Social values and material threat: the European Programme for Critical Infrastructure Protection

J. Peter Burgess

International Peace Research Institute, Oslo (PRIO)
E-mail: peter@prio.no

Abstract: Since the outset of Europe's role in the War on Terror, the protection of Europe's 'critical infrastructures' has been a central focus of the anti-terrorist effort. The purpose of this article is underscore the challenges involved in conceptualising critical infrastructure and its protection in terms of *social values*. These difficulties, we will suggest, are not merely roadblocks standing in the way for effective anti-terror policy making. They challenge European policy makers in all fields to revisit and reflect upon the meaning and aim of anti-terror protection.

Keywords: European programme for critical infrastructure protection; European Union; terrorism; social value; culture; threat.

Reference to this paper should be made as follows: Burgess, J.P. (2007) 'Social values and material threat: the European Programme for Critical Infrastructure Protection', *Int. J. Critical Infrastructures*, Vol. 3, Nos. 3/4, pp.471–487.

Biographical notes: J. Peter Burgess is Research Professor at PRIO, the International Peace Research Institute, Oslo, Leader of PRIO's Security Programme, and Editor of *Security Dialogue.* He coordinates a number of international research projects in the fields of risk, security and political culture. He has published 11 books and over 40 articles in the fields of political science, security studies, philosophy, history and cultural studies. His most recent article, 'dialektischer Kosmopolitismus' is forthcoming in the *Zeitschrift für internationale Beziehungen 13(2).*

1 Introduction

Central to traditional arguments for motivating European construction and, not least, for winning the hearts and minds of its sceptics have been the evocative notion of a common European history, culture and values. Certain essential traits shared by all or most Europeans, it is alleged, make desirable or even inevitable institutionalisation of that commonality through the European project.[1] Even from the sober perspective of neo-functionalism, a certain idea of shared interests is central to explaining the successes and failures of the European project. Yet among the many European responses to the terrorist attacks of 9/11 and in particular the subsequent attacks of Madrid and London, the European has been a far less evocative and far less idealistic or spiritual concern for European commonality: the fate of Europe's shared critical infrastructure.

Since the outset of Europe's role in the War on Terror, the protection of Europe's 'critical infrastructure' has been a central focus of the anti-terrorist effort. Indeed, in the four intervening years since the attacks in New York and Washington witnessed a flurry of political activity, beginning with the adoption in the European Council of a "Proposal for a Council Framework Decision on Combating Terrorism" (Council of the European Union, 2001a) and leading through a rapid evolution to the release, on 17th November 2005, of a Green Paper on a EPCIP.

Yet, what does the focus on critical infrastructure aim to achieve? What are its assumptions and what can it accomplish? It is clear that the pending plans for a comprehensive EPCIP have the potential tremendous utility, gathering knowledge and experience for protecting a range of structures that play a crucial role is our way of life. However, conventional thinking about 'protection' in general and "critical infrastructure protection" in particular is inadequate to meet the challenge posed by transnational terrorism. The problem, we will argue in the following, lies in the basic understanding of what threat is, what it means to predict it, what it means to react to it, and what special challenges are brought by the new era of transnational terrorism. The purpose of this paper is to underscore some of the difficulties and challenges involved in conceptualising critical infrastructure and its protection in terms of *social values*. These difficulties and challenges, we will suggest, are not merely roadblocks standing in the way for effective anti-terror policy making. They force the European policy makers in all fields to revisit and reflect upon the meaning and aim of anti-terror protection.

2 Defining critical infrastructure through terrorist threat

Of course, reflection on the nature of terrorism and responses to it did not begin in 2001. The pre-history of the European Union anti-terrorism policy-making reaches as far back as 1997 and policies formulated by the Council of Europe (1977). To the degree that it brings innovative provisions to the entire field of justice and home affairs, the Treaty of Amsterdam (European Commission, 1997) also contributes an important set of principles on the nature of terrorism in Europe. Terrorism was also considered by the European Councils of Tampere in 1999 and Santa Maria da Feira 2000 (http://eu.eu.int/en/info/eurocouncil.htm) and was central to the Commission's 2000 review of progress on the creation of the area of "freedom, security and justice" (European Commission, 2000).

Still, quite naturally, the attacks of 11th September 2001 gave rise to a new generation of reflection on terrorism. EU political leaders acted swiftly after in the days following the attacks, culminating in an initial plan of action released on 21st September 2001 (Council of the European Union, 2001a). Yet, it is first at the close of 2001, in a "Proposal for a Council Framework Decision on Combating Terrorism" that the Council begins to come to grips with the complicated matter of setting out the terms and definitions of the fight against terrorism.

The Framework Decision takes its point of departure in the *principles* upon which the European Union and the project of the European construction are based, deriving from these principles both the justification for combating terrorism and the guidelines for carrying out the combat. 'Terrorism', it confirms, is a violation of the basic principles of the European construction, "a threat to democracy, to the free exercise of human rights and to economic and social development" (Council of the European Union, 2001b). And yet, the move from the understanding of terrorism as the violation of a set of principles to the challenge of protection of critical infrastructure is a large though unavoidable one. Article 1 of the decision, 'Terrorist offences' defines terrorism along three general lines:

- "seriously intimidating a population"
- "unduly compelling a government or international organisation to perform or abstain from performing any act"
- "seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation".

