[1]Mohit Sharma,
[2]Sajud E.,
[3]Naranjan Goklani,
[4]Krishna Chaubey

Public-Private Partnerships in Cybersecurity: A Strategic Approach to National Threat Management

Journal of Electrical Systems

Abstract: - With the rapidly evolving profile of cyber threats, achieving national cybersecurity can no longer be solely the state's responsibility. Public-private partnerships (PPPs) have become the key mechanism for bridging the capability, intelligence, and response gap between governments and private sector actors, who wield immense influence over strategic national infrastructure. Drawing on an international case study and Comparative public policy model analysis. This research examines the strategic utility of PPPs for the management of national threats. It critically examines the structural, legal, and operational barriers to effective collaboration and sets out a governance model—S.A.G.E.™—created to institutionalize PPPs for the achievement of long-term resilience. Based on the analysis of the United States, the European Union, India, Israel, and Singapore, this paper illustrates How cooperative management of cybersecurity enhances national security, enhances threat information sharing and supports a multi-layered defense strategy. This paper finds that coordinated policy approaches, joint Responsibility, and secure engagement frameworks are central to developing. Effective public-private partnerships for the cyber era.

Keywords: information, partnerships, management, PPPs

Introduction: In today's digitized world, where cyberspace has become an important platform for commercial activities as well as national security, the demand for cybersecurity has transformed from a single technical concern to a strategic imperative. Cybersecurity has moved beyond its status as an information technology concern; it has become a part of national security. Modern governments are confronted with a fast-changing array of adversaries, ranging from transnational cybercrime syndicates to state sponsors. These actors have a tendency to attack the virtual infrastructures controlled by the private sector, which has control over 80% of a country's critical assets, such as energy grids, financial networks, and telecommunications networks [1]. This is an operations paradox: while the state has the responsibility for national security, the operation and governance of the digital world is largely within private industry's control. In such an arrangement, traditional top-down government action is insufficient. Cybersecurity defense works best through an interdependent governance model in which government and private industry can operate as co-equal partners in the prevention of threats, detection, response, and recovery.

Public-private partnerships (PPPs) offer such a framework. PPPs are basically examples of structured collaboration between the state and private sector parties. For cybersecurity, PPPs facilitate real-time sharing of intelligence on threats, coordinated response to incidents, shared

risk assessment, and shared investment in protection technology. PPPs leverage the strategic guidance and legitimacy of governments with the innovation and infrastructure management capabilities of the private sector. Yet, even though the concept of PPPs has gained popularity globally, its implementation

remains unbalanced. Legal ambiguity, trust deficits, incentives misalignment, and lack of standardized frameworks continue to hinder their efficiency. Moreover, as the threats in the cyber world are becoming increasingly advanced, so should the mechanisms for cooperation. Ad-hoc coordination is no longer enough; instead, there is a need for a strategic, institutionalized, and scalable approach that incorporates PPPs into

the fabric of national cybersecurity governance. Through a critical assessment of PPP models in the United States, European Union, India, Singapore, and Israel, we set out the best practices and areas for improvement. We then offer the S.A.G.E.™ model—Safety and Security, Accountability and Ethics, Global Governance, Engagement, and Privacy—as a unified strategy for increasing public-private cybersecurity collaboration. By

[1]Amazon Web Services Email mailmohitsharma1010@gmail.com

[2](Alumnus),Pace University Email Selinjulliparambil@pace.edu

[3]Amazon Web Services Email- narangoklani@gmail.com

[4]Ernst and Young ,Email -Krish89.chaubey@gmail.com

adopting this model, governments can align stakeholder efforts, break down operational silos, and develop strong cyber ecosystems that can repel national-scale threats.

Finally, this study calls for the institutionalization of PPPs within the national cybersecurity platforms, not as an auxiliary function but as a natural pillar of contemporary threat management.

2. The Strategic Importance of Public-Private Partnerships on Cybersecurity

2.1 National Reliance on Private Infrastructure

Modern societies are effectively reliant on computer networks controlled by private companies. In the US alone, nearly 85% of key infrastructure—transportation systems, telecommunications networks, finance networks, and power grids—are owned by private companies [2]. Thus, while the state must maintain national stability, it has no direct control over the networks that are most vulnerable to cyberattacks. The same patterns can be seen across the European Union, India and Southeast Asia.

