CHAPTER 17

MASSIVE CONVENTIONAL TERRORIST ATTACK AS A THREAT TO CRITICAL INFRASTRUCTURE SECURITY

EKATERINA STEPANOVA

Dr. Ekaterina Stepanova is Senior Fellow and Programme Leader of the Armed Conflict and Conflict Management Programme at the Stockholm International Peace Research Institute (SIPRI), Stockholm, Sweden.

1. Introduction

The main focus of this chapter is the interface between terrorism and the security of the technological and economic systems vital for the functioning of society and the economy – the so-called critical infrastructures (CIs). When it comes to this subject, there is a certain disconnect between experts on technology, weapons and infrastructure security, on the one hand, and academic experts on terrorism, on the other. While technicians and managers prioritise the vulnerabilities of infrastructure and risks in terms of what is technologically possible, terrorism experts focus on the motivations and organisational forms of groups that employ terrorist means. They also highlight the specifics of terrorism as a form of political violence, compared to other forms of armed violence.

Terrorism is the most asymmetrical form of political violence, as it is designed in such a way that its broader destabilising political and psychological effects (human effects) go far beyond its actual damage to human lives or infrastructure. When it comes to terrorism, the sheer number of casualties, incidents, metres of pipeline or the number and size of buildings destroyed is of less critical importance than terrorists' *ability to affect politics* through the use of or threat to use violence against civilians or infrastructure *in an asymmetrical way,* that is, by causing a disproportionately high impact with relatively limited means. This ability depends on the political context, the timing, the type of society that is under attack or the broader disruption that an attack on a physical object can cause. A terrorist incident

may, for instance, result in limited damage and/or casualties, but still achieve its goal of political destabilisation. Terrorist acts of a certain type may be extremely rare – such as the high-profile mass-casualty Islamist attacks on transport systems in Madrid in March 2004 or London in July 2005 – but have significant political impact.

In this sense, for terrorists to pose a threat of global and strategic significance, there is no need to cause a catastrophe on a global scale. Rather, a terrorist threat amounts to a global one if terrorists manage to affect global politics or politics globally. Whether and the extent to which this ability is related to attacking CI – or necessitates CI collapse – is the subject of this chapter.

The specifics of terrorism as an asymmetrical form of political violence are crucial for defining "massive terrorism". When applied to terrorism, the term "massive" means "mass- or high-impact" rather than "mass destruction" or "mass casualties". Mass casualties and destruction may be an important part of, and significantly contribute to, a terrorist act's high impact, but are neither a *sine qua non*, nor, at times, sufficient to produce the broader politically devastating and destabilising effect – the mass impact – that terrorism aims to create.

The primary means of choice for massive terrorist attacks remain *conventional* and are dominated by conventional bombings.[1] While weapons, explosives and other materials and means of delivery employed by terrorists tend to be relatively available, inexpensive and, in most cases, not particularly sophisticated, the use of these standard, conventional means can produce catastrophic consequences. Terrorists have also infrequently used non-conventional – chemical, biological, radiological and nuclear (CBRN) – materials and weapons, but all the *mass destruction* caused by terrorism has so far resulted from the use of conventional means.[2] Of the larger non-conventional terrorist attacks in the past 25 years, only the 1995 attack on the Tokyo subway by Aum Shinrikyo had a mass impact,[3] but even that attack resulted in less damage and disruption than large-scale conventional terrorist attacks, which are incomparably more widespread, consistently more deadly, have caused more damage and, in most cases, have a larger impact than non-conventional attacks.

[1] It needs to be stressed, however, that for terrorists, weapons, materials and other technical means, while important, are not the main strategic resources or the most critical advantage in their asymmetrical confrontation with the state or the international community. Rather, their main strengths and comparative advantages are the extremely high mobilising power of their extremist ideologies in certain segments of society, coupled with the unconventional organisational forms and models employed. For more detail see E. Stepanova, *Terrorism in Asymmetrical Conflict: Ideological and Structural Aspects* (Oxford: Oxford University Press, 2008). This combination is also supported by rapidly upgraded information and communications capabilities and the growing financial autonomy of violent non-state actors, including those employing terrorist means.