The latter definition covers both a broad range of actual violations and the *threat* of committing such violations: attacks on individuals and their personal integrity, including kidnapping, hijacking, the development of certain types of weapons, the release of certain substances, interfering with or disrupting water supply such that human life is endangered and what can best be considered a notion of attack on critical infrastructure:

> "… causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss." (Council of the European Union, 2001b)

Destruction what we generally speak and understand as *critical infrastructure* (we will return to this term below) is thus defined as a 'terrorist offence' in the cases where such destruction is likely to 'endanger human life' or 'cause economic loss'. The definition contains two elements, the first concerning human life, the other concerning economic loss.

- In substance, the kind of destruction that causes the endangerment or loss of human life relates to 'conventional' discussions of terrorism. These include, among other things, the problem of distinguishing between a terrorist attack and ordinary assault or murder, the question of the intentionality of causing terror, fear or an experience of threat, in addition to juridical issues of criminality. (The Council in the same document follows the USA in distancing the European conception of terrorism from a criminal act, instead ascribing the terrorist to the class of 'warrior' to which the conventional rules of war can be applied).
- Destruction of the kind that causes 'major economic loss' makes a circular reference to a primitive definition of infrastructure: objects of destruction that imply economic, instead of human loss. Human loss refers to the first type of terrorist destruction. The notion of economic loss, on the contrary, seeks to distinguish purely material objects: bridges, railroads, waterworks, electrical facilities and internet services. The potential loss they imply is understood as the earning potential implicit in such infrastructure. When such infrastructure is destroyed, it can no longer generate earnings.

This first post-9/11 approach to the notion of infrastructure is thus built on an essentially economic distinction between income-generating and non-income-generating objects. In any common sense perspective, the distinction is indispensable but not as water-tight as one might wish. Not the least, it is clear that human loss could just as easily be construed as loss of economic value. Without work, there is no generation of income.

3 The problem of critical infrastructure protection after Madrid

The Madrid bombings on 11th March 2004 brought the spectre of trans-national terrorism to the European doorstep, accelerating the political efforts to confront this threat. The terrorist attacks were not the first instance of terrorist violence in Europe, far from it. But they constituted the first major European event stemming from a new generation of terrorism, and thus set in motion a new phase of political action and a new effort to understand the threat at hand.

On 25th March 2004, the European Council published its "Declaration on combating Terrorism", setting out the updated European strategy against terrorism. The Declaration reiterates the assertion of the pre-9/11 Declaration that terrorism is an attack "against the values on which the Union is founded" and builds its response in particular on a theme of international 'solidarity' (Council of the European Union, 2004a). This solidarity, reiterated in the "Declaration on Solidarity against Terrorism" annexed to the same document, has a double scope. On the one hand, it intends to link the European experience of terror brought home in Madrid on March 11th with the US experience of 9/11, drawing political force from a tense transatlantic relation (Rees and Aldrich, 2005). On the other hand, it evokes a certain acutely European specificity in the experience and understanding of the attack and lays the foundation for a particularly European response. While it is true that the language of solidarity corresponds in part to the invocation of Article 5 of the NATO Charter by the USA after the attacks of 9/11 (Gordon, 2001) referring as it does to Article 42 of the draft Constitutional Treaty, it also evokes the notion, emerging from the discourse of the European values implicit and explicit in the text that a particularly European attack requires a particularly European response. This is not the first manifestation of a European attempt to forge an alternative policy to the US approach in the War on Terror; it is, however, an important element in matching the European vulnerabilities with the European capacities (Hoffmann, 2003). In a different light, however, by underscoring the notion of 'solidarity' in Article 2 of the "Declaration on Combating Terrorism" the European Council also sets out the primary precondition for advancing the concept of *European* critical infrastructure, namely the *interconnectedness* of European commerce and livelihoods through transnational infrastructures. While it may be true that the destinies of Europeans are linked through their shared spiritual heritage espoused by Jean Monnet in the early days of the European project, they are unavoidably linked through the material structures and infrastructures upon which they share a dependence.

The 25th March Declaration provides considerably impetus for the preparatory actions on the part of the Council and the Commission. On 20th October 2004, the Commission releases not less than four documents that prove central to the European approach to terrorist threat in general and to critical infrastructure in particular. The scope of the European anti-terror strategy is set out in the communication "Prevention, Preparedness and Response to Terrorist Attacks" (European Commission, 2004d) underscores the importance of dialogue between public and private sectors that will prove essential to the protection of privately held critical infrastructures. It notes the need for both cooperation between national agencies and coordination with third-country agencies responsible for infrastructures of importance for European commerce. Measures directed toward commercial interests are further detailed in the Commission communication on the "Prevention of and the Fight against Terrorist Financing" (European Commission, 2004b). "Preparedness and Consequence Management in the Fight against Terrorism" (European Commission, 2004c) focuses on preparation for the aftermath of terrorist attack, including events related to infrastructure.

4 The threat to infrastructure

The concepts and principles that form the basis for the project of protecting critical infrastructure in Europe are set out in a fourth Commission communication, "Critical Infrastructure Protection in the Fight against Terrorism" (European Commission, 2004a). It is here that officials first begin to grapple with the challenge of defining the criticality of critical infrastructure, of understanding what threatens it and formulating approaches to protect it.

The communication begins with the assumption that motivates the entire project of confronting terrorist threat, namely that "the potential for catastrophic terrorist attacks that affect critical infrastructures is increasing". The political climate of our time, both in the wake of the previous attacks in the USA and Europe, and the US-lead War on Terror, have increased the likelihood of attacks. A subset of such potential attacks either target critical infrastructure or carry secondary affects for them. But what additionally makes the communication's fundamental assertion truer and perhaps more essential for the well-being of European society is the reality that Europeans, to varying degrees across social, cultural, religious and geographical boundaries, are increasingly dependent upon high technological infrastructures, first and foremost, internet and telecommunications.

