liesch, P. W., & Steen, J. (2010). Terrorism and international business: A research agenda. *Journal of International Business Studies*, *41*(5), 826–843.

Czinkota, M. R., Knight, G. A., Liesch, P. W., & Steen, J. (2005). Positioning terrorism in management and marketing: Research propositions. *Journal of International Management*, *11*(4), 581–604.

Czinkota, M. R., & Ronkainen, I. A. (2005). A forecast of globalization, international business and trade: Report from a Delphi study. *Journal of World Business*, *40*(2), 111–123.

Czinkota, M. R., & Ronkainen, I. A. 2009. Trends and Indications in International Business. *Management International Review*, *49*(2), 249–265.

Doh, J., McGuire, S., & Ozaki, T. (2015). The Journal of World Business Special Issue: Global governance and international nonmarket strategies: Introduction to the special issue. *Journal of World Business*, *50*(2), 256–261.

Drakos, K. 2004. Terrorism-induced structural shifts in financial risk: Airline stocks in the aftermath of the September 11th terror attacks. *European Journal of Political Economy*, 20(2): 435–446.

Eisenhardt, K. M. & Graebner, M.E. (2007). Theory Building from Cases: Opportunities And Challenges, *Academy of Management Journal*, 50 (1), 25–32.

Enders, W., Sandler, T., & Gaibulloev, K. 2011. Domestic versus transnational terrorism: Data, decomposition, and dynamics. *Journal of Peace Research*, 48(3): 319–337.

Enderwick, P. 2001. Terrorism and the international business environment. *AIB Insights*, (Special Electronic Issue), 1-6.

Enderwick, P. 2006. Managing the new global Threats, *University of Auckland Business Review*, 8(2), 63-74.

Fleischer, A., & Buccola, S. 2002. War, terror, and the tourism market in Israel. *Applied Economics*, 34(11): 1335–1343.

Frey, B. , Luechinger, S. & Stutzer, A. 2007. Calculating tragedy: Assessing the costs of Terrorism', *Journal of Economic Surveys*, 21(1): 1-24.

Gephart Jr., R. P., van Maanen, J., & Oberlechner, T. 2009. Organizations and Risk in Late Modernity. *Organization Studies*, 30(2/3): 141–155.

Gereffi, G. (1999). International trade and industrial upgrading in the apparel commodity chain. *Journal of International Economics*, 48(1), 37–70.

Gereffi, G., Humphrey, J., & Sturgeon, T. (2005). The governance of global value chains. *Review of International Political Economy*, 12(1), 78–104.

Gereffi, G. & Lee, J. 2012. "Why the world suddenly cares about global supply chains", *Journal of Supply Chain Management*. 48(3): 24-32.

Gilbert, C., Eyring, M., & Foster, R. 2012. "Two Routes to Resilience", *Harvard Business Review*. (December). pp. 3-9.

Global Terrorism Database (GTD). 2018. National Consortium for the Study of Terrorism and Responses to Terrorism (START). Retrieved April 2017, from http://www.start.umd.edu/gtd/

Goerzen, A., Sapp, S., & Delios, A. 2010. Investor Response to Environmental Risk in Foreign Direct Investment. *Management International Review*, *50*(6), 683–708.

Grosse, R. 1989. *Multinationals in Latin America*. London: Routledge.

Grosse, R., 2016. *Emerging Markets: Strategies for Competing in the Global Value Chain*. London: Kogan Page.

Hanson, G. H., Mataloni, R. J., & Slaughter, M. J. 2005. "Vertical Production Networks in Multinational Firms", *The Review of Economics and Statistics*, 87(4): 664-678.

Harvey, M. G. 1993. A Survey of Corporate Programs for Managing Terrorist Threats. *Journal of International Business Studies*, 24(3), 465–478.

Hasnat, Baban, 2015. "US National Security and Foreign Direct Investment", *Thunderbird International Business Review*. Vol. 57, No. 3 May/June. pp. 185-196.

Institute for Economics and Peace. 2014. *Global terrorism Index.* Measuring and Understanding the impact of Terrorism, Retrieved August 20, 2015.

Intelligence Community Analytic Report (ICAR). 1995. *The Foreign Terrorist Threat in the United States*, 1, 95-13, July 1995, V.

Jabbour, M. J., & Thomas, S. 2015. From the Editors: Managing Risk and Resilience. *Academy of Management Journal*, 58(4): 971–980.

