CoESS

Acting as the voice of the **security industry**

Confederation of European Security Services

The Security Continuum in the New Normal

Sixth European Security Summit
WHITE PAPER

Rome,
10 October 2019

FederSicurezza

CONFCOMMERCIO
IMPRESE PER L'ITALIA

Table of Contents

Avv. Luigi Gabriele
President of FederSicurezza

E' ormai da tempo che sosteniamo con estrema convinzione il concetto di "filiera" della sicurezza privata: dall'impiantista a chi si occupa di antipirateria marittima o di sorveglianza dei centri per migranti, fino ai più moderni esperti di cyber security, parliamo di professionisti della sicurezza che, ciascuno per le proprie competenze, compongono un indotto in crescente evoluzione e che genera un forte valore sociale, sia pur spesso non adeguatamente riconosciuto.

In un contesto socio economico in cui le risorse pubbliche destinate agli uomini e ai mezzi delle Forze dell'Ordine scarseggiano, e a fronte dei sempre nuovi pericoli, fisici e virtuali, percepiti dalla collettività, la filiera della sicurezza privata rappresenta una componente fondamentale per rispondere a 360 gradi ad una domanda di sicurezza in costante evoluzione, dalla tutela del patrimonio e dal supporto nel controllo del territorio alle richieste di tutela della persona tout court e all'antiterrorismo.

Un sistema di sicurezza realmente integrato non può infatti prescindere da una complementarietà – e non da una sovrapposizione – tra sicurezza di emanazione statuale e imprese di sicurezza privata, e da una efficace sinergia tra capitale umano e tecnologia.

Le nostre risorse sono numericamente e qualitativamente pronte ad affrontare le sfide attuali e future, in accordo al progresso tecnologico ma senza mai dimenticare l'insostituibilità del fattore umano adeguatamente professionalizzato e valorizzato.

Sicurezza vuol dire professionalità, e più di ogni altra cosa riteniamo che sia proprio la "cultura" della sicurezza l'elemento imprescindibile sul quale lavorare.

L'interesse della "filiera" deve essere al primo posto, e possiamo perseguirlo solo se siamo compatti, specialmente a livello associativo.

For quite some time, we have been strongly supporting the concept of a private security "chain". Whatever their function, may they be guards, maritime anti-piracy agents, guards working in migrants' centres, or experts in cyber security, they are all highly qualified security professionals. They perform a competent service in constant evolution and generate high social added value. And yet we feel that they should be better recognised.

In a socio-economic context where public resources to protect people and to enforce the law are increasingly scarce, in a context of new dangers, be they physical or virtual, the private security industry represents a key element. Only with the support of private security is it possible to meet a constantly evolving demand for a comprehensive security offer, which includes protecting assets, the territory and people and also support anti-terrorism policies.

A fully integrated security system absolutely requires complementarity, not superposition, between public security forces and private security companies, and requires an efficient synergy between human resources and technologies.

Our resources are numerous and to take up the current and future challenges, we have to integrate the technological progress while keeping the invaluable human factor, which gives our service its professionalism and value.

Security means professionalism and more than anything else, the most essential element, security "culture".

The interests of the "chain" need to prevail, and we can only reach this objective if we remain united, especially at the association's level.

Foreword

Marc Pissens
President of CoESS

This 6th White Paper on "The Security Continuum in the New Normal" addresses a very crucial issue. It integrates all the important demands that CoESS has been making since its inception 30 years ago.

In the last five years, these demands have become even more meaningful, with the wave of terrorism that has intensified in the middle of this decade. The fact that public spaces have become the main target of terrorist attacks has brought the discussion of security in an area where many stakeholders, public and private, are involved, as well as citizens. Securing public spaces is very different from protecting Critical Infrastructures, such as airports or nuclear power plants. Finding a balance between facilitation and security in transport infrastructures, for example, is hard enough. Offering citizens actual security (not only a perception of security) in public spaces while keeping them open and accessible, and at the same time not giving the impression that an attack is imminent through too much presence of police or even the army is no easy task. In this "New Normal", in spite of the authorities' best efforts, the zero risk does not exist and terrorist attacks will happen, unfortunately. Therefore, not only do we need to prevent them from happening and Intelligence Services are indeed foiling attacks almost on a daily basis in Europe. But we must also be ready to effectively respond whenever such attack happens, and to recover as quickly as possible from it.

In both these areas, optimised cooperation between law enforcement (LEAs), government agencies and private security companies (PSCs) can help. Two million private security guards are active in Europe, of which 1.5 in the EU. They are deployed in locations where police are not necessarily, and certainly not permanently, present. To tap into the potential of millions of eyes and ears is an opportunity that a number of countries have already seized, by creating public-private partnerships (PPPs) and agreements for the exchange of information. In doing so, they are seeking to optimise resilience by making sure there is no weak link in the security chain. This is the meaning of the "Security Continuum". With respect to the intervention capacity, guards are first in line responders, and they cannot be treated in the same way as the general public with respect to the type of information they require to perform their duties. For example, they may need to be informed that the threat level in a certain location has been heightened, so as to be more vigilant and ready to intervene efficiently. Information needs to be forwarded to them when an attack is imminent or already going on. That is rarely the case today, also due to the lack of legal frameworks facilitating PPPs and the exchange of information.

"Clearly, the time has come to step up
the cooperation in the interest of
both LEAs and PSCs, and
for the better protection
of society in general."

The convergence of the professionalisation of Private Security, its willingness to positively contribute to the Security Continuum and the increasing technological dimension of security solutions creates perfect conditions and timing for an optimised partnership. As outlined in the previous CoESS White Paper on "The New Security Company", the paradigm of static guards vs technology is being replaced by that of optimised solutions, in which guards and technology form a whole that is bigger than the sum of its parts.

Clearly, the time has come to step up the cooperation in the interest of both LEAs and PSCs, and for the better protection of society in general.

In order to understand how best to set up and maintain this cooperation, and ensure that it is successful, we have collected examples throughout Europe, have analysed them and extracted best practice and guidelines *(Chapter 3)*. These take stock of the history of the industry *(Chapter 1)* and the change that our society and industry are witnessing, as well as the actions needed to manage that change *(Chapter 2)*. Chapter 4 then summarises the CoESS commitments and demands to the EU.

Since the very beginning of their history on earth, human beings have sought to protect themselves against dangers and threats. Safety and security are considered fundamental needs, coming immediately after physiological needs, as highlighted by Abraham Maslow in his hierarchy of needs. Later, when they became sedentary and created cities, communities would protect themselves with physical barriers or by organising human protective security organisations, at first private, and then public. Nowadays we increasingly seek the best combination of people and technologies to protect assets, infrastructure and, more importantly, people, whether they are at home, at work or in public spaces. The next frontier for private security will no doubt have to do with Artificial Intelligence, Big Data and Predictive Protection, the Internet of Things and many more concepts we have not yet invented and will become part of Augmented Security.

Against this background, and bearing in mind that security is a fundamental right for every European citizen, the cooperation of public and private security entities has to also be fully aligned with citizens' rights for privacy and data protection. This is all the more reason to create a clear framework that can reassure citizens that security and freedom are not in opposition but rather complementary. We need to break down silos in order to face the current and future challenges. Together, building mutual trust.

Chapter 1

Private Security in Europe: then and now

Today there are two million private security guards in Europe. Private security companies (PSCs) are present in every citizen's life: they conduct controls at airports and concert halls, secure Critical Infrastructure, and protect shopping malls and private property. But private security has always played an important role in protecting citizens and businesses against crime. In fact, the understanding of public security as a state monopoly is a rather recent one, actually dating from the 19th century. Since then, private security has become (again) an important stakeholder in protecting assets, people and infrastructure. More recently, its footprint has been widening as it has been given new missions by or in partnership with Law Enforcement Agencies (LEAs).

The last two decades have been placed under the sign of economic crises, technological evolutions, socio-political and demographic changes. Demands from clients and our security environment have changed very fast. This is the private security's "New Normal". As a response to some of these disruptions, the concept of the "New Security Company" has emerged, seeking to shift from the "manned/static guarding vs technology" to the "security solutions" paradigm.

The widening footprint of services provided by PSCs, which has evolved at a different pace in various Member States, but has now become a reality and accepted concept, known as "The Security Continuum", requires that the cooperation between LEAs and PSCs benefits from a number of general rules and follows certain principles and values. This is the condition for an effective global security framework that fully plays its protecting and preventing role, and that all players can therefore trust and rely upon.

Private security as the historical norm

History shows that private security has taken many forms and was prevalent in times when public order could not be fully guaranteed by the State. For example, King Charles V of Spain issued in 1518 a norm that regulated destructions and forest clearance in the mountains to prevent that towns would be deprived of wood and shelter for the cattle, and agreed that each local jurisdiction would choose a person in charge of the surveillance and control of such areas. These first "rangers" are the ancestors of what is now known as a private security guard.

