THE HAGUE
10 Oct. 2024

7th European Security Summit

CoESS

Nederlandse Veiligheidsbranche

International SecurityLigue

WHITE PAPER

Öffentlich-private Partnerschaften: Das Potenzial für verbesserte Sicherheit freisetzen

BDSW
BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT

VSÖ
VERBAND DER SICHERHEITSUNTERNEHMEN ÖSTERREICHS

VSSU

Über die Autoren des Papiers:

Die CoESS (**Confederation of European Security Services** / Verband der Europäischen Sicherheitsdienstleistungsunternehmen) vertritt seit 35 Jahren die private Sicherheitsbranche in ganz Europa. Die CoESS setzt sich dafür ein, hohe Standards für Professionalität und Qualität in der Sicherheitsbranche zu fördern und politische Maßnahmen zu unterstützen, die das Wachstum und die Professionalität der Branche stärken.

Die **Nederlandse Veiligheidsbranche** (die niederländische Sicherheitsvereinigung) vertritt die niederländische Sicherheitsbranche seit 85 Jahren. Der Verband vertritt die Interessen der Unternehmen im Sicherheitssektor auf nationaler Ebene und pflegt Kontakte zu Regierung, Parlament und anderen Interessengruppen. Die Nederlandse Veiligheidsbranche vereint kleine und mittlere Unternehmen sowie große zertifizierte Unternehmen, vertritt 90 % des Marktumsatzes und ihre Mitglieder beschäftigen 32.000 qualifizierte Sicherheitskräfte.

Die **International Security Ligue** ist die globale Vereinigung privater Sicherheitsorganisationen, die sich der Förderung von Sicherheitsstandards weltweit widmet. Mit dem Fokus auf die Förderung von Best Practices und der Förderung internationaler Zusammenarbeit bietet die International Security Ligue eine globale Perspektive auf Sicherheitsherausforderungen und Lösungen. Ihre Beiträge helfen, die Diskussion in einen breiteren internationalen Kontext zu stellen.

Danksagungen:

Die CoESS ist den folgenden Personen sehr dankbar für ihre gründliche Durchsicht, das Teilen ihres Wissens und ihrer Expertise sowie für die Verbesserung dieses Dokuments:
Eduardo Cobas Urcelay, Generalsekretär, APROSER
Alexander Frank, stellvertretender Generaldirektor, CoESS
Jonas Maas, PhD Forscher, Abteilung für Kriminologie, Strafrecht und Sozialrecht, IRCP, Universität Gent
Drs. René R.K. Siccama Hiemstra, Direktor, G4S Niederlande
Garett Seivold, Chief Content & Communications Officer, The International Security Ligue

Haftungsausschluss:

Herausgeber:

Catherine Piana
Generaldirektorin
CoESS aisbl
56 Avenue des Arts
1000 Brüssel
Belgien
catherine@coess.eu
www.coess.eu

Design & graphics:
https://blog.acapella.be/

Photo credits:
© AdobeStock: 189459003: Patrick Daxenbichler, 734099125*: PikePicture, 490783520: Pixel-Shot, 920222022*: Andres Mejia, 856511461*: Curioposs, 546319561: NongAsimo
**Generated with AI*

© iStock: 1461413822: HJBC, 1316755706: Flex Point Security, 836601774 and 836601946: Naypong, 1219733094: MARHARYTA MARKO, 1575562418: Jacob Wackerhausen, 1393855287: Galeanu Mihai, 1281959537: NicoElNino, 1472468738: Irene Puzankova, 1498077737: CASEZY, 1444503376: Marta fernandez, 1480307525: gorodenkoff, 1460172015: Tippapatt, 506815322: artJazz, 908827618: AndreyPopov

© Shutterstock: 131124554: Michael Dechev

INHALTSVERZEICHNIS

Vorwort

Die private Sicherheitsbranche wird zunehmend als ein wichtiger Partner von Strafverfolgungsbehörden anerkannt, wenn es um den Schutz von Menschen, Vermögenswerten und Infrastruktur geht. Diese Anerkennung hat in den letzten Jahren zugenommen, angetrieben durch bedeutende globale Herausforderungen wie die COVID-19-Pandemie und die anhaltende Bedrohung durch Terrorismus. In diesen Krisen haben private Sicherheitsdienstleistungsunternehmen (PSD) und ihre engagierten Mitarbeiter ihr unerschütterliches Engagement für den Schutz der Gesellschaft unter Beweis gestellt sowie entscheidende Rollen in der Prävention übernommen.

Infolgedessen wenden sich Regierungen in ganz Europa zunehmend an die private Sicherheitsbranche zur Unterstützung, insbesondere angesichts des Arbeitskräftemangels bei den Strafverfolgungsbehörden. Während sich die Strafverfolgung auf ihre Kernaufgaben konzentrieren muss, sind Private-Sicherheitsdienstleistungsunternehmen (PSD) gut positioniert, um eine Reihe ergänzender Aufgaben zu übernehmen. Diese Partnerschaft hat sich nicht nur als effizient, sondern als notwendig erwiesen, da PSD Professionalität, Innovation und modernste Technologie einbringen – wesentliche Elemente moderner Sicherheitsstrategien.

Obwohl sie in privatem Besitz sind und kommerziell orientiert arbeiten, können PSD einen großen Beitrag zur Sicherheit im öffentlichen Bereich leisten, sowohl als beauftragte Dienstleister als auch als Mitwirkende, indem sie Augen und Ohren der 2 Millionen Sicherheitskräfte in Europa nutzen, die täglich ihr Bestes geben, um unsere Welt sicherer zu machen.

Öffentlich-private Partnerschaften (Public-Private-Partnerships – PPPs) stellen eine enorme Chance dar, Sicherheitsmaßnahmen durch Komplementarität zu verbessern. Der Erfolg dieser Partnerschaften wird durch die zunehmende Professionalität der privaten Sicherheitsbranche und ihre Fähigkeit zur Innovation ermöglicht. Mit den richtigen rechtlichen Rahmenbedingungen können PSD, Strafverfolgungsbehörden in einer Vielzahl von Missionen unterstützen und öffentliche Ressourcen für spezialisiertere Strafverfolgungsaufgaben freisetzen.

Wir fordern die Behörden auf, diese Partnerschaften weiterhin zu fördern, PSD nicht als Untergebene, sondern als essenzielle Partner im Sicherheitskontinuum zu betrachten. Gleichzeitig drängen wir die private Sicherheitsbranche, diese sich entwickelnde Rolle zu übernehmen und weiterhin Führungsstärke sowie Engagement für den Schutz unserer Gesellschaften zu zeigen. Gemeinsam können wir ein stärkeres, widerstandsfähigeres Sicherheitsrahmenwerk aufbauen, das besser in der Lage ist, den Herausforderungen von heute und morgen zu begegnen.

Vinz van Es,
Vorsitzender,
CoESS

Ard van der Steur,
Vorsitzender, Niederländische
Sicherheitsbranche (NVB)

Zusammenfassung

Dieses Weißbuch hat zum Ziel, öffentlich-private Partnerschaften (Public-Private-Partnerships - PPPs) in Europa zu identifizieren, zu definieren und zu beschreiben, wobei ihre entscheidende Rolle bei der Verbesserung der Sicherheit in verschiedenen Umfeldern hervorgehoben wird. Durch die Nutzung theoretischer Quellen und die Darstellung von Best Practices zeigt es, wie die Zusammenarbeit zwischen Strafverfolgungsbehörden und privaten Sicherheitsdienstleistungsunternehmen (PSD) die Gesamt-Sicherheit und gesellschaftliche Resilienz stärkt. Darüber hinaus behandelt das Papier die Herausforderungen, die die Effektivität von PPPs behindern, und gibt Empfehlungen für die beteiligten Akteure, diese Barrieren zu überwinden, Schlüsselkriterien für den Erfolg umzusetzen und das Potenzial von PPPs zu optimieren.

Eine Gelegenheit zur Komplementarität und gesteigerten Effizienz

Die in diesem Papier betrachteten öffentlich-privaten Partnerschaften umfassen alle Formen der Zusammenarbeit zwischen Strafverfolgungsbehörden und PSD. Sie kombinieren die Stärken und Ressourcen öffentlicher Sicherheitskräfte mit den spezialisierten Fähigkeiten privater Sicherheitsdienstleistungsunternehmen. Diese Zusammenarbeit adressiert komplexe Sicherheitsherausforderungen effizient und stellt einen umfassenden Ansatz zum Schutz von Menschen, Vermögenswerten und Infrastruktur sowie der Gesellschaft als Ganzes sicher. Die Synergie ermöglicht eine erweiterte Sicherheitsreichweite, nutzt fortschrittliche Technologien und verbessert die strategische Ressourcenzuteilung im gesamten Sicherheitsbereich.

Bedeutung und Auswirkungen

PPPs optimieren den Ressourceneinsatz, indem sie es den Strafverfolgungsbehörden ermöglichen, sich auf ihre Kernaufgaben zu konzentrieren, während PSD die Dimensionen der Prävention und Erkennung übernehmen. Diese Partnerschaften verbessern die operativen Fähigkeiten, bieten Skalierbarkeit als Reaktion auf sich ändernde Sicherheitsanforderungen und führen innovative Lösungen für das Sicherheitsmanagement ein. Diese strategische Zusammenarbeit führt zu einer verbesserten Flexibilität bei den Operationen und einer proaktiven Haltung in der Sicherheitsplanung.

Höhepunkte

PPPs sind nur in 9 von 27 EU-Mitgliedstaaten rechtlich möglich, hauptsächlich in westeuropäischen Ländern, in denen sie unterschiedliche Realitäten abdecken. Während einige Mitgliedstaaten fortgeschrittene Partnerschaften auf der Grundlage formaler Rahmenbedingungen haben, sind andere informell, lokal und vorübergehend. Der Schutz von Objekten und Ereignissen variiert ebenfalls, ebenso wie die Aufgaben, die den PSD zugewiesen werden.

Es gibt eine Korrelation zwischen dem Professionalisierungsgrad der Branche, der Reife des rechtlichen Rahmens und der Tiefe der Zusammenarbeit zwischen Strafverfolgungsbehörden und PSD.

Dieses Papier beschreibt die Vorteile der Durchführung von PPPs, einschließlich:

- **Ressourceneffizienz:** Private Unternehmen unterstützen Strafverfolgungsbehörden, indem sie präventive und Überwachungsaufgaben übernehmen, wodurch öffentliche Ressourcen für Strafverfolgungsbehörden freigesetzt werden, damit diese sich auf ihre Kernaufgaben konzentrieren können.
- **Fortgeschrittene Spezialisierung:** PPPs bringen modernste Technologie und spezialisierte Fähigkeiten ein, die besonders in Bereichen wertvoll sind, in denen sie spezielles Know-how entwickelt haben, wie z.B. Zugangskontrolle, Fernüberwachung und -kontrolle, Schutz bestimmter Infrastrukturen (kritische und andere) usw.
- **Strategische Flexibilität:** Die Fähigkeit, Sicherheitsmaßnahmen dynamisch an die jeweilige Situation anzupassen, verbessert sowohl die proaktive als auch die reaktive Einsatzfähigkeit.

Auswirkungen auf die Sicherheitslandschaft

Die zunehmende Komplexität und Vielfalt der Bedrohungen erfordert einen Wandel hin zu einem integrierteren und reaktionsfähigeren Sicherheitsrahmen. Dieser Ansatz verbessert nicht nur die unmittelbare Reaktion auf Bedrohungen, sondern unterstützt auch eine nachhaltige Sicherheitsstrategie, die sich an zukünftige Herausforderungen anpasst. Die Auswirkungen gehen über unmittelbare Sicherheitsverbesserungen hinaus und deuten auf langfristige Vorteile für die öffentliche Sicherheit und das Vertrauen hin.

Herausforderungen und Strategien zur Überwindung von Hindernissen in PPPs

Obwohl öffentlich-private Partnerschaften erhebliche Vorteile bieten, sehen sie sich auch spezifischen Herausforderungen gegenüber, die ihre Effektivität beeinträchtigen können. Zu den wesentlichen Hindernissen gehören Fragen des Vertrauens und der Informationsweitergabe, unterschiedliche betriebliche Kulturen zwischen öffentlichen und privaten Einrichtungen sowie regulatorische Einschränkungen, die die Zusammenarbeit behindern können.

Um diese Herausforderungen zu überwinden, empfiehlt dieses Weißbuch mehrere Maßnahmen, von denen die folgenden besonders wichtig sind:

1. Vertrauen und Transparenz stärken: Der Aufbau von Vertrauen ist von grundlegender Bedeutung. Initiativen wie gemeinsame Schulungen, gemeinsame operative Planung und regelmäßige Treffen mit den beteiligten Akteuren können ein gegenseitiges Verständnis fördern und das Vertrauen stärken. Klare Kommunikation und Transparenz in den Betriebsabläufen und Entscheidungsprozessen sind entscheidend, um eine zuverlässige Partnerschaft zu entwickeln.

2. Harmonisierung von Standards und Praktiken: Die Entwicklung gemeinsamer Standards und Praktiken im öffentlichen und privaten Sektor innerhalb von PPPs kann kulturelle und operative Unterschiede verringern. Mögliche Bereiche, um die Zusammenarbeit zu optimieren könnten Schulungen, Sicherheitsprotokolle, Dateninteroperabilität, Schwachstellenbewertungen und Komplementarität in Reaktionsstrategien umfassen.

3. Regulatorische Anpassungen: Es ist erforderlich, bestehende Gesetze und Vorschriften anzupassen, um PPP-Rahmenwerke zu unterstützen und den Informationsaustausch zwischen PSD und Strafverfolgungsbehörden zu ermöglichen. Die Gesetzgebung sollte die qualitätsorientierte Auftragsvergabe und kooperative Maßnahmen unterstützen sowie den Informationsaustausch fördern, anstatt ihn zu behindern. So wird sichergestellt, dass sowohl öffentliche als auch private Einrichtungen unter einem unterstützenden rechtlichen Rahmen arbeiten, der das gegenseitige Vertrauen stärkt und die Zusammenarbeit fördert. Schließlich sollte die Gesetzgebung auch sicherstellen, dass Strafverfolgungsbehörden ein gutes Verständnis für die Befugnisse von PSD haben. Dies könnte in die grundlegende Ausbildung des Personals der Strafverfolgungsbehörden aufgenommen werden.

„PPPs verbessern nicht nur die aktuellen Sicherheitsmaßnahmen, sondern bereiten Organisationen auch auf zukünftige Bedrohungen vor.“

Durch die gezielte Bewältigung dieser Herausforderungen können PPPs nicht nur ihre operative Effektivität steigern, sondern auch eine widerstandsfähigere und anpassungsfähigere Sicherheitsinfrastruktur schaffen. Diese Bemühungen erfordern kontinuierliches Engagement und Entwicklung aller beteiligten Akteure, um den fortgesetzten Erfolg und die Weiterentwicklung von PPPs im Sicherheitssektor zu gewährleisten.

Abschließend lässt sich sagen, dass öffentlich-private Partnerschaften im modernen Sicherheitsapparat unverzichtbar sind. Durch die effektive Kombination der einzigartigen Stärken von Strafverfolgungsbehörden und PSD verbessern PPPs nicht nur die aktuellen Sicherheitsmaßnahmen, sondern bereiten Organisationen auch auf zukünftige Bedrohungen vor. Dieses Weißbuch unterstützt die fortlaufende Entwicklung und Verfeinerung von PPP-Rahmenwerken, um deren positiven Einfluss auf die öffentliche Sicherheit zu maximieren.

1. Einleitung

Dieses Weißbuch zu öffentlich-privaten Partnerschaften (PPPs) im Sicherheitsbereich ist eine gemeinsame Initiative der europäischen, niederländischen und internationalen Organisationen der Sicherheitsbranche: der Confederation of European Security Services (CoESS), der Nederlandse Veiligheidsbranche (NVB), unterstützt von der International Security Ligue (ISL). Diese Organisationen bringen eine Fülle von Fachwissen und Erfahrung ein und bieten eine umfassende und maßgebliche Perspektive auf die sich entwickelnde Landschaft der privaten Sicherheit, einschließlich der Zusammenarbeit mit Strafverfolgungsbehörden zum Schutz von Menschen, Vermögenswerten und Infrastruktur.