Infrastructures by their very nature are interconnected, 'synergistic', as the communication points out. They link other facilities and other kinds of physical installations across broad geographical spaces. They are also synergistic in terms of the way they join different segments of society. Infrastructures traverse any number of sectors of industry, different zones and levels of local, regional, state and inter-state economies, different layers of the life of individuals, cultures and societies. This is already the case at the national level, but given the cultural variations across national borders it is even more relevant on the European level.

There is also variation across the differing types of infrastructures covered by the strategy. The notion of 'critical infrastructure' is itself defined in the communication as:

> "… those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health safety, security or economic well-being of citizens or effective functioning of governments." (European Commission, 2004a)

The understanding of critical infrastructure is necessarily *negative*. What is in essence critical about critical infrastructure is based on what may be the result of the critical infrastructure being lost or damaged. It is a scenario of the absence of resources, services and facilities that creates their value in the effort to prevent their destruction. Yet the meaning of such absence or loss is highly variable, not only across the vast variety of social settings where such disruptions are more or less variable, but also across the different types of infrastructures such as they are set out by the official documents. According to the Commission communication, these substantial types are: energy installations and networks, communications and information technology systems including software, hardware and the internet, finance and banking facilities, health care facilities such as hospitals and research facilities, pharmaceutical production, means of food production and distribution, water storage and delivery, transport facilities such as airports, sea ports, railways transit networks, production, storage and transport of hazardous goods, and government services (European Commission, 2004a). The variety of types of critical infrastructures leaves one at pains to generalise about their common characteristics in technical or structural terms. Yet what links them all is their transformability into something of *value* for a society and a culture.

5 Prioritising infrastructure

In addition to the list of substantial critical infrastructure installations, the Commission communication also identifies a set of *relational* aspects of critical infrastructure. These are *scope*, *magnitude* and *effects of time*. These three 'measures' of the criticality of critical infrastructure essentially plot the overlapping spheres of value and threat. 'Scope' refers to the geographic area that would be affected by loss or unavailability of the infrastructure. It thus measures both actual physical interconnectedness of installations in different geographical areas, and also the economic and social interconnectedness of the areas. The physical overlapping of spheres implies a social interdependency as well. 'Magnitude' is meant to measure the *degree* of weakening or collapse of one infrastructural installation as a function of the other. It is thus another measure of interconnectedness, one which considers the 'vertical' penetration of influence, a depth-version of measurement of the value of the infrastructure in one sector of society (civil, economic, cultural, environmental, political, etc.) relative to an other. Lastly, *effects of time*, is also a measure of the social and cultural resilience of infrastructure. It does not measure the time necessary for replacing potentially damaged infrastructure, but rather the ability of the social function to re-establish itself by the same means, or by other alternative means. It thus measures a kind of culturally determined flexibility, taking into account the emotion and psychological effects of the damage.

These socially and culturally determined qualifiers of infrastructure vulnerability provide the basis for what the Commission communication calls security or risk 'management': the process of "understanding risk and deciding upon and implementing actions to reduce risk to a defined level, which is an acceptable level of risk at an acceptable cost" (European Commission, 2004a, p.3.2). Risk, like the anticipation of attack or damage by natural cause is, to an important degree, based on perception of danger, assessment of value and consideration of likelihood. It is not solely a function of calculation but rather also of understanding. It has a socially, culturally, even religiously determined character. In other words it involves inter-subjective reactions to interdependent physical structures. The exception may of course be reactions to the internet understood as critical infrastructure. Although it exists as a complex physical infrastructural installation, its existence for most is more or less imaginary. And though most have become accustomed to interruptions and slow-downs, the prospect of a total breakdown approaches the unthinkable. Ironically the internet was first conceived in the 1960s as a communication system that could withstand nuclear attack (Castells, 1996, p.45).

5.1 Toward a European Programme for Critical Infrastructure Protection

The European Council of 17–18 June followed on its Declaration of 25th March by emphasising the urgency of acting in a number of priority areas, in particular, intelligence and the exchange of information. The Commission was asked to prepare an "overall strategy to enhance the protection of critical infrastructures" (Council of the European Union, 2004c). In its Fall meeting in 2004 the Council affirmed the Commission's intention to propose both a EPCIP and a Critical Infrastructure Warning Network (CIWIN) at the same time as it approved the European Union 'Solidarity Programme' (Council of the European Union, 2005b) and the Commission communication on "Prevention, Preparedness and Response to Terrorist Attacks" (Council of the European Union, 2004b).

The 2004 Commission communication concludes by announcing a plan to enhance the EU's ability to protect critical infrastructure though the institution of a EPCIP. The document defines the EPCIP as:

> A programme to provide enhanced security for critical infrastructure as an ongoing dynamic national partnership among EU institutions, critical infrastructure owner/operators and EU Member States to assure the continued functioning of Europe's critical infrastructure. (European Commission, 2004a, Annex)

In addition, the communication proposes the organisation of a Critical Infrastructure Warning Information Network (CIWIN), which it defines as:

> A EU network to assist member states, EU institutions, owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure. (European Commission, 2004a, Annex)

The coupling of the two programmes, one for the protection of transversal installations and structures, the other for transversal communication expresses the need for interaction across a number of spheres. Transversal communication is not only among the technical needs in order to assure the effective coordination of critical infrastructure protection, it is also among the very objects of the protection. (The various forms of communication and synchronisation necessary in order to give the EPCIP its desired 'transboundary' effect will also include protection of the CIWIN). As we have already indicated and will explore further below, it is precisely the transversal dimension that presents the greatest challenge to the coordination of critical infrastructure protection, both on the technical/security level and in terms of the institutional support necessary in order to make sense of a variety of infrastructure installations across a variety of domains and social, economic and cultural settings. This is because the transversal axes that link similar or identical installations do not forcibly link identical risks. In this sense, the shift in the Commission communication from concern for horizontal variation in the nature and intensity of risk and threat to the *physical* and financial similarities between linked installations is reflected again in the EPCIP Green Paper of November 2005.