Today's understanding of public security only dates back to the French Revolution and Jean-Jacques Rousseau's *"contrat social"*[1], establishing public order and law. Through the social contract, citizens gained (in principle) security and civil rights in exchange of respecting the sovereignty of the State. Until then, and in the absence of actual law enforcement, normal citizens were in charge of the protection and surveillance tasks. Truly effective police structures started to exist in many countries only as of the Napoleonic Age.

The beginning of private security companies

With the industrial revolution, new kinds of crime and risks to public order emerged. By the end of the 19th century, the extension of trade, commerce and urbanisation led to vulnerabilities to public security and private property like robberies in stocks and burglary, nocturnal activities and crime, rise of disadvantaged areas and "urban disorder" – extensive challenges ordinary police forces didn't have the capacities to deal with alone.

---

[1] Danny Vandormael (2018): Pas de Panique. Brussels, Belgium.

As a result, the first professional night-watchmen appeared in Europe.[2] As early as the 1850s, hotels and department stores such as *"Les Magasins du Louvre"* in Paris set up internal security services.[3] In 1850, in the United States of America, Scotsman Allan Pinkerton founded the Pinkerton National Detective Agency, a private security guard and detective agency. Pinkerton became famous when he claimed to have foiled a plot to assassinate president-elect Abraham Lincoln, who later hired his agents for his personal security during the Civil War.[4] The first European private security company was founded in Italy already in 1870.[5] The German *"Hannoveraner Wach- und Schließ"* was founded in 1901 and rapidly saw a considerable increase of business in times of a booming economy and increasing crime rates. The services that these companies offered were primarily keeping watch for fires and guarding entrances and gates.[6] Many of today's industry's predecessors were founded in this era. Private security companies were born.

Private security companies today

After the two World Wars, European societies have been subject to tremendous disruptors: globalisation, urbanisation, demographic change, climate change, the emergence of international terrorism. Multiple waves of technological developments and the digital revolution have added another layer of public security challenges, but offered new solutions to the industry. Today, we live in a constantly changing world, a new normal with numerous drivers of change *(see chapter 2)*.

Private security has evolved with these developments. Security in Europe is no longer imaginable without the massive capacity of the security industry with its around 2 million licensed guards.[7] Private security guarding of public buildings and (critical) infrastructure as well as screening/security services at airports, football stadiums and concert halls are today for most European citizens self-evident and fully accepted.

At the same time, spending in public security forces has been increasingly restrained: growth in the private security sector has significantly outstripped public expenditures on police services. In the EU as a whole, the number of private security guards is just under the total number of police officers [8] and, in the United Kingdom for example, the number of private security guards is higher than that of policemen. [9] In 2014, private security turnover reached a third of public expenditures on police service. In 2000 this ratio was only a quarter.[10]

"Security industry in the EU with its around 2 million licensed guards."

[2] Danny Vandormael (2018): Pas de Panique. Brussels, Belgium.

[3] Déborah Sellam : (2017): Evolutions et mutations de la sécurité privée - Une étude de différents modèles de regulation. Lyon, France.

[4] https://www.britannica.com/biography/Allan-Pinkerton

[5] http://www.cittadinidellordine.com/cdo_cittadini_ordine_storia.php

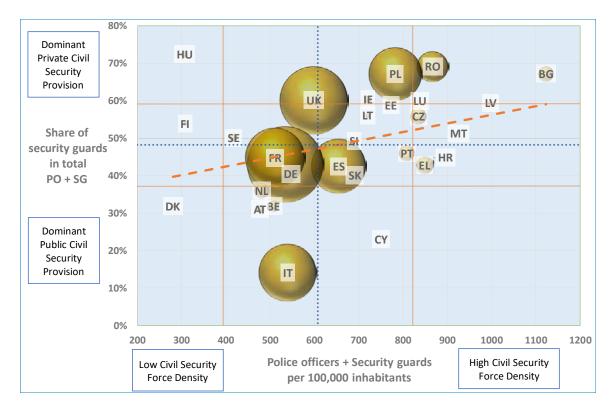[6] Danny Vandormael (2018): Pas de Panique. Brussels, Belgium.

[7] Paul Baker, Andrea Broughton (2018): Anticipating, Preparing and Managing Employment Change in the Private Security Industry. Brussels, Belgium.

[8] Paul Baker, Andrea Broughton (2018): Anticipating, Preparing and Managing Employment Change in the Private Security Industry. Brussels, Belgium.

[9] Mark Button & Peter Stiernstedt (2018) : Comparing private security regulation in the European Union, Policing and Society, 28:4, 398-414, DOI: 10.1080/10439463.2016.1161624

[10] Paul Baker, Andrea Broughton (2018): Anticipating, Preparing and Managing Employment Change in the Private Security Industry. Brussels, Belgium.

Graphic: Paul Baker, Andrea Broughton (2018): Anticipating, Preparing and Managing Employment Change in the Private Security Industry. Brussels, Belgium.

Tasks of the new security company

Even if manned guarding and mobile patrol services, alongside transport of valuables, remain the bedrock of the industry, the range of services provided by PSCs is expanding: for instance special event security, crowd management, guarding of Critical Infrastructure and transport, security consulting and training, employee/background screening, alarm and video system monitoring (and response), security system integration, and cybersecurity. Furthermore, technology is playing an increasing role and is also changing as well as expanding these tasks and the way that they are performed. Already in 2015, CoESS published a White Paper dedicated to *"The New Security Company: integration of services and technology responding to changes in customer demand, demography and technology"*. The White Paper describes the ongoing paradigm shift from the "static guard" to the combination of human and technology services, generally referred to as "security solutions".

The challenge of organising security today is to adapt to the widening of missions undertaken by private security and establish an effective cooperation between LEAs and PSCs so as to form a *security continuum*. Unfortunately, in many countries private security regulation is not adapted yet to this challenge and is based on assumptions of the past century.

PSC regulation in Europe

CoESS and its members stand for an industry that provides high professionalism and quality from the employment conditions of employees to excellent training and use of innovative technology. Quality goes of course together with highest safety standards of people, assets and organisations – and with compliance. It is crucial for the environment the industry operates in that providers of private security solutions meet the highest quality criteria.

Against this background, CoESS has seen a positive development in the regulation of PSCs at national level. A few statistics (based on a survey in 34 European countries):

→ **Regulation:** Licensing for PSCs is mandatory by law in 31 European countries, for guards in 28. In 31 countries the private security industry is regulated by sector-specific legislation.

→ **Social dialogue:** There are sector-specific binding collective labour agreements for the private security industry in place in ±58% of European countries.

→ **Vetting:** For operational staff, recruitment requirements demand a clean criminal record, background screening and/or a testimonial of good moral character in 33 countries.

→ **Rights and powers:** In 26 of all the European countries, private security guards have the same rights and powers as any other citizen. In 8 they can exercise additional powers.

→ **Training:** There is, by law, an obligation for private security guards to follow basic training in 33 European countries, however training levels vary significantly among Member States.[11]

Adapting legislation to today's and tomorrow's challenges

Still, legislation needs to be forward-looking and address issues related to the widening of the industry's missions. Private and public sector partners urgently have to work together and develop legally fit frameworks and regulations. Further development of public–private partnerships (PPPs) will require the creation of coordination and cooperation models that promote maximum effectiveness and efficiency of overall prevention, security provision and information exchange efforts.

This requirement for adapted regulation is not new, to the contrary. Security legislation is a living and maturing process that is regularly adapted to the current context. We can see this in France for example: as of the 1980s, terrorist attacks against French public spaces, transport and buildings have led to a rise in the demand for private security services and, importantly, respective legislation – for example regarding tasks in close protection, airport security and video surveillance of (critical) infrastructures. An important objective was always to take burden off law enforcement forces. The privatisation of airport security was a reaction to the reduction of government spending in public security, increased civil aviation traffic and tightened airport security measures due to terrorism.[12]

The second generation of terrorist attacks in the early 2000s in Europe led to a further extension of private security services in many countries. Already the 9/11 attacks on the World Trade Centre in New York and the Pentagon in Washington D.C. were a similar driver of change in the private security industry which led to the understanding that the organisation of public security and coordination between public and private players needed to be more efficient.

---

[11] CoESS (2013): Facts and Figures – Private Security in Europe 2013.

[12] Cédric Paulin (2015): « La sécurité privée à l'aune du terrorisme », Fondation pour la recherche stratégique, note n° 074/2015, 8 p.