Aufbauend auf der Grundlage des CoESS-Weißbuchs „Das Sicherheitskontinuum in der neuen Normalität“[1] geht dieses Dokument tiefer auf die Dynamik der öffentlich-privaten Partnerschaften im Sicherheitssektor ein. Die Veröffentlichung hob die Notwendigkeit einer nahtlosen Zusammenarbeit zwischen öffentlichen und privaten Sicherheitsorganisationen hervor, um die aktuellen Sicherheitsherausforderungen effektiv zu bewältigen. Dieses Weißbuch beabsichtigt, dieses Konzept weiter auszubauen, neue Einblicke, Strategien und Empfehlungen für eine verbesserte öffentlich-private Zusammenarbeit im Sicherheitssektor zu bieten. Im Besonderen wird das Papier den Stand der PPPs in Europa und die Chancen für die Behörden aufzeigen, die Hindernisse und Lösungen darlegen und Empfehlungen für die Zukunft machen.

[1] *Confederation of European Security Services (CoESS). (2019). “The Security Continuum in the New Normal”. Retrieved from https://coess.eu/.*

Ziele des Papiers:

1. Definition von PPPs im Sicherheitsbereich in Europa: Kapitel 2 zielt darauf ab, das Konzept der PPPs im europäischen Sicherheitskontext zu klären, eine klare Definition und Reichweite festzulegen, die die verschiedenen Formen und Strukturen der Zusammenarbeit zwischen PSD und Strafverfolgungsbehörden in verschiedenen Ländern und innerhalb ihrer jeweiligen rechtlichen Rahmen umfasst.

2. Chancen und Erfolgskriterien von PPPs darlegen: Der erste Teil von Kapitel 3 untersucht die Schlüsselfaktoren, die zum Erfolg von PPPs im Sicherheitssektor beitragen, wie Vertrauen, effektive Kommunikation, ein unterstützender rechtlicher Rahmen und interoperable Technologie. Es wird untersucht, wie diese Elemente eine produktive Partnerschaft fördern, die die Gesamt-Sicherheitsziele verbessert.

3. Hindernisse identifizieren und analysieren: Trotz der potenziellen Vorteile gibt es mehrere Herausforderungen, die die Effektivität von PPPs behindern. Der zweite Teil von Kapitel 3 diskutiert häufige Hindernisse, wie den Aufbau von Vertrauen zwischen Entitäten mit unterschiedlichen Kulturen und operativen Philosophien, die Schaffung eines gemeinsamen Verständnisses für komplementäre Rollen und die Etablierung einer gemeinsamen Denkweise der aktiven Zusammenarbeit. Ein eigener Abschnitt widmet sich der sensiblen Frage des Informationsaustauschs.

4. Vorstellung bestehender Modelle: Durch die Präsentation verschiedener erfolgreicher PPP-Modelle bieten Kapitel 4 und 6 konkrete Beispiele dafür, wie diese Kooperationen in der Praxis funktionieren. Diese Fallstudien zeigen die operativen Details, Governance-Strukturen und heben die spezifischen Kontexte hervor, in denen diese Partnerschaften gedeihen.

5. Empfehlungen für die verschiedenen PPP-Stakeholder: Kapitel 5 zieht Best Practices und akademische Literatur zu PPPs heran, um innovative Ansätze und Lösungen vorzuschlagen. Diese Diskussion soll die Leser inspirieren und ihnen umsetzbare Strategien an die Hand geben, um die Umsetzung und Effektivität von PPPs in ihren eigenen Kontexten zu verbessern.

Abschließend enthält Kapitel 7 eine Checkliste der International Security Ligue zur „Schaffung einer effektiven Partnerschaft im Bereich der privaten Sicherheit". Sie kategorisiert und listet Kriterien, die von der Branche als relevant angesehen werden, um die Voraussetzungen eines PSD zu bewerten, eine Partnerschaft einzugehen.

Durch diese Ziele möchte dieses Weißbuch die Diskussion fortsetzen und vertiefen, wie wir besser zusammenarbeiten und stärkere, effektivere Partnerschaften schmieden können, die den komplexen Sicherheitsherausforderungen der heutigen Welt gerecht werden. Durch ein gründliches Verständnis sowohl der Mechanismen als auch der Herausforderungen von PPPs möchte das Papier den Weg für integriertere und effektivere Sicherheitsstrategien in Europa und darüber hinaus ebnen.

„Dieses Weißbuch untersucht, wie wir besser zusammenarbeiten und stärkere, effektivere Partnerschaften schmieden können."

2. PPPs: Definitionen, Umfang und Relevanz

„Die Aufgaben und Kompetenzen von privaten Sicherheitsdienstleistungs-unternehmen (PSD) und damit auch die Konzepte von PPPs unterscheiden sich in den einzelnen europäischen Ländern.“

2.1. Definition und Umfang von PPPs im Kontext der Sicherheit und dieses White Paper

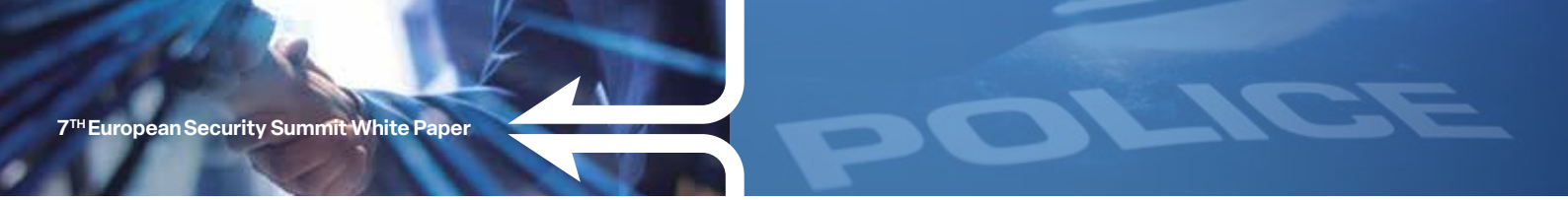
Es gibt verschiedene Definitionen von PPPs, aber dieses Papier verfolgt eine breite und flexible Perspektive, die alle Situationen umfasst, in denen die Polizei oder andere Strafverfolgungsbehörden mit der privaten Sicherheitsbranche zusammenarbeiten, nämlich:

- Ein Privater Sicherheitsdienst schützt einen öffentlich zugänglichen oder anderen Standort im Auftrag und/oder unter der Aufsicht der Strafverfolgungsbehörden;

- Die von einem PSD ausgeführten Aufgaben erfordern eine Zusammenarbeit zwischen diesem Unternehmen und einer Strafverfolgungsbehörde. Dies umfasst den Schutz und die Zugangskontrolle von privaten, öffentlich zugänglichen Orten wie Einkaufsbereichen, kulturellen Sehenswürdigkeiten und religiösen Stätten sowie kritischer Infrastruktur oder anderen sensiblen Standorten und Veranstaltungen. Die Zusammenarbeit mit Strafverfolgungsbehörden ist erforderlich bei präventiven Maßnahmen, um potenzielle Risiken und Bedrohungen zu verstehen und falls die Intervention einer Strafverfolgungsbehörde erforderlich wird. Strafverfolgung und öffentliche Sicherheit sind nationale Aufgaben. Daher unterscheiden sich die Aufgaben und Zuständigkeiten von PSD sowie die Konzepte der PPPs von Land zu Land in Europa. Wir betrachten daher viele verschiedene Modelle von PPPs, die wiederum von den jeweiligen nationalen Gesetzen beeinflusst werden.

2.2. Die wirtschaftliche, soziale und operationelle Begründung für PPPs und wie sie die Sicherheitsziele verbessern

Europa besteht aus einer Vielzahl unterschiedlicher Modelle, rechtlicher Rahmenbedingungen und Ansätze, bei denen private Unternehmen Aufgaben im Auftrag der Strafverfolgungsbehörden oder in



Zusammenarbeit mit ihnen übernehmen. Diese unterschiedlichen Rechtssysteme haben auch eine unterschiedliche Abgrenzung der Aufgaben, die von den Strafverfolgungsbehörden und von der privaten Sicherheit übernommen werden. Während es eine klare Abgrenzung für die Kernaufgaben und -missionen der Strafverfolgungsbehörden gibt, gibt es eine weichere Grenze für die peripheren Aufgaben, die keine Autorität oder ein Monopol auf Gewalt beinhalten und von Land zu Land schwanken. In diesem Bereich können mehr Aufgaben von der privaten Sicherheit unterstützt werden. Damit dies jedoch geschehen kann, müssen Regierungen, Strafverfolgungsbehörden und die Gesellschaft dieses PPP-Konstrukt anerkennen, akzeptieren und ihm vertrauen. In ihrer Arbeit[2] hebt L.A. Bisschops, eine Kriminologin, die 2022 ihre Masterarbeit über PPPs schrieb, hervor, dass mehrere Elemente zur Stärkung der öffentlich-privaten Partnerschaften vom politischen Klima abhängen.

Wo PPPs existieren, sind sie meist das Ergebnis verschiedener Faktoren und Treiber:

- Anhaltende Kapazitätsprobleme in den Strafverfolgungsbehörden, unter anderem aufgrund von Arbeitskräftemangel, und die Fähigkeit von privaten Sicherheitsdienstleistungsunternehmen, diese zu kompensieren und so die Kosteneffizienz zu steigern;
- Unzureichende öffentliche Ressourcen zur Bewältigung aller Sicherheits- und Präventionsaufgaben;
- Steigende Kriminalitätsraten und/oder die Nachfrage nach mehr Sicherheit, die nicht vollständig von den Strafverfolgungsbehörden gedeckt werden kann;
- Die zunehmende Komplexität und das Ausmaß von Sicherheitsherausforderungen, die die Einbeziehung von spezialisiertem Personal erfordern, das nicht unbedingt in den Strafverfolgungsbehörden verfügbar ist;
- Professionalisierung und Digitalisierung des Sicherheitssektors, wobei PSD in Ausbildung, Technologie und Infrastruktur investiert haben, um ihre Fähigkeiten zu erweitern. Die Notwendigkeit, die Aufgaben des öffentlichen Sektors auf die Kernmissionen zu rationalisieren, die durch die Autorität und Befugnisse der Strafverfolgungsbehörden gekennzeichnet sind, wie zum Beispiel die Anwendung von Gewalt.

Bis jetzt waren öffentlich-private Partnerschaften eine attraktive Möglichkeit, die Risikoverteilung zu optimieren, unter der Annahme, dass private Akteure die Risikoverteilung effizienter als öffentliche Organisationen vornahmen, während öffentliche Akteure besser in der Lage waren, alle administrativen Aspekte effektiver zu adressieren. Die aktuellen Umstände lassen jedoch darauf schließen, dass öffentlich-private Partnerschaften nicht nur attraktiv, sondern auch notwendig sind. Die Leistung von Organisationen im Sicherheitssektor, sowohl im öffentlichen als auch im privaten Bereich, steht angesichts der sich schnell ändernden Bedrohungslandschaft vor dem Hintergrund eines strukturell problematischen Arbeitsmarktes unter Druck.

Aufgrund der Art der von ihr erbrachten Dienstleistungen ist die private Sicherheitsbranche in der Lage, die Strafverfolgungsbehörden zu unterstützen, indem sie Aufgaben übernimmt, die nicht Teil ihrer Kernaufgaben sind, und ihr Fachwissen als Ergänzung zu den spezifischen Aufgaben und Befugnissen der Strafverfolgungsbehörden einbringt.

2.3. Überblick über PPP-Konzepte und -Modelle

Es gibt zahlreiche Arten von PPPs, und in diesem Dokument sind Beispiele wie folgt aufgeführt:

- **Informationsaustausch:** Private Sicherheitsdienstleistungsunternehmen melden verdächtiges Verhalten oder Personen an die Strafverfolgungsbehörden und umgekehrt;
- **Prävention illegaler Handlungen:** Zugangskontrollen in öffentlich zugänglichen Bereichen wie Sport- oder Kulturveranstaltungen, Verkehrs-Knotenpunkten usw.;
- **Zusammenarbeit bei Übungen und Schulungen;**
- **Risikobewertungen und Sicherheitsbewertungen;**
- **Schutz kritischer Infrastruktur:** Obwohl dies der Schwerpunkt eines zukünftigen CoESS-Papiers sein wird, gibt es einige Beispiele in diesem Papier, die zeigen, wie PPPs den Schutz und die Resilienz von kritischer Infrastruktur verbessern können. Im aktuellen Kontext des Krieges in der Ukraine werden PSD zunehmend nicht nur zum Schutz militärischer Infrastruktur mit verschiedenen personellen und technologischen Mitteln herangezogen, sondern auch, um zusätzliche Mittel in Betracht zu ziehen, um Staaten zu unterstützen, falls sie aktiv in den Konflikt eingreifen müssen.

[2] *Bisschops, L. A. (2022). Een internationaal kwalitatief onderzoek naar het verstevigen van publiek-private samenwerking in het Nederlandse veiligheidsdomein – Übersetzung: Eine internationale qualitative Studie zur Stärkung öffentlich-privater Partnerschaften im niederländischen Sicherheitsbereich [Masterarbeit, Universität Amsterdam, Ermittlungscriminologie].*

SCHLÜSSELFAKTOREN FÜR ERFOLGREICHE PPPS EMPFEHLUNGEN AUS DEM CoESS WEISSBUCH ZUM SICHERHEITSKONTINUUM IM NEUEN NORMAL

Im Weißbuch zum „Sicherheitskontinuum im neuen Normal" formulierte CoESS die Erfolgskriterien für PPPs anhand von 4 Kernwerten:

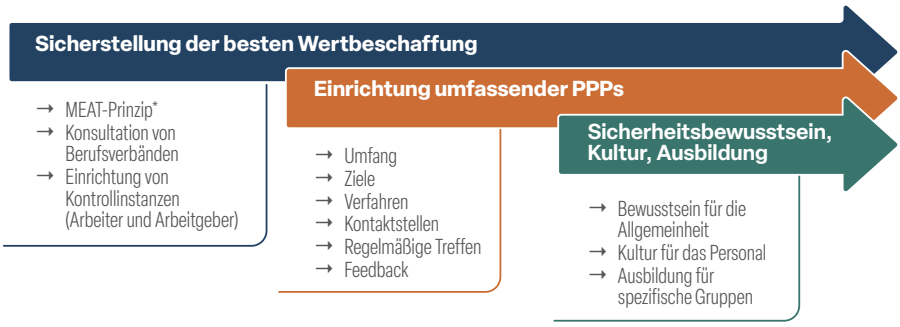
Sicherheit: Sicherstellung des Schutzes und der Sicherheit des Kunden und des Personals des Dienstleisters durch die Auswahl nur legitimer Unternehmen für PPPs. PSD müssen nachweisen, dass Sicherheitskräfte ordnungsgemäß lizenziert, ausgewählt und geschult sind, dass die Arbeitsbedingungen gewährleistet sind, und dass sie gut ausgerüstet und geschützt sind.

Compliance: Sicherstellung, dass Unternehmen die Gesetze, Vorschriften sowie die Branchenstandards und Zertifizierungen strikt einhalten.

Qualität: Da Sicherheit eine spezielle Art von Dienstleistung ist, sollte der Kostenfaktor niemals das primäre Kriterium bei der Etablierung eines PPPs sein. Die EU-Sozialpartner im Bereich der privaten Sicherheitsdienste, CoESS und UNI Europa, haben gemeinsam ein Handbuch für „Qualität bei der Beschaffung privater Sicherheitsdienste"[3] veröffentlicht, das erklärt, wie Qualität objektiv gemessen und die besten Anbieter ausgewählt werden können, im Gegensatz zu den billigsten.

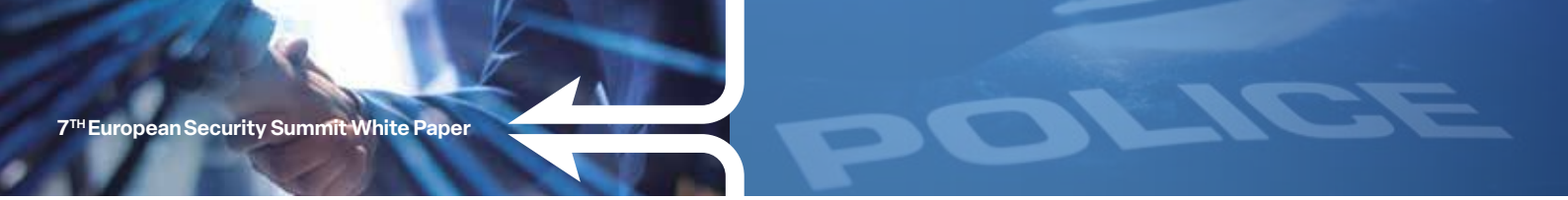
Vertrauen und öffentliche Akzeptanz: Es ist offensichtlich, dass es keine Partnerschaft ohne Vertrauen zwischen den Beteiligten geben kann und, weiter gefasst, ohne das Vertrauen der Bürger, deren Schutz letztlich in diesen Partnerschaften auf dem Spiel steht.