Like so many inter-state affairs that fall under the aegis of the European Union, the institutional challenges of critical infrastructure are considerable. The 2004 communication evokes the well-travelled notion of *subsidiarity*, noting the practical impossibility of protecting all infrastructures by "European level measures" and underscoring that a number of directives and regulations already existing on the European level and that any further action must take the form of assistance for industry and Member State governments. Consistent with the principle of subsidiarity, it constitutes yet another Commission proposals with the aim of enhancing harmonisation, coordination or cooperation, but leaving to national infrastructures the responsibility of the national agencies and private owners.

What information can and should be shared between Member States? On what terms and under what conditions can information about critical infrastructure in one Member State or in one locality or region, for that matter, be relevant in terms of protecting infrastructures in others. To what degree and in what sense is information about threatened electrical supply in Portugal useful and transferable to authorities as close by as southern France? In one sense or another, to be sure. Yet the associability of the two cases is clearly limited. And no doubt that associability will have its most comprehensive effect in one domain in particular: the transferral of *the image of vulnerability and fear*. In other words: the successful execution of terrorism.

On 13th April 2005, the Commission establishes the framework programme on "Security and Safeguarding Liberties" (2007–2013) containing a programme for the "Prevention, Preparedness and Consequence Management of Terrorism" (European Commission, 2005a). One month before the July London bombings, the Council approves the revised Action Plan on Terrorism explicitly announcing the intention to establish a general strategy for a programme for protection of critical infrastructure "with potential transboundary effects". Finally, following the London attacks, the Council issues a "Declaration on the EU response to the London bombings" in which it reaffirms its commitment to establishing a EPCIP. When the Council sums up progress on the EPCIP in October of 2005, it underscores the same need. "There is recognition that Member States have ultimate responsibility of managing arrangements for protection of critical infrastructure with their national borders" (Council of the European Union, 2005a). The political motivation within the Commission and Council is thus solid and the events make the need for a strategy for critical infrastructure protection no less imperative. After two consultation seminars in the Fall of 2005, the Green Paper on EPCIP is released.

5.2 The cultural significance of critical infrastructure in the EPCIP Green Paper

The *aim* of the EPCIP, as formulated in the Green Paper, is "to secure that there are adequate and equal levels of protective security on critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements throughout the Union". The paper itself takes the form of a set of questions with the aim of obtaining feedback. Like most key documents, the EPCIP Green Paper stands and falls upon its concept and definitions. The political process of developing the EU doctrine on critical infrastructure, which we have briefly charted here, develops a consistent set of definitions, beginning with the basic definition of 'critical infrastructure' set out in the 2004 Commission communication "Critical Infrastructure Protection in the Fight against Terrorism" cited above.

Yet, where the CIP document of 2004 attempts to provide an exhaustive list of nine concretely related critical infrastructure, The EPCIP Green Paper does not limit the notion of infrastructure to the *material* objects or facilities from whose loss we might suffer. Instead, it further differentiates three types of 'infrastructure assets':

- public, private and governmental infrastructure assets and interdependent cyber and physical networks
- procedures where relevant individuals that exert control over critical infrastructure function
- objects having cultural or political significance as well as 'soft targets', which include mass events (i.e., sports, leisure and cultural) (European Commission, 2005b).

This way of forming the conceptual matrix of the EPCIP is a prudent one. Given the challenges of interactivity, synchronising and harmonisation, the concrete differences between infrastructures and the variation between the criticalness of these infrastructures is formidable. By focusing on the 'assets' provided by infrastructures, one can more adequately reach their socially and culturally underlying value underpinnings and thereby begin to understand the meaning of threats to them. Firstly, "public, private and government" assets are variable according to Member State governmental structures, political structures and overall makeup of the national political systems of government, in addition to local infrastructural facilities, geographical and economic settings, reach and intensity of use and dependency on internet, etc. Second, the structures of private and public ownership of infrastructure facilities are dependant upon state and regional laws, regulations and norms, and the particular level of saturation of infrastructure by agencies of control. Lastly, and perhaps most neglected in earlier conceptualisations of the critical infrastructure protection, are the "objects having cultural or political significance".

The EPCIP Green Paper thus seeks, in its way, to take hold of the reality that critical infrastructure does not *only* include physical installations, oil platforms, railroads, pipelines, generator stations, etc., but also the somewhat *less* material or physical items that support them or which, as the case may be, are independent of them. These are the networks of socially and culturally determined values, which precede, presuppose, surround and help to operate the heavy physical installations. They are the 'procedures', the knowledge-based principles of operation as well as the knowledge itself, which form the basis of the existence and operation of the critical infrastructure. This also includes the norms and standards of operation on which such operation is based.