Responding to new vulnerabilities in public security

What is new today is that, with the recent attack waves on public spaces mostly in Europe, we have moved to another stage, where the demand for and imprint of private security in the security chain has extended even more – making public-private partnerships increasingly necessary. Private prevention activities become more connected and contextualized with the fight against terrorism. Private security has in practice received and accepted a responsibility to participate alongside the police force in this work – but the legislative framework is often missing.[13]

The current security challenges we are faced with are significant and call for action. While Eurostat estimates suggest that the number of recorded crimes in the EU has, for most categories, fallen over recent years (from 2008 to 2016)[14], European society is repeatedly witnessing waves of terrorism mostly from Jihadists, but also from left- and right-wing extremists.[15] Between 2004 and 2016, terrorism has cost the EU about €185 billion in lost GDP and around €5.6 billion in lost lives, injuries and damages to infrastructure.[16]

The number of failed, foiled, and successful terrorist attacks perpetrated by Islamic extremists in Europe increased by 725 percent between 2007 and 2017, with attacks in the United Kingdom, France, Germany, Spain, Belgium, Sweden, Denmark, the Netherlands, and Finland. Since 2014, France alone has suffered more than 250 deaths and over 2,000 victims of injuries due to Jihadist terrorist attacks. In June 2018, the British counterterrorism strategy, CONTEST, noticed an increased threat from terrorism since 2011. The July 2018 French government plan against terrorism characterised the threat as "endogenous, diffuse, [and] pervasive."[17]

The current "generation" of terrorists is attacking soft targets in the public space that cannot be safeguarded in their quantity and complexity by police forces alone: concert halls and stadiums (Paris 2015, Manchester 2017), public gatherings (Nice 2016, Berlin 2016, Barcelona 2017, Strasburg 2018), transportation networks (Brussels 2016, Istanbul 2016, Utrecht 2019), ordinary supermarkets (Paris 2015, Hamburg 2017). Such tactics put a central challenge to police forces: threats can be everywhere, which means that in theory the police needs to prevent attacks and protect citizens everywhere.

Many of the attacks have led to an increased visibility of armed forces in the streets due to strained police capacities, particularly in countries that witnessed recent attacks like France and Belgium. However, such monitoring and surveillance tasks are no core tasks of armed forces. They are trained to operate and intervene in crisis regions and war theatres. At the same time, the threat has constantly been at the second highest level for several years in the United Kingdom, France and Belgium – an unsustainable situation for already strained police and army forces. Even worse, this puts the police in a position where it cannot play out its strengths and fulfil intelligence, (armed) intervention and prosecution tasks they are trained for and have special rights for.[18] Doing more with less public resources becomes increasingly unsustainable.

[13] Cédric Paulin (2015): « La sécurité privée à l'aune du terrorisme », Fondation pour la recherche stratégique, note n° 074/2015, 8 p.

[14] Eurostat Crime Statistics. Available at : https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime_statistics (visited May 2019)

[15] Europol (2018): European Union Terrorism Situation and Trend Report 2018. Available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 (visited May 2019)

[16] European Parliament Research Service (2019): Cost of non-Europe in the area of freedom, security and justice. Available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2019/631730/EPRS_BRI(2019)631730_EN.pdf (visited May 2019)

[17] Europol (2018): European Union Terrorism Situation and Trend Report 2018. Available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 (visited May 2019)

[18] Danny Vandormael (2018): Pas de Panique. Brussels, Belgium.

Private security as complementary support to police forces

This is where private security comes in. It is not a question of simple outsourcing, but complementarity and pragmatic solutions to work towards the highest possible level of public security. Private security can free up police resources, so law enforcement forces can focus on complex tasks for which they have the equipment, training and special rights – for example in counterterrorism.

Public forces have taken over an exploding number of preventive missions that should not belong to their core activities, such as guarding of buildings and administration, including police stations and military bases. Several factors are taken into account when opting to select PSCs vs the police to complete missions: cost-efficiency matters, of course, but so does the specific training and the focus of missions. For example, in airports, the screening of passengers and baggage has become a very specialised job, which does not need to be performed by policemen. If preventive and protective tasks can be taken over by private security under respective regulation and strict public oversight of activities, it is a choice of the State to decide whether they will be. Public forces do not lose control of public security because tasks are delegated. Oversight of private security activities can be well defined in contracts and reporting procedures.

It is important to recognise that private security has decade-long experience in securing assets such as Critical Infrastructure, special events and (semi-) public spaces. In addition, companies constantly invest in the future, including training of personnel and application of state of the art technologies in order to propose the best and most appropriate security solutions. They constantly assess emerging risks to enhance resilience within an evolving threat environment. LEAs do not have the same pressure and are not as close to the market needs as PSCs. At the same time, technology provides additional opportunities for better coordination and cooperation among public and private forces – for example when it comes to providing access to video surveillance images to the police.

The new Security Continuum

Since its creation, CoESS has been calling for a larger, more complementary and cooperative security chain between public and private security – including respective regulation of tasks, competences, responsibility, liability and quality control of PSCs at national level. It is important that both private security and police do not stand in artificial competition with each other and, instead, exchange information as partners in a set legal framework, which respects and protects data privacy and confidentiality, also in the light of the General Data Protection Regulation. Private security guards perform a valuable range of preventive missions and represent an untapped potential that could be better used by police forces. Likewise, they need to be aware of risk and threat developments to effectively carry out protective missions. For example, in Brussels in March 2016, PSCs operating in urban transport were informed of the airport attacks by the media, at the same time as the general public. An hour later, another bomb went off in a metro station. For an optimised level of prevention and response, it would be necessary to establish a form of urgent communication from LEAs to PSCs and vice versa. For the security of special events, such as international government meetings, football matches and concerts, effective PPPs already exist in certain countries. Best practice could be drawn from them.

Any effective European regulatory approach must start at the national level. It is a question of identifying effective models for PPPs and private security regulation that combine a strict framework guaranteeing the professionalism and quality of private security services without slowing down the industry's development and entrepreneurial freedom. In the long-term, we hope this will result in the definition of a balanced, harmonised, efficient and industry-friendly European legislative framework for the development of the industry. This call is anything but new and doesn't only come from CoESS. A European Council Recommendation from 13 June 2002 regarding cooperation between the national authorities responsible for the private security sector already encouraged cooperation and

collaboration with a view to exchanging information in accordance with national law. To this end, a meeting of the national authorities responsible for the private security sector should have been organised every two years. In 17 years, such meeting happened only once in an informal set-up, at the request of CoESS, during the Fourth Security Summit in Stockholm (2013).

However, and thanks to pro-active engagement of the private security industry in this matter, there are best practice examples at national level: in Belgium, the most recent national regulation of the industry within the EU clearly defines and broadens its competences according to the new security environment we live in. It is a proof of the importance and recognition of PPPs.

Selected best practices are illustrated in Chapter 3 of this White Paper.

CoESS: accomplishments and way forward

CoESS will continue to raise the understanding of private security at European level and promote the importance of PPPs in the new normal. We have come a long way since the Services Directive 2006, where we successfully raised awareness to the fact that for public security reasons, it is essential that private security be excluded from the text. For many good reasons, internal security remains a sole competence of EU Member States. This is most importantly due to the fact that internal security architectures are grown out of complex historical, societal and political contexts to which PSCs have adapted – for example in terms of training and quality requirements and competences of security guards. It is crucial that national LEAs continue to have influence on these security architectures.

For many years, security has therefore not been high on the European agenda. Since the early 2000s, this has changed, as a result of the increasing number of terrorist attacks and evolution of international crime. CoESS has been contributing pro-actively to the EU's work as a partner and has been promoting the exchange of best practices across countries – on legislation, but also threat developments and solutions. We are part of 16 official EU Expert Groups at the European Commission, including the EU Operators Forum on the Protection of Public Spaces. In 2017, CoESS' Director General Catherine Piana was invited to hold a speech at the European Parliament's Special Committee on Terrorism. Thanks to EU funding projects and White Papers from our experts across Europe, CoESS regularly delivers new solutions and research to the European security community – most recently on how to tackle Insider Threats at Critical Infrastructure (please find more information at help2protect.info).

Together with its social partner UNI Europa, CoESS has provided a Best Value Guide for public procurement of PSCs and an overview of drivers of change impacting the industry and employees now and in the future *(see chapter 2)*.

CoESS' work at ISO and CEN level is part of the industry's general strategy to emphasise quality and raise awareness to the added value PSCs bring to the entire security value chain. CoESS is, for example, chairing the Committee of European CEN Standard TC 439 "Private Security Services".

The private security industry's values – quality, safety, compliance and trust – are at the core of everything CoESS does to help tackle today's challenges to public security and drivers of change. The next step is to form an effective Security Continuum: a continued cooperation with policymakers, LEAs, and the public.

In security, there is a common say: "The security chain is as strong as its weakest link". With an effective Security Continuum, private security and law enforcement can make sure that there is no weak link.

To find out more about our activities, visit **www.coess.org**.