In dem Papier bedauerte CoESS, dass es keine allgemeinen Rahmenbedingungen für PPPs und keine Protokolle für den Informationsaustausch gab. Das Papier schlug drei aufeinanderfolgende Schritte vor, die eingerichtet werden sollten, um PPPs zu schließen, die im folgenden Diagramm zusammengefasst werden können:



**Hinweis: MEAT steht für „Most Economically Advantageous Tender" (wirtschaftlich vorteilhaftestes Angebot). Es handelt sich um eine Bewertungsmethode, die als Auswahlverfahren verwendet werden kann und es der vertragsschließenden Partei ermöglicht, den Vertrag auf der Grundlage von Aspekten der Angebotsabgabe zu vergeben, die über den Preis hinausgehen.*

[3] *CoESS and UNI Europa. (2014). Buying Quality Private Security Services. https://www.securebestvalue.org/.*



DIE „GOOD PRACTICES DER EUROPÄISCHEN KOMMISSION ZUR UNTERSTÜTZUNG DES SCHUTZES ÖFFENTLICHER RÄUME“ UND EMPFEHLUNGEN FÜR DIE ÖFFENTLICH-PRIVATE ZUSAMMENARBEIT

Eine wichtige Grundlage für die öffentlich-private Zusammenarbeit beim Schutz öffentlicher Räume ist das Arbeitsdokument der Europäischen Kommission 2019/140[4] zu „Good practices to support the protection of public spaces“, das gemeinsam von der Kommission, den Behörden der Mitgliedstaaten, Betreibern öffentlicher Räume und dem Verband der Europäischen Sicherheitsdienstleistungsunternehmen (CoESS) entwickelt wurde. Wichtige Good Practices in Bezug auf die öffentlich-private Zusammenarbeit umfassen:

- **Sicherheitskultur:** Entwicklung einer gemeinsamen Sicherheitskultur, die zwischen öffentlichen Behörden, privaten Akteuren und Bürgern geteilt wird.

- **Vulnerabilitäts- und Risikoanalysen:**
  - Regelmäßige Vulnerabilitätsanalysen, die in einem öffentlich-privaten Kooperationsansatz durchgeführt werden, gefolgt von maßgeschneiderten Sicherheitsmaßnahmen.
  - Öffentliche Behörden sollten Risikoanalysen und Informationen nach Bedarf teilen, und es sollte eine vertrauensvolle und rechtzeitige Kommunikation und Zusammenarbeit etabliert werden, die einen spezifischen Informationsaustausch über Risiken und Bedrohungen zwischen den zuständigen öffentlichen Behörden, der lokalen Strafverfolgung und dem privaten Sektor ermöglicht.

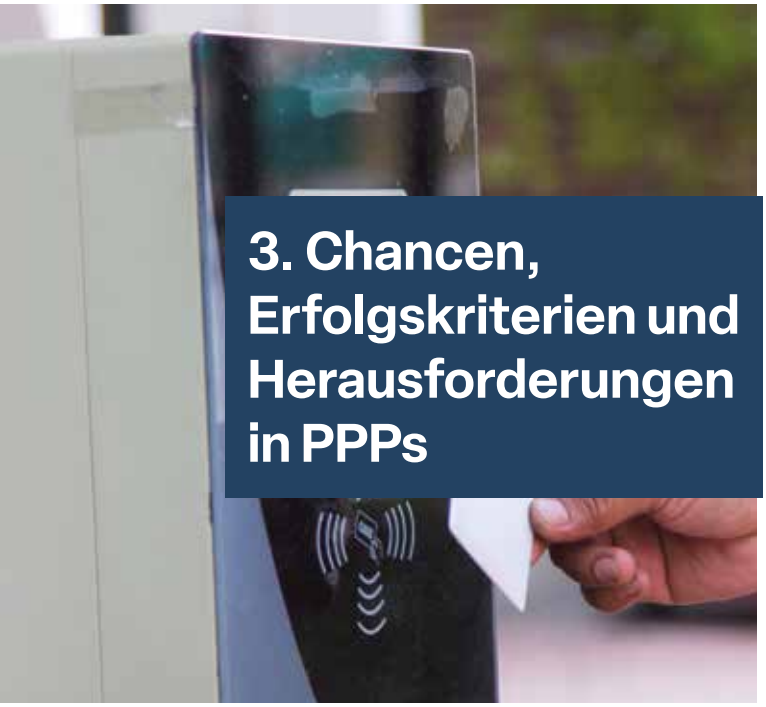
- **Klare Rollen, Verantwortlichkeiten und Kommunikation:**
  - Öffentliche und private Betreiber sollten eine kompetente Person sowie eine Vertretung benennen, die die Bedrohungslandschaft versteht, die jeweilige Einrichtung oder Veranstaltung gut kennt und sicherstellt, dass diese Person die entsprechende Schulung erhält.
  - Jeder Akteur, der in der Sicherheitskette involviert ist, sollte Kontaktstellen benennen und die jeweiligen Rollen und Verantwortlichkeiten in der öffentlich-privaten Zusammenarbeit in Sicherheitsfragen klären (z. B. zwischen Betreibern, privatem Sicherheitsdienst und Strafverfolgungsbehörden) sowie für eine bessere Kommunikation und Zusammenarbeit auf regelmäßiger Basis.
  - Betreiber sollen ein effizientes Management und Kommunikation in Krisensituationen mit Mitarbeitern und Kunden sowie mit der Strafverfolgung sicherstellen, unter Verwendung von Technologie, Krisenkommunikationsteams und klaren Botschaften.

- **Schulung:**
  - Mitarbeiter, die in der Einrichtung oder bei der Veranstaltung eingesetzt werden, sollten ordnungsgemäß geschult und regelmäßig in der Bedienung der Tools, die sie verwenden, fortgebildet werden.
  - Regelmäßige Sicherheitsübungen durchführen, die helfen, das Niveau der Vorbereitung zur Abschreckung und Reaktion auf einen Angriff zu ermitteln, unter Einbeziehung aller relevanten Interessengruppen (z. B. Rettungsdienste, Spezialkräfte und andere relevante Dienstleister).

- **Physische Sicherheit:** Öffentliche und private Akteure müssen gemeinsam berücksichtigt werden, um Schutzaspekte bei der Gestaltung von Gebäuden und anderen Räumen besser zu integrieren.

- **Insider-Bedrohungen:** Basierend auf der Vulnerabilitätsbewertung und in enger Zusammenarbeit mit den Strafverfolgungsbehörden sollten Betreiber öffentlicher Räume Hintergrundüberprüfungen und gegebenenfalls eine Überprüfung des Personals im Einklang mit nationalen Gesetzen sowohl vor als auch während ihrer Einsätze in Betracht ziehen. Das von der EU finanzierte AITRAP-Projekt (www.help2protect.info), das von CoESS koordiniert wurde, bietet ein Online-Schulungsprogramm zu Insider-Bedrohungen und ist ein gutes Beispiel für ein solches Tool.

[4] *European Commission. (2019). Commission Staff Working Document: Assessment of the 2018 Country Reports on the implementation of the European Union's legal framework on data protection.*



3. Chancen, Erfolgskriterien und Herausforderungen in PPPs

„Private Sicherheit ergänzt die Strafverfolgung, indem sie einzigartige Fähigkeiten und Perspektiven bietet, die die gesamten Sicherheitsbemühungen verstärken.“

3.1. Chancen

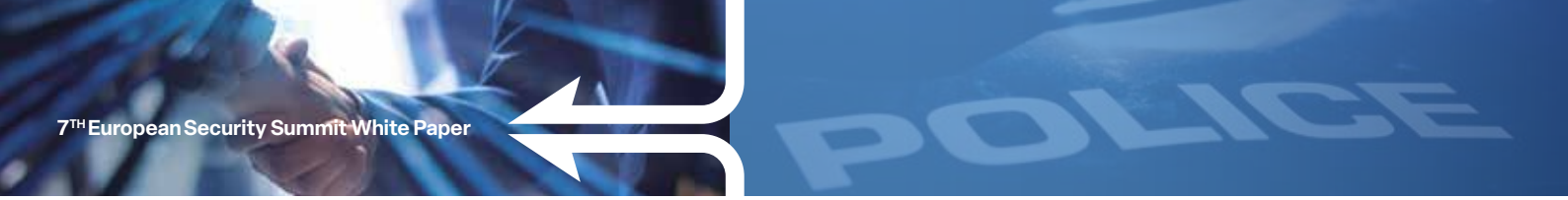
Die Hauptchance von PPPs liegt in der Komplementarität der Stärken der beteiligten Akteure:

Von der öffentlichen Seite:

- **Autorität und der Einsatz von Gewalt, wenn erforderlich**
- **Geheimdienstinformationen, die von spezialisierten staatlichen Behörden gesammelt werden**
- **Zugang zu vertraulichen Informationen**
- **Legitimität bei der Durchführung dieser Aufgaben und das Vertrauen der Bürger**
- **Rechenschaftspflicht und Kontrolle**

Von der privaten Seite:

- **Operative Expertise und Unterstützung der Arbeitskräfte:** PSD bieten spezialisierte Expertise in Prävention und Erkennung und setzen fortschrittliche Technologien wie digitale Überwachung und Risikobewertungen ein, die den Strafverfolgungsbehörden nicht immer zur Verfügung stehen. Durch die Übernahme dieser Aufgaben unter regulierten und streng überwachten Bedingungen entlasten PSD nicht nur die Ressourcen der Strafverfolgungsbehörden, sodass diese sich auf spezialisierte Aufgaben wie die Terrorismusbekämpfung konzentrieren können, sondern verbessern auch die allgemeine Sicherheitswirkung, ohne die öffentliche Sicherheitskontrolle zu gefährden. Diese Partnerschaft ermöglicht es den Strafverfolgungsbehörden, die Fähigkeiten des privaten Sektors strategischer zu nutzen.
- **Verbesserte Sicherheit und spezialisiertes Wissen:** Private Sicherheitsdienste ergänzen die Strafverfolgungsbehörden, indem sie einzigartige Fähigkeiten und Perspektiven bieten, die die gesamten Sicherheitsbemühungen verbessern, insbesondere in spezialisierten Bereichen wie der Flughafensicherheit, bei denen die Passagier- und Gepäckkontrollen effizient von PSD durchgeführt werden. Mit umfangreicher Erfahrung in der Sicherung kritischer Infrastrukturen und öffentlicher Räume konzentrieren sich PSD auf die frühzeitige Prävention und Erkennung im Rahmen des kriminellen Planungszyklus, sodass beide Parteien sich auf ihre Kernkompetenzen konzentrieren können. Dies trägt erheblich zu Sicherheitsoperationen bei und ermöglicht es den



PSD, schnell auf dringende Bedürfnisse zu reagieren, oft schneller als die Strafverfolgungsbehörden.

- **Innovative Technologien und Ressourcen zu deren Betrieb:** Unternehmen investieren in die Schulung von Personal und den Einsatz modernster Technologien, um die besten Sicherheitslösungen anzubieten und Risiken kontinuierlich zu bewerten, um die Resilienz in einer sich ständig weiterentwickelnden Bedrohungslandschaft zu erhöhen. Im Gegensatz zu den Strafverfolgungsbehörden, denen der Wettbewerbsdruck und die Kundenorientierung fehlen, sind PSD stärker auf Marktbedürfnisse ausgerichtet. Darüber hinaus erleichtert Technologie eine bessere Koordination und Zusammenarbeit mit öffentlichen Kräften, wie etwa den Austausch von Videoüberwachungsdaten mit den Strafverfolgungsbehörden. Im Einklang mit dem Konzept der „Neuen Sicherheitsgesellschaft“[5] verfolgen PSD zunehmend einen integrierten Sicherheitsansatz, der Menschen, Technologie und Prozesse kombiniert, einschließlich Investitionen in die involvierten Mitarbeiter.

- **Eine Kultur der Effizienz und Leistungsmessung:** PSD agieren in einem wettbewerbsorientierten Umfeld, das eine starke Kultur der Leistungsmessung fördert. Diese Kultur kommt den Strafverfolgungsbehörden zugute, indem sie strenge Standards und Metriken einführt, um Sicherheitsprotokolle zu bewerten. PSD verwenden diese Metriken, um die Wirksamkeit ihrer Sicherheitsmaßnahmen zu beurteilen, und bieten ein Modell, das die Strafverfolgungsbehörden nutzen können, um ihre eigenen Operationen zu verbessern. Die Einführung dieser Praktiken trägt dazu bei, die Leistung der Strafverfolgungsbehörden zu verbessern, Sicherheitsmaßnahmen mit messbaren Ergebnissen in Einklang zu bringen und möglicherweise das öffentliche Vertrauen und die Zufriedenheit zu erhöhen. Durch die Kombination dieser Stärken können Risiken besser gesenkt und die Resilienz der geschützten Objekte gestärkt werden.

3.2. Erfolgskriterien

Damit das PPP die Komplementarität optimiert, müssen mehrere Elemente vorhanden sein.

Basierend auf den Kriterien im Weißbuch „Das Sicherheitskontinuum in der neuen Normalität“, der Empfehlung der Europäischen Kommission, den Beobachtungen im SAFE-CITIES-Projekt, der Überprüfung der Literatur zu PPPs und den Interviews mit PPP-Akteuren, gehen wir davon aus, dass die folgenden Kriterien für den Erfolg erforderlich sind:

I. Vertrauen

a. Vertrauen zwischen den Partnern: Dies umfasst das Vertrauen zwischen den Führungskräften jeder Seite und die Förderung einer Vertrauenskultur unter den Beteiligten an der Umsetzung des PPP, um sicherzustellen, dass alle Teilnehmer an die Zuverlässigkeit und Integrität ihrer Partner glauben.

b. Vertrauen in Prozesse: Sicherstellung klarer Rollen und Verantwortlichkeiten, Transparenz darüber, wie Ressourcen verwendet werden, und explizite, rechenschaftspflichtige Entscheidungsprozesse.

c. Vertrauen in Technologie: Betonung der Sicherheit, Interoperabilität und des Schutzes von Daten, die zur Unterstützung des PPP verwendet werden, einschließlich sicherer und cyber-sicherer Kanäle für den Live-Datenaustausch.

d. Auswahl von Qualitätsdienstleistern: Die Auswahl von Partnern, die hohe Standards in Bezug auf Qualität und Professionalität wahren, trägt erheblich zum Vertrauen und zur Wirksamkeit der Partnerschaft bei.

II. Kompetenz und Anerkennung von Werten

a. Anerkennung und Wertschätzung der einzigartigen Kompetenzen, die jeder Partner in die Partnerschaft einbringt, und das Verständnis darüber, wie diese Kompetenzen zum Gesamtziel der Partnerschaft beitragen.

III. Kommunikation und Zusammenarbeit

a. Förderung offener Kommunikation und eines rechtzeitigen Austauschs relevanter Informationen, um sicherzustellen, dass alle Partner informiert und eingebunden sind. Dies umfasst den Austausch einer gemeinsamen Taxonomie und Terminologie zwischen den Strafverfolgungsbehörden und PSD.

b. Förderung einer kollaborativen Denkweise, bei der alle Parteien ihre gemeinsamen Interessen an der Erreichung der gemeinsamen Ziele anerkennen.

c. Ausrichtung von Schulungsprogrammen in allen erforderlichen Bereichen.

[5] *Dieses Konzept wird im CoESS-BDSW Weißbuch „Das Sicherheitsunternehmen: Integration von Dienstleistungen und Technologie als Reaktion auf Veränderungen in der Kundennachfrage, Demografie und Technologie“ – 2015 beschrieben.*

IV. Kultur und Flexibilität

a. Förderung einer Kultur der Ehrlichkeit und Gerechtigkeit, bei der Feedback im Sinne einer kontinuierlichen Verbesserung ermutigt wird und Fehler als Lernmöglichkeiten und nicht als Gründe für punitive Maßnahmen behandelt werden.

b. Aufrechterhaltung der Flexibilität innerhalb der Partnerschaft, die eine kontinuierliche Bewertung und Weiterentwicklung ermöglicht, um sich an neue Herausforderungen und Chancen anzupassen.

c. Sicherstellung, dass die Kultur alle Ebenen der Hierarchie sowohl bei den Strafverfolgungsbehörden als auch bei den PSD durchdringt, sowohl von oben nach unten als auch von unten nach oben.

