

Public-Private Partnerships for Infrastructure Security

NOVEMBER 13 **2025**

YAVA
Beyond
Innovation.
Beyond Borders.

CONTENT

Section 1	Industry Analysis	
	Strategic Importance of Public-Private Partnerships	1
	Challenges Faced by Governments	2
Section 2	YAVA's Role in Industry	
	Role of Private Sector Specialists	4
Section 3	Examples of Specialist Support Technologies	
	YAVA's Portfolio	6
Section 4	Case Studies and Success Stories	
	Case Studies	8
Section 5	Quantitative Data and Trends	8
Section 6	Call to Action	
	Embrace Partnerships for a Safer Future	12
Section 7	Conclusion	13
Section 8	Current YAVA Mandates	13

YAVA – Beyond Innovation. Beyond Borders | Copyright © 2025 | YAVA.com

YAVA – Beyond Innovation. Beyond Borders | Copyright © 2025 | YAVA.com

Strategic Importance of Public-Private Partnerships

Governments worldwide are increasingly recognizing that safeguarding critical infrastructure cannot be achieved by the public sector alone. Many essential services, such as energy grids, transportation, telecommunications and healthcare, are owned or operated by private entities. This means a "whole-of-society" approach is needed, where government and industry combine forces to bolster resilience. In NATO countries, for example, alliances now emphasize two-way cooperation with the private sector on emerging threats. A NATO 2023 resilience symposium underlined the crucial role of industry in securing infrastructure and supply chains, calling for deeper public-private collaboration. As NATO's 2030 initiative noted, modern conflicts are "increasingly defined by bytes and big data as much as by bullets," so engaging tech companies is vital.

In the Gulf Cooperation Council (GCC) region, similar trends are evident. GCC governments like the UAE are partnering with specialized tech firms to protect digital infrastructure and respond to cyber threats. The UAE's national cybersecurity strategy explicitly prioritises strong public-private partnerships. Recently, the UAE Cyber Security Council signed an MoU with a private cybersecurity company (ORYX Labs) to share threat intelligence and respond to incidents collaboratively. This partnership model is seen as "absolutely vital" for quick incident response – leveraging private expertise alongside government resources. A GCC-wide analysis of millions of data points on cyber readiness concluded that closing critical security gaps "will only be possible through public-private partnerships." In other words, governments alone cannot keep pace with fast-evolving threats, and must tap into the innovation and agility of the private sector

Section 1: Industry Analysis

Across Asia, public-private collaboration is equally strategic. Disaster-prone countries in ASEAN have advocated PPPs to enhance emergency preparedness, noting that the "immense resources required to manage disasters…will not be achieved" without active private sector involvement. For example, Japan and South Korea have enlisted robotics and telecom firms to develop early warning systems and post-disaster recovery tools, combining government oversight with industry innovation. In India, programs like the Defence Innovation Organisation's iDEX bring startups into defence procurement, reflecting a broader Asian trend of governments partnering with tech entrepreneurs. Whether the goal is improving public safety, disaster response or cyber defence, PPPs offer a way to leverage cutting-edge solutions that governments would struggle to develop alone.

In summary, public-private partnerships are now seen as foundational to effective infrastructure security and resilience, providing the expertise, technology and shared responsibility needed to protect the public.

Commented [NI3]: Do we need to spell this out?

Commented [NI2]: Again, add link

YAVA – Beyond Innovation. Beyond Borders | Copyright © 2025 | YAVA.com

YAVA – Beyond Innovation. Beyond Borders | Copyright © 2025 | YAVA.com

Challenges Faced by Governments

Despite the clear need, governments face several challenges in adopting advanced technologies for infrastructure protection. Key hurdles include:

- Budget Constraints: Public agencies operate under finite budgets and competing priorities. Deploying state-of-the-art security tech (from AI surveillance to counter-drone systems) can require significant upfront investment. Many governments struggle to fully fund these projects on their own, especially when also maintaining legacy infrastructure. In areas like disaster mitigation, there is often a funding gap between what is needed for resilience and what public budgets allow, which is why private co-investment is attractive. (Notably, studies show every $1 spent on resilience saves several dollars in disaster losses, easing long-term burdens.)