Chapter 2

Private security companies in Europe – Challenges and opportunities

The contents of this chapter are mainly sourced from the report "Anticipating, Preparing and Managing Employment Change in the Private Security Industry", co-produced by CoESS and UNI Europa and funded by the EU in 2018. Some parts have been adapted to this White Paper and express a more concrete position than in the report.

Not unlike other sectors, the private security industry is faced with a series of 'mega' trends that are radically altering the economic, societal, and technological environment in which the industry operates. The many drivers – whether digitalisation, demographic evolution and migration, or a changing security threat environment (for example due to radicalisation and terrorism or organised crime) – will undoubtedly result in a mix of incremental and disruptive transformations in the business environment for private security providers, both in terms of shifts in market demand and in terms of their business models and operations.

The private security industry faces a number of immediate and future challenges:

→ Accelerating the integration of traditional on-site guarding with remote and mobile guarding, supported by new technological solutions.

→ Coping with demographic change and the ageing of the workforce.

→ Attracting and retaining younger generations into the private security industry.

→ Adjusting to changes in the content of jobs as some 'tasks' disappear and new ones appear.

→ Adapting to a widening of missions undertaken by private security and the increasing dimensions of public–private partnerships (PPPs) to deliver security to citizens and businesses.

Economic and employment situation of the private security sector

The general picture for the sector as a whole in Europe is that growth in turnover slowed significantly following the onset of the financial and economic crisis that began in 2008, while total employment was stagnant between 2009 and 2015. However, the most recent available data show evidence of a return to growth, in parallel with the strengthening of the overall economic situation. Industry sources report some labour market tightness, with firms encountering difficulties in recruiting sufficient workers and finding workers with the right skills profile.

Available Eurostat data for the broader category of security and investigation activities (NACE 80)[19], reveals marked differences across EU Member States in the age composition of the workforce, with many central and eastern European countries, the Baltic States, Germany and the UK having high proportions of older employees in the workforce. Looking forward, these countries may face growing employment pressures caused by the need to replace older employees as they retire from the workforce. By contrast, younger age groups typically account for a higher proportion of the workforce in the northwest of continental Europe (including Scandinavia) and France. In terms of gender composition, male workers dominate employment in the private security industry, with the share of female security guards in Europe estimated at only around 15%.

---

[19] NACE 80 covers private security activities (NACE 80.1), security systems service activities (NACE 80.2), and investigation activities (NACE 80.3). Within the EU28, private security activities (NACE 80.1) account for 80 to 85 % of total turnover in security and investigation activities (NACE 80).

Overview of drivers of change

For the purposes of the "Anticipate Change" project, the major trends – or drivers of change – that were anticipated to influence the private security industry in Europe were grouped into the following categories:

→ Global conditions: globalisation and environment.

→ Demographics, migration and urbanisation.

→ Technology.

→ Societal factors: crime levels, security threats and public perceptions.

→ Widening of the private security domain.

Over the past decades, **globalisation** has accelerated due to a combination of trade liberalisation and emerging market growth, alongside technology developments and falling transport costs that have facilitated flows of goods, services, labour (talent), capital, information and data. Globalisation may make supply chains more efficient, but, by breaking up production processes and increasing their geographical dispersion, it makes them more vulnerable to disruption.

There is clear evidence that greenhouse gases are causing **climate change** and driving a complex mix of unpredictable changes to the environment while further taxing the resilience of natural and built systems.[20] There may be an increase in refugee and migrant flows resulting from the adverse effects of climate change and natural disasters, and governments will face a difficult challenge in achieving the right combination of adaptation and mitigation strategies.

Europe is facing an **ageing population** due to a combination of increased life expectancy and declining fertility rates. Shifting dependency ratios will put pressure on social institutions, businesses, and economies. At the same time, businesses and workers will need to adjust to an older workforce and potential shortages of workers. Pressures on pension systems may mean that workers need to work for longer, while workforce participation will need to be promoted, and older workers encouraged to develop the skills required to be active and productive participants in the workforce.

---

[20] KPMG (2013), 'Future State 2030: The global megatrends shaping governments'. Available at: http://www.kpmginstitutes.com/content/dam/kpmg/governmentinstitute/pdf/2013/future-state2030.pdf

Immigration could provide one possible solution to Europe's ageing population. The process of integrating immigrants is, however, a highly contentious political issue with clear divides between those who see controlled immigration of skilled labour as a way to pay for higher social spending, and those that see high levels of immigration as a threat to social stability. It is also the case that immigrants will age themselves, and their birth rates quickly mirror those of the overall population. Consequently, it is argued that immigration can only delay but not solve the problem of ageing populations. There is also a difficulty in background checking immigrants, especially if they come from war zones, making their entry into the Private Security Industry difficult or in certain cases, impossible.

"As of 2008,
±75% of EU population
lives in urban areas."

There is also a growing **urbanisation** trend: as of 2008, more than 50% of the world's population lives in urban areas. In Europe, this figure is close to 75%, although there are considerable differences in the size and spatial distribution of urban developments across countries. This trend is expected to continue, particularly with capital cities witnessing significant growth in populations. Cities are, however, seen as more prone to crime, violence or vandalism than rural areas. Furthermore, the higher concentration of people impacts on infrastructure and service requirements, resource needs and supply, and exposure to natural and man-made disasters.

Successive waves of **security and information technology** developments are improving access to data and creating opportunities for the emergence of new industries and new types of jobs. The impacts of emerging technologies on the job markets and the workforce risk being extremely profound. On the one hand, developments in automation and machine learning have the possibility to make millions of jobs obsolete, either completely or partially for specific tasks carried out by workers today. As a consequence, salaries of low-skilled workers in developed countries (already subject to downward pressure from technology and global competition from low-cost production locations) could become more vulnerable. At the same time, new technologies are enabling workplace innovations that will bring changes to working behaviour; for example, remote working, co-working spaces and teleconferencing. Workers that are unable to adjust to these new task demands may see their employment prospects deteriorate, either in terms of the number or quality of jobs available.

Eurostat estimates suggest that the number of **recorded crimes** in the EU has, for most categories, fallen over recent years.[21] The rise of terrorism and public fears around potential terrorist attacks and the associated targeting by terrorists of public spaces and events where private security guards work raises important issues on the potential exposure of guards to terrorist incidents and their role within PPPs for counterterrorism.

The recently released Eurobarometer survey of **Europeans' attitudes to security**[22], reveals a significant decrease in the proportion of respondents who think that the EU is a secure place, from 79 % in 2015 to 68 % in 2017. Fears centre on terrorism, organised crime, natural and man-made disasters, cybercrime and the security of the EU's external borders.

As explained in chapter 1, the growing presence of private security has been accompanied by a **widening of the scope of services provided**. Even if manned guarding and mobile patrol services, alongside transport of valuables (cash-in-transit), remain the bedrock of the sector, the range of services provided by private security companies has expanded tremendously. A complex set of factors influence the potential for the widening of the private security domain. These involve matching service needs of customers – and expectations of citizens – with cost-effective and efficient delivery, while ensuring transparency and proper accountability.

Impacts and consequences for the private security industry

In terms of **globalisation**, the private security industry, in its role as a frequent support for the police force, which may become more prominent in the future, may become more involved in trying to manage the different instabilities and outcomes caused by globalisation. This is linked to the widening of the private security domain, which is explored in chapters 1 and 3 of this Whiter Paper.

Climate change may lead to a greater concentration of the population in urban areas, which in turn may increase demand for the services of the private security industry in terms of crowd management, event management and other public order duties. Similarly, the sector may be called upon to help manage refugee and migrant flows: it is already involved in these activities in many countries. Maintaining the integrity of supply and logistics operations could also become a major part of the private security sector's work.

The **economic recovery, although varying in its extent from country to country**, has generally led to a decrease in unemployment around Europe. For the private security sector, high levels of employment are likely to lead to recruitment difficulties in countries where the sector is seen as less attractive in terms of employment opportunities. There has not been a great deal of evidence to date that the economic recovery has resulted in significant wage growth. However, as there are high levels of involuntary part-time work and atypical working overall in the labour market, if the private security industry focused on improving terms and conditions of employment, this could be an opportunity to significantly increase the attractiveness of the sector to potential employees.

The **ageing population** has many implications for the private security sector. In terms of employment, adjustments may need to be made for an older workforce in relation to working conditions, working environment and adaptation to technological change. As workers are likely to need to work for longer due to pressure on pension systems, the industry will need to think about how to accommodate workers who remain in employment past their mid-sixties. A key challenge will be to ensure that older workers develop the skills that they need to maintain active participation in the sector. At the same time, attracting young talent with required skills will be key to cope with labour shortages, but also the increased use of technology and automation can help to some extent.

---

[21] Eurostat Crime Statistics. Available at : https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime_statistics (visited May 2019)

[22] European Commission (2017a), 'Special Eurobarometer 464b: Europeans' attitudes towards security'. Available at: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDet ail/instruments/SPECIAL/surveyKy/1569.