V. Rechtlicher Rahmen und Verbindung zur Regierung

a. Aufbau eines robusten rechtlichen Rahmens, der die Rollen, Verantwortlichkeiten und operationalen Grenzen für private Sicherheitsdienstleistungsunternehmen innerhalb der Branche klar definiert und sicherstellt, dass diese allen Beteiligten kommuniziert und verständlich gemacht werden.

b. Sicherstellung, dass der Rahmen regelmäßige Bewertungen der Partnerschaft unterstützt, um mit den Zielen der öffentlichen Sicherheit und Sicherheit in Einklang zu bleiben.

c. Verbesserung der Verbindung zwischen Regierung und privaten Sicherheitsnetzwerken, um Transparenz, Rechenschaftspflicht und regelmäßige Updates zur Leistung und strategischen Ausrichtung zu gewährleisten.

d. Förderung eines Rahmens, der Ressourcen in Bezug auf Personal und Technologien bündelt, um so die operativen Fähigkeiten und die Effizienz zu steigern.

VI. Daten- und Technologieverwaltung

a. Priorisierung der Dateninteroperabilität, um eine nahtlose Kommunikation und den Informationsaustausch über verschiedene Plattformen und Organisationen hinweg zu ermöglichen.

b. Implementierung von Rahmenwerken für den Informationsaustausch, die klar, strukturiert und in der Lage sind, komplexe operative Anforderungen zu unterstützen, ohne die Sicherheit zu gefährden.

3.3. Hauptverbesserungsbereiche

Basierend auf Literatur und Interviews mit PPP-Stakeholdern sind die folgenden Bereiche diejenigen, in denen der größte Verbesserungsbedarf besteht. Lösungsansätze werden in Abschnitt 5 erörtert.

→ **Fehlen formaler und umfassender Rahmenwerke sowie entsprechender Gesetzgebung für PPPs:**
- PPPs basieren sehr oft auf guter Absicht und persönlichen Beziehungen. Wenn einer der Hauptakteure der PPP in eine andere Position wechselt oder in den Ruhestand geht, kann die PPP leiden oder sogar aufhören zu existieren.
- Es gibt oft kein allgemeines Rahmenwerk, auf das sich die Partner beziehen können, weshalb sie auf Interpretation oder Erwartungen angewiesen sind.
- Die Gesetzgebung enthält oft keine Bestimmungen zur Schaffung von Partnerschaften oder zur Ermöglichung und Regulierung des Informationsaustauschs zwischen Strafverfolgungsbehörden und PSD.

- **Gegenseitige Anerkennung von Kompetenzen und Fähigkeiten:**
  - Es fehlt an Verständnis und Wissen seitens der Strafverfolgungsbehörden über die Fähigkeiten und Kompetenzen von privaten Sicherheitskräften, was die Zusammenarbeit und die persönlichen Beziehungen innerhalb der Partnerschaft beeinträchtigen kann. Mehrere Experten schlugen vor, dass die Mitarbeiter der Strafverfolgungsbehörden in ihrer Grundausbildung detaillierte Informationen über den rechtlichen Rahmen erhalten sollten, in dem PSD und private Sicherheitskräfte tätig sind, einschließlich ihrer Aufgaben und Grenzen.

- **Effektive Kommunikation zwischen Strafverfolgungsbehörden und PSD:**
  - Dies beinhaltet die Verwendung derselben Taxonomie und Terminologie. In einem Interview mit einem PSD und ihrem Gegenüber bei der Strafverfolgungsbehörde wurde hervorgehoben, dass die Verwendung des spezifischen Informations-„Codings" der Strafverfolgungsbehörde durch PSD-Mitarbeiter einen entscheidenden Unterschied in der Bewertung der Berichte durch die Strafverfolgungsbehörde gemacht hat. Die Strafverfolgungsbehörde räumte den Berichten Glaubwürdigkeit ein, weil sie in ihrer Sprache übermittelt wurden, und die PSD-Vertreter fühlten sich ernst genommen und besser berücksichtigt.

- **Behandlung der Kostenfrage:**
  - In ihrem Papier über PPPs[6] empfehlen Steden und Meijer, dass private Parteien stärker in die PPP einbezogen werden können, wenn sie in der Lage sind, Kosten an ihre Kunden weiterzugeben oder wenn die Kosten gerechter zwischen den beteiligten Parteien aufgeteilt werden. In den Best Practices, die in Kapitel 6 untersucht werden, werden die Kosten in den meisten Fällen entweder nicht erwähnt oder ausdrücklich als vollständig vom PSD getragen angegeben.

- **Schaffung einer echten Partnerschaft unter Berücksichtigung der Ungleichgewichte zwischen öffentlichen und privaten Akteuren**.

[6] *Steden, R. van, & Meijer, R. (2018). Publiek-private samenwerking in tijden van diffuse dreiging: Een onderzoek naar diversiteit in werkwijzen en kansen in de Nederlandse en Vlaamse context. Den Haag: WODC.*

Ein besonders sensibles Thema: der Informations-austausch

In einem sensiblen Bereich wie dem Informationsaustausch, für den in Sicherheitskreisen, sogar zwischen Strafverfolgungsbehörden, von Natur aus eine starke Zurückhaltung besteht, besteht die Notwendigkeit, zu erklären, warum dies nützlich und notwendig ist und wie letztlich alle davon profitieren werden. Wie der Informationsaustausch unter Beachtung der Allgemeinen Datenschutzverordnung (DSGVO) erfolgen kann, ist ebenfalls eine Frage, die einer eingehenden Analyse bedarf. Der folgende Abschnitt soll die Vorteile eines solchen Austauschs hervorheben. Es ist auch wichtig zu betonen, dass die von den Strafverfolgungsbehörden gesammelten Informationen nicht notwendigerweise in ihrer Gesamtheit nützlich sind. Was private Akteure möglicherweise interessiert, ist der „umsetzbare" Teil der Informationen oder der Intelligenz. Ein Beispiel: Es mag für private Akteure nicht hilfreich sein, die Verursacher einer rechtswidrigen Handlung zu identifizieren, sondern vielmehr, wie eine rechtswidrige Handlung sie betreffen könnte. Zum Beispiel ist die Tatsache, dass an einem bestimmten Ort ein Terroranschlag stattgefunden hat, für PSD, die Orte oder Objekte im Umkreis des ursprünglich angegriffenen Objekts schützen, nützliche Information. Dies stellt keinen Verstoß gegen eine laufende Untersuchung dar und es ist nur eine Frage der Zeit, bis die Information öffentlich wird.

Es könnte nützlich sein, eine Umfrage unter PSD und Strafverfolgungsbehörden durchzuführen, um herauszufinden, welche Art von Informationen und Erkenntnissen nützlich sein könnten und in welchem Format diese weitergegeben werden könnten.

Die Vorteile eines besseren Informationsaustauschs:

- Kriminalitäts-Skripting: Bessere Bedrohungsanalysen durch Identifizierung von Trends und Mustern
- Vorhersageprozesse: Verbesserte Fähigkeit, Sicherheitsvorfälle und Straftaten vorherzusagen
- Verbesserte operative Effizienz und Ressourcenzuteilung sowie besser gezielte Patrouillen
- Verbesserte Mitarbeitervorbereitung und damit verbesserte Mitarbeitersicherheit
- Bessere Fähigkeit, das Gesamtbild zu sehen
- Schaffung von Kontinuität zwischen den verschiedenen Akteuren und damit Reduzierung von Schwachstellen
- Insgesamt bessere Entscheidungsfindung und bessere Servicebereitstellung
- Bereitstellung von Lernmöglichkeiten für alle Akteure in der Partnerschaft.

Die Herausforderungen beim Teilen von Informationen:

- Unterschiedliche Mandate und rechtliche Befugnisse
- Datenschutz- und Privatsphärengesetze und -sicherheit sowie deren Auslegung, einschließlich Interoperabilität
- Mangelndes Vertrauen.

Lösungsansätze:

- **Erstellung und Dokumentation von Verfahren für den Informationsaustausch**, um Klarheit und Transparenz zu schaffen. Dies wird in der ISO-Norm 22396:2020, „Richtlinien für den Informationsaustausch zwischen Organisationen", weiter erläutert.
  - Durch die Nutzung bestehender Werkzeuge für den Informationsaustausch:
    - Sicherheitsfreigaben auf verschiedenen Ebenen
    - Vertraulichkeitsvereinbarungen (NDAs) gemäß dem „Traffic Light Protocol" (TLP)[7].

- **Klarstellung der nationalen Auslegung der DSGVO und anderer Datenschutzgesetze**, um Bedenken hinsichtlich der Privatsphäre zu zerstreuen, indem ein Teil der Unsicherheit, die sie mit sich bringen, beseitigt wird. Die CoESS hat einen Brief von 23 Bereichen an die Kommission unterzeichnet, in dem eine Bestätigung des risikobasierten Ansatzes der Verordnung als Leitprinzip[8] gefordert wird.

- **Vertrauen stärken:**
  - Durch Förderung von persönlichen Kontakten und regelmäßigen Treffen
  - Durch die Schaffung von gemischten (öffentlichen und privaten) Teams und/oder die Einrichtung von Verbindungsstellen in jedem von ihnen, bei denen vertrauenswürdige Personen („Informations-Vermittler") für den Informationsaustausch benannt werden
  - Durch Bereitstellung von Rückmeldungen zur Nutzung der von den Beitragsleistenden bereitgestellten Informationen und Förderung des Gefühls der Mitwirkung.

- **Engagement für Sicherheitskultur und Datenschutz zeigen.**

- **Technologie zur Weitergabe von Informationen auf dedizierten und verschlüsselten Plattformen nutzen.**

ISO 22396:2020 zum Informationsaustausch zwischen Organisationen

Dieses ISO-Dokument erkennt die Entwicklung der Risikolandschaft aufgrund der zunehmenden Vernetzung zwischen privaten, staatlichen und nichtstaatlichen Organisationen an, was zu sich überschneidenden und grenzüberschreitenden Risiken führt. Es betont den größeren Bedarf an Zusammenarbeit und Informationsaustausch, um die Resilienz und Sicherheit zu erhöhen. Effektive Zusammenarbeit erfordert den sicheren Informationsaustausch zwischen beiden Sektoren, um Schwachstellen zu reduzieren und die organisatorische Effektivität zu verbessern. Herausforderungen umfassen die Definition von Koordinierungsverantwortlichkeiten und den Schutz sensibler Geschäftsinfos. Ein erfolgreicher Informationsaustausch kann das Wissen erweitern, die Resilienz erhöhen und zusätzliche Vorteile wie einen verbesserten Zugang zu eingeschränkten Informationen und den Aufbau von Gemeinschaften bieten.

Das Leitdokument beschreibt Prinzipien, Rahmenwerke und Prozesse, um robuste Mechanismen für den Informationsaustausch zu etablieren.

Es richtet sich an private und öffentliche Organisationen, die Anleitung für die Schaffung der Bedingungen benötigen, die den Informationsaustausch unterstützen. Wie jede ISO-Richtlinie oder -Norm ist es urheberrechtlich geschützt und kann daher nicht in diesem Weißbuch reproduziert werden. Es muss über nationale Normungsorganisationen oder direkt über die ISO erworben werden.

[7] *Das Traffic Light Protocol (TLP) wurde entwickelt, um den Informationsaustausch zu erleichtern. TLP ist eine Reihe von Kennzeichnungen, die sicherstellen, dass sensible Informationen mit der entsprechenden Zielgruppe geteilt werden. Es verwendet vier Farben, um die erwarteten Austauschgrenzen anzuzeigen, die vom Empfänger bzw. den Empfängern angewendet werden sollen.*

[8] *Gemeinsame Erklärung zum Bericht über die Umsetzung der DSGVO von 23 Organisationen, einschließlich der CoESS – siehe Pressebereich der CoESS-Website, Positionspapiere https://coess.eu/.*

4. Kartierung von PPPs in Europa

Im Jahr 2021 führte die CoESS eine Umfrage in 29 europäischen Ländern durch, von denen 24 Mitgliedstaaten der EU sind. Nur 9 Länder berichteten, dass sie PPPs (Private-Public Partnerships) implementiert haben, nämlich: Belgien, Dänemark, Finnland, Frankreich, Deutschland, Italien, Spanien, Schweden und die Niederlande. Diese Umfrage wurde einige Jahre später durch eine weitere Umfrage im Rahmen des von der EU finanzierten SAFE CITIES-Projekts ergänzt. Ziel dieses Projekts ist es, den Schutz öffentlicher Räume zu verbessern, indem ein Sicherheits- und Verwundbarkeitsbewertungsrahmen bereitgestellt wird, der durch eine interaktive Plattform unterstützt wird.

Die CoESS ist einer der Partner des großen SAFE CITIES-Konsortiums, das 16 Partner aus 9 Ländern vereint, darunter Universitäten, Kommunen, Strafverfolgungsbehörden und Innenministerien.

Im Rahmen dieses Projekts führte die CoESS eine Umfrage unter seinen Mitgliedern durch, ergänzt durch Desktop-Recherchen, um folgende Punkte zu identifizieren:

- Rechtliche Rahmenbedingungen als Grundlage für PPPs in öffentlichen Räumen
- Aufgaben und Kompetenzen von Unternehmen
- Rahmenbedingungen für PPPs
- Erfahrungen mit gemeinsamen Sicherheits- und Verwundbarkeitsbewertungen.

Wie bereits erwähnt, hängen die PPPs und Empfehlungen von der rechtlichen Grundlage in jedem Land ab, insbesondere davon, ob private Sicherheitsdienstleistungsunternehmen (PSD) Aufgaben in öffentlichen, zugänglichen Räumen übernehmen dürfen und, falls ja, in welchen Räumen und mit welchen Aufgaben.

Die wichtigsten Ergebnisse waren, dass PPPs, wo sie existierten, in der Regel Teil formeller Rahmenwerke waren, die auf kommunaler Ebene organisiert und dauerhaft angelegt waren, und meist Folgendes umfassten:

- Kontaktstellen zwischen Strafverfolgungsbehörden, PSD und anderen Akteuren (75 %)
- Regelmäßiger Informationsaustausch auf Managementebene (65 %)
- Echtzeit-Informations- / Datenaustausch im Falle von Vorfällen (55 %).

Die am wenigsten genutzten Mittel der Zusammenarbeit waren:

- Ressourcensammlung (30 %)
- Gemeinsame Verwundbarkeitsbewertungen (17 %)
- Gemeinsame Schulungen (10 %).

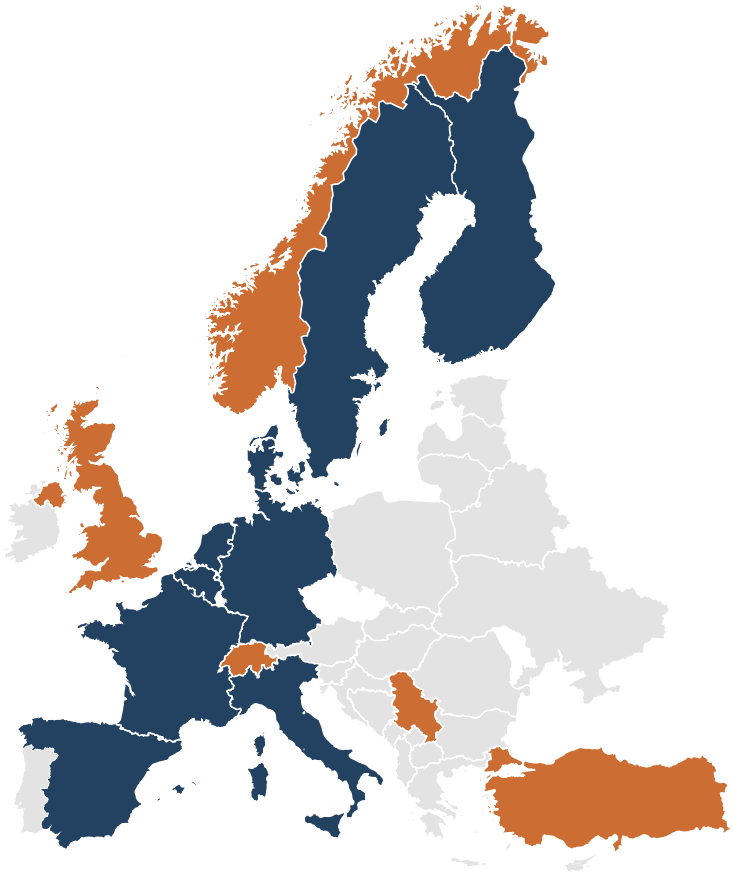
Der Hauptgrund, der dafür genannt wurde, war das mangelnde Vertrauen in die Datenteilung. Private Sicherheit wurde oft als nachträglich eingesetzter Vollzugsdienst angesehen, und die Befragten waren der Meinung, dass der einzige Weg, dies zu ändern, über den Aufbau von Vertrauen und Qualitätskontrolle führen müsse.

