



Critical Infrastructure Security and Protection

The Public-Private Opportunity

White Paper and Guidelines by CoESS
And its Working Committee Critical Infrastructure

December 2010



CoESS – Confederation of European Security Services
Jan Bogemansstraat | Rue Jan Bogemans 249
B-1780 Wemmel, Belgium
T +32 2 462 07 73 | F +32 2 460 14 31
E-mail: apeg-bvbo@i-b-s.be | Web: www.coess.eu



Responsible publisher

CoESS General Secretariat:

Ms. Hilde De Clerck (Secretary-General of CoESS)

Jan Bogemansstraat | Rue Jan Bogemans 249

B-1780 Wemmel, Belgium

T + 32 2 462 07 73 | F +32 2 460 14 31

E-mail: apeg-bvbo@i-b-s.be | Web: www.coess.eu

CoESS Registered Office:

8, rue de Milan, F-75009 Paris, France

Copyright disclaimer

Unless stated to the contrary, all materials and information (studies, position papers, white papers, surveys and their future results) are copyrighted materials owned by CoESS (Confederation of European Security Services). All rights are reserved. Duplication or sale of all or any part of it is not permitted. Electronic or print copies may not be offered, whether for sale or otherwise, to any third party. Permission for any other use must be obtained from CoESS. Any unauthorised use of any materials may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes.



Table of Contents

Executive Summary	4
Confederation of European Security Services (CoESS).....	5
Critical infrastructure and its security and protection today.....	5
National policies	7
Best practices and case studies	8
United Kingdom – Project Griffin	8
Germany – Security Partnership Programme	9
Spain – Police and private security partnership.....	9
How does CoESS see the way forward?	9
General	9
The importance of public-private security partnerships.....	10
Guidelines for stakeholders.....	12
General	12
Responsible decision-makers	12
Owners and operators of critical infrastructure	13
Private security companies	14
Action plan	15
Conclusion	16



Executive Summary

Critical infrastructure in Europe is owned, operated, regulated and protected by a complex mixture of public and private organisations.

The Confederation of European Security Services (CoESS), as the representative organisation for European private security services, strongly believes there is a far greater role to be played by its members and their affiliated private security companies in securing and protecting critical infrastructure in a way which brings benefits to all – the responsible authorities, the infrastructure owners and operators, the end-users of critical infrastructure, the private security companies and the general public at large.

This document highlights some examples of where public-private cooperation is functioning to the benefit of all stakeholders involved.

It also contains suggestions on how these examples could be used as best practices and followed and implemented elsewhere.

Finally, this document also provides guidelines for all parties involved on how to best secure and protect critical infrastructure.



Confederation of European Security Services (CoESS)

CoESS, the Confederation of European Security Services, is the European umbrella organisation for 30 national private security companies' associations. It was founded in 1989. CoESS is the only representative European employers' organisation defending the interests of the private security industry and is recognised by the European Commission (DG Employment, Social Affairs and Equal Opportunities) as a European sectoral social partner in accordance with the European Treaties.

CoESS' core objective is to defend the interests of its national member federations and of their member companies, both at European and at international level, and to represent those joint interests, in particular through its involvement in the work aimed at harmonising national private security legislation and regulations.

CoESS represents 21 EU Member States and a total of 28 countries, which translates into some 50,000 private security companies employing a total of approximately 1.7 million private security guards. The European private security industry generates a yearly turnover of around € 23 billion Euros.

CoESS' member federations cover a wide range of private security services including, but not limited to: cash-in-transit (CIT), cash processing, security training, bodyguarding, beat patrol, commercial manned guarding, in-house manned security, event security (crowd control), door supervising, alarm monitoring, CCTV monitoring and mobile alarm response.

Further information on CoESS' activities and projects is available on www.coess.eu.

Critical infrastructure and its security and protection today

Critical infrastructure is commonly understood to encompass physical assets, networks or organisations whose disruption or disabling would cause severe, lasting damage to social and economic life. Various national authorities have drawn up broadly similar lists of economic sectors which are covered by this definition: they generally include energy, water and food supplies, waste management, key transport networks (major airports and rail interchanges), financial institutions and cash supply, health services and state emergency response organisations.

Across EU Member States and their neighbours, this critical infrastructure is very often managed through some type of public-private ownership.



The ways in which they are secured and protected vary in the European countries from a mixture of state authorities (police, specialist protective services and occasionally the military), over in-house private security officers, to being fully contracted out to private security companies.