It is important to underscore the degree to which this third kind of critical infrastructure overlaps not only with the other two 'assets' but with the first category of critical infrastructures, the heavy installations. Indeed that one type of critical infrastructure cannot be distinguished from the other, for *all* critical infrastructure has cultural and political significance. That is what makes it critical. There is no critical infrastructure that does *not* have cultural significance. Or rather an infrastructure that does not contribute in a broad sense to creating or transforming social, cultural and political value is not *critical*. Moreover, this is the very reason why it is under threat. The threat to Europe's critical infrastructure is not, or not totally, to be derived from the economic value with which it is associated, not because of the economic value of the oil, electricity, service and information it delivers. The distinction between critical infrastructure, on the one hand, and 'infrastructure assets' formulated by the Green Paper, which have "cultural or political significance", on the other, is a false one. The cultural and political significance of infrastructure is precisely what makes it critical, what makes it a critical infrastructure. All critical infrastructure has cultural and political significance. Indeed it is not the objective or material value of any given installation that makes it an interesting target for terrorist attack, but rather its cultural and political valence. Its value springs from its ability to generate cultural and political meaning. Indeed my suspicion is that targets with higher social, cultural and political value may actually be more attractive to potential attackers than the more apparently vulnerable ones.

The threat of terror thus should rightly open a debate on values, about what is valuable and valueless, about what is dispensable and indispensable. What is value and how do we measure it?

6 Material and non-material value

There is a wide range of theories of value (Joas, 1997, 2000; Simmel, 1989 (1898); Durkheim, 2004 (1924); Mesure, 1998; Kuhn, 1975; Edel, 1988).[2] For our purposes we wish to simply differentiate between and economics-based notion of value and a culturally or social-based notion. According to neoclassical economics, the *value* of a thing is identical to the *price* it would bring in an open market. It is the worth of something relative to the other things. Historically the debate on economic value has revolved around the degree to which things have *intrinsic* value, and such value can be added or transformed. According to the more culturally or socially based conceptions of value, the value of a thing is based on the particular *quality* of thing that makes it valuable, i.e., either principles or standards that are socially accepted or moral ideas about what is good and right.

Thus, in social terms, it is the not the *materiality* of infrastructure that determines its value to society and thus to terrorism; it is rather the social, culturally determined *ideas* of value, historically, geographically, environmentally, and also economically determined standards and measures. It is therefore not sufficient to refer solely to material or economic measures of value when considering critical infrastructures. This is true for at least three reasons.

- The market value of commodities produced, converted, or transported by critical infrastructures varies as a function of a number of non-objective variables such as confidence, trust, fear, political climate and current events. The variation in oil price is a significant example of this, but not the only.
- The cost of financing, or re-financing critical infrastructures (also) varies as a function of non-rational or non-material factors, with fear, mistrust and insecurity at the forefront.
- Threat is in part *created*, or at the very least supported, by the presence of critical infrastructures. The construction of infrastructure entails the construction of threat. Therefore the *value* of critical infrastructure is not determined by, but certainly linked to, the danger of its destruction. The concept of 'critical infrastructure', and in particular the *criticalness* of critical infrastructure is a product of the age of transnational terrorism.

There is thus the need for a kind of return to conceptual basics, to the basic ideas, concepts and definitions surrounding social values in Europe, in order to adequately understand the challenge European critical infrastructure. One basic principle is that *threat* involves an *assessment of value* and that value is a fundamentally social, cultural and ethical term. To determine a threat is to situate a thing – in this case, critical infrastructure – in a system of values that are structured and determined by the sphere of European society and culture. What then is a threat?

7 Threat and social value

A threat is not simply an unknown danger lying in wait, ready to be launched upon us in some unknown way at some unspecified time. Threat is not incidental or accidental, or at least not entirely so. Nor is the effect of a threat independent of those targeted by it. Threat is not determined by others alone. It is co-determined by those who are under threat. For this reason, it is the presence of critical infrastructure, which creates threat by virtue of creating value. Threat is implicitly linked to what has value for us. It is linked to the possibility that what we hold as valuable could disappear, be removed or destroyed. Objects of no value cannot be threatened in the same sense as those that do have value. The key to understanding threat therefore lies in understanding the value systems which link human *interests*, *values* and things, such as infrastructures. We must understand the way that these values are connected to the technological systems and infrastructures that in turn support them.

What, then, is the threat of *terrorist* attack? Terrorism goes well beyond ordinary threat by aiming at the *fear of loss* of what has value, and by aiming to produce a signal effect of meanings about the insecurity *that is already presents*. How are value, threat and fear linked? The ideal terrorist act tries to find the perfect fit between what we value, the fear of its loss implicit in that value, and the political interests sought by those who carry out the act, though this link is however never perfect or ideal. While infrastructure experts know and understand technical weaknesses in critical infrastructures, the threat analysis must also take into account the potential destruction of material things and the social, cultural, spiritual and even moral values they are associated with.

Thus, if the programme of protection launched by the EPCIP Green Paper is successful, it will be so because it succeeds not only to encourage *material* protection for valuable critical infrastructures but rather because it encourages *semiotic* protection, that is, protection against the creation of unwanted symbolic meaning (Baudrillard, 2001, pp.39, 40). It is not the disrupted trains service, or oil production, not even the poisoning of a local water supply, for example, which is significant for the terrorist, as horrible as these things may be. Rather, it is the loss of *confidence* in rail service, oil production, water supply and in infrastructural services, in general.

It is not the reality of a computer virus in itself that we have to fear and which a terrorist might use as his or her tool, but rather the fear of the release, the presence of a negative *symbolic* virus, the contagion of insecurity, which disseminates distrust and fear, both in the world of private commercial services around which the European society is organised, but also in terms of international trust and faith in a globalised market system. We must therefore not fall back into a logic of the military fortress in which the protection of material supplies is a key to victory. We must remain aware of the socially and culturally determined systems of meaning, which are the central concern of a terrorist threat. It is less our physical security that needs assurance, as it is our *moral* insecurity.