As the digital infrastructure underlying national economies becomes increasingly recognized as a target for criminal and geopolitical cyber behavior, the role of the private sector in defending it is not only important But crucial. The 2021 Colonial Pipeline ransomware attack caused severe fuel supply disruptions along the U.S. East Coast, demonstrating The potential of a single private sector failure to have a broad national consequences [3].

2.2 Closing the Capability-Responsibility Gap

PPPs bridge the structural divide between capability and responsibility. Governments offer regulatory authority, intelligence know-how, and diplomatic clout. Private companies provide technical capability, innovation, and ownership of key assets. Together, these assets create a synergistic system for cyber resilience.

For instance, the United States' Joint Cyber Defense Collaborative (JCDC), which is headed by the Cybersecurity and Infrastructure Security Agency (CISA), unites federal agencies and top technology firms to actively counter cyber attacks [4]. It is a demonstration of how organized collaborations can provide combined threat landscapes, enabling preventive measures and shared incident response.

2.3 Combining Motivations to Engage

Despite the obvious need for cooperation, private sector entry into PPPs is generally restrained by risk aversion. The main concerns are reputational risk, confidentiality of information, loss of competition, and unclear liability arrangements. To stimulate participation, governments need to create policy levers such as

•Legal safe harbors for disclosure of incidents

• Investment tax credits or vouchers for cybersecurity

• Co-branded certification for complying companies

The European Union's NIS2 Directive places mandatory risk management and incident reporting duties on operators of critical services, but also offers support through national authorities [5]. This balance of obligation and Incentives can be utilized as a template for encouraging greater private-sector involvement.

2.4 Cybersecurity as a Vital National Security Imperative

The distinction between national security and cybersecurity has become blurred. Advanced ransomware operations now bring down public infrastructure. Nation-state actors infiltrate supply chains to insert long-term espionage platforms. The 2020 SolarWinds attack, blamed on a Russian intelligence agency, hacked multiple U.S. federal organizations and Fortune 500 firms [6]. Likewise, the Log4j vulnerability exposed billions of devices globally to remote code execution attacks [7].

These events prove that cyberattacks, even non-military cyberattacks, can destabilize economies and governments. Cyber resilience, as such, is a public good—one that requires a multi-stakeholder approach.

2.5 Building Resilience through Collaborative Readiness

Successful PPPs extend beyond reactive threat sharing. They institutionalize collective preparedness through:
• Cross-sector cybersecurity exercises

• Real-time threat intelligence exchanges

• Joint risk assessment and mitigation planning

• Joint development of cybersecurity standards

India's national computer emergency response team, CERT-IN, works with internet service providers and banks to run nationwide cyber simulations [8]. The joint exercises not only increase technical readiness but also build trust, praised as the most important asset in successful public-private cyber defense.

3. Global Frameworks of Public-Private Partnerships in Cybersecurity

Public-private partnerships (PPPs) within the realm of cybersecurity have manifested in various ways across the globe, influenced by the unique regulatory frameworks, the sophistication of digital infrastructure, and the prevailing threat landscape within each nation. Some countries emphasize voluntary cooperation models, whereas others have adopted mandatory legislative measures to enforce collaboration. This section examines five notable case studies—the United States, European Union, India, Singapore, and Israel—to gain insight into the development and implementation of PPPs.

3.1 United States: Collaborative Efforts via CISA and JCDC

The United States is generally considered to be leading in the operationalization of cybersecurity PPPs. The Cybersecurity and Infrastructure Security Agency (CISA) is one of the lead agencies responsible for overseeing partnership efforts with the private sector. Organized as a part of the Department of Homeland Security (DHS), CISA oversees federal cybersecurity programs in Sixteen key critical infrastructure sectors [9].