As far as threats to critical infrastructure are concerned, these can be man-made, for instance the result of terrorism or other criminal activity, but can also come from nature – from severe weather such as storms, volcanic eruptions or floods or other environmental disaster. In so far as critical infrastructure is dependent on people to operate it, it can also be threatened by disease such as influenza pandemics which may incapacitate large numbers of critical personnel.

The European Union has recently started initiatives in the field of critical infrastructure protection. This European Critical Infrastructure Directive¹ focuses on so-called ‘European’ critical infrastructure (ECI) – assets or systems whose disruption would have a major impact on at least two EU Member States, or a Member State other than the one in which the asset or system is located.

The Directive mandates Member States to identify all such infrastructure, ensure a risk assessment is carried out for all its elements and to ensure an Operator Security Plan (OSP) is drawn up. The broad headings which must be included in each plan are set out in the Directive. Each Member State must check that its ECI elements each have an OSP. If any ECI operator has failed to draw up such a plan, the Member State may take “any measures deemed appropriate” to ensure it does so.

Member States must report every two years to the European Commission “generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector”. The Commission will have no role in assessing the quality of Operator Security Plans and in fact will not see them.

The Directive states it concentrates on the energy (electrical, oil and gas) and transport (road, rail, air, inland and ocean shipping and ports) sectors, but will be reviewed to examine whether other areas should be added, and mentions the ICT sector as a possible additional sector.

Although this EU initiative constitutes a first important step towards a more fully integrated EU approach, the effects of the Directive are rather limited. Considering only European critical infrastructure, it leaves aside the large majority of critical infrastructure that does not fall under the definition of EU critical infrastructure and hence remains out of the scope of the Directive.

¹ Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>.



Indeed, most critical infrastructure remains national or even local. Equally, the obligations the Directive imposes on EU Member States are rather timid and leave the largest part of competence and decision-making regarding European critical infrastructure up to the Member States.

CoESS nevertheless believes that the principles regarding definition, approach, methodology and implementation of this Directive can inspire or set an example for those EU Member States who have not yet, in a substantial way, addressed the security and protection of critical infrastructure in their national policies.

National policies

It is today clear that most EU Member States, as well as other European countries, have dedicated attention and analysis to the issue of national critical infrastructure protection. Many national programmes and policies in this field exist. However, it is CoESS' feeling that these programmes and policies still remain too much on a political level and do not provide sufficient guidelines or directions/instructions for the actual day-to-day security and protection of critical infrastructure. Moreover, considering individual countries' policies, one has to conclude that these policies vary widely as to definition, objectives and approach.

As part of the preparatory work for the present document, CoESS undertook a survey among its member federations into national regulations on critical infrastructure protection. Its member federations completed questionnaires on the issue and reported wide variations between countries on issues as basic as the definition of what constitutes 'critical infrastructure', as well as on the question of how the security and protection of such infrastructure should be maximised. Perhaps most surprisingly, several countries have no official definition of critical infrastructure and therefore no rules on how it should be secured and protected.

CoESS believes that in the current global security environment this is an important omission. It also means that by definition, European governments cannot be sure they have a shared understanding of the issues when discussing national critical infrastructure protection.

When looking at the present reality related to this concrete security and protection, some good examples can be identified.



Best practices and case studies

CoESS, with its broad experience drawn from its member federations, has identified important examples of public and private organisations working together to secure and protect critical infrastructure. These include amongst others:

- A programme led by the United Kingdom police to train private security officers in counter-terrorism awareness and response and share relevant intelligence with them
- A scheme in German cities under which mobile private security patrols transmit incident information and intelligence to the police, effectively tripling the number of mobile patrolling assets on the streets at night
- Spanish cooperation between the private security sector and the police including an official database of private security contracts and the manpower associated with them and a dedicated telephone hotline to enable the police to share information with private security officers

CoESS believes these schemes show the powerful benefits of public-private cooperation in securing and protecting critical infrastructure and other assets.

United Kingdom – Project Griffin

Project Griffin was established six years ago by the City of London police, responsible for security in the UK capital's financial district, which has been repeatedly targeted by terrorists. It is made up of four key activities:

- Awareness days for private security officers, delivered by the local police. These focus on how to recognise, respond to and report suspicious activity such as terrorist surveillance of a potential target.
- Online refresher courses which maintain participants' interest and skills and enable formal accreditation.
- Regular communication between police and security officers, either by conference call, SMS message or e-mail, to ensure current intelligence and incident reports are disseminated in a timely manner.
- Emergency deployments: private security officers who have undergone Griffin training may be used by police to support them in responding to incidents, for instance in establishing and manning cordons.