8 The value of destruction

Nothing is worth protecting or even saving if it does not have value. Nothing that serves or unites what we hold to have value can be abstracted from a certain kind of value. With this indispensability is inextricably associated the 'cost' of its loss and the negative foundation of its worth to us and to others. Perhaps more crucially is this context of a response to terrorist threat, to the insertion of a concern for the value of critical infrastructure into the war on terror: nothing is worth attacking if it has no value. As absurd or uncivilised as it might be characterised by many, terrorism has a distinct function and logic. Indeed it is this logic, which assures the force of its name. If we know something to be terrorism – and all the signs of our public discourse would indicate that we do – then there is a distinct structure or form to it, and thereby a distinct predictable. By the same token, terrorism respects a certain logic of threat. Terrorism formulates a certain aim; be it predominantly the aim of causing fear, weakening social and political solidarity, disrupting the institutional function of society, and disrupting the exercise of casually expected freedoms of liberal society, it is clearly instrumental (GAO, 2005; O'Neil and Dempsey, 1999–2000).[3] It is a means to an end; judge as one must both its ends and means, it obeys, more or less efficiently, an instrumental rationality. International networks of terrorist financing accelerate and consolidate the standardisation and generality of this tendency (Lia, 2005, pp.96–140). Terrorism thus chooses its targets and its means of attack in a manner that lends itself to predictability. The central axis of this logic is, for the terrorist as it is for civil society, in turn the notion of value. Terrorism is without effect if it does not effect what has value for others. Both the ability to successfully weaken society by attacking its infrastructure and the ability to protect society by protecting its infrastructure depend on a calculus of value, value that is socially and culturally determined.

The economic-material view of value is particularly inept at seizing the value of spectacle implicit in today's terrorism. The new generation of terrorism creates the spectre of a new kind of destruction, namely the *spectacular*. One of the great innovations of the 11th September attack on New York was that it was orchestrated in order to take place before the eyes of millions. The menace is based on what was orchestrated. The understanding of critical infrastructure, first conceptualised by the US Office of Homeland Security, then exported, like so many things American, to Europe, is based on a new approach, a new set of questions to security in general, and on a new set of questions about what is secure and how to secure it. Yet, ironically enough, our infrastructures were not equally 'critical' before the moment they became presumed objects of terrorist attacks. In other words, the 'threat' of terrorism has taught us what is 'critical'; it has shown us how to distinguish the 'critical' from the 'non-critical'. Indeed the threat to our infrastructures has drawn attention to how 'critical' they actually are, leading us to wonder whether our critical infrastructures actually had the same value before the era of trans-national terrorism as they do now.

9 The cross-border effects of terrorist threat

What about the so-called 'cross-border effects'? The EPCIP Green Paper takes pains to differentiate between 'critical infrastructures' in general and 'EU critical infrastructure'. The latter, according to the Commission communication is "determined by its cross-border effect, which ascertains whether an incident could have a serious impact beyond the territory of a Member State (MS) where the installation is located" (European Commission, 2005c). The notion of interdependency of critical infrastructures is thus recognised and developed within the EU doctrine. A particular kind of infrastructure is exposed to a particular variety of linked or transnational threat.

Yet, from a certain point of view, this categorisation of interdependency begs the very question of transnational terrorism. For what characterises the terrorist threat of our day and age is precisely its interdependence. There is no terrorism that does not – through the forces of globalisation, through the media, networks of exchange of information – exploit the interconnectivity of critical infrastructure that both connect the world through the interwoven nature of the global economy and through the interconnectedness of the global information society.

Despite the overt material loss involved in a major terrorist attack, it is not the *physical* interconnectivity of critical infrastructure – the interlinking of plants and facilities – that is decisive in the determination of threat. It is far more the interconnectivity of people who share, values and who experience them as threatened by their relation – surmised, presumed, calculated or predicted – to other events.

The interconnectivity associated with the attacks of 11th September 2001 that truly counts, has little or nothing to do with the 'real' or material connection to the events, the loss of services from the destruction offices and murdered clerks and lawyers, the deliveries rendered impossible, the lost train connections because of collapsed underground stations. Rather, the lost interconnectivity is related to the self-assurance of all workers in all skyscrapers the world over in the aftermath. Yes, there is real destruction in terrorist violence, let there be no doubt about it. But the *terrorism* itself does not lie in the *real* destruction; it lies in the *transferral* of that real destruction to imagined or possible destruction. That transferral happens through the informational and economic interconnectedness of the global society, not in the simple, material interconnectedness of the critical infrastructure. The (EPCIP) Green Paper, like conventional thinking about terrorist violence in general, thus does not address protection against terrorism, but rather protection against material breakdown or damage.

10 Classical war and the logic of terrorism

For better or worse the notion of consequence management, such as it is formulated in the EPCIP Green Paper, rests on such an idea of *protection*. But what is protection? Protection, as it is formulated in this and other relevant documents, implies a calculable, verifiable, and most importantly, repeatable relationship between the object, the value of the object and the value of the gains made by destroying. This relationship, what philosophers would call 'instrumental rationality', is, for example, clearly visible in scenarios of conventional early-modern warfare of the kind theorised by von Clausewitz in *On War* (1978 (1832)). Where a critical infrastructure, let us say an oil refinery, contributes to the economic or technological nourishment of an enemy combatant, in this case by producing fuel and other petroleum-based products to be used in the prosecution of war, destroying or damaging the installation shifts the balance of the conflict in favour of the attacker. Furthermore, many ethical philosophers would agree that such destruction falls under the aegis of what is called *jus in bellum*, the just or correct prosecution of war, depending, of course, on the nature and motivation of the war in general.