The private security sector is likely to be at the forefront of managing the flow of **immigrants**, as is already the case in many countries, and potentially helping to contain any social unrest associated with increased flows of immigrants. This raises issues for the sector such as the need to ensure that guards have the necessary skills and competences to deal with the duties associated with this. The social partners have already addressed many of these issues in their 2016 joint declaration on the role of the private security sector in light of the increasing number of refugees in Europe.

Technology has already had a significant impact on the private security sector: remote monitoring and the use of drones and robots has already changed the role and job content of guards. The advent of new technology presents both opportunities and challenges for the sector. One challenge is the potential negative effect on employment levels. There is also an opportunity in that technology may be able to take on some of the more mundane tasks in the sector, leaving guards free to engage in more complex and interesting tasks. Training will be needed in order to enable workers to adapt to the new types of tasks that they may be required to carry out. There is likely to be a requirement for workers to shift from routine and automatable tasks, such as surveillance activities, to tasks that are complementary to new technologies, but that typically are new, more complex and more demanding. There are also challenges for employers and the social partners in terms of the changing profile of the workforce: a greater number of workers whose job content consists of technology-related tasks may mean redefining pay scales and career tracks in company agreements and collective agreements, in order to accommodate workers with a different background and skills set to those whose jobs involve more traditional guarding tasks.

There are on-going issues related to serious and organised crime, however, especially related to the role of new technology, in the area of cybercrime. The overall decrease in traditional crime may mean that there is less demand for guarding services: a reduced risk of vandalism and burglary may lead to more remote-controlled guarding rather than having a guard on site, accelerating an existing trend.

Increases in **terrorism** and targeting by terrorists of public spaces and events where private security guards work raises important issues on the potential exposure of guards to terrorist incidents but also their potential role within PPPs for counterterrorism. Security guards are often first on the scene in a terrorist attack on a public space such as a large entertainment event or an airport. It is therefore crucial that they have the necessary training and equipment to deal with this eventuality.

As explained in chapter 1, in order to address issues related to the **widening of the sector** into other areas, it will be important for sector representatives to be actively involved in discussions with their public sector partners in terms of developing legal frameworks and regulations relating to the widening of the functions that are assigned to the private sector. At the same time, further development of PPPs will need the creation of coordination and cooperation models that promote maximum effectiveness and efficiency of overall security provision, whilst ensuring that the delivered services correspond to the needs and expectations of citizens.

Challenges to address in the coming years

Employment and terms and conditions

→ Should there be national minimum standards? There is a role to play for social partners in ensuring effective enforcement of legislative, social, fiscal and administrative obligations of all PSCs, and where necessary, sanctions for non-compliance. Are there best practices that can be transposed from one Member State to the other?

→ Background checks need be made quicker and there should be consistency across the EU in what information is checked and how often it is updated. This is especially important to prevent and detect Insider Threats. The system put in place for Aviation Security could be used for inspiration, even if not all the elements can be transposed in other areas.

→ Online employment and recruitment platforms will become more relevant for the sector in the future. CoESS is already addressing this subject internally and is also discussing it within the European Social Dialogue.

→ Ensure that guards are properly protected when doing their job from a health and safety, environmental, security and equipment perspective.

Training

→ Up- and reskilling could enhance the employability of existing workers.

→ A periodical refresher training for existing management and guards can help keep pace with fast evolving technologies, risks and legislation.

→ More structured training for young and new workers and those moving into the sector from other sectors should be provided.

→ There is a need to adapt to new skills needs, including technology and soft skills.

→ The social partners could explore the feasibility of e-learning platforms at EU level for soft skills. An initiative by CoESS Members is available on line in this regard at https://trainbrainsoft.jimdo.com/.

→ The skills required to work effectively at the interface between public and private security need to be determined and developed.

→ Intercultural and intergenerational training and mental and physical health support and training will also need to be further explored.

Increasing the attractiveness and quality of the sector

→ Communication campaigns could help to raise the profile of the sector and showcase the work of guards and the human face of the profession. This could include campaigns to increase the diversity of the sector's workforce. Some major leaders of the industry have already adapted their communication in this respect.

→ It is vital to ensure a balance between stability and flexibility that is acceptable to both employees and employers.

→ The vicious circle of low wages, low costs and low quality needs to be addressed.

→ The industry needs to look into the opportunities of diversifying the workforce, e.g. including more women and staff from different ethnic backgrounds.

→ Promote the role that private security plays for society as a whole.

Regulatory reform and market functioning

→ Enforcement of specific procurement rules, where the "Most Economically Advantageous Tender" (MEAT) criteria are fully abided by, needs to continue and intensify. Concretely, any private security service should be selected on the basis of quality for at least 50% of quality criteria, and private security services to Critical Infrastructure should be based on at least 60% of quality criteria.

→ Promotion of social and quality criteria clauses in public tenders also need to continue and intensify. This can be facilitated by existing EU Standards on services (CEN TC 447) and private security (CEN TC 439), such as EN 16082:2011 (Airport Security) and EN 16747:2015 (Maritime/Port Security).

→ Information and education campaigns directed at public and private sector customers would be useful, possibly building on the joint statement on the 2014 Directive on public procurement and the social partners' best value guide.

→ Organise a sharing of relevant national legislation in English in individual Member States, as far as possible, in order to better understand national situations and challenges. CoESS has developed a "legal matrix" in order to collect such information.

→ Ensuring that there is a control mechanism or institution to verify the healthy functioning of the market and, where necessary, enforce the rules and sanctions for non-compliance or infractions.

Coping with the challenges of technology

→ CoESS, in particular its Guarding Committee, conducts regular brainstorming sessions to assess the upcoming challenges and opportunities that technology offers, including cybersecurity issues, and how they can be anticipated.

→ CoESS also conducts benchmarking exercises with other industries.

Widening the scope of the sector

→ CoESS is continuously gathering best practice from its Members and, in Chapter 3, is making suggestions for guidelines in respect with PPPs, both for Critical Infrastructure Protection (CIP) and the protection of public spaces.

→ The next step is to establish a dialogue with practitioners from both LEAs and PSCs in order to explore further concrete solutions that can be put in practice in the field.

Chapter 3

The Security Continuum

The previous chapters and the report of the recent (2017-2018) project on "Anticipating Change in Private Security Employment", co-led by UNI Europa and CoESS, and financed by the EU, note that the private security industry's footprint is increasing. With a change in society also comes a change in how it protects itself. Some of the industry's new missions include tasks that were previously carried out by the police and other law enforcement agencies (LEAs), demanding for innovative services of highest quality. For the companies performing these missions, CoESS therefore requests that, already in the procurement and contracting phase, clear and strict quality criteria be agreed upon and abided by. This is essential to maintain a high level of service, which in turn will ensure that authorities and citizens trust the private security industry to take over these tasks in the domain of prevention and protection.

Furthermore, the threats to, and vulnerabilities of, both Critical Infrastructure and, more recently, public spaces or so-called "soft targets" urgently require a closer and more effective cooperation between private security companies (PSCs) and LEAs. Whereas public-private partnerships (PPPs) have been used and information has been exchanged informally between LEAs and PSCs for several decades, the "new normal" security environment requires that PPPs and the information exchange be taken to the next level. The rise in terrorist attacks since 2004 in Europe has intensified the realisation that the PSCs can offer a potential of additional eyes and ears, when adequately informed and trained, and therefore reinforce the intelligence gathering and thus the prevention and detection capability of LEAs, as outlined and demonstrated in Chapter 1 of this White Paper.

As a consequence, it is necessary to regulate the approach taken for PPPs, so as to create a Security Continuum, i.e. a harmonious and complementary security concept to the service of citizens, public and private assets, as well as infrastructure. While some elements can only be determined at national level, a common approach, exchange of best practices and, in some cases, EU legislative instruments are required in order to achieve this Continuum.

Since 30 years now, CoESS has been seeking to raise the legislators' awareness to the need to step up the quality and compliance standards for private security in general, but even more so for those PSCs that protect Critical Infrastructure and/or engage into PPPs. In the course of this exercise, CoESS has collected best practice from all over Europe regarding the most advanced and successful forms of cooperation. On this basis, CoESS studied the elements in those examples that determined their success. These conditions, as well as proposed guidelines for PPPs and the exchange of information between LEAs and PSCs, are addressed in this chapter as a basis for further discussion with the stakeholders.

Examples that have been used include the following:

→ **Italy:** The Ministry of Interior created a protocol for public-private cooperation "Mille occhi sulla città" (literally: "A thousand eyes on the city") in 2010. Criteria and modalities of cooperation between stakeholders are described in further details in the respective agreements signed in 2010, and renewed without changes in 2013 and 2019.