Project Griffin has been rolled out to approximately half the police forces in the UK as well as to ports and airports, which have specialist security arrangements. It has also attracted attention in the United States, Australia and Singapore.

Germany – Security Partnership Programme

In a number of German cities private security companies have come together with the local police to pool information and transmit it to the police. In these projects mobile patrols by private security companies, travelling between customer sites, may spot suspect persons or vehicles or may witness possible unlawful activity. The officers transmit this to their company operations centre which then passes it on to the local police for assessment and possible further action.

These projects have proven to be highly efficient and are very welcomed by the German police forces. Through incorporating private mobile patrols the number of ‘surveillance vehicles’ on the street each night has been more than doubled (in some cases even tripled) in comparison to the number of police vehicles patrolling these cities.

In one German city, Dusseldorf, for instance, the scheme has led to more than 500 reports of suspect activity including 12 burglaries and one fire.

Spain – Police and private security partnership

In Spain, the police recognise that private security officers are a valuable potential resource. For this reason all contracts signed between private security companies and their customers must be registered with the police, including details of the numbers of staff involved and services provided.

The police have also established a 24-hour telephone number to enable them to communicate rapidly with the private security industry.

How does CoESS see the way forward?

General

CoESS believes that in the current security environment, security and protection of critical infrastructure from malevolent action and natural disaster must be given a higher priority by all stakeholders.



Security – meaning activities and measures to reduce the likelihood and impact of criminal and terrorist action – and resilience – meaning the ability to withstand and recover from deliberate or naturally-occurring disruption – must be built into the design and operation of critical infrastructure and not added on as an afterthought. Indeed, ‘building in’ security rather than ‘bolting on’ measures as an afterthought can reduce security costs, improve security effectiveness and has the potential to enhance, rather than hinder, an installation’s ‘core business’.

CoESS wishes to see the security and protection of critical infrastructure maximised through an explicit recognition by policymakers of the complexity of the issue, involving as it does public, private and in some cases hybrid actors. CoESS wishes to see an explicit allocation of roles and responsibilities for protection. Perhaps most importantly, it wishes to ensure common standards of risk assessment are adopted so that best practice is used to apply appropriate levels of security and protection to each piece of infrastructure.

The importance of public-private security partnerships

Securing and protecting critical infrastructure is one of the most suited areas for public-private partnerships, given their often public (national or local) character, which is translated in public ownership or public management or public objective. It is also undoubtedly a development in Europe in general regarding private security that more and more sectors and assets are taken away from public security to the benefit of the private security sector. CoESS does not want to make a judgement on this development, but witnesses in all European countries an increasing presence of private security companies and private security guards in the public domain. Reasons for this are numerous: the increasing feeling of insecurity amongst all parts of society, the limited resources of police and other public security bodies, the ever-increasing quality and professionalism of private security services and, last but not least, the innovative and flexible added value private security can provide based on its longstanding expertise.

The afore-mentioned case studies clearly demonstrate that well-defined, well-managed and well-monitored public-private partnerships are efficient, effective and, without any doubt, increase the security of critical infrastructure.

Mentioned case studies also demonstrate that, in order to be successful, these partnerships must comply with certain criteria. These include: an open dialogue between responsible public authorities and private security providers, clear instructions regarding the role of each partner, a clear legal or contractual framework, regular evaluation moments and necessary corrections and improvements when and where needed. It goes without saying that this interaction must take place within formalised joint structures specifically set up in view of the concerned partnership.



In order to fulfil these criteria and to optimise the success and efficiency of public-private partnerships for the security and protection of specific critical infrastructure, it is vital that each partner fully understands its role, responsibilities and limits. It is CoESS' opinion that, due to a lack of knowledge of these elements, public-private partnerships for the security and protection of critical infrastructure throughout Europe are still underdeveloped and not being used so as to reach their maximum potential.

CoESS therefore in the present document provides guidelines of which it is convinced that, when strictly followed, critical infrastructure can be secured and protected in a better and more efficient way to the benefit of all stakeholders involved.

In November 2009 the European Commission launched its Communication on Developing Public-Private Partnerships². The Communication provides some very interesting and useful ideas which are fully in line with CoESS' vision on public-private partnership in the field of security.