[2] At the time of writing, all mass-destruction terrorist attacks have been exclusively carried out with the use of conventional explosives, such as the bombing of the Federal Building in Oklahoma City by Timothy McVeigh or the bombings of the United States embassies in Kenya and Tanzania by al–Qaeda, or with "unconventional" use of conventional means, such as flying the hijacked civil aviation airliners into the World Trade Center and the Pentagon on 11 September 2001.

[3] For more detail, see J.V. Parachini, "Comparing motives and outcomes of mass casualty terrorism involving conventional and unconventional weapons", *Studies in Conflict and Terrorism*, Vol. 24, No. 5, September 2001, p. 390.

[4] Author's calculations based on incident data from the Global Terrorism Database (GTD–2), http://www.start.umd.edu/data/gtd.

2. Policy Challenges

(a) The Scale of Terrorist Threats to Infrastructure

A sound way to start is to ask how often infrastructure assets and nodes become targets of terrorist attacks, compared to other targets. The available data show that infrastructure targets have remained a relatively underexploited resource for terrorists. Critical infrastructure makes up a relatively minor share of modern terrorists' targets, lagging far behind civilians and places of public gathering, as well as political or government-related targets. For instance, the 547 infrastructure targets attacked by terrorists in 1998-2004 formed less than 7 percent of the global total of 7954 terrorist targets in the same period.[4]

Of the 547 infrastructure attacks, 51 percent targeted rail and road transport; 30 percent targeted utilities, including energy infrastructure; 11 percent targeted air transport; four percent targeted (tele)communications; two percent were directed against maritime transport; and 1.5 percent were aimed at food and water supply, making public transport systems (air, ground, underground) the most favoured infrastructure targets for terrorists.

(b) Attacks on Public Transport Systems: The Limited Overlap between Mass-casualty and Infrastructure Terrorism[5]

While there is some overlap between mass-casualty terrorism and infrastructure terrorism, it is mostly confined to attacks on *public transport systems*. Terrorists, from the global to the local, tend to prioritise attacks in public places that by definition have a high potential to result in mass casualties. However, even terrorist attacks against transport systems only partly overlap with mass-casualty attacks, while attacks against other types of infrastructure usually do not cause mass casualties. Long before the events of 11 September 2001, the absolute majority of multiple-target cases where mass-casualty attacks overlapped with attacks against infrastructure were accounted for by attacks on public transport. For instance, of the total of 76 mass-casualty bombings carried out in the second half of the 20th century,[6] only 34 involved attacks on infrastructure – almost exclusively transport systems, predominantly airlines and airports (17 incidents) but also trains and railway stations (seven incidents), buses and bus terminals (six incidents) and, less frequently, ships and ferries.[7] More recently, in 1998-2004, 15 percent of all attacks against airlines, 13.5 percent of attacks against other transport systems (rail and bus) and 10 percent of attacks against maritime targets were mass-casualty attacks.

If an attack primarily aims at mass casualties by targeting public gathering places, its link to critical infrastructure – usually, public transport systems and nodes – may simply be instrumental, that is, a critical transport system is chosen as a target mainly to inflict and magnify casualties and to underscore the attack's symbolic meaning, which was apparently the case for the attacks of 11 September 2001. Both civilians and critical infrastructure per se may be equally important targets when a terrorist attack aims to cause mass casualties and,

[5] Mass-casualty terrorist attacks can be defined as indiscriminate attacks primarily on civilians, resulting in 25 or more civilian casualties, and may range from large-scale attacks (up to hundreds of casualties) to catastrophic attacks when casualties are counted in thousand(s), such as the events of 11 September 2001 in the United States.

[6] For the list of bombings see C. Quillen, "Mass Casualty Bombings Chronology", *Studies in Conflict and Terrorism*, Vol. 25, No. 5, September 2002.