The function of the conventional war target is instrumental. It can be interrupted instrumentally. The function of a terrorist target is psycho-symbolic. Its logic must be understood differently. It is clear that the European infrastructure is under threat. But the logic of this threat is entirely different than that which permits a response that is in tune with our expectations. In a late-modern war, a railway installation could very well serve as the object of attack. Experts in the fields of critical infrastructure, in their planning, development and operation are at least as technically capable – most likely more capable – than terrorist attackers who would seek to disrupt them. Security against terror is thus not a competition between two technical heads. It is not a battle of the engineering brains whereby we deploy all our technical know-how in order to develop technological systems to shelter against aggression that will take the form of technical superiority. Moreover, in traditional warfare, the connection between attack and consequence is stable and, above all, predictable, allowing both authorities and populations to systematically plan for the attack, managing, in effect, its consequences before it happens.

The terrorist logic of threat differs from this conventional one in a number of crucial aspects.

- The primary *value* of the target for the terrorist is *symbolic*, not material.
- The primary *value* of the target is not determined by its use-value. The material, economic, strategic consequences of destroying or not destroying the target cannot be directly correlated or calculated with any particular geopolitical aim.
- The value of the target has political and social consequences in fields and domains *not associated with* the target. The consequences of terrorist threat are not military, but *social* and *cultural*. Terrorist threat is both affected by and causes changes in social and cultural values.
- The *value* of the target is not stable or fixed. The determination of value of a target cannot be transferred or repeated from one target to another. The risk and value-basis of risk, the danger and the value consequences that the threat implies vary from one *social* setting to another. Like value itself, it cannot be determined objectively and consistently.
- The determination of the value of a terrorist target has a second-order dimension. In other words, the determination of a target and means of attack is derived from perceptions of the symbolic significance of both. These vary according to the public mood, the political ambiance, the economic conditions, and the sense of freedom, patriotism, etc.
- The determination of the consequences of an attack – the presupposition of any consequence management – is also second order. The *moral* disruption such an attack would cause in a population, the ideological or symbolic effect it has, will depend upon a number of factors not objectively present or even associated with the attack itself. Rather, they are determined by previous experience, previous fears, allusions, associations and meanings. They depend upon already existing fears and on political tendencies. They depend on the social, cultural and moral values of the population. Lastly, they depend on the vision of the future and the scenarios of fear created by the present attack.

Thus, where in a traditional war the aim of violence is the destruction of the potentially destructive force of the object, according to the logic of terrorism it is not the material value of the target, but its symbolic function. A railway line during the Second World War could very well be the target of a military attack. The purpose of such an attack would be to actually disrupt the primary function of the line, namely, the transport of goods and personnel, both of which could be deployed in the further war effort.

In other words, there is significant doubt that one can make a consistently rational connection between threat and consequence. Thus 'consequence management', as it is defined in the EPCIP Green Paper, will have to be an imprecise science at best. To improve the calculation – precisely by dampening the calculability of the calculation – the values associated with social, cultural, moral dimensions of society must be integrated with all the imprecision that these imply.

The same can be said about the principle of 'proportionality' suggested by the EPCIP plan. Determining the correct level of response will always depend upon a determination of risk, which is not objectively, concretely anchored. The so-called 'relative criticality' of the logic of threat is not equivalent to the 'relative criticality' determined according to the rationality of value implicitly established by the installation itself, that is, by the economic cost of disruption.

How does one circumvent the challenge posed by a lack of instrumental link between goals and values, between violent means and symbolic ends? It is true that, in principle, one could formulate a general set of measures, protecting all things from all dangers. The resources involved in such a universal plan, in effect, casting a blanket of protection over the entire European continent, is, however, probably prohibitive.

11 Conclusion: the meaning of terror

The aim of a terrorist attack is to create a certain kind of meaning. The successful terrorist attack is meaningful and projects enduring meaning. Terrorist threat to critical infrastructure is not about critical infrastructure, it is about threat. The aim is not to disrupt electrical supply; it is to disrupt confidence in electrical supply. Threat, or rather *more* threat, will also be the desired result of terrorism. That is what sets it aside from classical war combat.

The notion of European critical infrastructure protection thus clearly grows out of two lines of reflection, more or less at odds with each other. One is an extrapolation of the essential economic freedoms embedded in the long-term project of European construction: subsidiarity, autonomy and liberal principles. These cannot be disturbed by a system of harmonisation and coordination. It is a realist discourse relating to the real damage that potentially could be caused by violent attack of one kind or another. The other is a reflection on the notion of threat and the nature of interconnectedness. This is a discourse of the imaginary, the playing field of terrorism.

Terrorism nourishes a fundamental sense of insecurity that inhabits us all. Even though the attack is over, the target destroyed, damage done, people hurt or killed, the attack is essentially a reference to another, future attack, to an attack that has not yet taken place, but that is living in our imagination, an attack that is brewing in the hearts of every man and women. The attacks of 11th September 2001 were catastrophic only in part because of what *actually* happened that day. But they were also catastrophic because they fulfilled a collective fantasy of fear and destruction. We can see evidence of this fantasy in countless catastrophe films of the last decades. In this sense, the terrorist attack of the future is not really in the future at all. It has already taken place in our minds. The danger, fear, trepidation, and economic, social and moral costs are already being paid today. But how?