Jain, S., & Grosse, R. 2009. Impact of Terrorism and Security Measures on Global Business Transactions: Some International Business Guidelines. *Journal of Transnational Management*, 14(1): 42–73.

Kastenmüller, A., Greitemeyer, T., Aydin, N., Tattersall, A. J., Peus, C., Bussmann, P., … Fischer, P. 2011. Terrorism threat and networking: Evidence that terrorism salience decreases occupational networking. *Journal of Organizational Behavior*, 32(7): 961–977.

Kobrin, S. J. (2017). Bricks and Mortar in a Borderless World: Globalization, the Backlash, and the Multinational Enterprise. *Global Strategy Journal*, 7(2), 159–171.

Kotabe, M. 2005. Global security risks and international competitiveness. *Journal of International Management*, 11(4): 453–455.

Laqueur, Walter (1987) The Age of Terrorism, London: Weidenfeld & Nicolson.

Liou, D.-Y., & Lin, C.-H. 2008. Human Resource Planning on Terrorism and Crises in the Asia Pacific Region: Cross-National Challenge, Reconsideration, and Proposition from Western Experiences. *Human Resource Management*, 47(1): 49–72.

Lee, H.-J., & Reade, C. 2015. Ethnic homophily perceptions as an emergent IHRM challenge: evidence from firms operating in Sri Lanka during the ethnic conflict. *International Journal of Human Resource Management*, 26(13): 1645–1664.

McIntyre, J. & Travis, E. F. 2006. Global supply chain under conditions of uncertainty: economic impacts, corporate responses, strategic lessons. In: Suder, G. (Ed.) (2006). *Corporate Strategies under International Terrorism and Adversity*, E. Elgar Publications. (pp. 128-160).

McNulty, Y., & De Cieri, H. 2011. Global Mobility in the 21st Century: Conceptualising Expatriate Return on Investment in Global Firms. *Management International Review*, *51*(6), 897–919.

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2015). *Global Terrorism Database* [gtd1993_0814dist.xlsx]. Retrieved from https://www.start.umd.edu/gtd.

Organisation for Economic Co-operation and Development (OECD) (2002). OECD Risk awareness tool. Organisation for Economic Co-Operation and Development, Paris.

Oetzel, J. M., & Getz, K. 2011. Why and how might firms respond strategically to violent conflict? *Journal of International Business Studies*, 43(2): 166–186.

Oetzel, J. M., Bettis, R. A., & Zenner, M. (2001). Country risk measures: how risky are they? *Journal of World Business*, 36(2), 128–145.

Oh, C. H., & Oetzel, J. 2011. Multinationals’ response to major disasters: How does subsidiary investment vary in response to the type of disaster and the quality of country governance? *Strategic Management Journal*, 32(6): 658–681.

Pananond, P. (2013). Where Do We Go from Here?: Globalizing Subsidiaries Moving Up the Value Chain. *Journal of International Management*, 19(3), 207–219.

Pananond, P. (2015). Motives for foreign direct investment: a view from emerging market multinationals. *Multinational Business Review*, 23(1), 77–86.

Paulus, P., & Mühlfeld, K. 2017. Host country language skills and expatriates’ cross-cultural adjustment in the presence of fear of terror. *Journal of Global Mobility*, *5*(4), 418–442.

Porter, M. E. 1985. *Competitive advantage: creating and sustaining superior performance*. New York: Free Press.

Prieto-Rodríguez, J., Rodríguez, J. G., Salas, R., & Suarez-Pandiello, J. 2009. Quantifying fear: The social impact of terrorism. *Journal of Policy Modeling*, 31(5): 803–817.

Reade, C. 2009. Human resource management implications of terrorist threats to firms in the supply chain. *International Journal of Physical Distribution & Logistics Management*, 39(6): 469–485.

Reade, C., & Lee, H.-J. 2012. Organizational Commitment in Time of War: Assessing the Impact and Attenuation of Employee Sensitivity to Ethnopolitical Conflict. *Journal of International Management*, 18(1): 85–101.

Roche, E. and Blaine, M. (2014) The Intelligence Gap: What the Multinational Enterprise Can Learn From Government and Military Intelligence Organizations, *Thunderbird International Business Review*, 57 (1), January/February, 3–13.

Rose, A. (2009) A Framework for Analyzing the Total Economic Impacts of Terrorist Attacks and Natural Disasters, *Journal of Homeland Security and Emergency Management*, 6(1): 1547-7355.

Rugman, A. M., Verbeke, A., & Nguyen, Q. T. K. 2011. Fifty Years of International Business Theory and Beyond. *Management International Review*, *51*(6), 755–786.