[7] Mass casualty bombings that involve non-transport infrastructure appeared to be an exception rather than the rule and included one industrial target (a cement factory run by the Palestinian Liberation Organisation) and two financial infrastructure targets: the Bombay Stock Exchange bombed in March 1993 and the Central Bank in Colombo, Sri Lanka, bombed in January 1996.

for instance, destabilise transport systems (as demonstrated by the Madrid and London bombings).

In contrast, if the terrorists' main targets were energy, information and communications systems, water supply, banking and finance or other infrastructure, the attack would not necessarily aim at or result in mass casualties or, in fact, in casualties as such, although the destabilising impact might be significant. Only 4.5 percent of attacks against telecommunications systems and 1.8 percent of attacks against utilities, and no attacks against food and water supply systems, resulted in mass casualties.[8]

It is not surprising that attacks in public places that by definition have a high potential to result in mass casualties, rather than attacks against infrastructure per se, appear to be the priority targets for terrorists of different types and at different levels from global to local. While a mass-casualty bombing in a crowded public place speaks for itself as a terrorist act, an attack against infrastructure may not necessarily be easily or immediately recognised as such. Attacks in public places, including public transport systems, rank first in terms of targets for al-Qaeda-inspired transnational terrorists,[9] followed by government-, police- or security forces-related targets, foreign nationals or tourists. The highest-ranking of all infrastructure targets other than public transport – the oil industry – ranks only fifth.[10] Overall, the past and present dynamics of terrorist attacks reveal that the main vulnerabilities to a massive attack have been underscored by the juncture of major public gatherings and public infrastructure, especially public transport systems. It is this combination that is most likely to result in a catastrophic attack. The latest worrying sign is a clear and relatively recent trend for a growing number of mass-casualty attacks against transport infrastructure other than air transport.

[8] Author's calculations based on GTD data (GTD–2), *op. cit.*, note 4.

[9] Not to be confused with the use of terrorist means, alongside other tactics of armed struggle, by territorially based Islamist movements combining Islamism with nationalism (e.g. by Lebanese Hezbollah in the 1980s and 1990s or by Palestinian Hamas).

[10] A. Schmid, "Terrorism and Energy Security", Memorial Institute for the Prevention of Terrorism (MIPT) Insight Report, March 2007, pp. 1-2.

(c) Attacks on the Energy Sector and Other Infrastructure in the Context of Protracted Armed Conflicts

Most infrastructure attacks other than those targeting public transport are relatively low-scale in terms of casualties and damage, causing limited and localised disruption that allows for relatively rapid recovery. If these attacks have become more frequent, better coordinated and more disruptive, it is mostly at the local and national levels, in the context of select ongoing armed conflicts – usually in hydrocarbon-rich areas with extended energy infrastructure, such as Nigeria, Colombia or the post-2003 Iraq. For instance, 45 percent of attacks in Nigeria in 1998-2004 targeted infrastructure. Although 90 percent of the infrastructure targets were oil-related, mostly personnel kidnappings, only one highly disruptive pipeline explosion would qualify as a mass-impact event, and even it did not result in mass casualties. Colombia suffered 20 percent of all infrastructure attacks worldwide from 1998 to 2004 (19 percent of all terrorist attacks in Colombia in these years targeted infrastructure, either independently or in combination with other targets). Attacks against infrastructure in Colombia have so far shown the highest level of coordination, compared to other areas of armed conflict, and frequently involve simultaneous attacks on several infrastructure targets at once. The targeting has been highly diversified, with 54 percent of all infrastructure targets related to the energy sector, 27 percent to transport, 10.5 percent to the financial sector and 5.7 percent to communications. Nonetheless, no more than 15 percent of all the infrastructure attacks had any impact beyond localised disruption and there were only two mass-casualty attacks on infrastructure in the seven-year period.[11]

A more recent example of direct attacks against infrastructure aimed at undermining the basis of the "enemy" economy is provided by the frequent blowing up of pipelines by insurgents in post-invasion Iraq. Complete and up-to-date post-2003 data on attacks against infrastructure targets in Iraq are not yet available, but some sources put the number of oil-related attacks in the first three post-invasion years at 300. While attacks against infrastructure, particularly against the energy sector, in areas of such protracted armed conflict usually contribute to preventing oil-sector recovery or complicate oil exports, the

[11] All calculations made by the author on the basis of data available from the Global Terrorism Database (GTD–2), *op. cit.*, note 4.

direct damage, whether in Iraq, Nigeria or Colombia, is usually relatively quickly repaired.