→ **UK:** Project Griffin, established in April 2004, is a pilot joint venture between private businesses, the City of London Police (CoLP) and the Metropolitan Police (MPS), which initially involved three major City-based financial institutions. The aim of the project is closer cooperation between LEAs and other actors including PSCs, educating the latter on up-to-date counterterrorism information, tactics and procedures. With the help of such enhanced PPPs, security guards are enabled to act as eyes and ears of the police and can support on emergency response if necessary. Since its inception, Griffin has expanded nationally and internationally and is nowadays viewed as the most effective and successful example of PPPs on counterterrorism security issues. It is now called ACT – Action Counters Terrorism.

→ **The Netherlands:** Police and PSCs agreed in various cities and locations, some being public spaces, others being Critical Infrastructure, on a protocol on the exchange of information. At Rotterdam Seaport exists for example the project "Oog en Oor".

→ **France:** Security representatives signed in 2019 a protocol, which allows the exchange of operational information between LEAs and private companies at the local level – giving substance to the "Security Continuum".

→ **Norway:** The Oslo Police District and the Confederation of Norwegian Enterprises (NHO Service) outlined in a guide cooperation models between the police and the security industry in 2016. The guide defines the boundary between duties and areas of responsibility of the police and those of the security industry and provides a reference work with suggested solutions and measures for increased cooperation.

→ **Spain:** For almost a decade LEAs have established cooperation programmes with the private security sector in their respective competence area (e.g. Red Azul at the Policia Nacional, and Programa Coopera at the Guardia Civil), all based on mutual exchange of information and reciprocity. Similar programmes exist at the level of the Basque and Catalan Police Forces.[23]

---

[23] For more information visit https://www.policia.es/org_central/seguridad_ciudadana/unidad_central_segur_pri/red_azul_presentacion.php and http://www.guardiacivil.es/es/servicios/seguridadprivada/colaborasegupriva/plancoopera/index.html

PPPs and Public Procurement

A PPP is a "partnership between an agency of the government and the private sector in the delivery of goods or services to the public"[24].

This concept is linked with that of best value procurement. In compliance with the principles of equality of tenderers and free and fair competition, the authorities call for applications from service providers and, on the basis of pre-defined criteria, will select the best candidate to perform the mission according to the contract and arrangements.

The EU rules on Procurement (Directive 2014/24/EU) are an important step in setting criteria for public procurement, introducing the so-called MEAT principle (Most Economically Advantageous Tender). The latter proposes procurement criteria that also take account of qualitative, technical and sustainable aspects of a tender submission. However, these rules only apply to public buyers and are only compulsory above a certain value . In addition, there has been, in CoESS' opinion, too much margin for manoeuvre left to the Member States, so that they may pick and choose exclusion criteria. In effect most of them continue to give much more weight to price than to quality, often at the expense of social responsibility and security – the potential effect of this approach is creating security gaps and thereby threatening public security at large. In the current threat picture, CoESS therefore argues that security cannot be selected on the basis of the lowest cost bidder only.

In order to close this gap and encourage quality buying, known as "best value procurement", CoESS and UNI Europa, with EU funding support, have jointly written a manual to help buyers select PSCs on the basis of objective quality criteria. This manual can be found in 14 languages at securebestvalue.org. An interesting project is also being developed with CEN TC 447 at the initiative of the European Commission's DG GROW, to produce a horizontal services standard covering all procurement, public and private, and enhancing the MEAT principle.

Furthermore, CoESS has been active for over a decade producing and maintaining standards[25] prioritising the protection of Critical Infrastructure sectors for which EU legislation already exists, namely aviation security and port/maritime security. Since 3 years, CoESS has been actively working within CEN TC 439 (Private Security Services) on a future overarching standard for private security suppliers protecting Critical Infrastructure, which will be followed by Critical Infrastructure sector-specific standards. These could include railway, energy, water, and other Critical Infrastructure sectors according to the level of priority identified by the TC.

Unfortunately, too many buyers – even in governmental organisations – are still going for the lowest cost and are disregarding the best value approach, which in security, and especially at a time where so many threats are present and emerging, is a very dangerous option.

Therefore, CoESS is now asking for a more stringent approach, whereby quality should weigh at least 50% for any type of private security service, which is already the case thanks to recent legislation in Spain, and 60% for security services within Critical Infrastructure.

---

[24] Source Encyclopaedia Britannica www.britannica.com

[25] EN 15602:2008 – Private Security Services Terminology, EN 16082:2011 Airport and Aviation Security Services and EN 16747:2014 Maritime and Port Security Services

Conditions for successful PPPs

As indicated above, several PPPs were studied in order to draw conclusions on success factors. The cases studied cover both Critical Infrastructure and public or semi-public spaces, previously known as "soft targets". Selected best practice examples are explained later in this chapter.

We have grouped the success criteria and respective recommendations for action around the four core values of CoESS: quality, safety, compliance and trust.

SAFETY: only legitimate companies should be selected to enter into PPPs in order to ensure the protection and safety of the clients and the providers' staff.

→ Guards shall be duly licensed, according to the various national legislation that are enforced.

→ Working conditions shall ensure that the guards are well equipped and protected.

→ Guards shall be well selected, vetted and screened. Background checks are not harmonised regarding contents, and documents provided by other EU Member States are difficult to authenticate. Furthermore the duration for the checks can vary significantly from one region or country to the other, and most PSC legislation requires that the guards be checked before they can be trained.

→ Guards should be adequately trained for the environment they will work in. Minimum training criteria should be set at EU level for guards active in transport, where a cross-border impact is high.

COMPLIANCE: companies should strictly comply with laws and regulations and should meet agreed industry standards and certifications.

→ PSCs shall abide by the legislation in place regarding their specific activity, and should meet all their fiscal, social and administrative obligations.

→ PSCs shall abide by the collective agreements.

→ PSCs shall meet European industry standards (CEN) that have been developed by private security industry experts and standardisation bodies, and shall be certified to these standards, where applicable. Standards that have been developed by the industry (CEN 16082, 16747 mainly) are not sufficiently known by stakeholders or they may choose to ignore them. The obligation to abide by those standards should be established within the PPPs, so that non-certified companies should not be able to bid for private security services. In the case of services to Critical Infrastructure, adherence to international standard ISO 9001 certification or equivalent quality standard should be mandatory.

→ Compliance with legal obligations, as indicated above, is in some cases optional, and this should not be possible for security providers. A different regime should exist for security services than for other business services. Security is a very special activity that is key to maintaining the integrity of society in all its components. It is an enabler and yet it is still too often considered as a mere commodity or cost.

QUALITY: Provision of qualitative services and procurement of security providers based on quality criteria is a condition of major importance for a PPP to work out and to build trust among stakeholders.

→ CoESS and its members, as well as trade unions shall promote the Best Value Manual approach to the relevant stakeholders, i.e. potential public and private buyers of private security services, so that these are selected based on best value, not on lowest cost.

→ Trade Associations are not systematically consulted to check whether the calls for tender abide by the best value principles. This should be changed.

→ Member States shall promote and support the application of MEAT (Most Economically Advantageous Tender) criteria in tenders related to public security. Quality should weigh at least 50% for any type of private security service, and 60% for security services within Critical Infrastructure. This enhances the adherence to safety and compliance criteria of companies.

→ The EU should continue delivering meaningful and practice-oriented guidelines on best value procurement to professionalise public buyers and support the implementation of EU Directives on Public Procurement. The guidance document on Innovation Procurement was an important first step. CoESS looks forward to the publication of the European Commission's "Buying Social Guide" and calls on the Commission to involve social partners in the drafting process.

→ Not every country has a Social Dialogue, and CoESS encourages its members and trade unions to establish and maintain a dynamic dialogue – for example to ensure the adherence to social minimum standards and socially responsible quality criteria in the procurement of private security services.

→ In many countries, PSCs are not able to face possible third parties' claims in the event of an incident, which could relate to amounts exceeding available insurance coverage – leading to professional security providers dropping out of calls for tenders. With the support of the EU, Member States need to address the issue and establish coherent liability regimes.

→ CoESS shall continue to develop and promote the uptake of industry standards that focus on quality.

TRUST: Trust-building is the basis for PPPs. Without trust, there's no meaningful collaboration and exchange of information.

→ The role of Trade Associations and Chambers that represent the interests of PSCs needs to be recognised through a dialogue with the authorities. In particular, when issuing a call for tender, the responsible authority should check with the Trade Associations and Trade Unions that its formulation allows for the legal, administrative, fiscal and social obligations to be met.

→ The role and responsibilities of LEAs and PSCs need to be very well and clearly defined, so that expectations are clear from both sides.

→ A framework needs to be established for regular communication between LEAs and PSCs: the format, regularity and contents of the information exchanged should be defined, as well as the contact persons in charge.

→ The PPP needs to be regularly evaluated and improved, based on the "Plan Do Check Act" model.