Schneckener, U. 2002. *Netzwerke des Terrors*, Berlin: Stiftung Wissenschaft und Politik, December.

Sheffi, Y.. 2002. Supply chain management under the threat of international terrorism. *The International Journal of Logistics Management,* 12(2): 1-11.

Sheffi, Yossi, and Rice, 2005. “A Supply Chain View of the Resilient Enterprise”. *Sloan Management Review*. (Fall). pp. 41-48.

Shrivastava, P. 2005. Managing Risks in the Age of Terror. *Risk Management, 7*(1): 63–70.

Siggelkow, N. (2007). Persuasion with case studies. *Academy of Management Journal*, 50: 20–24.

Spich, R., & Grosse, R. 2005. How does homeland security affect US firms’ international competitiveness?, *Journal of International Management*, 11(4): 457–478.

Stevens, C. E., & Newenham-Kahindi, A. (2017). Legitimacy Spillovers and Political Risk: The Case of FDI in the East African Community. *Global Strategy Journal*, 35(1), 10–35.

Suder, G. (Ed.) 2004. *Terrorism and the International Business Environment*. Edward Elgar Publications, Cheltenham.

Suder, G. (Ed.) 2006. *Corporate Strategies under International Terrorism and Adversity*, E. Elgar Publications , Cheltenham.

Suder, G. & Czinkota, M. R. 2005. Towards an understanding of terrorism risk in the MNE, *Multinational Business Review*, 3(3): 3–23.

Suder, G., Liesch, P., Inomata, S., Meng, B., Michaelova, I. 2014. The evolving geography of production hubs and regional value chains across East Asia: Trade in value-added, *Journal of World Business*, 50(3): 404-416.

Sullivan-Taylor, B., & Wilson, D. C. 2009. Managing the threat of terrorism in British travel and leisure organizations. *Organization Studies*, 30(2/3): 251–276.

UNCTAD. 2013. World Investment Report: Global Value Chains: Investment and Trade for Development. http://unctad.org/en/PublicationsLibrary/wir2013_en.pdf

US Census Bureau, 2018. QUARTERLY RETAIL E-COMMERCE SALES 1st QUARTER 2018. https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

Wagner, S. M., & Bode, C. 2006. An empirical investigation into supply chain vulnerability. *Journal of Purchasing and Supply Management*, 12(6): 301–312.

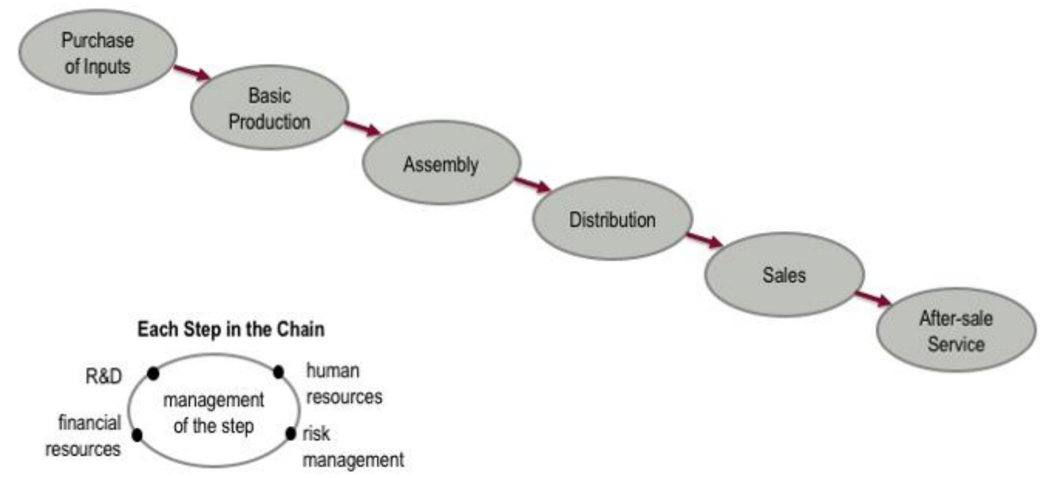
Wang, X., & Nayir, D. Z. 2006. How and when social network is important? – Comparing European expatriates’ adjustment in China and in Turkey. *Journal of International Management*, 12(4): 449–472.

Wernick, D. A. 2006. Terror incognito: International business in an era of heightened geopolitical risk. In G. Suder (Ed.), *Corporate strategies under international terrorism and adversity*. Cheltenham, UK: Edward Elgar Publishing Ltd.