Apart from these areas, the relatively limited scale and impact of most attacks against infrastructure may partly be explained by the fact that most of the infrastructure nodes and hubs that governments deem "most critical" are not soft, but hard targets. These "harder" targets range from nuclear plants to oil infrastructure hubs (processing plants) and liquefied natural gas (LNG) terminals. Not surprisingly, cases of attempted large-scale disruption of such hard CI nodes, such as the failed attack at the world's largest oil processing facility, Abqaiq in Saudi Arabia, in February 2006,[12] remain exceptions rather than the rule. In contrast, some of the physical assets in utilities infrastructure, including oil and energy infrastructure (large oil fields, thousands of miles of pipelines or electrical cables) are much softer targets and absolute physical protection is often hard to ensure. However, most of the damage caused to such an extended infrastructure, including that which results from intentional attacks, tends to be localised and the system can be repaired relatively quickly. In other words, the more critical the infrastructure element or function, the harder it is to target, while the softer it is as a target, the less critical it is.

3. Responses

Infrastructure security strategies address vulnerabilities to all sorts of damage, disturbance and harm, including catastrophic attacks, natural disasters and industrial or technological incidents. These threats range in scale from adverse events to potential catastrophes (low-probability but high-consequence events that, on average, comprise about one percent of all adverse incidents). Despite the reservations made above, in the post-11 September 2001 context, critical infrastructure security strategies, particularly that of the United States (US), are still dominated by two interrelated strategic approaches.

The first approach to preparedness for and response to threats to critical infrastructure has evolved from the one-hazard (terrorism-centred) strategy of the years immediately after 2001 to the two- or

[12] For more detail on the attempted attack and its impact on Saudi energy security, see K.R. Al-Rodhan, "The Impact of the Abqaiq Attack on Saudi Energy Security", Center for Strategic and International Studies paper, Washington, DC, 27 February 2006.

multiple-hazards approach of the second half of the decade. The terrorism-centred, one-hazard approach primarily focused on protecting critical infrastructures and key assets from terrorist attack, and paid less attention to more common threats. This approach was clearly followed by the US government in the aftermath of 11 September 2001, and anti-terrorism dominated the prevention and preparedness activities of the Department of Homeland Security. Following the CI collapse in the US Gulf Coast as a consequence of the failure to respond to Hurricanes Katrina and Rita in 2005, the US government started to approach infrastructure security with a greater focus on selected dangers not limited to terrorism. Strategically, the imbalance was addressed by shifting from a one-hazard approach to a multiple-hazards approach tailored to hedge against several, select anticipated (both natural and man-made) disasters. This approach has long been the preferred choice for and within the European Union.

In line with the one or multiple-hazards visions guiding the dominant threat perceptions in the world's leading states, until recently the dominant response strategy, both in the US and elsewhere, has been almost exclusively centred on *CI protection*, that is, on the protection of concrete assets and structures from imaginable, anticipated and predictable dangers. This approach is dominated by *prevention* and *resistance* strategies that are disproportionately affected or even, at times, dictated by ad hoc reactions to the latest largest threat or disaster (be it a series of massive terrorist attacks or a series of particularly destructive natural disasters). As this approach is tied to hedging against a few larger scale expected man-made, technological or natural disasters, it unsurprisingly fails to hedge against future, often unexpected, threats or to accurately predict them. The CI-protection approach mostly relies on formal, relatively centralised command and control arrangements and on a narrow professional elite, such as security agencies and other "first responders". Its communications strategy emphasises specialised technology or inter-agency communication and "one-to-many" communication with the population.