- Slow Procurement Cycles: Government procurement is notoriously slow and complex. A Gartner survey found that public-sector organizations have an average technology buying cycle of about 22 months, roughly 3 times longer than the ~7-month average in other industries. Multiple layers of approval, strict bidding regulations and auditing requirements drag out timelines. By the time a solution is purchased, the technology or requirement may have evolved. One analyst noted that each jurisdiction's unique rules, and fear of breaking them, add legal complexity that delays projects. Such slow cycles hinder governments from quickly adopting innovations.

Section 1: Industry Challenges

- Regulatory and Bureaucratic Complexities: Public agencies must navigate a thicket of regulations – from privacy laws and safety certifications to export controls and data sovereignty rules. Adhering to these is cumbersome and can deter adoption of new tech. For example, security agencies in one country might be constrained from using certain foreign-made drones or software due to regulations, limiting options.

  Inter-agency coordination is another challenge: critical infrastructure often spans federal, state and local authorities, each with its own processes. Aligning on standards and approvals (e.g. for deploying surveillance sensors or sharing data) can be extremely complex and time-consuming.

- Lack of Internal Tech Expertise: Government departments may lack sufficient in-house expertise to evaluate, implement and manage advanced technological solutions. There is often a skills gap in areas like AI, cybersecurity and autonomous systems. In the U.S., for instance, the federal government faces a "severe shortage of digital expertise" in fields such as AI and cybersecurity. This talent gap means agencies might not fully understand specialised products or how to integrate them with legacy systems. Public IT teams are also stretched maintaining existing systems, with limited bandwidth to experiment with new tools. The result is that promising technologies can be overlooked or improperly implemented.

These challenges make it difficult for governments to innovate at the speed of today's threats. Budget limits constrain procurement, bureaucracy slows it and skill gaps complicate implementation. Recognizing these pain points explains why many governments are eager to seek help from private sector specialists who can fill the void.

Commented [NI4]: Can we add reference link?

Commented [NI5]: Could add link

STRATEGIC IMPORTANCE OF PUBLIC-PRIVATE PARTNERSHIPS

From protecting energy grids to ensuring national security, governments are increasingly relying on private sector partnerships to safeguard critical infrastructure. NATO, GCC and ASEAN countries highlight the importance collaboration for resilience and cybersecurity preparedness, leveraging the private sector's agility to tackle evolving threats.

NATO's 2030 initiative highlights the role of private tech in modern conflicts.



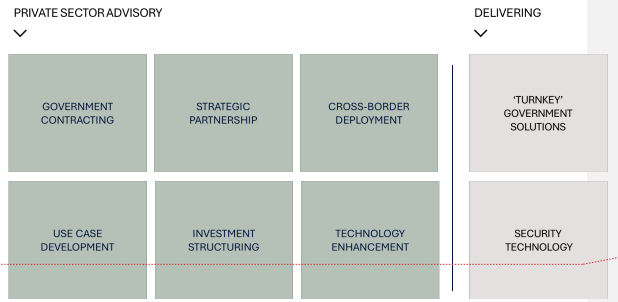
YAVA – Beyond Innovation. Beyond Borders | Copyright © 2025 | YAVA.com

Role of Private Sector Specialists

Private sector specialist firms like YAVA have emerged to bridge the gap between fast-moving tech innovation and the public sector's needs. These companies act as force multipliers for government initiatives, offering turnkey solutions and advisory services that address the challenges outlined above. In essence, firms like YAVA fill a crucial role by providing:

New-age Technologies	Specialists source and curate advanced technologies, offering ready-made solutions from global markets.
Compliance-Ready Systems	Ensuring technologies meet government regulations and standards, including certifications and procurement rules. Their expertise speeds up the process, reducing risk and ensuring solutions are government-ready.
Strategic Advisory and Integration	Providing consulting to adapt technologies to local needs, guiding deployment and integration. Helping governments prioritise high-impact projects and offer ongoing support to ensure successful implementation.
Filling Expertise Gaps	YAVA embeds experts like engineers and cybersecurity analysts within government teams to address skills shortages. Ensuring effective use of technologies and facilitate information sharing between the public sector and industry.