One of the key developments is the establishment of the Joint Cyber Defense Collaborative (JCDC) in 2021. The JCDC unites major federal agencies like the NSA, FBI, and ODNI with major technology partners like Microsoft, Google, CrowdStrike, and Amazon Web Services. The collaboration allows for:
•Joint creation of shared threat intelligence

• Real-time sharing

•Coordinated response to emerging threats (e.g., Log4j, SolarWinds)

The U.S. also supports Information Sharing and Analysis Centers (ISACs)—sector-specific discussion forums for private companies to exchange threat information under legal safe harbors [10].

Besides, Executive Order 14028, signed in May 2021, mandates greater coordination between public and private actors through logging of cybersecurity incidents, zero-trust adoption, and software supply-chain security [11]. These measures brought the U.S. closer to a federated but disciplined PPP model, balancing regulatory control with private sector reactivity.

3.2 European Union: NIS and NIS2 Directives Regulatory Requirements

The European Union (EU) has a more institutionalized, legalistic approach to public-private cooperation on cybersecurity. Its key tool is the 2016 Directive on Security of Network and Information Systems (NIS). The new NIS2 Directive, adopted in 2022, expands the scope and enforcement authority of member states.

Under NIS2:

• Critical and important actors (e.g., energy, transport, finance, digital infrastructure) are required to put in place cybersecurity risk management measures.

• Incidents need to be reported to the national authorities.

National CSIRTs act as a central point for facilitating intersectoral exchange.

The European Union Agency for Cybersecurity (ENISA) supports member states through offering guidelines, coordinating cyber exercises (e.g., Cyber Europe), and facilitating sectoral cooperation [12]. A striking feature of the approach in the European Union is a bias towards realizing harmonization among several jurisdictions. Though this does present an added layer of complexity, it at the same time brings up the floor level of Resilience by making every important infrastructure provider legally required to be a member of public-private partnerships on cybersecurity.

3.3 India: National Critical Infrastructure and CERT-IN Frameworks

India has made serious efforts towards having a formal public-private partnership in cybersecurity. The Indian Computer Emergency Response Team (CERT-IN) acts as the nodal agency for threat intelligence and incident response coordination. It has entered into partnerships with banks, ISPs, telecom service providers, and other key sectors [13]. India established the National Critical Information Infrastructure Protection Centre (NCIIPC) in 2014, which is under the National Technical Research Organisation (NTRO). NCIIPC is designed for protection of infrastructure in banking, telecommunication, transportation, and power sectors. NCIIPC also has a system of formal registration and audit of critical private institutions.

Most notably, CERT-IN has launched initiatives such as:

• Public and private sector organizations cyber cybersecurity exercises every year.

Vulnerability coordination projects with top vendors

• Public warning and mitigation steps focused on impending threats.

In 2022, CERT-IN released guidelines compelling private companies to:

• Report within six hours of cybersecurity incidents

•Keep logs for 180 days• Sync timekeeping devices with the Indian Standard Time (IST). Although the directive was criticized for its compliance requirements, it reflected India's growing regulatory boldness in shaping public-private cyber defense cooperation [14].

3.4 Singapore: Cybersecurity as an Inclusive National Effort

Singapore has emerged as a cybersecurity policy leader. Singapore's 2018 Cybersecurity Act offers an open legal regime for PPPs. The Singapore Cyber Security Agency (CSA) leads national initiatives and closely works with critical information infrastructure (CII) owners, mostly private operators.

The major initiatives are:

•ASEAN-Singapore Cybersecurity Centre of Excellence, with the responsibility of training public and private stakeholders Safer Cyberspace Masterplan is focused on the security of digital infrastructure used by citizens and businesses.

• The Cybersecurity Labelling Scheme (CLS) promotes compliance with underlying security standards by device makers.

Singapore's PPP model is underpinned by:

• Statutory requirements of CII industries to be audited and drilled

• Real-time alerting and vulnerability disclosure programs

• Targeted grants to facilitate private cybersecurity innovation

This is an integrated "whole-of-nation" response that makes Cybersecurity is not just a government issue, but everyone's concern in society[15].

3.5 Israel: Defense-Driven Innovation in Cybersecurity Cooperation

Israel's national cyber policy reflects its military-tradition of strategic planning and operational readiness. The Israel National Cyber Directorate (INCD) initiates PPPs according to the guiding vision of national resilience by private innovation.