The need for a certain degree of CI protection against more regular and better known threats can hardly be disputed and will inevitably be higher for some infrastructures, such as public transport, CBRN-related infrastructure, and so on, than for others. Overall, however, the protection-centred approach has been generated by, and is better tailored to, the culture, economy and logic of the past industrial

era and is hardly adequate or sufficient for the post-industrial, globalising, information-age world.[13] One example of this culture and logic was the harsh political and public reaction in the US to the US Foreign Investment Committee's approval of the purchase from a British firm of the six largest US port facilities (New York, New Jersey, Philadelphia, Baltimore, New Orleans and Miami) by Dubai Ports World, which is owned by the government of Dubai. As it became clear that the political controversy was not subsiding, eventually, the competitive and efficient Dubai Ports World had to sell the US port operations to a US buyer.[14] This scandal not only undermined an economically sound and beneficial deal and hampered foreign investment, it was also a political insult to a US ally. It also demonstrated the dominance of overly protective "fortification" political and public moods and perceptions in the US post-11 September 2001.

One of the main reasons behind the continuing endurance of this mechanical protection-centred approach as a guiding strategy of CI security, despite its growing inefficiency, may have little to do with technology or threat assessment. It can be better explained by certain political and business interests that financially and politically benefit from projects centred on protective systems and technologies, even as the intense lobbying activities of these interest groups waste much of the homeland security budget. Not surprisingly, the political actors and business contractors that benefit from the status quo are unwilling to make any fundamental, rather than piecemeal, changes to the inflexible and, by now, obsolete CI protection vision and practices.

4. Dilemmas and Implications

Infrastructure: how critical? The standard definition of CI refers to economic sectors and technological systems that are both vulnerable and vital for the security and stable functioning of a society. It usually

---

[13] See, e.g. L.J. Perelman, "Shifting Security Paradigms: Toward Resilience" in "Critical Thinking: Moving From Infrastructure Protection to Infrastructure Resilience", Critical Infrastructure Protection (CIP) Discussion Paper (Washington DC: George Mason University, 2007), p. 26.

[14] "US lawmakers criticise ports deal", *BBC News*, 21 February 2006, http://news.bbc.co.uk/2/hi/ americas/4734728.stm; M. Jacobson and D. Jacobson, "Middle Eastern Investment in the United States: Avoiding Another Dubai Ports World Controversy", The Washington Institute Policy Watch No. 1240, 5 June 2007, http://www.washingtoninstitute.org/pdf.php?template=C05&CID=2611.

implies transport; the energy sector, water supply and other utilities; communications; the banking and financial sector; the chemical, biological and nuclear industries, and so on. The disruption, let alone destruction or collapse, of these systems would be likely to significantly adversely affect the state, society and the economy.

In protection-centred approaches to CI security, priority is determined by the presumed degree of infrastructure's criticality, that is, how critical it is for the stable functioning of the economy and society. However, from the point of the potential impact of infrastructure disruption on public security and the stable functioning of the economy, the very notion of criticality needs to be questioned. There are at least two major problems with criticality as it is understood within a protection-oriented CI framework that emphasises preparedness and response to the small number of anticipated risks to selected infrastructures.

First, the protection-centred approach fails to differentiate between infrastructure that may be critical from the point of view of the safe and stable functioning of the economy and society and that which is critical for terrorists. While groups engaged in terrorist activity, on the one hand, and governments or businesses, on the other, may both view some infrastructure, such as key transport nodes, as critical, not everything that is critical for the economy and society automatically becomes a critical target for terrorists, in terms of maximising the political and psychological impact of potential disruption. For instance, national or international key assets, such as major monuments and iconic buildings, skyscrapers or large government facilities that play more of a symbolic than functional role, may be no less – or even more – critical, desirable and accessible targets for terrorists than some CI sectors.