Section 2: YAVA's Role in Industry



Commented [NI6]: Emerging?

The table outlines service areas critical to the successful delivery of government and security technology solutions.

- Government contracting focuses on navigating procurement processes to facilitate partnerships between the public and private sectors.
- Strategic partnership emphasises collaboration with key stakeholders to drive mutual goals.
- Cross-border deployment ensures that solutions are effectively implemented in international markets while complying with local regulations.
- Use case development identifies specific applications for technologies in diverse environments, optimizing their effectiveness.
- Investment structuring involves organising funding and resources to support long-term project success.
- Technology enhancement focuses on refining and upgrading existing solutions to meet evolving needs.

Together, these elements combine to provide comprehensive turnkey government solutions, particularly in the security technology sector, ensuring efficient, scalable and compliant implementations.

ROLE OF PRIVATE SECTOR SPECIALISTS

Private firms like YAVA bridge the gap between the public and private sector by providing cutting-edge technologies, compliance-ready systems and strategic advisory to help governments overcome their internal challenges. These firms enable faster, more effective implementation of critical infrastructure security solutions.

YAVA – Beyond Innovation. Beyond Borders | Copyright © 2025 | YAVA.com

YAVA's Portfolio

YAVA's portfolio spans public safety, counter-drone defence, humanitarian fintech, autonomous military systems, secure communications, surveillance, disaster & aid management, UAVs and cybersecurity. In each of these areas, YAVA operates as an integrator and accelerator.

Sector	Description
Public Safety	Provides smart city solutions, such as AI-powered CCTV and gunshot detection systems. Experts integrate hardware and software to deploy real-time crime centres, helping law enforcement monitor and analyse crime data.
Counter-Drone Systems	Develops and deploys counter-UAS technologies for protecting airports and critical sites. Experts integrate radio-frequency jamming or drone "takeover" systems while ensuring legal compliance and military radar integration.
Humanitarian Fintech	Implements fintech solutions for crisis aid, such as e-wallets and blockchain for aid tracking. Specialists help governments and NGOs quickly distribute funds to citizens with less fraud, as seen in the UN's blockchain pilot for Ukrainian refugees.
Autonomous Military	Supports defence agencies with autonomous drones and AI-driven systems. Experts help integrate cutting-edge defence tech into military R&D, ensuring compliance with NATO standards and navigating export controls.

Section 3: Examples of Specialist Support Technologies

Sector	Description
Secure Communications	Builds encrypted communication networks for first responders and defence. Works with telecom providers to ensure secure, interoperable communications, especially during disasters or major events when commercial networks fail.
Surveillance & Intelligence	Deploys surveillance systems with AI analytics for early threat detection. Experts manage system integration, from cameras to AI software, while ensuring compliance with privacy laws and enhancing situational awareness.
Disaster & Aid Management	Develops platforms for disaster response coordination and resource management. Experts recommend technologies for real-time incident management and satellite-based damage mapping to improve government response efficiency.
UAV Drones	Supplies drones for border surveillance, infrastructure inspection and search and rescue. Experts help governments integrate drones into projects, providing training and maintenance for full operational deployment.
Cybersecurity Systems	Provides national-scale cybersecurity solutions, including threat intelligence platforms and intrusion detection systems. Specialists help governments implement AI-driven threat hunting, incident response and information sharing partnerships.

CHALLENGES FACED BY GOVERNMENTS

Governments face budget constraints, slow procurement cycles, regulatory complexities and a lack of internal tech expertise when adopting advanced technologies. These challenges slow the integration of necessary solutions, underscoring the need for private sector collaboration.

Key Stat: Public procurement cycles take 22 months, 3 times longer than in the private sector.

REFLECTING THE REST OF THE DOCUMENT, WOULDN'T THIS SLIDE BE A SUMMARY OF YAVA'S PORTFOLIO?