→ In order for the PPP to be effective, a "security chain mindset" needs to be shared by all participants and this is a challenge highlighted, for example, in the Dutch project on the exchange of information. In order to overcome this, regular meetings allow people to gradually know and trust each other. Sharing successes with both sides is also a way to reinforce the feeling of "being in this together". The responsibility to develop and maintain this "security chain mindset" should be held at managerial level.

→ No framework exists for PPPs at EU level and for the exchange of information. There should be at least common EU guidelines that could be recommended to the Member States to remove barriers to PPPs. Efforts to first assess these barriers in detail shall be intensified on EU-level, for example in relevant expert groups such as the EU Operators Forum.

Guidelines for PPPs in security

Step 1: Ensure Best Value Procurement

→ Public and private procurers should make sure that the call abides by (1) the laws and obligations to PSCs, to (2) the MEAT principle, as well as by (3) collective agreements and (4) any relevant standards.

→ Procurers should consult with relevant Trade Associations or Chambers and with Trade Unions.

→ Member States should set up an observatory composed of 50% Trade Unions and 50% Trade Associations under chairmanship of authorities, which conduct a market surveillance function. Such "observatories" exist in Spain and in Portugal.

Step 2: Set up comprehensive PPP Agreements

→ Determine the scope of the cooperation, clear operational and measurable objectives, and each party's commitment to reach them.

→ Description of roles, responsibilities/liabilities and missions of each party and clarify expectations for the LEA, the PSC and the Client.

→ Determine the procedures and routines for the operational cooperation.

→ Determine the procedures for the exchange of information (timing, format, contact points) and levels of classified information that can/needs to be exchanged.

→ Determine the contact points and meetings where LEAs and PSCs can exchange information and experience, as well as give any necessary feedback.

→ Set up regular meetings, attended by participants at managerial level and with the competences relevant to the agenda (permanent members and ad hoc members).

→ Agree on formats and procedures for the meetings and give space to feedback and improvement.

Step 3: Promote and implement security awareness, culture and training programmes as part of the PPP

The parties should identify and meet the needs for security awareness, culture and training with the environment covered by the PPP, depending on the targeted audience:

→ Security awareness: the general public should be encouraged to report any suspicious behaviour or activity to a central contact point.

→ Security culture: the staff working in the environment should be sensitised to security issues and understand how they are part of the chain, including Insider Threats.

→ Security training for specific groups of security or security-related staff.

Selected Best Practice Examples

Norway – Sentrum Model[26]

Strengthened cooperation between the police and private security companies is an overall objective for the authorities. One of the core tasks that the Norwegian police has set itself in its strategy plan for 2010-2015 was to develop effective cooperation solutions with other participants and service providers. This is a response to society's demand for stability, security, and the effective combating of crime. It is also a request from the Parliament to ensure a local police force with good local knowledge and a broad interface with local communities and citizens.

The "Sentrum" model in Oslo, which has been in practice since the early 2010s, has developed different areas for cooperation between the police, security industry, public sector participants and voluntary organisations, including a security guard meeting, and a bouncer (doorman) meeting. Another important element of the cooperation is the elaboration of special analysis forms. Areas where this cooperation is live include shopping centres, as well as urban environments.

PSCs have seen the benefit of surveying and analysing criminal activity – particularly in areas and locations with persistent challenges. Here, the special analysis forms have helped to increase the understanding of knowledge-based strategies and target-oriented management – with less focus on emergency and short-term solutions.
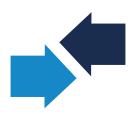
The security guard meetings also have another important function – namely to lower the threshold for contact and increase each party's understanding of the others' role and functions. Experience shows that the Sentrum model has helped to establish an open and honest dialogue between the participants.

The security guard meeting takes place once a week between the police and PSCs at the Sentrum police station. Personnel from the police at Sentrum and Grønland police stations participate, along with personnel from various departments, depending on incidents or current criminal cases.

The police is responsible for leading the security guard meetings and for taking minutes, which are distributed to all the participants after each meeting. The analysis and intelligence forms are used by the PSCs. Each PSC submits the form latest the day before the meeting. The information is reviewed by the police prior to the meeting, and discussed either at the plenary meeting or at a separate meeting with the relevant PSC, as necessary.

The success criteria have been:

→ The police is responsible for holding and guiding the meetings.

→ Fixed weekly meetings.

→ The participants submit their forms prior to the meeting.

→ Follow-up of cases and evaluation of incidents.

→ Participants are at management level.

26 Source: Police and security industry guide, Politiet Oslo Politidistrikt/NHO Service, Oslo 20.10.2016, Version 2.1

A practical example of this cooperation is operations in shopping centres. There is shared responsibility for the security between the police and the PSCs. For example, security guards observe activities that may be indicative of crime or security threats. They report to the police according to the template intelligence form. There is also a similar arrangement for urban environment, with area security guards who patrol outdoor areas that are accessible to the general public in densely populated districts. Their duties in this environment include:

→ Observe and report drug dealing.

→ Encourage people breaching the peace (noise or other) to cease their behaviour or leave the area.

→ Observe violence, including muggings/fights. Police must be notified immediately in this case, but it is lawful for them to intervene, whilst being mindful of their own safety.

The Netherlands – Oog en Oor[27]

The example outlined below is one of 10 projects presented in a booklet published by the Dutch Trade Association representing Private Security, Nederlandse Veiligheidsbranche, focused on the exchange of information between the police and PSCs.

Project "Oog en Oor" in the Seaport of Rotterdam is a cooperation between the Seaport Police and 2 PSCs.

The background to the project was the difficulty to react to incidents because of fragmented and therefore unavailable information and hence lack of adequate response. It was decided to set up a common real-time information exchange between the partners in the security chain. The type of information was from the police side the information about suspicious vehicles, goods, people, pictures and modus operandi of which PSCs should be aware in order to protect the port environment. From the PSCs side, they report observations that are relevant to the police. The information is exchanged on an internet platform that was specifically set up for this project.

In general terms this project made police and private security guards more aware and alert to suspicious activities and the platform is described as user-friendly and responsive. The number of eyes and ears on the port area has been significantly increased. The responsiveness and sense of initiative has also risen. PSCs have reported that the feedback from the police has had a positive effect on the security guards involved, who even during commuting were more alert to suspicious activities.

The report about the project highlights the need to give feedback about the follow up on cases, in order to maintain the PSC staff motivated and to keep the feeling alive of "being in this together".

Italy - Mille Occhi sulla città[28]

This initiative was first launched in 2010. It is a protocol between the government (Ministry of Interior), the association of Italian communes and several private security associations.

The agreement is based on the realisation that:

→ Citizens' security is a common good, the protection of which requires the synergetic action of the authorities and the private sector.

---

[27] Literally "Eye and Ear"

[28] Literally "Thousand eyes on the city", find more here: http://legacoop.produzione-servizi.coop/protocollo-mille-occhi-sulla-citta-aperto-tavolo-tecnico-per-rinnovo/

→ The coordination of public and private initiatives needs to be part of a "security system" governed by the principles of coordination and subsidiarity.

→ There is a need to "reach the maximum level of cooperation between the authorities in charge of public security, the national police forces, as well as the local police forces and PSCs, which are a complement to the public security".

Over 50 cities across Italy have been implementing the programme since the early 2010s and this number continues to increase.

The agreement states that private security, within its activities of "complementary security", may perform duties of observation and collect information relevant and useful for the police forces in order to prevent crime. In doing this, the document specifies that the PSCs may not perform public functions. The type of information is not described in detail but pertains to public order and security, including environmental factors that may impact urban security.

Criteria and modalities of cooperation between stakeholders are described in further details in the agreements signed in 2010, and renewed without changes in 2013 and 2019. The contents and implementation are discussed at a "technical table", which is also in charge of standardising procedures and technologies for the communication of information. The "technical table" is coordinated by the Central Directorate of Criminal Police.

The Guards, where relevant, may join police training programmes in order to perform their information collection and reporting.

The programme is monitored and evaluated by the authorities and proposals are made for its improvement, which are discussed by the public and private stakeholders.

Operational characteristics: police control rooms dispatch relevant information to private security control rooms, so that these can alert the respective patrols, and thereby increase the number of operators able to monitor situations. This is subject to the information not being under secrecy or operational restriction, and compliant with GDPR rules.

Examples of information exchanged include:

→ Suspicious vehicles or persons.

→ Possible escapes from crime scenes.

→ Theft of vehicles.

→ Assistance to people: children, older or confused people or people requiring assistance.

→ Presence of obstacles on roads or tracks.

→ Interruption of deliveries of sources of energy.

→ Any other situation arising suspicion that a crime is about to be committed.

→ Significant urban degradation or social unrest.