Second, the CI-protection approach fails to take account of the relative nature of what is or may become critical in a modern dynamic globalised economy. Indeed, with the exception of public transport, the nuclear and oil industries and the drinking water supply, it is increasingly hard to know which assets are most critical in the globalised economy. In fact, given the overall level of global interdependence and efficiency optimisation, *any* infrastructure, including production of a seemingly routine commodity or material, may turn out to be critical at some point – it may even be the case that a seemingly localised breakdown may suddenly become a matter of urgent global concern.[15] The degree of its criticality is often unclear before a disruption occurs: if even industry insiders can hardly predict such critical breakdowns, how can political terrorists be expected to be aware of the relative criticality of economic infrastructure assets?

The problems with criticality and the sheer impossibility of protecting all infrastructures from all threats are not the only challenges in the CI security domain. Of the many other dilemmas with implications for critical infrastructure security, the two most frequently cited are:

- *National versus international responsibility*: While critical infrastructure security is primarily a *national* responsibility, listed as a "domestic security measure" by the United Nations (UN) Counterterrorism Committee and as one of the homeland security mission areas by the US Government, threats to infrastructure increasingly involve cross-border or *transnational* disturbances or *international* attacks. In a globalising world, new information, communications, energy and transport technologies lead to more infrastructure becoming part of larger international networks. This highlights the shared interest in protecting against common threats. These interests require international cooperation, even though there are many obstacles to such cooperation, including, for instance, objective gaps in the technological potential and resources and differences between various national CI systems.
- *State versus private control and responsibility*: Some of the main differences between the developed post-industrial states and societies and the less developed states are in the degree of state and private control of CIs. In the West, a specific challenge to CI protection is the need to protect largely decentralised, privately owned and run assets that make up the lion's share of CI. For instance, 85 percent of CIs in the US are privately owned and the US Department of Homeland Security

[15] The textbook example is provided by the explosion at a Sumitomo Chemical Co. plant in Japan in 1993 that led to major disruption of the global computer industry caused by a shortage of computer chips, as the company provided 60 percent of the high-grade epoxy resin for integrated circuit packages, but the critical cut was not made before the actual disaster occurred. Virtually all the rest of the world's supply was provided by another Japanese firm. For more detail see J. Robertson, "Sumitomo epoxy resin plan gutter", Reed Business Info Electronic News, 12 July 1993.

has responsibility in only five of the 13 CI sectors. In many other countries, such as China or Russia, much of the critical infrastructure is run by the government, and this higher degree of state control by default implies a greater role for the state in CI protection. Many countries, however, are less dependent on high-technology information and management systems in CIs than the most economically developed states, which – ironically – might partly compensate for the less developed states' endemic weaknesses in ensuring CI security, such as the general inflexibility of CI systems, the lack of market solutions and insufficient funding.

5. Future Trajectories: Why Terrorist Threats to Infrastructure Security Matter

Terrorist and other intentional attacks, such as sabotage and criminal activities, are relatively important threats to critical infrastructure but are hardly the most common threats, compared to technological incidents or natural disasters. However, even though it is important to keep in mind all of the reservations made above about the scale of terrorist threats to critical infrastructure, this chapter argues that the importance of the issue is not too much exaggerated, or at least not as hugely overstated as, for instance, the issue of CBRN terrorism, for at least four reasons.

First, compared to technological or natural disruptions, terrorist attacks may have additional types of effect on infrastructure. In addition to *direct infrastructure effects* (disruption of function through direct attack on a critical node or system), most large-scale disruptions, man-made or otherwise, also have some *indirect infrastructure effects*, such as cascading disruption, financial consequences for the state and society and some degree of destabilisation – often through public and private *reactions* to an attack. The overall level of direct damage even from major terrorist attacks is incomparably lower than, for instance, that from natural disasters or technological catastrophes. However, neither technological incidents nor natural disasters are specifically planned and designed to maximise their indirect, broader destabilising effects, while terrorist attacks are. Furthermore, for terrorists, indirect effects, including those from attacks on infrastructure, are usually more politically important than direct damage. In addition to direct damage and indirect effects, terrorists may seek to gain control of infrastructure elements and nodes in order to exploit them to disrupt another target. This third element is specific to deliberate, man-made terrorist, sabotage or criminal attacks.