The INCD collaborates closely with: • Technology firms and cybersecurity startups (typically founded by graduates of Unit 8200) • University research centers and institutions • Operators of essential services (e.g., transport, electricity, water)

Israel, in 2016, initiated the CyberNet platform—a cloud-based, safe platform for sharing indicators of compromise (IOCs) and threat intelligence across sectors [16]. Israel also holds CyberStorm exercises, practicing national-level cyberattacks under the guidance of private sector partners. The government offers tax

credits and research, and development grants to finance development in cybersecurity, thus compelling the private sector to treat security as both a social obligation and a business opportunity. The PPP model of Israel illustrates how shared national identity, legal certainty, And trust can create a strong and resilient cybersecurity ecosystem.

Summary of Global Approaches

Country	Model Type	Legal Mandate	Key Agency	Private-Sector Role
USA	Federated Voluntary	Medium	CISA/JCDC	Threat sharing, response, R&D
EU	Regulatory Binding	High	ENISA, CSIRTs	Mandatory risk controls, reporting
India	Hybrid Directive	Increasing	CERT-IN, NCIIPC	Cyber drills, logging, disclosure
Singapore	Whole-of-Nation	High	CSA	Legal compliance, co-audits, grants
Israel	Innovation-Driven	Medium-High	INCD	Collaborative R&D, intelligence sharing

3.6 Comparative Analysis of Global PPP Frameworks

Though each nation's PPP framework architecture is determined by its geopolitical environment, regulatory culture, and level of digital development, most of the critical dimensions are found to be comparable. They are governance frameworks, based in law, stakeholder involvement, operational sophistication, and incentive regimes.

Examination of the five models (U.S., EU, India, Singapore, and Israel)

uncovers strengths and inherent systemic pitfalls.

3.6.1 Centralized vs. Distributed Governance Framework

The U.S. approach is defined by its federated, distributed governance, with semi-autonomous agencies such as CISA and JCDC supported by sector-specific ISACs. Flexibility may be achieved with this approach but runs the risk of fragmentation in the absence of coordination mechanisms.Singapore and Israel have, however, adopted centralized governance models, where one national agency (CSA and INCD, respectively) leads strategy, implementation, and outreach across public and private sectors. The EU model is in a hybrid position. Although every member state retains sovereignty over its execution by national CSIRTs, coordination at the

higher level falls on ENISA. The two-layered design encourages harmonization but demands great intergovernmental cooperation.

India's approach is moving from a decentralized to a more centralized structure, that is, through increased powers of CERT-IN and the increasing role of NCIIPC. Enforcement and responsiveness vary by sector, especially in rural and semi-urban regions.

3.6.2 Legal and Regulatory Framework

One of the most significant distinctions is whether membership in PPPs is voluntary or legally required. The U.S. mainly uses voluntary participation based on executive orders, guidelines, and incentives. The EU and Singapore, in contrast, compel adherence to specific cybersecurity standards with binding legislation (e.g.,NIS2 Directive and Singapore's Cybersecurity Act).

Israel's PPP model is quasi-mandatory in nature, employing legal means and a A strong national security narrative to coerce participation. India is also moving towards closer regulation through CERT-IN guidelines and data protection legislation, though it is encountering legal hurdles as a result of resistance from the industry.

3.6.3 Level of Stakeholder Involvement

Their coverage and intensity also vary. Singapore and Israel are instances of a "whole-of-nation" approach toward bringing academia, industry, government, and society together in planning an effort in cybersecurity. Such countries actively cultivate cybersecurity R&D through the portals of innovation districts and defense-tech accelerators.

The U.S. model is deeply involved with large technology vendors and infrastructure providers, but suffers from gaps in reaching small- and medium-sized enterprises (SMEs). Likewise, the EU model, While extensive, it has demonstrated uneven engagement across sectors and members states, particularly in newer or economically weaker areas. India's model is adding state-by-state cybersecurity coordination centers, but it remains highly centralized and has not scaled up much into broader digital supply chains or MSMEs.

3.6.4 Incident Coordination and Operational Maturity

Both Israel and the United States, operationally mature as they are, are characterized by advanced incident detection and response infrastructure. The proactive vulnerability management through the joint model JCDC has been established with private cybersecurity organizations, and Israel's national CyberNet, which enables real-time correlation of threats across sectors are instances.