YAVA – Beyond Innovation. Beyond Borders | Copyright © 2025 | YAVA.com

Section 4: Case Studies and Success Stories

Case Studies

Real-world examples around the globe illustrate how public-private partnerships have tangibly improved infrastructure security and disaster response:

01 / **Detroit's Project Green Light**
→ Local businesses and Detroit Police partnered to install high-definition cameras and improved lighting, reducing violent crime by 23% and nearly 50% at pilot sites through faster response times and deterrence. Read more

02 / **UAE Counter-Drone Deployment**
→ UAE security agencies partnered with D-Fend Solutions to deploy advanced counter-drone technology, protecting critical infrastructure and public events by rapidly intercepting rogue drones in sensitive airspace. Read more

03 / **FirstNet – U.S. Nationwide First Responder Network**
→ U.S. government and AT&T launched a $46.5 billion 25-year partnership, providing secure, high-speed communication to over 25,000 first responders, improving disaster response and operational coordination. Read more

04 / **UNHCR Blockchain Aid Distribution**
→ UNHCR and Stellar Development Foundation partnered to distribute cash aid via blockchain to displaced Ukrainians, enabling fast, transparent aid delivery without the need for bank accounts or physical cash. Read more

05 / **NATO and Tech Startups – DIANA and Innovation Funds**
→ NATO's DIANA program and Innovation Fund invest in private tech startups, integrating civilian tech like AI and drones into military operations, enhancing situational awareness and advancing defence tech solutions. Read more

And many more…

Section 5: Quantitative Data and Trends

Data & Market Trends

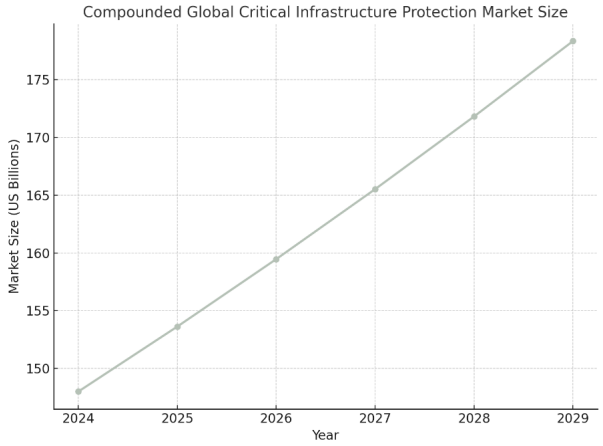


***Figure 1:** Global Critical Infrastructure Protection Market Size - Global spending on critical infrastructure security (physical and cyber combined) is steadily rising. The market is projected to grow from roughly $148 billion in 2024 to $178 billion by 2029. *(Source: Data)*

This approximate CAGR of 3.8% reflects global government initiatives to strengthen infrastructure and the corresponding rise in private sector solutions being deployed. Notably, analysis shows that government regulations and collaborative security efforts (like those led by DHS/CISA in the U.S., and similar programs in Europe and Asia) are key drivers of this growth.

In short, governments are investing more each year in infrastructure protection, often via private vendors, creating a large and growing market for PPPs.

QUANTITATIVE DATA AND TRENDS

Global spending on infrastructure protection is growing, projected to reach $178 billion by 2029. Government partnerships with private firms drive this market, offering both financial returns and enhanced security outcomes.

Key Stat: The infrastructure protection market will grow from $148 billion in 2024 to $178 billion by 2029.

YAVA – Beyond Innovation. Beyond Borders | Copyright © 2025 | YAVA.com

Data & Market Trends

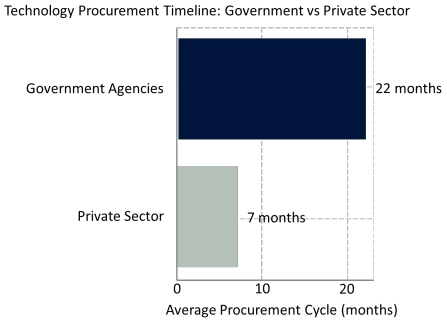


*Figure 2: Technology Procurement Timeline – Government vs. Private Sector. Public procurement of technology averages 22 months in buying cycle time, far slower than the 6–7 months typical in the private sector. *(Source: Data)*

This table highlights a significant challenge: by the time nearly two years pass in a government tech project, private firms have iterated through multiple product cycles. The figure underscores why partnerships are attractive – leveraging ready solutions from industry can compress deployment timelines.