Second, in the post-11 September 2001 context, terrorism is not only commonly regarded as the main threat to infrastructure, but also as a heavily anticipated one. But is it really a well-predicted and predictable threat? While one may, of course, try to assess or predict the general potential for terrorism in a given country, as, for instance, the Economist Intelligence Unit did as part of The Global Peace Index initiative,[16] the abundance and diversity of vulnerable, soft, non-military targets in modern societies and the wide variety of forms and manifestations of terrorism make it hard to predict massive attacks in general. It is even harder to identify concrete CI targets in particular, beyond the usual exceptions of key public transport systems and select conflict-torn areas with extensive energy infrastructure and hydrocarbon resources. The intersection of large concentrations of people and transport systems is one of the obvious choices for modern non-territorial, transnational terrorists such as al-Qaeda-inspired cells that, due to their transnational global agenda, may aspire to affect global politics. However, as is noted above, the most frequent of the other infrastructure targets – the oil industry – only ranked fifth out of transnational terrorists' targets. Otherwise, it is particularly hard to predict which concrete infrastructure targets are likely to be favoured by these ideologically rather than operationally connected autonomous, self-generating cells with an explicitly transnational agenda.[17]

Third, as security increases around more predictable targets, such as airports and airlines, terrorists tend to shift their focus to less protected assets. In other words, if terrorists need a critical target, including an infrastructure target, they will find one: simply enhancing counterterrorist protection measures for one target or type of target with little or no net security benefit to other infrastructures only makes it more likely that terrorists will favour the other targets.

---

[16] Global Peace Index, "Methodology and Data Sources", http://www.visionofhumanity.org/gpi/about-gpi/methodology.php.

[17] Attempts to solve the problem at the national level (e.g. in the United States) by strengthening an outside perimeter or border regime, rather than hardening each critical infrastructure object individually, cannot suffice, as today's terrorist threats are rarely purely external or purely internal and the boundary between the two has become more blurred than ever.

Finally, coming back to terrorists' willingness and ability to exploit various "unconventional" ways, if not necessarily non-conventional materials, to magnify the scale and impact of their attacks, it may be easier for them to experiment with *targets* than with *means*, that is, they may prefer to step up attacks against infrastructure, which is still an underexploited target resource, than to attempt to acquire CBRN potential.

6. Policy Recommendations

The terrorism-specific challenges to critical infrastructure identified above provide the basis for concrete policy recommendations for both public authorities and, where appropriate, the private sector. If a heightened focus on a mass terrorist attack as a threat to CI is of some added value in solving the dilemma of the relative criticality of CI, then security investment should prioritise sectors and nodes: (a) that are subject to *all three types of effects* from terrorist attacks (direct disruption, indirect destabilising effects and exploitation for the purpose of hitting other targets); and (b) that the increased security of which would produce some net security benefit for other infrastructure sectors.

It is also clear from the above that, even as terrorist attacks on infrastructure may, in rare cases, involve CBRN materials, excessive security investment to protect against the CBRN terrorist threat should be avoided. More attention should be paid to increasing civil infrastructure security, especially that of public transport systems, vis-à-vis a range of threats, including mass terrorist attacks – a goal that poses a no less significant challenge than CBRN-related security issues.