Zu den Aufgaben, die unter PPPs in verschiedenen Ländern fallen, gehören die folgenden:

- Wo private Sicherheitsdienstleistungsunternehmen (PSD) Dienstleistungen in öffentlichen, zugänglichen Räumen anbieten dürfen, umfasst dies in der Regel öffentliche Veranstaltungen sowie Sport- und Festspielstätten. Weitere öffentliche Räume, die abgedeckt werden, sind Krankenhäuser, Asylzentren, öffentliche Verwaltungseinrichtungen und Freizeiteinrichtungen wie Parks oder Strände. Im Sommer 2024 arbeiteten PSD in Zusammenarbeit mit den französischen Strafverfolgungsbehörden, um die Olympischen Spiele in Paris zu schützen.
- Mehrere Länder setzen PSD zur Unterstützung des Strafvollzugs ein: Perimeterüberwachung, Transport von Inhaftierten, Bewachung von Inhaftierten in Polizeistationen.
- Die Luftsicherheit ist ebenfalls ein Bereich, der in Deutschland als Teil von PPPs genannt wird, während sie in anderen Ländern zu den Aufgaben gehört, die im Gesetz über private Sicherheit aufgeführt sind.
- Die Sicherheit im öffentlichen Verkehr wird ebenfalls als Bereich für PPP genannt, ebenso wie Verkehrsknotenpunkte und Häfen sowie die Überwachung und der Schutz von öffentlichen Gebäuden, militärischen Anlagen oder Stationen.

In Spanien und Portugal sieht das Gesetz vor, dass private Sicherheitsdienste eine besondere Verpflichtung haben, auf Anfrage der Sicherheitskräfte zu unterstützen und mit ihnen zusammenzuarbeiten, indem sie deren Anweisungen in Bezug auf die Dienstleistungen befolgen, die die öffentliche Sicherheit betreffen oder in deren Zuständigkeitsbereich fallen. Interessanterweise berichteten von den 5 Nicht-EU-Ländern, die an der Umfrage teilnahmen, alle von bestehenden PPPs, nämlich Norwegen, Serbien, der Schweiz, der Türkei und dem Vereinigten Königreich.

„In Spanien und Portugal sieht das Gesetz vor, dass private Sicherheitsdienste eine besondere Verpflichtung haben, auf Anfrage die Sicherheitskräfte zu unterstützen und mit ihnen zusammenzuarbeiten.“



EU-Länder: Vorhandensein von PPPs

Nicht-EU-Länder: Vorhandensein von PPPs

5. Politische und strategische Empfehlungen

Unter Berücksichtigung früherer Veröffentlichungen der CoESS, Empfehlungen der Kommission, akademischer und anderer Literatur sowie bewährter Praktiken, die in diesem Dokument untersucht wurden, sind im Folgenden Bereiche aufgeführt, in denen CoESS Maßnahmen empfehlen würde.

Europäische Gesetzgeber:

- Überarbeitung der öffentlichen Vergabegesetzgebung, um die Einhaltung von Tarifverträgen durch Bieter (sofern diese bestehen) zu gewährleisten und den Vergabebehörden Rechtssicherheit bei der Verwendung von Auswahlkriterien im Zusammenhang mit qualitativen Arbeitsbedingungen, angemessener Ausbildung und innovativen Dienstleistungen zu bieten.

- Bestätigung des risikobasierten Ansatzes als leitendes Prinzip bei der Auslegung und Anwendung der Allgemeinen Datenschutzverordnung (DSGVO), z. B. durch eine gezielte Bewertung der Auslegungen der Artikel 6, 9 und 23 im nationalen Recht durch die Europäische Kommission sowie einen konstruktiven Dialog zwischen den Regulierungsbehörden, den Datenschutzbehörden und der Industrie.

- Erstellung von Leitlinien und Empfehlungen für PPPs, die auf den besten Praktiken im Weißbuch basieren.

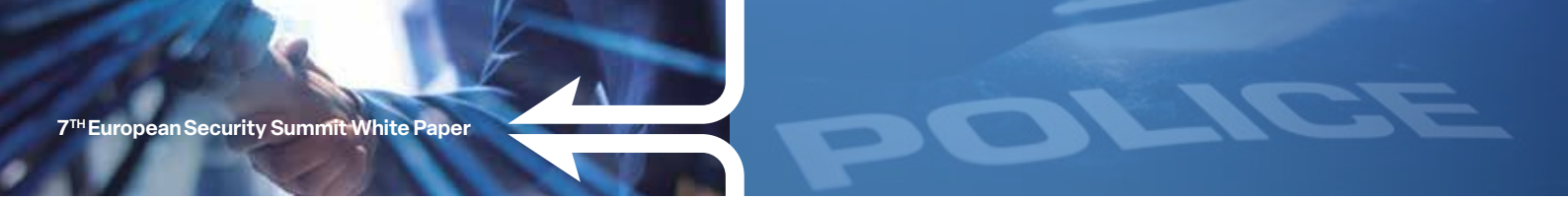
Nationale Gesetzgeber:

- Überprüfung der Gesetzgebung: Überprüfung bestehender Gesetze, um sicherzustellen, dass sie effektive und rechtmäßige PPP-Operationen unterstützen und rechtliche Barrieren für den Informationsaustausch und die Zusammenarbeit beseitigen.

- Etablierung klarer rechtlicher Rahmenbedingungen: Definition der Rollen und Verantwortlichkeiten von öffentlichen und privaten Sektoren in PPPs, um Klarheit und Compliance sicherzustellen.

- Förderung der Standardisierung: Förderung der Entwicklung standardisierter Verfahren für PPP-Operationen, um Konsistenz in verschiedenen Regionen und Sektoren zu gewährleisten.

- Die Komplementarität von Strafverfolgungsbehörden – und PSD-Mitarbeitern sollte in den jeweiligen Ausbildungsplänen berücksichtigt werden, und es sollten Brücken zwischen den beiden ermöglicht werden.



Strafverfolgungsbehörden:

- Verbesserung der Ausbildung und Integration: Sicherstellen, dass Strafverfolgungsbehörden darin geschult werden, wie sie effektiv mit privaten Sicherheitsdienstleistungsunternehmen zusammenarbeiten können, einschließlich des Verständnisses der Fähigkeiten und Grenzen der privaten Sicherheit.
- Regelmäßige Bewertungen: Implementierung regelmäßiger Bewertungen der Wirksamkeit von PPPs und gegebenenfalls Anpassungen zur Verbesserung der Ergebnisse und zur Wahrung des öffentlichen Vertrauens.
- Informationsaustauschprotokolle: Entwicklung von Protokollen, die einen sicheren, geschützten und effizienten Informationsaustausch zwischen öffentlichen und privaten Stellen ermöglichen, ohne die Datenschutzstandards zu gefährden.

Betreiber geschützter Räume:

- Verwundbarkeitsanalysen: Zusammenarbeit mit sowohl privaten Sicherheitsdienstleistungsunternehmen als auch Strafverfolgungsbehörden, um regelmäßige Verwundbarkeitsanalysen von Objekten durchzuführen, um potenzielle Sicherheitsrisiken zu identifizieren und zu mindern.
- Klare Kommunikationskanäle: Etablierung und Aufrechterhaltung klarer Kommunikationswege mit Sicherheitsanbietern und Strafverfolgungsbehörden, um eine schnelle Reaktion und den Informationsfluss während Vorfällen zu gewährleisten.
- Investitionen in Sicherheitsinfrastruktur: Investition in fortschrittliche Sicherheitstechnologien und -infrastruktur, die die Effektivität der Sicherheitsmaßnahmen vor Ort erhöhen und größere Sicherheitsbemühungen unterstützen können.

Private Sicherheitsdienstleistungsunternehmen (PSD):

- Qualität und Compliance: Sicherstellen, dass die höchsten Qualitäts- und Compliance-Standards in allen Sicherheitsoperationen eingehalten werden, um Vertrauen und Zuverlässigkeit bei öffentlichen Partnern und der Gemeinschaft aufzubauen.
- Spezialisierte Informationen: Bereitstellung relevanter Informationen an Sicherheitspersonal zu öffentlichen Sicherheitsprotokollen, Notfallreaktionen und den spezifischen Sicherheitsbedürfnissen der Umgebungen, die sie schützen.
- Technologische Fortschritte: Investition in und Bereitstellung von modernster Sicherheitstechnologie, die die öffentlichen Sicherheitsmaßnahmen ergänzen und die kollektive Sicherheitslage verbessern kann.

„Die Komplementarität zwischen den Mitarbeitern der Strafverfolgungsbehörden und den Mitarbeitern der privaten Sicherheitsdienste sollte in ihren jeweiligen Ausbildungsplänen berücksichtigt werden, und Brücken zwischen den beiden sollten möglich gemacht werden.“

6. Beste Praktiken

Dieser Abschnitt beschreibt einige Beispiele für bewährte Praktiken in PPPs auf verschiedenen Ebenen (national, regional oder lokal) und unterschiedlichen Arten (formelle Rahmenwerke, operative oder punktuelle Kooperationen). Obwohl wir versucht haben, sie entlang der gleichen Aspekte zu strukturieren, haben wir nicht alle erforderlichen Informationen, um dies vollständig zu tun.

6.1. Nationale Partnerschaften

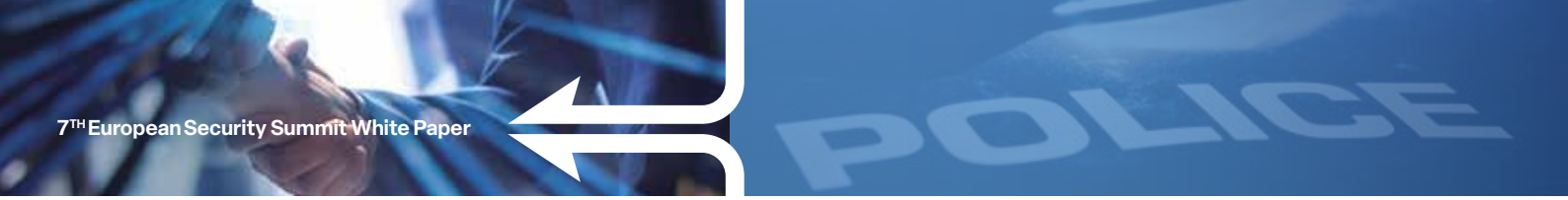
Die Programme Red Azul und COOPERA – Spanien

Seit fast einem Jahrzehnt haben Strafverfolgungsbehörden in Spanien Kooperationsprogramme mit dem privaten Sicherheitssektor in ihrem jeweiligen Zuständigkeitsbereich etabliert, wie z. B. das Red Azul-Programm der Policia Nacional und das Coopera-Programm der Guardia Civil, die alle auf dem gegenseitigen Informationsaustausch und der Gegenseitigkeit basieren. Ähnliche Programme existieren auch auf der Ebene der Baskischen und Katalanischen Polizei.

Das Red Azul-Programm zwischen der spanischen Nationalpolizei und der privaten Sicherheit wurde 2012 ins Leben gerufen und etabliert ein Modell der professionellen Zusammenarbeit mit Komplementarität und Mitverantwortung. Ziel ist es, Ressourcen zu bündeln, eine gemeinsame operative Planung zu entwickeln und Informationen aus der privaten Sicherheit in das Geheimdienstsystem der Nationalpolizei zu integrieren. Es geht über das aktuelle Modell der gesetzlichen Anforderungen hinaus und bewegt sich von der bloßen Nutzung von Ressourcen der privaten Sicherheit durch die Strafverfolgungsbehörden zu einem Szenario des Ressourcenaustauschs, das die Etablierung einer echten „Sicherheitsallianz“ zwischen der privaten Sicherheit und der Nationalpolizei umfasst.

Im Rahmen der Zusammenarbeit mit dem privaten Sicherheitssektor übernimmt die Nationalpolizei folgende Verpflichtungen:

- **Gegenseitigkeit:** Je nach Grad der erreichten Zusammenarbeit (siehe weiter unten) wird von der Nationalpolizei ein wechselseitiger Informationsaustausch und Unterstützung bereitgestellt, um das effiziente Erfüllen der Aufgaben der privaten Sicherheitsdienste zu gewährleisten.



- **Integration und Verteilung von Informationen:** Die Informationen der privaten Sicherheit werden in das Geheimdienstsystem der Nationalpolizei integriert, um von den zuständigen Polizeieinheiten genutzt zu werden.

- **Teilnahme an der Planung:** Bei der operativen Planung der Nationalpolizei wird die aktive Teilnahme der Dienste und Fähigkeiten der privaten Sicherheitsdienstleistungsunternehmen berücksichtigt.

- **Kontinuierliche Verbesserung:** Die Nationalpolizei berücksichtigt alle Verbesserungsvorschläge zur Zusammenarbeit, die vom privaten Sicherheitssektor gemacht werden.

Auf der anderen Seite übernehmen die privaten Sicherheitsdienstleistungsunternehmen (PSD), die sich für die Teilnahme am Kooperationsprogramm mit der Nationalpolizei entschieden haben, folgende Verpflichtungen:

- **Verwendung der vorgesehenen Verfahren und Kanäle:** Die PSD müssen die von der Nationalpolizei bereitgestellten Verfahren und Kanäle nutzen, um die verschiedenen Kooperationsaktivitäten durchzuführen.

- **Bereitstellung von Informationen:** Die PSD müssen der Nationalpolizei alle Informationen zur Verfügung stellen, die sie über Straftaten oder Ereignisse hat, die die öffentliche Sicherheit betreffen könnten und in ihrem Zuständigkeitsbereich liegen.

- **Erfüllung der Pflicht zur Unterstützung und Zusammenarbeit:** Die PSD sind verpflichtet, der Nationalpolizei jederzeit die notwendigen Informationen und Unterstützung im präventiven und ermittlerischen Bereich zu geben, sowohl aus eigener Initiative als auch auf Anfrage der Polizei.

- **Sorgfältiger Umgang mit Informationen:** Die PSD müssen die von der Nationalpolizei erhaltenen Informationen sachgemäß nutzen, um die Sicherheit der Bürger zu verbessern sowie die Effektivität und Effizienz des privaten Sicherheitsdienstes zu steigern und dies nur für die Zwecke, für die die Informationen angefordert und bereitgestellt wurden.

Diese Zusammenarbeit respektiert vollständig das rechtliche Rahmenwerk in Spanien und basiert ausschließlich auf den Bedürfnissen der öffentlichen Sicherheit sowie gegenseitigem Vertrauen und Loyalität.

Für den Informationsaustausch und die operative Unterstützung von der Nationalpolizei an die private Sicherheit müssen folgende Voraussetzungen erfüllt sein:

- **Die Anfrage muss der Tätigkeit oder Funktion der PSD entsprechen und für den Dienst erforderlich sein.**

- **Die Anfrage muss potenziellen oder relevanten Nutzen für die öffentliche Sicherheit haben.**

- **Die Antwort wird auf das beschränkt, was für die Anfrage wirklich relevant und angemessen ist.**

Die Informationen, die im Rahmen des Red Azul-Programms von der Nationalpolizei bereitgestellt und empfangen werden können, beziehen sich auf die Kommunikation von Sicherheitsvorfällen und Alarmen, besonderen Ereignissen, der Ausführung von Plänen, festgenommenen, identifizierten oder gesuchten Personen, gestohlenen oder verdächtigen Fahrzeugen, Kriminalitätsarten, Kriminalitätsentwicklung, Informationsbulletins, Berichten, Hintergrundprüfungen und anderen ähnlichen Informationen, die der öffentlichen Sicherheit zugutekommen könnten.