Singapore has incorporated real-time alerting capability into its national SOC and has one of the most stringent cyber audit regimes in Asia. The EU has interoperability problems across member states but is improving through regional joint exercises (e.g., Cyber Europe).

India's CERT-IN has also improved at carrying out national drills, albeit uniform implementation issues persist.

3.7 Common Challenges and Lessons

In spite of the national divergence, common strands of challenge reappear through comparative analysis:
• **Trust Deficit**: Non-state actors refuse to provide sensitive information to governments owing to the danger of regulatory punishment or harm to their reputation. Even in experienced PPP settings like the U.S.,

firms are slow to report incidents, fearing repercussions from the law.

•**Incentive Discrepancy**: Most public-private partnerships are founded on altruism as opposed to strategic incentives. Absence of tax incentives, liability protection, or purchasing incentives discourages volunteering, most notably among small firms.

• **Legal and Jurisdictional Uncertainties**: Transborder data flows, differing definitions of "critical infrastructure," and parallel mandates blur compliance uncertainty. The EU has attempted to minimize this by way of NIS2, but fragmentation persists.

• **Technical Standardization Gaps**: While bodies like NIST (United States), ENISA (European Union), and CSA (Singapore) offer cybersecurity standards, their sectoral or voluntary nature is likely to discourage large-

scale adoption. Standardized benchmarks in information exchange protocols, risk classification, and post-breach disclosure processes are required.

• **Private Sector Capacity Deficit**: In the majority of developing economies, even service providers of essential services are not following basic cyber hygiene.

The ability of the private sector to provide significant contributions to PPPs is hence imbalanced across sectors and countries.

These enduring pressures lend weight to a universal governance framework that is robust enough to accommodate national contexts while also strong enough to ensure uniform cross-sector cooperation. It is where the S.A.G.E.™ framework, initially developed to govern AI, can be adapted and applied to cybersecurity PPPs.

3.8 Shifting to the S.A.G.E. System

The S.A.G.E.™ approach—safety and security, accountability and ethics, global governance, and engagement and privacy—was originally designed as an international AI policy harmonization paradigm. Its rational design, however, also is well-suited to the governance issues raised by cybersecurity PPPs. Each pillar directly responds to one of the systemic failures evidenced across the case studies:

• **Protection and Security**: Aligns with the requirement for mutual protection of critical infrastructure by harmonized technical procedures and forward-looking cooperation.

• **Accountability and Ethics**: Addresses the trust deficit and liability by defined roles, legal safeguards, and transparency norms.

• **Global Governance**: Solves regulatory fragmentation by offering a scalable meta-framework that can be embraced by industries and nations.

• **Engagement and Privacy**: Encourages stakeholder participation by providing privacy assurance, shared training, and ethical information sharing.

Through embedding these blocks in national cybersecurity plans, the government organizations are able to transform public-private partnerships from hoc arrangements into formal structures that ensure long-term resilience.

4. Building Public-Private Partnerships in Cybersecurity: The S.A.G.E.™ Framework

As established in the above sections, the global use of public-private Partnerships to improve cybersecurity are bedeviled with structural contradictions, trust deficits, regulatory fragmentation, and incentive imbalances. Consequent upon this, this paper proposes an application of The S.A.G.E.™ framework—designed originally to harmonize international AI governance—into a combined strategy to institutionalize and simplify PPPs as a means to counteract cybersecurity threats. S.A.G.E.™ is a system with four primary pillars:

1. Safety and Security

2. Accountability and Ethics

3. International Governance

4. Engagement and Privacy

Each pillar provides a particular intervention to address the overall issues of PPPs in practice. Together, they constitute an integrated governance model that can promote national cybersecurity as well as international interoperability.

4.1 Safety and Security: Collective Resilience Across Critical Infrastructure In information security, Safety and Security mean the technical and operational controls to safeguard private and public infrastructures. This intrinsic nature stresses that security measures should not be siloed into one or other sector But seek an integrated endeavor that is crafted through collaborative planning,visionary investment, and ongoing threat

evaluation.