The two broader, and not necessarily terrorism-specific, strategic directions for improving CI security can be summarised as follows:

- *From a multiple hazards to an all-hazards approach.* A mere switch from a one-hazard to a multiple-hazards strategy cannot substitute for the most comprehensive *all-hazards approach*, as the selection of several hazards, rather than a single hazard, for official attention and security investment implies excluding other hazards, including unknown and unanticipated threats. It is more important to recognise that one simply cannot anticipate all possible hazards and to plan both on the basis of what is known and on the expectation of surprise threats and risks.
- *Beyond protection: Resilience against uncertainty.* The growing internal complexity of public and private organisations and the diversity and multiplicity of risks, internal vulnerabilities and external threats bring factors such as uncertainty and unintended consequences to the forefront of CI security. They call into question traditional risk management approaches that involve the linear process of planning, preparedness, response and recovery. Of growing importance for CI security is the adaptability and resilience of organisations, rather than mere protection from and resistance to multiple and often unpredictable threats. Not surprisingly, a gradual shift in national security perceptions and priorities from CI protection to CI resilience has been observable in recent years.

In contrast to a protection-centred strategy, the *CI resilience* approach aims to achieve systems designed with an ability to adapt to change under conditions of uncertainty. Resilience here implies ability to withstand and recover from surprise and unanticipated threats – whether physical threats or, for instance, resource shortage – either back to the original state or an adjusted state based on new requirements. The resilience-centred approach implies adaptation and endurance through flexibility, agility and acceptance of and reliance on socio-technical innovation. Reduction of the infrastructure vulnerability profile is achieved through a combination of redundancy, lower cost, dispersal, reduced scale, self-healing and self-adaptive capability, accelerated repair and recovery, and so on.

In terms of control and management strategies, the resilience approach takes account of the fact that modern complex systems often tend to behave in unexpected ways, with many unintended consequences, and opts for "adaptive management" rather than the more traditional tight command and control arrangements. In terms of communications strategy, resilience is best provided by and associated with the network-type "many-to-many" models that take full account of the new social-technical environment of the "information age" of mobile telephones, the Internet and the blogosphere, rather than the hierarchical one-to-many communications pattern. The flexible and adaptive many-to-many communications systems have little or no

critical infrastructure to protect, not to mention that they save on the costs associated with huge infrastructures.[18]

Examples of relatively resilient systems, employing different instruments and elements of resilience, range from the Saudi oil infrastructure nodes that combine physical protection with abundant redundant capacity, preventing disruption of infrastructure function,[19] to the relatively resilient crisis management and response system in London,[20] which largely worked, if not perfectly, in the aftermath of the July 2005 terrorist attacks, allowing the public transport system to resume normal operations the next day and limiting the economic impact for London, the United Kingdom and the global financial markets to a relatively minor one.

7. Conclusions

Both protection and anticipation strategies to hedge against highly probable, or expected, risks, and measures to increase adaptability and resilience that are more appropriate for unexpected threats are needed for CI security. The balance between the two may vary from one infrastructure to another: for transport systems where the threats are more easily identifiable, the main focus is by default on protective measures, while, for instance, in information technology, telecommunications and the financial sector, greater emphasis on resilience, diversity and redundancy is a must. A balanced approach combining systematic action to reduce known risks and the capacity to quickly adapt to unknown or unanticipated risk is the optimal CI security strategy. It is also one that is most in line with the general drive in CI security strategies and practices towards an all-hazards approach.

Last but not least, a more resilient infrastructure is also less attractive to a group planning a massive terrorist attack of any type. A balanced strategy that combines protection against known attacks with resilience against uncertain ones not only better suits the critical infrastructure security needs of a post-industrial, information age, but may also provide a more adequate response to the large-scale threats posed

[18] A good example of a resilient communications system is provided by Skype – a decentralised communications system that distributes peer-to-peer (P2P) software among millions of users around the world.

[19] Al-Rodhan, *op. cit.*, note 12.

[20] For more detail, see the website of the interagency London Resilience Partnership, http://www.londonprepared.gov.uk.

by actors employing terrorist means. In fact, modern terrorists, especially modern non-territorial, supranational al-Qaeda-inspired cells, appear to have mastered resilience better than governments have. They offer little or no critical infrastructure to attack, have developed advanced Internet-generation information and communications capacities and have adopted loose, adaptive and resilient organisational forms and patterns of coordination.[21]

[21] For more detail see Stepanova, *op. cit.*, note 1, pp. 140-149.