Many delays occur even before formal procurement (e.g. building the business case, which 74% of public sector respondents said takes a long time).

Collaborative approaches, like pilot programs and as-a-service models offered by companies, can help circumvent some of these delays by starting small and scaling faster. Speed is critical in security; a protracted 22-month timeline could mean operating with outdated defences in the interim.

Section 5: Quantitative Data and Trends

Value of Private Sector Procurement	Description	Source
ROI of Resilience Investments	Investing in disaster-resilient infrastructure offers a high ROI, with $1 spent on risk reduction saving $6 to $15 in post-disaster costs. Public-private partnerships in cybersecurity and other resilience projects have measurable economic benefits, such as preventing costly incidents and saving millions in economic losses.	Source
Effect on Risk and Incident Reduction	Public-private cybersecurity partnerships have reduced vulnerabilities by 30%. In public safety, crime reductions of up to 48% have been achieved. For instance, Detroit saw a 23-48% reduction in crime, while Rochester saw a 36% drop in homicides and 29% drop in shootings.	Source
Government Spending Priorities	Governments are allocating funds for innovation partnerships and co-investment programs. Examples include the UK's NSSIF and NATO's 1 billion Euro Innovation Fund. These funds aim to foster public-private collaboration, with over 50 countries launching dedicated funds to facilitate tech partnerships.	https://www.nif.fund/

In summary, public-private collaborations are not just a theoretical trend but a rapidly growing practical reality, driven by increased investment and the delivery of tangible ROI through risk reduction and improved security metrics. The quantitative evidence – from market growth figures to percentage drops in incidents – provides a compelling business case for governments to further embrace partnerships as a cornerstone of their infrastructure protection strategy.

EMBRACE PARTNERSHIPS FOR A SAFER FUTURE

Governments and tech firms must engage in proactive public-private partnerships to safeguard infrastructure against growing threats. By embracing these collaborations, they can accelerate technology deployment, reduce risks and build more resilient communities.

Key Stat: The critical infrastructure protection market will reach $180 billion by mid-decade. WE'RE IN MID DECADE – SHALL WE SAY 2025?

Section 5: Call to Action

Both sides need to address policy and trust challenges to maximize partnership value. This includes developing clear frameworks for data sharing (so that private entities can share threat data without legal hurdles, and governments can share non-sensitive data to help industries innovate).

Public communication is also important – citizens should be made aware of how PPPs are enhancing their safety, to build support for these initiatives. Successful partnerships, like Detroit's Green Light or FirstNet, often cite community engagement and stakeholder buy-in as keys to success. When people understand that a new surveillance system or a new drone program is a joint effort to keep them safe, they are more likely to welcome it.

Finally, it's important to keep *measuring and iterating*. The partnerships should be data-driven, continually evaluating metrics like reduction in incidents, response times, cost savings and public satisfaction. This data should inform adjustments to the partnership approach, ensuring continuous improvement. Luckily, as shown, many partnerships are already yielding positive data – a strong foundation to build upon.

In a world where threats transcend borders and sectors, public-private partnerships have moved from a nice-to-have to a necessity. The strategic trend is clear across NATO, the GCC, Asia and beyond: those nations and cities that harness the ingenuity of the private sector are more secure and resilient than those that do not. The private sector, for its part, gains not only a sizable business opportunity but also the chance to contribute to societal well-being on a grand scale. Companies like YAVA exemplify the win-win: governments get turnkey access to innovation and expertise, while tech providers gain entry to impactful projects and often, sustainable revenue streams.

The time to act is now. Waiting means falling further behind the curve of technological change and threat evolution. By embracing partnerships, governments can turn perceived weaknesses (budget limits, red tape, skill gaps) into strengths – leveraging private funding, efficiency and knowledge. Likewise, tech companies that embrace the complexity of public sector work can open new frontiers of innovation (think of the advancements spurred by NASA's partnerships in space, now being mirrored in cybersecurity and defence). Both must approach the relationship in good faith, with shared goals and clear agreements, as evidenced by the success stories cited.