The fundamental weakness in our 'defences' against terrorist violence is that they builds upon a set of *technological values*. Yet, a terrorist attacker will not seek to disrupt the critical infrastructure with technical aims. Terrorist attack aims at a different pillar of critical infrastructure: its symbolic value. That value cannot be swept away by deploying more or stronger fortress solutions. The symbolic meaning can only be countered with the force of meaning.

References

Baudrillard, J. (2001) *L'esprit du Terrorisme*, Galilée, Paris.

Castells, M. (1996) *The Rise of Network Society*, Blackwell, London.

Council of Europe (1977) *The Convention on the Suppression of Terrorism.*

Council of the European Union (2001a) *Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September 2001.*

Council of the European Union (2001b) *Proposal for a Council Framework Decision on Combating Terrorism.*

Council of the European Union (2004a) *Declaration on Combating Terrorism*, European Union, Brussels.

Council of the European Union (2004b) *Presidency Conclusions*, Council 16–17, December.

Council of the European Union (2004c) *Presidency Conclusions*, Council 17–18, June.

Council of the European Union (2005a) *EU Critical Infrastructure Protectin (CIP), Presidency Conclusions Annex.*

Council of the European Union (2005b) *EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks.*

Durkheim, É. (2004 (1924)) *Sociologie et Philosphie*, Presses Universitaires de France, Paris.

Edel, A. (1988) 'The concept of value and its travels in twentieth-century America', in Murphey, M.G. and Berg, I. (Eds.): *Values and Value Theory in Twentieth-Century America. Essays in Honor of Elizabeth Flower*, Temple University Press, Philadelphia.

European Commission (1997) *Treaty of the European Union*, Office of Official Publications of the European Communities, Luxemburg.

European Commission (2000) *The Response of the European Union to the Anti-Personnel Landmines Challenge*, European Commission, Luxembourg.

European Commission (2004a) *Crticial Infrastructure Protection in the Fight against Terrorism.*

European Commission (2004b) *On the Prevention of and the Fight Against Terrorist Financing*, Commission of the European Communities, Brussels.

European Commission (2004c) *Preparedness and Consequence Management in the Fight against Terrorism.*

European Commission (2004d) *Prevention, Preparedness and Response to Terrorist Attacks*, Commission of the European Communities, Brussels.

European Commission (2005a) *Communication Establishing a Framework Programme on 'Security and Safeguarding Liberties' for the Period 2007–2013, Proposal for a Council Decision Establishing the Specific Programme 'Prevention, Preparedness and Consequence Management of Terrorism', for the Period 2007–2013, General Programme 'Security and Safeguarding Liberties', Proposal for a Council Decision Establishing the Specific Programme 'Prevention of and Fight against Crime' for the Period 2007–2013, General Programme 'Security and Safeguarding Liberties'.*

European Commission (2005b) *Green Paper on a European Programme for Critical Infrastructure Protection*, European Commission, Brussels.

European Commission (2005c) *Green Paper on a European Programme for Critical Infrastructure Protection*, European Commission, Brussels.

GAO (2005) *Critical Infrastructure Protection*, Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities, Government Accountability Office, Washington DC.

Gordon, P.H. (2001) 'NATO after 11 September', *Survival*, Vol. 43, p.89.

Hoffmann, S. (2003) 'US-European relations: past and future', *International Affairs*, Vol. 79, p.1029.

Joas, H. (1997) *Die Entstehung der Werte*, Frankfurt am Main, Suhrkamp.

Joas, H. (2000) *Kriege und Werte. Studein zur Gewaltgeschichte des 20*, Verbrück Wissenschaf, Jahrhunderts, Göttingen.

Kuhn, H. (1975) 'Werte – eine Urgegebenheit', in Gadamer, H-G. and Vogler, P. (Eds.): *Neue Anthropologie*, Georg Thieme, Stuttgart.

Lia, B. (2005) *Globalisation and the Future of Terrorism: Patterns and Predictions*, Routledge, London.

Mesure, S. (1998) *La rationalité des valeurs*, Presses Universitaires de France, Paris.

O'Neil, M.J. and Dempsey, J.X. (1999–2000) 'Critical infrastructure protection: threats to privacy and other civil liberties and concern with government mandates on industry', *Depaul Business Law Journal*, Vol. 12, p.97.

Rees, W. and Aldrich, R.J. (2005) 'Contending cultures of counterterrorism: transatlantic divergence or convergence?', *International Affairs*, Vol. 81, p.905.

Simmel, G. (1989 (1898)) *Einleitung in Die Moralwissenschaft. Eine Kritik der Ethischen Grundbegriffe*, W. Hertz, Berlin.

von Clausewitz, C. (1978) *Vom Kriege*, Stuttgart, Rowohlt.

Notes

[1] Many thanks to Naima Mouhleb for research assistance in the preparation of this paper.

[2] Perhaps not surprisingly the classical modern concept of *value* emerges from the experience of World War I (Joas, 2000, pp.34–36) though the basic questions to which it responds are formulated in the texts of Nietzsche, Freud and Marx. By opening the question of values we are touching upon a lively and important contemporary debate, originating in Nietzsche's *The Genealogy of Morals* (1887), which there we are unable to treat here. The classical *sociological* positions to which we refer originate in Simmel (1989 (1898)) and Durkheim (2004 (1924)), see Mesure (1998) and Joas (1997). For a general overview see Kuhn (1975) and Edel (1988).

[3] For experience from the US efforts see GAO (2005) and O'Neil and Dempsey (1999–2000).

Website

http://eu.eu.int/en/info/eurocouncil.htm/.