Why is the European Commission bringing forward this Communication?

This is a policy priority for the Commission, referred to in the European Economic Recovery Plan and in President Barroso's Political Guidelines for the next Commission. The focus is on building a functioning cooperation framework between public and private sectors, information exchange and networking activities, continuing the provision of innovative financing and innovative organisation of PPP projects.

What are public-private partnerships (PPPs) according to the European Commission?

Public-private partnerships are forms of cooperation between public authorities and businesses, in general with the aim of carrying out infrastructure projects or providing services for the public. These arrangements have been developed in several areas of the public sector and within the EU are used in particular in the areas of transport, public buildings or environment.

What are the potential social benefits of using PPP?

If properly designed and implemented, PPPs can bring real benefits in terms of helping governments to finance infrastructure investment in a more efficient way, freeing up scarce resources to devote to other national spending priorities (e.g. meeting citizens' basic needs in education or health care) and obtaining better value for money.

² COM(2009) 615 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 19 November 2009 on Mobilising private and public investment for recovery and long-term structural change: developing Public-Private Partnerships: http://ec.europa.eu/archives/growthandjobs_2009/pdf/european-economic-recovery-plan/ppp_en.pdf.



Important social benefits may be incorporated into a project. These can include quality criteria such as the frequency or cleanliness of services to be provided to citizens, or safety conditions, or measures to tailor the project to the specific needs of local or national communities. It is up to the contracting authority to define in the contractual terms the results and social objectives it wishes to achieve.

Guidelines for stakeholders

General

When considering partnerships for the security and protection of critical infrastructure, as mentioned previously, different stakeholders can be identified.

First, there are the responsible decision-makers (governments, politicians). On a more concrete level, there are the owners and operators of critical infrastructure and, last but not least, there is the private security services industry.

Responsible decision-makers

As already indicated, policies are moving, both at the EU and the national level. These policies should include the possibility of public-private partnerships, however, it is important that, when policies are considering cooperation with private security companies for the security and protection of critical infrastructure, the necessary attention should be given to quality. Although many national legislations on private security tend to guarantee at least a minimum level of quality through strict legal criteria for setting up private security companies or for working as a private security guard, special focus should be given to the specificities of critical infrastructure as set out above.

CoESS therefore recommends that national legislations regarding private security include a special licence or authorisation when critical infrastructure security and protection is concerned. This could be achieved through additional licensing and operational criteria for private security companies wishing to secure critical infrastructure or through compulsory specific training programmes for private security guards in this area.

As already stated, dialogue is crucial in public-private security partnerships. Not only during the execution or the implementation of a partnership, but equally and even more importantly, before defining and determining policies.



It is crucial that the private security sector and its representative organisations be consulted as of the very first stages of conceptualisation of approaches and possible strategies. It is obvious that such strategies and policies will largely depend on the national or local framework in which they must be developed. Elements such as political context, geographic location, legislative approach and historical and cultural factors have a great impact. Once again, also from this perspective, private security companies have a large expertise and therefore a valuable contribution to make, as they operate on a daily basis in this context.

Owners and operators of critical infrastructure

First of all and as already briefly mentioned before, a major development must be mentioned. Whether or not we are immediately aware of it, guarding services are becoming more and more a part of everyday public life. As an increasing number of security functions, which were previously carried out directly by public authorities, are contracted out, private security companies are becoming increasingly involved in ensuring public security, including in critical infrastructure. This often includes the guarding of highly sensitive sites. Just as any private customer, competent public authorities at European, national, regional and local level are therefore increasingly finding themselves in a position of having to select external contractors for the provision of such services. Public procurement officers have in the past often had to make such decisions without adequate guidance on quality criteria, which might be brought to bear on such decisions. Despite the sensitive nature of many of the public sites and locations to be serviced, CoESS' research has shown that the majority of public authorities today select security contractors solely on the basis of the lowest price. This is partly the result of declining public budgets, but can also be attributed to a lack of available guidance which could assist contracting authorities in selecting a "best value" provider.

To this end, CoESS has developed a 'Best Value Manual'. This manual was written for those contracting authorities who are keen to ensure that they are selecting a provider to carry out guarding functions which can combine quality with a favourable price rather than settling for the lowest price bidder. It aims to provide these contracting authorities with a user-friendly tool designed to assist them in defining their needs in the area of guarding security services more clearly in relation to different sites and guarding tasks. A special website has been dedicated to the Manual and its tools: www.securebestvalue.org.