Die Informationen, die von der Nationalpolizei an die private Sicherheit weitergegeben werden, hängen von dem erreichten Kooperationsgrad zwischen den beiden Parteien ab. Eine Bewertung wird auf Grundlage der Wirksamkeit und des Engagements der PSD durchgeführt, das mit der Nationalpolizei nachgewiesen wurde. Innerhalb dieser Bewertung gibt es vier Kooperationsgrade – der erste ist der mit dem geringsten Informationsbeitrag, der letzte der mit dem höchsten, dank der aktiven und kontinuierlichen Teilnahme der PSD.

Konkrete Organisation der Red Azul Zusammenarbeit:

1. MANAGE: Dieses Programm ist administrativer Natur und richtet sich an private Sicherheitsdienstleistungsunternehmen (PSD), Abteilungen und Büros. Auf diese Weise wird die Zusammenarbeit gefördert, und etwaige betriebliche Bedürfnisse oder Probleme der Kooperation werden hauptsächlich bewertet und erkannt.

2. OPERA: Ein operatives Programm, das sich hauptsächlich an Wirtschaftsverbände und Gewerkschaften, PSD sowie Sicherheitsabteilungen und Detekteien richtet.

3. INFORM: Ein Kommunikationsprogramm, das auf den Sektor abzielt, um allgemeine und spezifische Informationen je nach Handlungsbereich bereitzustellen. Es verwendet verschiedene Werkzeuge, um die Verteilung von Informationen zu verbessern.

4. WATCH: Dieses Kommunikationsprogramm richtet sich an Mitarbeiter privater Sicherheitsdienstleistungsunternehmen und hat zum Ziel, einen Raum für Beziehungen mit ihnen zu schaffen. Um Zugang zum Programm zu erhalten, müssen die Mitarbeiter unter anderem ihre Berufsausweiskartennummer eingeben.

Mit der Einführung des COOPERA-Programms im Jahr 2010 hat die spanische Guardia Civil im Rahmen ihrer Befugnisse versucht, ihre öffentlich-private Zusammenarbeit mit dem Sicherheitssektor zu optimieren. Aufgrund des hohen Entwicklungsstandes des Sektors in Spanien zielt es darauf ab, die privaten Unternehmen zu integrieren, die öffentlichen Sicherheitsfähigkeiten zu verbessern, auszutauschende Daten zu definieren und weitere Ansätze zu entwickeln, um ein kontinuierliches Sicherheitsnetz sowie die Effektivität der Zusammenarbeit zu gewährleisten. Dem Programm können ordnungsgemäß registrierte und lizenzierte PSD freiwillig beitreten, es besteht aus folgenden Punkten:

- **Formaler Rahmen:** Das Unternehmen unterzeichnet ein Betriebshandbuch für die Zusammenarbeit. Der institutionelle Kontakt zwischen der Guardia Civil und den PSD wird auf Management-Ebene (zentralisiert) sowie auf operativer Ebene (regional) durchgeführt.
- **Austausch von Kontakten:** Bei Beitritt zum Programm geben PSD die Kontaktdaten des Direktors oder Sicherheitsmanagers an, der als Ansprechpartner für die Strafverfolgungsbehörden auf Management-Ebene fungiert. Zusätzlich werden bei Bedarf regionale Kontakte und Ansprechpartner zur Etablierung des operativen Programmniveaus und der entsprechenden Kommunikationskanäle bis hinunter zur lokalen Ebene bereitgestellt.
- **Sichere Kommunikationskanäle:** Die Kommunikationsmittel werden durch das Programm geregelt.
- **Regelmäßige Treffen:** Koordinierte Gruppen treffen sich mindestens zweimal jährlich auf operativer und einmal jährlich auf Management-Ebene. Es handelt sich um permanente Gremien, die Strafverfolgungsbehörden und PSD vertreten und von der Guardia Civil geleitet werden, ohne dass der dauerhafte Kontakt beeinträchtigt wird.
- **Informationsaustausch:** PSD stellen Informationen zu allen Aspekten zur Verfügung, die zur Verbesserung der Bekämpfung von Straftaten beitragen, z. B. über verdächtige oder kriminelle Aktivitäten, Beschwerden und Arbeitsweise krimineller Netzwerke. Für dringende Fälle gibt es spezielle Kommunikationskanäle. Strafverfolgungsbehörden stellen den PSD-Informationen zu Ereignissen oder Umständen zur Verfügung, die die Sicherheit von privaten Sicherheitskräften oder den Betrieb ihrer Dienste beeinträchtigen könnten, wie z. B. Straßensperrungen, Störungen der öffentlichen Ordnung, schwere Straftaten, Brände und andere Katastrophen sowie dringende Bedrohungen. Solche dringenden Informationen beinhalten Berichte zur lokalen Situation, Daten zur Terrorismusbekämpfung und Veränderungen im Bedrohungsbild, lokale oder allgemeine Schutz- und Präventionspläne sowie operative Informationen.
- **Berichterstattung:** Gemeinsame Berichte werden von der Guardia Civil erstellt, um eine gemeinsame Sicherheitskultur zu fördern und die Erstellung von Risikoanalysen für an dem Programm teilnehmende Einrichtungen zu erleichtern, die Aspekte im Bereich Sicherheit und Kriminalität betreffen. Diese Berichte basieren auf offenen Quellen und ausgetauschten Daten.
- **Gemeinsame Schulungen:** Die Guardia Civil koordiniert gemeinsame Schulungen mit verschiedenen Sicherheitsdiensten, sowohl auf Management- als auch auf operativer Ebene.

Mille Occhi sulla Città – Italien

- **Formaler Rahmen:** Das Projekt, das wörtlich „Tausend Augen auf die Stadt" bedeutet, wurde 2010 in Italien ins Leben gerufen, und die jüngste Vereinbarung zwischen den Beteiligten stammt aus Januar 2022. Das Prinzip besteht darin, dass private Sicherheitsmitarbeiter, während sie ihre Aufgaben ausüben, Informationen sammeln, die für die Polizei zur Prävention und Bekämpfung von Straftaten (einschließlich Umweltkriminalität) nützlich sind. Das Mille Occhi-Protokoll etabliert den Rahmen und empfiehlt, dass jede italienische Provinz das Programm umsetzt.
- **Kriterien zur Auswahl von PSD:** Der Polizeipräfekt identifiziert für jede Provinz die PSD, die in das Projekt aufgenommen werden sollen.
- **Ansprechpartner:** PSD benennen sogenannte Single Points of Contact (SPOC) für den Informationsaustausch.
- **Regelmäßige Treffen:** Ein Technisches Koordinierungsgremium (Tavolo Tecnico) wird zwischen den Parteien eingerichtet und von der Zentralen Direktion der Kriminalpolizei koordiniert, die die Standardisierung von Verfahren und die Nutzung von Technologie fördert.

- Es gibt eine regelmäßige Evaluierung der Umsetzung des Protokolls auf Provinzebene.

- **Informationsaustausch:** Die Polizei kann Informationen für Ermittlungen oder Alarmmeldungen an die PSD weitergeben, solange sie nicht die Geheimhaltung und Vertraulichkeit der Daten verletzen. Die Polizei kann Patrouillen warnen, um die Anzahl der Beamten zu erhöhen, die in der Lage sind, verschiedene Situationen zu überprüfen.

PSD sollen Aktivitäten melden, die in der Liste im Protokoll beschrieben sind:

- Verdächtige Personen oder Fahrzeuge
- Flucht von Tatorten
- Diebstahl von Autos oder Motorrädern
- Kinder, ältere Menschen, verwirrte oder in Not befindliche Personen
- Hindernisse auf den Straßen
- Unterbrechung der Energieversorgung
- Ältere Personen, die aus Krankenhäusern oder anderen Behandlungsorten geflüchtet sind
- Andere Situationen, bei denen ein bevorstehendes Verbrechen vermutet wird
- Besondere Situationen von städtischer Verwahrlosung und sozialer Unruhe.

- Schulungen werden vom Staat durchgeführt, um die Interaktion mit den relevanten öffentlichen Diensten zu fördern und die Beobachtungsaktivitäten mit einer präventiven Denkweise durchzuführen. Mitarbeiter von PSD können auch an anderen Schulungen oder Auffrischungsschulungen mit der Polizei teilnehmen.

- Das Mille Occhi Milano-Protokoll enthält folgende interessante Bestimmung: „Der Präfekt kann Schulungen für Mitarbeiter von PSD mit Unterstützung der Strafverfolgungsbehörden organisieren, um das berufliche Wissen und das Bewusstsein für die Verantwortung und Bedeutung der Aufgaben, die dem privaten Sicherheitsdienst übertragen werden, zu fördern."

- Die Kosten für die technischen Mittel und die Schulungen werden zu 100 % von den PSD getragen. Dies wird ausdrücklich im Rahmenprotokoll erwähnt.

Project Griffin (jetzt ACT Awareness) – Vereinigtes Königreich[9]

Projekt Griffin – Vereinigtes Königreich

Project Griffin ist eine nationale Antiterrorismus-Initiative, die vom National Counter Terrorism Security Office (NaCTSO) ins Leben gerufen wurde, um Städte und Gemeinden zu schützen, indem Unternehmen über Terrorismusbedrohungen aufgeklärt werden, insbesondere von Gruppen wie ISIS, Al-Qaida und deren Ablegern. Das Projekt wurde im April 2004 als Reaktion auf die sich entwickelnde Terrorismusbedrohung, die durch die Anschläge am 11. September 2001 in den USA und die folgenden Anschläge in London am 7. Juli 2005 hervorgehoben wurde, gestartet. Diese Initiative bezieht sowohl den öffentlichen als auch den privaten Sektor ein, um die nationale Sicherheit als gemeinsame Verantwortung zu betonen. Ursprünglich war das Projekt auf drei große Finanzinstitute in London beschränkt, mittlerweile umfasst es jedoch eine breitere Partnerschaft zwischen Unternehmen, der Polizei von London und der Metropolitan Police. Ziel von Project Griffin ist es, den Beteiligten zu helfen, die Bedrohung zu verstehen, Handlungsanweisungen während terroristischer Vorfälle zu geben und die Meldung verdächtiger Aktivitäten über Informationsveranstaltungen zu ermöglichen, die von geschulten Polizeiberatern geleitet werden. Diese Veranstaltungen bieten verschiedene Antiterrorismus-Module, die das öffentliche und Mitarbeiterwissen darüber erweitern, wie potenziellen Terroraktivitäten entgegengewirkt und darauf reagiert werden kann, und behandeln dabei ein breites Spektrum von Bedrohungen, von einfachen Angriffen bis hin zu hochkoordinierten Anschlagsplänen.

Die Mission von Project Griffin ist es, die Gesellschaft in die Zusammenarbeit mit der Polizei zu miteinzubeziehen, um terroristische Aktivitäten frühzeitig zu erkennen und zu bekämpfen. Das Projekt fördert die Stärkung des Sicherheitsbewusstseins in der Geschäftswelt und die Erleichterung des Informationsaustauschs vor, während und nach Krisen. Im Laufe der Zeit hat Griffin sich erheblich erweitert, um sich an die sich verändernden Bedrohungen, insbesondere durch ISIS, anzupassen und ist mittlerweile das Standardmodell zur Durchführung von Antiterrorismusaufklärung und -training in allen Polizeikräften in England und Wales. Es wurde auch von der Polizei Schottlands übernommen.

[9] https://www.gov.uk/government/publications/project-griffin

Die Effektivität von Project Griffin wurde insbesondere während der Londoner Bombenanschläge im Juli 2005 und bei anderen Vorfällen, einschließlich eines potenziellen Anschlags im Tiger Night Club im Jahr 2007, deutlich. Der Erfolg des Projekts hat zu seiner Einführung in mehreren Ländern geführt, darunter Singapur, Australien, Kanada und die USA, wo es in New Yorks Project Shield integriert wurde. Project Griffin veranschaulicht die Stärke von öffentlichen-privaten Partnerschaften zur Verbesserung der Gemeindesicherheit und zur Schaffung eines schwierigen Umfelds für Terroristen, das sich kontinuierlich an die sich entwickelnde Bedrohung durch Terrorismus anpasst.

Die Veranstaltungen sind kostenlos und können je nach verfügbarer Zeit und Modulen zwischen ein und sechs Stunden dauern. Die Module werden regelmäßig überprüft und aktualisiert und behandeln derzeit folgende Themen:

- Einführung in den Antiterrorismus
- Aktuelle Bedrohungslage
- Erkennen und Reagieren auf verdächtiges Verhalten
- Erkennen und Umgang mit Bomben (IED) und verdächtigen Gegenständen
- Bombendrohungen
- Reaktion auf Angriffe mit Schusswaffen und Waffen
- Erkennung gefälschter Dokumente
- Drohnen – Unbemannte Luftfahrzeugsysteme (UAS).

Am Ende jeder Veranstaltung erhalten die Teilnehmer ein Teilnahmezertifikat, das die abgedeckten Module zeigt, sodass Unternehmen die Entwicklung und das Bewusstsein ihrer Mitarbeiter überwachen und nachweisen können.

Seit dem 16. März 2018 hat die Counter Terrorism Policing (CTP) alle ihre markengeschützten Produkte unter dem Banner **ACT-Action Counters Terrorism** zusammengeführt. Project Griffin war eines dieser Produkte und ist jetzt unter dem Namen **ACT Awareness,** einer E-Learning-Plattform, bekannt.

6.2. Regionale Partnerschaften

Oslo: Leitfaden zur Zusammenarbeit zwischen Polizei und Sicherheitsindustrie

Der Leitfaden, erstmals 2015 veröffentlicht, ist eine gemeinsame Veröffentlichung des Osloer Polizeidistrikts und der Norwegischen Vereinigung für Dienstleistungen (NHO Service), die alle Dienste, einschließlich privater Sicherheitsdienste vertritt. Während einige Formen der Zusammenarbeit noch bestehen, ist die aktuelle Situation nicht mehr so ideal, wie sie im Folgenden beschrieben wird. Da der Leitfaden jedoch umfassend war und als Modell für öffentliche-private Partnerschaften (PPP) von der CoESS betrachtet wird, stellen wir hier die wichtigsten Merkmale nachfolgend dar.

Der formale Rahmen

- Ziel des Leitfadens war es, die jeweiligen Rollen und Verantwortlichkeiten der Polizei und der privaten Sicherheitsdienste zu definieren, Lösungen für eine bessere Zusammenarbeit zu bieten, einschließlich praktischer Elemente wie Verfahren und Berichtsformulare.

- Der Leitfaden umfasst 3 Hauptabschnitte:
  - Der Rahmen und die Prinzipien: Verantwortlichkeiten, Pflichten, Formen der Zusammenarbeit, Foren und der Austausch von Informationen. Zielgruppe sind die Managementebenen sowohl der Polizei als auch der privaten Sicherheitsdienste.
  - Routinen und Verfahren, die auf drei verschiedenen Arten von privaten Sicherheitsdiensten basieren: Sicherheitskräfte in Einkaufszentren, Sicherheitskräfte im urbanen Umfeld und Türsteher. Diese wurden ausgewählt, da sie die Bereiche sind, in denen Polizei und private Sicherheitsdienste am häufigsten miteinander interagieren.
  - Eine Erklärung, wie die Intelligenz- und Berichtsformulare verstanden und verwendet werden sollen. Dieser Abschnitt enthält auch ein Feedbackformular, das bei den Kooperationsgesprächen zwischen Polizei und Sicherheitsindustrie verwendet wird.

Gegenseitiges Verständnis und Wissen:

- Eine allgemeine Beschreibung der Polizei, einschließlich ihrer Verfahren und Rangordnung, sowie der privaten Sicherheitsindustrie wird bereitgestellt.

- Die Aufgaben und der rechtliche Rahmen werden sowohl für die Polizei als auch für die Sicherheitsbranche festgelegt. Zum Beispiel wird der Einsatz von Gewalt oder die Ausübung von Macht und Autorität erklärt.

Auswahlkriterien für private Sicherheitsdienstleistungsunternehmen (PSD): Anforderungen, die von Sicherheitsdienstleistungsunternehmen erfüllt werden müssen, beinhalten die Einhaltung gesetzlicher Vorschriften und die Notwendigkeit, einen festen Ansprechpartner zu haben, der auf Benachrichtigungen reagieren kann. PSD müssen einen Entscheidungsträger benennen, der an den Besprechungen teilnimmt. Sie müssen auch Feedback im entsprechenden Format und innerhalb einer vorgegebenen Frist liefern.