**Moving forward together
for a more resilient Europe**

Chapter 4

RECOMMENDATIONS AND
COMMITMENTS FOR 2019-2024

1. The European Security Union

The European Commission and Parliament brought considerable added value to the formulation of security policies and recommendations to Member States with the Security Union and Special Committee on Terrorism. In its Strategic Agenda for 2019-2024, the European Council put the protection of citizens and freedom at the top of its priorities for the upcoming legislative term.

It is up to all European institutions and stakeholders to deliver and continue the right path taken in the past legislature. CoESS is fully committed to this joint effort by offering its expertise and experience.

2. Legal framework for liability from Acts of Terrorism

In many countries, private security companies are not able to face possible third parties' claims in the event of an incident, which could relate to amounts exceeding available insurance coverage – leading to professional security providers dropping out of calls for tenders.

Only an EU approach can efficiently address this issue and create a coherent liability regime. Private security suppliers should not bear unlimited liability further to Acts of Terrorism.

CoESS commits to making proposals for a suitable liability regime.

3. European framework for the exchange of security-relevant information

Private security and police should be able to exchange information as partners in a set legal framework, which protects data privacy and confidentiality. Private security guards need to be aware of risks to effectively carry out protective missions while their intelligence needs to be used by police.

CoESS urges the European Commission to evaluate national barriers to the exchange of security-related information. Likewise, the European Council Recommendation (2002/ C 153/01) needs to be finally implemented after 17 years. CoESS commits to promoting the matter within the EU Operators Forum and to bringing together best practices and concrete proposals on how to transpose them.

4. Address the lack of skilled workers through high-quality Vocational Education and Training (IVET, CVET)

The shortage of skilled workers and skills mismatches are an existential challenge to European business. In addition to higher education, Initial (IVET) and Continuing Vocational Education and Training (CVET) are key to provide young people with the skills needed on the labour market, and to provide up- or re-skilling paths especially for elder employees.

It is important that the EU continues supporting the EU Member States, in collaboration with social partners, to improve uptake, quality assurance and funding in IVET and CVET.
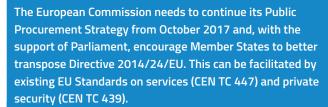
CoESS will continue to pro-actively move forward on this matter in cooperation with its Member Associations, BusinessEurope and its Social Partner UNI Europa.

5.

Enforce Best Value Procurement in the Security Sector

Public procurement of qualitative security services can save lives. Resilient security measures start with the selection of security providers that comply with common quality criteria and standards. But only few Member States took action so far and approved that at least 50% of criteria in public security tenders should be based on quality.

The European Commission needs to continue its Public Procurement Strategy from October 2017 and, with the support of Parliament, encourage Member States to better transpose Directive 2014/24/EU. This can be facilitated by existing EU Standards on services (CEN TC 447) and private security (CEN TC 439).

CoESS will continue to propagate high quality industry standards and steer procurers to implement the best value principle when buying private security services.[29]

Security is a basic human need and a fundamental right for every European citizen. In our globalised world, it is an enabler for our society and businesses to prosper, but also an elementary condition to foster a pro-European and democratic Union. Moving forward, the EU has to improve resilience and continue to deliver security in public spaces, Critical Infrastructure, and in people's daily lives.

As the voice of the private security industry, representing over 45.000 companies with around 2 million licensed guards in Europe, CoESS – together with its corresponding member ASSA-i – are strongly committed partners to the institutions. Since 30 years, their mission has been to bring added value to European policies and to foster a Union, which is well prepared for the numerous opportunities and challenges ahead.

6.

European minimum standards for security guard training in transportation

Although land, maritime and aviation transport in Europe have an important cross-border dimension, training requirements for security staff vary significantly among EU Member States – presenting a crucial shortcoming in cross-border transport security.

CoESS strongly recommends that the European Commission evaluates the lack of harmonisation of basic training requirements for security personnel operating at cross-border transportation hubs, and closes those security gaps that have been identified.

[29] To support the professionalisation of public buyers of security services, CoESS published in cooperation with UNI Europa and with financial support of the European Commission a Best Value Manual to be found on www.securebestvalue.org.

7. Update of the EU Aviation Security Framework

Common rules for aviation security, namely Regulation 300/2008 and Regulation 2015/1998, are interpreted very differently in EU Member States. Countries with loser interpretation become a loophole in the security chain. Further, legislation needs to address evolving risks such as Insider Threats, CBRN, non-metal weapons, drones and cyberattacks.

It is crucial that the Commission continues to advance on the future Aviation Strategy. CoESS commits to contribute to this process in partnership with ASSA-i through the Commission's Expert Group on Aviation Security SAGAS.

8. Revision of the Critical Infrastructure Protection Directive

CoESS highly welcomes the recently published evaluation of Directive 2008/114/EC. An ambitious follow-up is recommended that includes a more homogeneous definition of all Critical Infrastructure and risk assessments across Member States and a widened scope of the Directive.

In order to improve CIP, at least 60% of criteria in CIP procurement tenders should mandatorily be based on quality and explicit roles and responsibilities of security staff should be allocated. CIP further requires close public-private cooperation.

CoESS commits to continue its work on an over-arching standard for security services providers to Critical Infrastructure within CEN TC 439 – the CEN Technical Committee on Private Security Services.

9. A strong Internal Security Fund (ISF)

The ISF is a key pillar of the EU's security policies and counterterrorism efforts. In this regard, CoESS is calling for a strong future ISF that reduces administrative burdens for applicants, strengthens cooperation with the private sector, and responds in a flexible and efficient way to emerging security issues particularly to public spaces and Critical Infrastructure – including a respective financial envelope.

CoESS supports the Parliament's report on the Commission proposal establishing the ISF in the next long-term EU budget, and calls on co-legislators to find a rapid agreement both on the MFF and the future ISF.

After a very well received ISF-funded project on Insider Threat (AITRAP 2017-2018), CoESS will continue to constructively contribute to the identification of ISF funding needs, provide added value within ISF projects and deliver outcomes to the benefit of society.

10. Strengthened Social Dialogue

A strong social dialogue is crucial to address challenges to the labour market, including the lack of skilled workers and evolving working conditions. In practice, social partners know best how to tackle these challenges. The role of social partners, existing collective agreements and the subsidiarity principle must be respected.

Social dialogue should be strengthened and, where needed, funded efficiently across Europe by the ESF+.

CoESS is committed to its social dialogue with UNI Europa and continues to support its Member Associations in strengthening (or in certain cases establishing) national social dialogues.

About CoESS

The **Confederation of European Security Services (CoESS)** acts as the voice of the private security industry, covering **18 European Union (EU) Member States** and a total of **23 countries across Europe**, representing around **2 million licensed guards** and **45,000 companies**, and generating a **turnover of €40M+**. CoESS is a member of BusinessEurope.

The private security services provide a wide range of services, both for private and public clients, ranging from European Union institutions buildings to nuclear plants, airports, Critical Infrastructure facilities, inter-modal transport hubs, public transport stations and areas, and national governmental agencies and institutions (such as asylum seekers centres, public hospitals, universities, etc.).

As defined in CEN EN 15602 standard on "Security Services Providers – Terminology", "private security company" is one that provides private security services. Following the definition in the standard, services provided by security companies are aimed at the protection of people, property and assets. These may include the following services (non-exhaustive list):

➔ Manned guarding – access/exit control, airport security checks, armed security officer/guard, port security checks, reception security, site security, static guarding, store detective.

➔ Mobile patrolling and mobile site/area patrolling.

➔ Alarm response – alarms, monitoring and alarm receiving centre, alarm receiving and monitoring centre operator, alarm response, alarm response officer.

➔ Key holding – key holding and key storage.

➔ Event security – crowd controller, crowd control supervisor, crowd control management.

➔ Door security and supervisor.

➔ Close protection/body guarding.

➔ Public order services – city patrolling, transport security.

It excludes military services.

coess.org

The Aviation Security Services Association – international (ASSA-i) is a corresponding member of CoESS and represents private security companies that provide security services at airports. The members' activities have an international scope and include the surveillance and protection of civil aviation, in particular as regards the inspection of individuals, luggage and cargo, as well as any other relevant security action.

assa-i.org

For further reading

CoESS/UNI Europa: Anticipating, Preparing and Managing Employment Change in the Private Security Industry. A project funded by the European Commission, 2018.

ASSA-i: Chemical Threats to Civil Aviation, 2018.

CoESS: Best Practices in Transport Security, 2017.

CoESS: The Use of UAs in Private Security, 2017.

CoESS: Critical Infrastructure Security and Protection – the Public-Private Opportunity, 2016.

ASSA-i: Position Paper on the EU Aviation Strategy, 2016.

CoESS: The New Security Company, 2015.

CoESS/UNI Europa: Buying Quality Private Security Services. A project funded by the European Commission, 2014.

More information on **www.coess.org** and **www.assa-i.org**

Acting as the voice of the **security industry**

coess.org