Apart from the necessary attention to quality and best value, owners and operators of critical infrastructure must also be able to choose the right private security company, i.e. a company with the necessary authorisation, expertise, adequately trained staff and an operational structure in line with the requirements set out. From this follows the need for owners and operators to know private security companies are capable of delivering protection of critical infrastructure. Here, local police or other public security bodies can play a very crucial role.



As is the case with most organisations seeking to provide a service, the quality of the service rendered depends on a number of key factors. Of all these factors, the capabilities, skills and motivations of front-line staff is clearly the most important, as they are responsible for the day-to-day performance of the work, as well as the interaction with clients or the public. In addition, the operational planning and management of front-line staff and services has to be first-rate to ensure that the service is performed to the highest possible quality standard.

Of similar importance is the technical, operational and human resource infrastructure available to front-line staff and the contract management team. Finally, it is crucial that all operations are backed up by a company infrastructure which not only has the relevant track record to perform a quality service, but also displays a service philosophy which meets with the requirements of its client.

The four key areas in which the technical merit of a proposal for the supply of security services should therefore be assessed are as follows:

- Guarding personnel
- Contract management/operations
- Contract infrastructure
- The company

Private security companies

Private security companies themselves play a key role in establishing and implementing public-private partnerships for the security and protection of critical infrastructure. It has already been stated that a dialogue with all stakeholders is a key element of success. CoESS believes that private security companies should become more proactive and, upon own initiative, seek and establish contacts with responsible authorities, including owners and operators.

Private security companies must demonstrate to these possible partners their capability of securing and protecting critical infrastructure in an efficient and highly qualitative way. Undoubtedly, they can only do so when meeting all the criteria listed before. It is their responsibility to provide services in a highly ethical and professional way, to guarantee that staff is adequately trained (even if this means investing in extensive and non-compulsory recurrent and on-the-job training) and properly remunerated and so on. It is only through demonstrating these assets that they will be taken seriously by the party with the deciding power on how to organise security.

Equally vital is conducting a thorough risk assessment. It will also be the task of the private security company, in discussions with owners and operators, to demand a full and comprehensive risk assessment prior to any service being carried out.



Private security companies have often a great knowledge and expertise in risk assessments; it is their role to share with the owner-operator such knowledge and expertise and hence convince the owner-operator of the necessity of such an assessment and guide him through it.

Action plan

First of all, CoESS calls upon its member federations to integrate in their activities, strategies and analyses the issue of critical infrastructure security and protection. Given the potential increase in activities of private security companies in this segment, the topic must be high on the agenda. Member federations must, in close cooperation with their member companies having already a longstanding expertise, translate the guidelines of this document into concrete and workable tools taking into account the national and local context as described before.

CoESS calls upon governments and decision-makers to actively consider the advantages of public-private partnerships for the security and protection of critical infrastructure and develop and/or adjust policies accordingly. In this context, policymakers and operational leaders of protective services should consider whether there is scope for taking on board best practices and introducing them in their own decision-making processes.

CoESS believes that the following actions are crucial to any of the guidelines set out in this document:

- Establishment of discussion networks of critical infrastructure security actors (infrastructure owners and operators, security contractors, technology providers, state emergency services), to provide a forum for sharing experiences and best practice and to discuss issues affecting all of them
- Establishment of sound policies regarding the allocation of liability for acts of terrorism, the right insurance coverage and redress after such acts
- Improvement of procedures for appropriate information sharing between actors involved in critical infrastructure security and protection, particularly looking at sharing between state authorities and private actors
- Assuring the quality of protection of critical infrastructure, including consideration of options for the best way forward, for instance voluntary mutual inspection by experts; or compulsory auditing by a recognised authority



Conclusion

CoESS hopes that this White Paper and its Guidelines will stimulate the debate on this vital topic and will lead to coordinated action. As the representative body for the European private security services industry, CoESS of course stands ready to play a full part in this specific area.



**Critical Infrastructure Security and Protection:
The Public-Private Opportunity**

White Paper by CoESS – Confederation of European Security Services
© December 2010

CoESS – Confederation of European Security Services
Jan Bogemansstraat | Rue Jan Bogemans 249
B-1780 Wemmel, Belgium
T +32 2 462 07 73 | F +32 2 460 14 31
E-mail: apeg-bvbo@i-b-s.be | Web: www.coess.eu