Austausch von Informationen

Vorschriften zum Umgang mit Informationen:

- Der Leitfaden erkennt die Notwendigkeit des Informationsaustauschs an, benennt jedoch gleichzeitig die Einschränkungen, die das Gesetz in dieser Hinsicht setzt. Dies führt zu Problemen auf beiden Seiten. Der Leitfaden empfiehlt, dass dieses Thema von den relevanten Behörden und politischen Führern angesprochen werden sollte.

- Die Gesetzgebung erlaubt es der Polizei, Informationen mit Sicherheitsdienstleistungsunternehmen zu teilen, wenn dies notwendig ist, um gesetzliche Pflichten zu erfüllen oder rechtswidrigem Verhalten vorzubeugen, wie im Polizeigesetz zur Registrierung beschrieben. Die Beurteilung sollte berücksichtigen, ob der Informationsaustausch eine bessere Entscheidungsfindung ermöglicht. Zum Beispiel könnte die Polizei Informationen über einen Mitarbeiter eines Sicherheitsdienstleistungsunternehmens mit einem Drogenproblem haben, muss jedoch bewerten, ob der Austausch notwendig und verhältnismäßig ist. Jeder Fall erfordert eine individuelle Beurteilung, und Informationen sollten in der Regel schriftlich übermittelt werden, wobei elektronische Kommunikation verschlüsselt werden muss, wenn Vertraulichkeit erforderlich ist. Die Bewertung ergab jedoch, dass der Großteil des Informationsaustauschs derzeit mündlich erfolgt, ohne dass elektronische Aufzeichnungen geteilt werden, da rechtliche Einschränkungen bestehen.
  - Der Umgang mit Informationen in der Sicherheitsbranche unterliegt dem Gesetz zum Schutz personenbezogener Daten, das sowohl für den privaten als auch den öffentlichen Sektor gilt, wenn elektronische Werkzeuge verwendet werden oder Informationen in einem Register gespeichert sind. Die Polizei, die mit Kriminalfällen befasst ist, ist von diesem Gesetz ausgenommen. Sensible persönliche Daten erfordern eine Genehmigung der norwegischen Datenschutzbehörde und der Umgang mit ihnen muss strengen Handhabungsregeln folgen. Die Sicherheitsindustrie verwaltet personenbezogene Daten für Kunden im Rahmen von Datenverarbeitungsvereinbarungen und darf diese nur gemäß den schriftlich vereinbarten Bedingungen verarbeiten. Während die Polizei nicht vertrauliche Informationen mit Sicherheitsdienstleistungsunternehmen teilen kann, haben diese Unternehmen nicht die Erlaubnis, sensible Daten von der Polizei zu verarbeiten. Diese Einschränkung erschwert die Bemühungen, Verbrechen zu verhindern und aufzuklären, da die Polizei manchmal wichtige Informationen nicht mit Sicherheitsdienstleistungsunternehmen teilen kann. Während der Evaluation traten mehrere Vorfälle auf, bei denen die Polizei Informationen über aktive kriminelle Netzwerke (Bilder und Fahrzeuge) hatte, diese jedoch nicht an Alarm- und Sicherheitszentren in gefährdeten Gebieten weitergeben konnte. Dies erschwerte die Prävention und die Abwehr geplanter krimineller Aktivitäten.
  - Aus der Perspektive der privaten Sicherheitsbranche gibt es möglicherweise Einschränkungen hinsichtlich der Informationen, die sie teilen kann, da sie vertrauliche Informationen für eine Vielzahl von Kunden bearbeitet und Aufgaben an Objekten übernimmt, bei denen eine gesetzliche Geheimhaltungspflicht besteht. Die Polizei kann solche Informationen nur auf Gerichtsbeschluss erhalten.
  - Die Polizei profitiert erheblich von Informationen, die von der Sicherheitsbranche in Kriminalermittlungen, bei der Analyse von Vorfällen und Bedrohungen bereitgestellt werden. Ein problemorientierter Ansatz und eine Informationsdoktrin leiten die Strategie der norwegischen Polizei, die auf Zusammenarbeit mit externen Partnern setzt. Diese Zusammenarbeit ist entscheidend, um eine analytische und proaktive Arbeitsweise zu gewährleisten und die Ressourcen der Polizei optimal zu nutzen (Polizeistrategie 2010–2015).

- **Kanal für den sicheren Austausch von Informationen:** Das Osloer Polizeieinsatzzentrum verfügt über 20 Telefonleitungen, davon sind drei für die Sicherheitsbranche reserviert. Es ist daher wichtig, dass die Mitarbeiter der privaten Sicherheitsdienstleistungsunternehmen wissen, wann diese Leitungen genutzt werden müssen und wann die Notrufnummer 112 verwendet werden muss.

Regelmäßiges Treffen: Kontakt zwischen Sicherheitskräften und dem Polizeieinsatzzentrum: Das Polizeieinsatzzentrum priorisiert die Registrierung von Informationen von Sicherheitskräften, da diese möglicherweise den ersten Bericht über ein Ereignis liefern, das eine polizeiliche Nachverfolgung erfordert. Um unbefugte Anrufe zu verhindern, erfordert ein Verifizierungssystem, dass Sicherheitskräfte die Polizei über ihre Einsatzzentrale kontaktieren, welche ihre Identität überprüft, und die Situation beurteilt, bevor sie sie weiterverbindet. Sobald die Verbindung hergestellt ist, gibt der Sicherheitsmitarbeiter eine kurze Beschreibung des Vorfalls. Die Sicherheitsindustrie nutzt die Leitungen hauptsächlich für Identitätsprüfungen und allgemeine Anfragen, wobei eine Alarmleitung für schwere Straftaten vorgesehen ist. Sicherheitskräfte können auch die Notrufnummer 112 anrufen, wobei ihnen Kontrollfragen gestellt werden, um die Legitimität des Vorfalls zu überprüfen.

6.3. Operative und lokale Partnerschaften

Spanien: Schutz einer baskischen Polizeistation

Eine private Sicherheitsfirma führt Zugangskontrollen an einer baskischen Polizeistation durch.

Nachfolgend eine Beschreibung der Aufgaben im Rahmen dieser Mission:

- Überwachung und Schutz des Eigentums sowie der Personen, die sich möglicherweise auf dem Gelände aufhalten, durch Kontrollen, Patrouillen, Inspektionen und vorbeugende Maßnahmen, wie sie zur Erfüllung der Aufgabe festgelegt sind.
- Durchführung von Identitätsprüfungen bei Personen, die Zugang zur Polizeistation suchen, wobei sie entweder auf Baskisch oder Spanisch angesprochen werden, je nachdem, welche Sprache die Person verwenden möchte.
- Wachen können den Eintritt verweigern und relevante Informationen über den Besucher (einschließlich der Ausweisnummer), den Zweck des Besuchs und das Ziel innerhalb der Station aufzeichnen.
- Überwachung der in der Besucherparkzone geparkten Fahrzeuge und Verwaltung der Zugangssperren.
- Durchführung von Erstinspektionen aller Pakete, die das Gelände erreichen.
- Durchführung von Kontrollen mit dem Metalldetektor des Sicherheitsdienstes an Personen, die die Polizeistation betreten möchten, sowie an deren Gepäck, wobei alle nicht zugelassenen Gegenstände gemäß den Vorschriften entfernt werden.
- Durchführung von Stichprobenkontrollen an Fahrzeugen (einschließlich der Unterböden und Kofferräume).
- Überprüfung von Alarmen und eventuellen Anomalien an verschiedenen Punkten im Komplex, wenn dies erforderlich ist.
- Betrieb der CCTV-Systeme, die an der Polizeistation installiert sind:
  - Ein Kamerasystem ist eingerichtet, um die Perimeter der Polizeistation zu überwachen.
  - Kontinuierliche Aufmerksamkeit für das CCTV-Kontrollzentrum.
  - Überwachung der CCTV-Bildschirme und Steuerung der Kameras, Initiierung der entsprechenden Sicherheitsprotokolle im Falle von Vorfällen sowie Durchführung aller anderen Aufgaben, die im Einklang mit ihren regulativen Verantwortlichkeiten zugewiesen werden.
  - Analyse und Verwaltung der empfangenen Alarmsignale (Feuer, Lagerung, Einbruch, etc.) sowie Verwaltung der technischen Ressourcen, die ihnen zur Verfügung stehen.

Belgien: Schutz der lokalen Polizei in Antwerpen

Ein ähnliches Abkommen wurde zwischen der lokalen Polizei von Antwerpen und einer privaten Sicherheitsfirma geschlossen. Es handelt sich um einen 7-Jahres-Rahmenvertrag, im Rahmen dessen die PSD das Hauptquartier der lokalen Polizei von Antwerpen sichert. In den kommenden Jahren ist geplant, die Vereinbarung auf weitere Standorte zu erweitern.

- Zu den Aufgaben gehören die Zugangskontrolle für Besucher und die Verwaltung der Rezeption. Die Zugangskontrolle umfasst den Einsatz von Technologie, z. B. Metalldetektoren.

- Das Abkommen sieht vor, dass der Auftraggeber zusätzliche Dienstleistungen oder Lösungen von den PSD anfordern kann wie z. B. Veranstaltungssicherheit oder Unterstützung beim Betrieb technischer Ausrüstungen wie Drohnen und CCTV.

Polizeizonen Mechelen-Willebroek / Belgien

Seit der Verabschiedung des neuen belgischen Gesetzes zur privaten Sicherheit im Jahr 2017 haben die lokalen Behörden mehr Klarheit im Umgang mit Sicherheitsdienstleistungsunternehmen zur Verwaltung öffentlicher Räume gewonnen. Die Polizeizonen Mechelen und Willebroek, die seit den 1990er Jahren mit hohen Kriminalitätsraten konfrontiert sind, haben diese Gelegenheit genutzt, um einen umfassenden Aktionsplan für die öffentliche Sicherheit zu entwickeln, der die verstärkte Zusammenarbeit zwischen öffentlichem und privatem Sektor betont. Dies wird in einer Veröffentlichung[10] von Prof. Dr. Marc Cools und Veerle Pashley von der Universität Gent aus dem Jahr 2018 beschrieben.

Ein bemerkenswertes Beispiel ist die Konsortialüberwachung in der Industriezone Mechelen, wo die Zusammenarbeit zwischen Polizei und privatem Sicherheitssektor erfolgreich war.

Beschreibung der PPP:

Private Sicherheitsdienste im Rahmen eines befristeten Vertrags, welcher Perimeterkontrolle mit permanenter Sicherheitspräsenz, mobilen Patrouillen und alarmausgelösten Interventionen beinhaltet. An diesem Konzept sind mehrere Partner beteiligt – Sicherheitsdienstleistungsunternehmen, Polizei, Industriegebiete und die Regierung, koordiniert durch ein städtisches Kooperationsprotokoll. Sicherheitsdienstleistungsunternehmen. Dieser Konsortialansatz ist kosteneffizient, da die finanzielle Belastung unter den Unternehmen aufgeteilt wird. Auch wenn ähnliche Initiativen in Belgien existieren, war Mechelen-Willebroek das erste, das ein solches Modell umsetzte. Innerhalb dieses Kooperationsrahmens sind Sicherheitsdienstleistungsunternehmen verpflichtet, täglich an die Polizei zu berichten. Das neue Gesetz zur privaten Sicherheit erlaubt es auch, solche Rahmenvereinbarungen auf andere Bereiche wie Einkaufsviertel auszudehnen.

Das Antwerpener SHIELD-Programm – Belgien

Diese öffentlich-private Partnerschaft im Bereich der Terrorismusbekämpfung wird von Van Steden und Meijer in einem Papier über „PPPs in Zeiten diffusen terroristischen Bedrohung“[11] als Best Practice beschrieben.

Formelles Rahmenwerk

Das Antwerpener SHIELD-Programm dient als umfassendes Rahmenwerk für eine Reihe laufender und zukünftiger Initiativen der Polizei von Antwerpen, die speziell auf die Sicherheits- und Terrorismusbekämpfungsmaßnahmen im privaten Sektor abzielen. Diese öffentlich-private Partnerschaft basiert auf den Prinzipien des effektiven Informationsaustauschs, um die Sicherheitsmaßnahmen in der Stadt zu stärken.

Das Hauptziel der Antwerpener SHIELD-Initiative ist es, eine nahtlose Kommunikation zwischen der Polizei und dem privaten Sektor zu fördern, um damit die Möglichkeiten der Polizei zu verbessern, Terrorismus zu bekämpfen und die allgemeine öffentliche Sicherheit in Antwerpen zu erhöhen. Inspiriert vom SHIELD-Programm des New York Police Department, das seit langem den Informationsaustausch zwischen öffentlichem und privatem Sektor unter dem Motto „Terrorismusbekämpfung durch Informationsaustausch“ vorantreibt, strebt Antwerpen SHIELD an, dieses Modell zu replizieren. Das NYPD SHIELD-Programm hat erheblichen Erfolg bei der Förderung einer regelmäßigen, effizienten Kommunikation mit seinen Mitgliedern gezeigt und Antwerpen SHIELD will diesen Erfolg nachahmen, um die Sicherheitskooperation innerhalb seiner Zuständigkeit zu stärken. Antwerpen SHIELD bietet Schulungsprogramme für seine Mitglieder und stellt eine dedizierte Plattform für Bildung und Weiterentwicklung zur Verfügung. Diese Schulungen werden in verschiedenen Formaten angeboten, einschließlich Online-Tutorials und Schulungen vor Ort am Arbeitsplatz. Die Kurse, die kostenlos angeboten werden, vermitteln den Teilnehmern praktische Einblicke und Strategien zur Identifizierung und Reaktion auf terroristische Bedrohungen.

[10] *Cools, Marc, and Veerle Pashley. Private Veiligheid in Een Stedelijke En Gemeentelijke Context : Onderzoek Naar de Rol En Samenwerkingsmogelijkheden in Mechelen-Willebroek. Gompel&Svacina, 2018.*

[11] *Steden, R. van, & Meijer, R. (2018). Publiek-private samenwerking in tijden van diffuse dreiging: Een onderzoek naar diversiteit in werkwijzen en kansen in de Nederlandse en Vlaamse context. Den Haag: WODC.*

Die Implementierung von SHIELD im Antwerpener Diamantenviertel

Ein Teil des SHIELD-Programms ist die Sicherheitsvorkehrung im Diamantenviertel von Antwerpen, wo Polizei, die Gemeinde und mehrere private Sicherheitsdienstleistungsunternehmen zusammenarbeiten, um Kriminalität zu verhindern. Dieses Projekt wird häufig als Modell für Vertrauen und Respekt zwischen den Parteien sowie für eine hohe Zufriedenheit mit dem gegenseitigen Informationsaustausch genannt. Laut den Forschungen von Van Steden und Meijer liegt dies vor allem am Sicherheitsbüro des Antwerpener Welt-Diamanten-Zentrums, das als Informationsbroker zwischen den Interessengruppen fungiert.

Informationsaustausch: Das Sicherheitsbüro analysiert und verarbeitet Informationen, anonymisiert vertrauliche Daten, wenn erforderlich, und verteilt sie an diejenigen, die sie benötigen. Die Art der Informationen umfasst geopolitische Entwicklungen, verdächtige Situationen oder Aktivitäten, Bedrohungsbewertungen und Kamerabilder.

Formelles Rahmenwerk, SPOCs und regelmäßiges Treffen

Die PPP ist in einem Sicherheitsprotokoll und einer Kooperationsvereinbarung festgelegt, und es wird regelmäßiger Kontakt zwischen den relevanten Interessengruppen aufrechterhalten. Die Aufgabenteilung, Rollen und Verantwortlichkeiten sind allen Beteiligten klar, basierend auf einem schriftlichen Dokument.

Erfolgsfaktoren

- Geteiltes und gegenseitiges Vertrauen
- Die Interessengruppen wurden als Team mit Single Points of Contact (SPOCs) innerhalb der verschiedenen Akteure etabliert
- Konsens über den Umgang mit diffusen Bedrohungen
- Gemeinsames Gefühl der Dringlichkeit
- Bereitschaft, Kompromisse einzugehen.

Laut den Forschungen von Van Steden und Meijer erfüllt diese PPP alle in der Literatur zu diesem Thema genannten Erfolgskriterien.