Wernick, D. A., & Glinow, M. A. Von. 2012. Reflections on the Evolving Terrorist Threat to Luxury Hotels: A Case Study on Marriott International. *Thunderbird International Business Review*, 54(5): 729–746.

Zsidisin, G. A., Melnyk, S. A., and Ragatz, G. L. 2005. An institutional theory perspective of business continuity planning for purchasing and supply management. *International Journal of Production Research*, 43(16): 3401-3420.

Figure 1a: The Global Value Chain



revised from Grosse 1989, p. 159

Figure 1b: Terrorism in the Global Value Chain

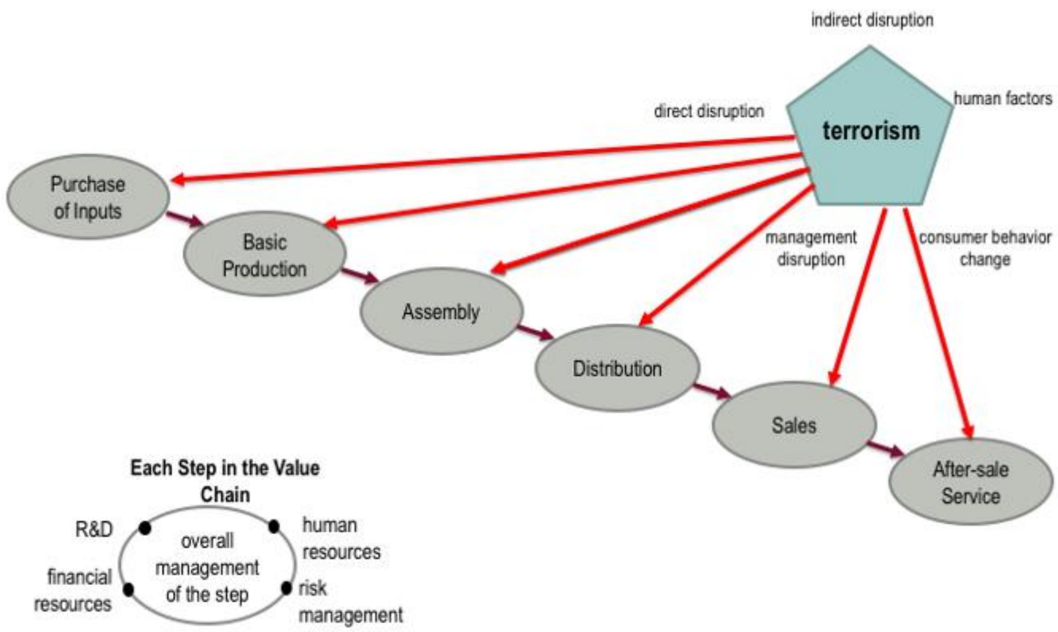


Table 1. Business Adaptation and Risk Transfer as Terrorism Resilience Methods

Business Adaptation Methods	Risk Transfer/Business Protection Methods
Locate facilities away for terrorism-prone locations	Use insurance policies such as the US government's TRIA program
Contract out production or other terrorism-prone activities to third parties	Build physical protection of facilities such as bomb-proof walls and metal detectors
Establish redundant facilities in case of attack on any one of them (as banks had in the 9/11 attacks)	Design software to avoid hacking or other computer/internet borne attacks
Train people to be able to operate more than one of the company's facilities, in case people at another facility are incapacitated	Hire protection companies such as Pinkerton or Kroll

Table 2 – Terrorist actions and responses in the value chain

Value chain stage	Terrorist action	Impacts/Costs	Responses
Purchase of inputs	Attack oil well or mine	Loss of needed production inputs	Diversify suppliers; add security to facilities
Basic production	Kidnap employees; attack factory or HQ	Hurts people; damages/destroys property	Add security protection; diversify production locations
Transport of goods along value chain	Destroy pipeline; hold up delivery vehicles	Destroys/damages property	Add alternative suppliers
Point of sale	Attack stores or clients	Hurts people and/or destroys/damages property	Add security protection
Input at each value chain stage			
Human resources	Create perception of threat by employees	People de-motivated; higher cost of insurance	Provide greater protection; avoid high-risk assignments
Research & development	Attack research facilities; cyber-crime	Potential loss of technology	Locate R&D away from terror-prone locations; invest in cyber-security
Risk management	Create new risks to facilities, people	Raises risk management costs	Protect with security; use insurance; diversify