YAVA – Beyond Innovation. Beyond Borders | Copyright © 2025 | YAVA.com

Section 6: Call to Action

Embrace Partnerships for a Safer Future

Global governments and technology providers must proactively engage in public-private partnerships to protect critical infrastructure and the public at large. The threat environment – cyberattacks, terrorism, natural disasters, pandemics – is growing more complex and severe. No single entity, public or private, has all the solutions. But together, they do.

For governments, the call to action is to reduce barriers and actively seek specialist partners like YAVA in their security and resilience initiatives. This means updating procurement models to be more agile (e.g. using pilot contracts, innovation challenges, PPP frameworks) so that private innovators can contribute to public missions without undue delay. It also means allocating funding specifically for partnerships – whether through venture funds, grants or co-funded projects – recognising that a modest public investment can unlock larger private sector contributions.

Governments should continue to foster information-sharing alliances and include private experts in strategic planning. The data and case studies show that when they do, the payoff is better technology, faster implementation and stronger security outcomes.

For private sector companies, the call is to **step up and engage with public needs**. Technology providers should view governments not just as clients, but as true partners in co-developing solutions to society's toughest challenges. This might mean tailoring products for public use cases, obtaining necessary certifications and being patient with bureaucratic processes – often facilitated by specialist firms like YAVA that know how to navigate these waters. The opportunity is enormous: with critical infrastructure protection spending nearing $180 billion by mid-decade (*link*), there is both a market and a moral imperative to help defend vital systems. Companies that succeed in this space tend to combine innovation with trust-building – showing public agencies that they can deliver reliably and securely at scale. By collaborating with intermediaries (consultants, integrators) who understand government context, tech firms can bridge cultural gaps and ensure their solutions truly address public sector pain points.

Section 7: Conclusion

Conclusion

In conclusion, the protection of public and critical infrastructure in the 21st century is a collective responsibility, requiring united action and strategic collaboration across all sectors to ensure resilience and security. The data is convincing, the case studies are inspiring and the path forward is for more regions and sectors to replicate these successes. By forging strong public-private partnerships, we can deploy advanced technologies smarter and faster, build more resilient communities and stay ahead of those who would seek to do harm. Governments and tech specialists should seize this moment to collaborate – the security and prosperity of our societies depend on it.

Copyright © 2025 YAVA London Ltd ("YAVA"). All rights reserved. The content provided herein is for informational purposes only and does not create any warranty of any kind. Any data contained herein is notional. Actual results and experiences may vary.

YAVA – Beyond Innovation. Beyond Borders | Copyright © 2025 | YAVA.com

Section 8: Current Mandates

Mandates (Past 6 Months)

01 / **RAKEZ**
→ YAVA accelerates business entry into the UAE, securing infrastructure and government partnerships for smooth expansion across key sectors.

02 / **ELB&T Global Expansion**
→ YAVA drives ELB&T's market growth, crafting targeted strategies for mobility, eco-tech and defence sectors across Europe, the Middle East and India.

03 / **Peace Drive Initiative**
→ YAVA leads the Peace Drive from Delhi to Dubai, managing stakeholder engagement, sponsorships and aligning with UNSDGs for lasting environmental impact.

04 / **UK-India Innovation Summit 2025**
→ YAVA coordinates UK-India partnerships, focusing on deep tech, AI and critical infrastructure, positioning Kolkata as an innovation hub.

05 / **STaR.AI**
→ YAVA shapes policies for responsible AI, advising leading institutions to ensure systems meet legal, societal and environmental standards.

06 / **Terminus Technologies**
→ YAVA expands Terminus' market presence in India and the UAE, driving commercial applications in smart city infrastructure, security and defence.

Commented [NI8]: Should this be included in the case studies/success stories section?

Commented [NI9]: Do we need to clarify who ELB&T are? What they do etc

Commented [NI10]: Maybe this needs to be clarified - what is the peace drive

5	YAVA.com	



GOVERNMENT & SECURITY IT SOLUTIONS PROVIDERS.