Niederlande – Zusammenarbeit zum Schutz des Königstages in Arnhem

Die Niederlande haben eine lange Tradition, ihren Souverän zu feiern, und seit Willem-Alexander den Thron bestiegen hat, wird der Königstag an seinem Geburtstag im April begangen. Er wird in vielen Städten gefeiert, deren Zentren sich in große Veranstaltungsgebiete verwandeln, in denen etwa 200.000 Menschen anwesend sind. Die Royals besuchen traditionell mehrere Orte, um den Tag mit der Bevölkerung zu feiern. Im Jahr 2009 gab es einen Mordversuch, bei dem ein Auto in den Zug raste. Acht Personen starben bei diesem Vorfall. Dies unterstreicht die Notwendigkeit, für das Ereignis einen angemessenen Schutz bereitzustellen.

In der Stadt Arnhem gibt es eine PPP, bei der der Bürgermeister zusammen mit dem lokalen Dreieck (Bürgermeisterbüro, Strafverfolgungsbehörden und private Sicherheitsdienstleistungsunternehmen) für eine sichere Veranstaltung mit weniger Polizisten sorgt, beispielsweise während des Königstags. Laut dem Bürgermeister wurden 2024 dank dieser PPP und der Unterstützung der privaten Sicherheitsdienstleistungsunternehmen 80 Polizisten weniger in Arnhem eingesetzt, als dies bei einer ähnlichen Großveranstaltung normalerweise der Fall wäre, sodass sie an anderer Stelle eingesetzt werden konnten. In einem Zeitungsartikel[12] über diese Zusammenarbeit erklärte der Bürgermeister, dass dadurch 2 Polizisten, für jeweils 40 Tage im Ermittlungsdienst eingesetzt werden konnten.

[12] *Gelderlander. (2024). "Een harde vuistslag in het feestgedruis, maar de dader wordt er in een oogwenk uitgepikt door Big Brother".*

CCTV ermöglicht es, jede potenzielle Quelle von Problemen in guter Bildqualität zu verfolgen, ohne die Szene zu stören.

Veranstaltungsorganisatoren sind für die Sicherheit an ihren Veranstaltungsorten verantwortlich. Die Stadt unterstützt bei Bedarf mit zusätzlicher Sicherheit oder Polizei. Dies ermöglicht eine schnelle und effiziente Reaktion, falls ein Vorfall eintritt.

Eingesetzte Dienstleistungen und Lösungen:

- 2024 ist das dritte Jahr, in dem die Stadt ein gemeinsames Kommandozentrum eingerichtet hat, das mit Bildschirmen ausgestattet ist, auf denen Aufnahmen von verschiedenen städtischen Kameras angezeigt werden. Das Zentrum wird von Personal der Stadt, Polizei, medizinischen Diensten, Feuerwehr, Vollzugsbehörden und privaten Sicherheitsdienstleistungsunternehmen besetzt. Alle Dienste werden als eine Einheit unter dem Kommando des Sicherheitskoordinators der Stadt geführt.
- Das Team, das für das Crowdmanagement verantwortlich ist, sorgt für die Vermeidung von Sicherheitsvorfällen und greift ein, wenn es notwendig ist.

„Laut dem Bürgermeister wurden 2024 dank dieser PPP und der Unterstützung durch private Sicherheitsdienste (PSD) 80 Beamte weniger in Arnhem eingesetzt, als es bei einer ähnlichen großen Veranstaltung normalerweise der Fall gewesen wäre. Sie konnten somit für anderen Tätigkeiten eingesetzt werden.“

7. Die Checkliste der International Security Ligue[13] für den Aufbau einer effektiven Partnerschaft im Bereich der privaten Sicherheit

„Eine sorgfältige Auswahl und enge Überwachung sind wichtiger geworden, da sich die Leistung verbessert hat: (a) weil sie die Unterschiede im Servicelevel, den man erhalten kann, verschärft hat; und (b) damit öffentliche Einrichtungen die Fortschritte, die die Branche erzielt hat, vollständig nutzen können.“

[13] https://www.international-security-ligue.org

Checkliste zur Bewertung des Anbieters: Zu prüfende Fragen vor Beginn der Zusammenarbeit			
	Ja	**Nein**	**Details/Hinweise/Erläuterungen**
Teil I. Hintergrund, Struktur			
Ist die Bereitstellung von Sicherheitsdienstleistungen und von Mitarbeitern das Kerngeschäft des Anbieters?			
Verfügt das Unternehmen über ein ausreichendes Fachwissen für den Auftrag?			
Hat das Sicherheitsdienstleistungsunternehmen Erfahrung mit der Erbringung von Dienstleistungen in ähnlichen Situationen wie der unseren?			
Entsprechen die operative und finanzielle Erfolgsbilanz und der Ruf des Unternehmens unseren Anforderungen?			
Hat eine Hintergrunduntersuchung ergeben, dass es keine Probleme gibt, die das Unternehmen von der Prüfung ausschließen könnten (z. B. Betrug, Korruption, Verstöße oder andere Vergehen in der Vergangenheit)?			
Ist das Unternehmen in der Lage nachzuweisen, dass es die Versicherungsanforderungen erfüllt?			
Hat das Unternehmen einschlägige Finanzunterlagen für die letzten drei Jahre vorgelegt?			
Ergibt eine Überprüfung der Finanzen des Unternehmens, dass es finanziell gesund ist?			
Kann das Unternehmen nachweisen, dass es allen steuerlichen oder sonstigen Verpflichtungen nachkommt?			
Hat das Unternehmen eine Liste von Kundenreferenzen vorgelegt?			
Gibt es Belege dafür, dass das Unternehmen einen Auftrag ähnlicher Größe, Struktur und Verantwortung erfolgreich abgewickelt hat?			
Hat das Unternehmen eine Liste ähnlicher Standorte vorgelegt, an denen seine Dienstleistungen besichtigt und überprüft werden können?			
Ist das Unternehmen nachweislich in der Lage, den von uns geforderten Standard an Dienstleistungen und Fachwissen zu bieten?			
Hat das Unternehmen seine Sicherheitsphilosophie erläutert und wie diese in Bezug auf unseren Vertrag umgesetzt wird?			
Ergibt eine Überprüfung, dass es keine ungewöhnliche Anzahl oder kein ungewöhnliches Muster von Beschwerden gibt?			
Weist eine Bewertung darauf hin, dass die Firma proaktiv dafür sorgt, dass ihre Zulassungen auf dem neuesten Stand sind?			
Ist das Unternehmen ein vollwertiges Mitglied eines anerkannten Berufsverbandes?			
Ist das Unternehmen frei von Interessenkonflikten oder finanziellen Verstrickungen, die ein negatives Licht auf uns werfen könnten?			
Hat das Unternehmen Branchenauszeichnungen erhalten oder ist es Mitglied in einer selektiven Industriegruppe?			

Checkliste zur Bewertung des Anbieters: Zu prüfende Fragen vor Beginn der Zusammenarbeit			
	Ja	**Nein**	**Details/Hinweise/Erläuterungen**
Teil II. Personal			
Reicht das bestehende Management des Unternehmens aus, um unsere betrieblichen Anforderungen zu erfüllen?			
Hat das Unternehmen seine durchschnittlichen jährlichen Arbeitskräfte und Führungskräfte angegeben in den letzten drei Jahren (Dauer-, Zeit- und Vertragsbedienstete)?			
Erfüllt oder übertrifft die Grundausbildung, die das Unternehmen seinen Sicherheitsbeauftragten bietet, unsere Anforderungen?			
Sind wir sicher, dass das Engagement des Anbieters für Integration und Vielfalt bei der Einstellung ein positives Licht auf uns werfen wird?			
Sind wir mit der Kompetenz der Ausbilder zufrieden, die das Unternehmen in seinen Schulungs- und Entwicklungsprogrammen einsetzt (interne oder externe Ausbilder)?			
Bietet das Unternehmen regelmäßige Auffrischungsschulungen für seine Mitarbeiter an?			
Kann das Unternehmen aktuelle Aufzeichnungen über die Ausbildung des Personals vorlegen?			
Sind die Qualifikationen des Unternehmens für Sicherheitsbeauftragte für uns akzeptabel?			
Entspricht die Überprüfung der Sicherheitsbeauftragten des Unternehmens unserem Standard für Zuverlässigkeitsüberprüfungen?			
Hat das Unternehmen in den letzten drei Jahren eine akzeptable jährliche Personalfluktuation verzeichnet?			
Gibt es Belege dafür, dass das Personal andere Qualifikationsanforderungen für die Aufgaben im Rahmen Vertrags erfüllt (Sprachkenntnisse, IT-Kenntnisse usw.)?			
Wurde der Nachweis erbracht, dass alle speziellen Schulungen, die für das Personal zur Erfüllung der Anforderungen des Auftrags erforderlich sind, durchgeführt wurden?			
Ist das Wachpersonal, das unseren Einrichtungen zugewiesen wird, erfahren in der Art der Arbeit, die es ausführen wird?			
Kann das Unternehmen den Nachweis erbringen, dass das Sicherheitspersonal für die Arbeit, der es beauftragt ist, geeignet ist?			
Kann das Unternehmen eine klare Verantwortungskette in Bezug auf die Verwaltung und die Betreuung des Vertrags vorweisen?			
Entspricht das äußere Erscheinungsbild des Vertragspersonals und der Ausrüstung unseren Standards (Uniformen, Fahrzeuge usw.)?			
Lassen die Fähigkeiten und das Fachwissen des Managementteams des Unternehmens darauf schließen, dass es in der Lage ist, hervorragende Planungs- und Serviceleistungen zu erbringen?			
Hat das Unternehmen Informationen über die Fähigkeiten und Erfahrungen der einzelnen Mitglieder des Managementteams und deren Zuständigkeiten im Rahmen des Vertrags vorgelegt?			
Lassen die Fähigkeiten und Qualifikationen der Führungsperson vor Ort darauf schließen, dass er den Auftrag effektiv ausführen kann?			
Sind wir mit den Fähigkeiten und dem Fachwissen des Vertragsmanagers zufrieden?			

Checkliste zur Bewertung des Anbieters: Zu prüfende Fragen vor Beginn der Zusammenarbeit			
	Ja	**Nein**	**Details/Hinweise/Erläuterungen**
Teil III. Programme, Pläne			
Gibt es Belege dafür, dass die Arbeitsbedingungen des Unternehmens für das Wachpersonal mit allen einschlägigen Rechtsvorschriften und/oder Tarifverträgen und Auslagenentschädigungen übereinstimmen?			
Sind die Gehalts- und Leistungsniveaus des Unternehmens für sein Sicherheitspersonal sowohl ausreichend als auch im Einklang mit den örtlichen gewerkschaftlichen, staatlichen und/oder nationalen Anforderungen?			
Entsprechen die Sicherheitsrichtlinien und -verfahren des Unternehmens den gesetzlichen Anforderungen?			
Verfügt die Firma über einen soliden Prüfungs- und Qualitätssicherungsrahmen (ISO-Konform usw.)?			
Verfügt das Unternehmen über ein solides Programm für die soziale Verantwortung der Unternehmen?			
Kann das Unternehmen nachweisen, dass es sich verpflichtet hat, die Gesundheits- und Sicherheitsrisiken für seine Sicherheitsmitarbeiter zu verringern?			
Verfügt das Unternehmen über einen Verhaltenskodex, ein Integritäts- oder Ethikprogramm?			
Verfügt das Unternehmen über eine Richtlinie zum Umgang mit Drogen, die unseren Anforderungen entspricht?			
Ist der Anbieter in der Lage nachzuweisen, dass Arbeitszeiten und Schichtmuster der Mitarbeiter nicht über die guten Praktiken resp. über das Arbeitsgesetz hinausgehen (aufeinanderfolgende Stunden, Tage, ausreichende Pausen usw.)?			
Werden alle Mitarbeiter über das Ethikprogramm des Unternehmens unterrichtet?			
Ergibt eine Überprüfung der Kundenrechnungen des Unternehmens, dass sie transparent und leicht zu verstehen?			
Kann das Unternehmen nachweisen, dass es über einen geeigneten Kanal für die Bearbeitung von Beschwerden, Rückmeldungen und Vorschlägen des Wachpersonals verfügt?			
Verfügt das Unternehmen über ein Karriereentwicklungsprogramm oder andere Karriereprogramme für sein Wachpersonal?			
Verfügt das Unternehmen über die für den Auftrag erforderlichen Zertifizierungen?			
Enthält der Einsatzplan des Unternehmens für den Auftrag alle erforderlichen Elemente?			
Reichen die im Einsatzplan vorgesehenen Technologien, Instrumente und Ausrüstungen aus, um hervorragende Dienstleistungen zu erbringen?			
Verfügt das Unternehmen über ein internes Compliance- und Qualitätsprogramm?			
Sind wir zufrieden mit den Plänen und Verfahren des Unternehmens zum Schutz von vertrauliche Informationen vor der Offenlegung zu schützen?			
Bietet der Krisenmanagementplan des Anbieters die Gewissheit, dass er in der Lage sein wird, uns in einer größeren Katastrophe zu unterstützen?			
Wurden alle mündlichen Zusagen oder Zusicherungen schriftlich festgehalten?			

Checkliste zur Bewertung des Anbieters: Zu prüfende Fragen vor Beginn der Zusammenarbeit			
	Ja	**Nein**	**Details/Hinweise/Erläuterungen**
Teil IV. Ressourcen, Unterstützung			
Verfügt das Unternehmen über ausreichende Reservekapazitäten, insbesondere über Redundanzen in den wichtigsten operativen Infrastrukturen, die rund um die Uhr in Betrieb sind, um die Anforderungen des Vertrags zu erfüllen?			
Ergibt eine Überprüfung der Managementstruktur und der Ressourcen des Unternehmens, dass die Fähigkeit besteht, auf Probleme innerhalb der geforderten Zeiten zu reagieren?			
Kann das Unternehmen nachweisen, dass es über genügend Personal verfügt, um die Anforderungen des Vertrags effektiv zu erfüllen?			
Ist die Firma in der Lage, bei Bedarf rechtzeitig zusätzliche personelle Unterstützung bereitzustellen?			
Ist der Anbieter in der Lage, die für die Erbringung der vertraglich vereinbarten Dienstleistungen erforderliche Ausrüstung und Ausbildung bereitzustellen?			
Sind wir mit der zusätzlichen oder speziellen Ausbildung, die das Unternehmen anbieten kann, zufrieden?			
Kann das Unternehmen seine Verfahren zur Einhaltung der Qualitätsstandards, zu denen es sich verpflichtet, darlegen?			
Sind wir mit unseren Möglichkeiten zufrieden, wenn ein Wachmann eine Schicht versäumt?			
Kann das Unternehmen für alle Systeme oder Ausrüstungen, die es im Rahmen des Auftrags bereitstellt, nachweisen, dass es in der Lage ist, das System effektiv zu betreiben und Instand zu halten?			
Sind wir damit zufrieden, wie das Unternehmen die Technologie einsetzt, um die Leistung der Mitarbeiter zu verbessern?			
Hat das Unternehmen ausreichende Informationen über die zur Verfügung stehenden Unterstützungsleistungen (z. B. Verwaltung, Rechnungsstellung usw.) bereitgestellt?			
Sind wir mit der Verfügbarkeit von unterstützenden Sicherheits- und sicherheitsbezogenen Diensten zufrieden?			
Sind wir mit dem operativen Plan des Unternehmens zur Überwachung der Vertragserfüllung zufrieden?			
Ist die Dienstplanmethode des Unternehmens ein Indikator für die Fähigkeit, die Sicherheitsanforderungen des Auftrags zu erfüllen?			
Kann das Unternehmen alle erforderlichen Zertifizierungen für die technische Ausrüstung vorweisen, die zur Erfüllung des Auftrags eingesetzt wird?			
Wenn das Unternehmen in bestimmten Fällen zusätzliche private Sicherheitsdienstleister als Subunternehmer einsetzt, ist dann sichergestellt, dass diese ebenfalls alle Qualitätskriterien erfüllen?			
Sind die Kommunikationsmittel und -systeme des Unternehmens für die Dienstleistungen geeignet?			
Sind wir mit den Mechanismen zufrieden, die das Unternehmen eingerichtet hat, um unsere Anforderungen abzuholen, Informationen auszutauschen und unsere Zufriedenheit zu bewerten?			


POLICE

CoESS

Nederlandse Veiligheidsbranche

International SecurityLigue