4.1.1 Integrated Threat Intelligence

One of the most basic advantages of PPPs is the ability to build a federated threat intelligence platform, where signals are collected from government intelligence agencies and commercial monitoring software. A more sophisticated version of this pillar would involve:

- Federated Cyber Attack Reporting Platforms
- Industry threat correlation mechanisms
- Utilization of machine learning and AI for predictive threat

Modeling the JCDC of the U.S. and Israel's CyberNet is anexcellent model for this purpose, but their architectures are still not globally standardized or interoperable. S.A.G.E.™ promotes a multi-stakeholder protocol development process, optionally chaired by ENISA or NIST, to develop cross-border interoperability standards.

4.1.2 Sector-Specific Drills

Penetration Testing Safety encompasses resilience testing by red teaming, penetration testing, and disaster recovery exercises. By mandating such testing on critical infrastructure providers and public agency coordination, governments can instill readiness into institutional environments. India's CERT-IN cyber exercises are a case in point, though take-up remains uneven by sector. Making this a requirement of operational licensing or sectoral certification would encourage compliance.

4.1.3 Pre-Emptive Technology Investment

Governments can encourage innovation in pre-emptive defense by: • Funding the development of zero-trust architectures • Offering tax credits to secure-by-design infrastructure. • Funding public-private cybersecurity laboratories. This not only strengthens the national defense system but also synchronizes the public security objectives with private research and development incentives.

4.2 Accountability and Ethics: Legal Trust and Shared Liability Trust is repeatedly called the weakest link in public-private cybersecurity initiatives. Firms do not want to risk regulatory sanction for breach notices; governments are concerned about reliance on opaque private technology. The Accountability and Ethics pillar offers a route to structural trust, on the basis of transparency, clear roles, and ethical duties.

4.2.1 Specific Responsibilities and Legal Safeguards

Governments ought to pass into law the extent of responsibility of each PPP stakeholder. They are:

- Creating standards for mandatory reporting
- Establishing liability thresholds in cooperative incident responses
- Creating "safe harbor" provisions for good-faith disclosures

For example, the EU NIS2 Directive sets out narrowly defined categories of "essential" and "important" entities and assigns each a specific task. Such a framework could be emulated for application to other jurisdictions and included in private-contractual contracts.

4.2.2 Ethical Data Sharing Frameworks

Public-private data sharing should be regulated by access protocols that are ethics-based in order to ensure:

- Minimal disclosure principles
- Role-based access control
- Usage tracking and auditability

A generic "cyber incident data license" could be developed, much like the open data licenses applied in the public health or environmental sectors.

4.2.3 Transparent Governance Process

Both industries should be willing to publish:

- Annual cybersecurity posture reports
- Incident response after-action review (as required, redacted)
- Remedy plan and audit results

This transparency engenders public confidence, stimulates ongoing refinement, and makes inter-sector accountability the rule

4.3 Global Governance: Synchronizing Across Borders and Sectors

Threats online extend beyond geographic borders. Global Governance under S.A.G.E.™ cross-border harmonization of regulation is therefore aimed at developing internationally harmonized PPP measures.

4.3.1 Cross-Jurisdictional Regulatory Interoperability

In today's interconnected world, it's crucial that we establish shared expectations for cybersecurity across different legal systems. To achieve this, we need a set of frameworks that focus on three key areas:

- Defining what constitutes critical infrastructure
- Creating guidelines for the timing of breach disclosures
- Developing global standards for classifying incidents

For instance, the Budapest Convention on Cybercrime and the OECD Guidelines for the Security of Information Systems lay the groundwork, but we need to tailor these to include perspectives from public-private partnerships (PPPs). Organizations like ISO, the G7 Cyber Expert Group, and the UN Open-Ended Working Group on ICT Security can play vital roles in making this collaboration successful.

4.3.2 International PPP Clearinghouses

S.A.G.E.™ foresees the creation of Cybersecurity Public-Private Partnership Clearinghouses within regional structures (e.g., ASEAN, EU, AU) to:

- Catalog national PPP programs
- Pair cross-border capacity-building partners
- Discuss non-sensitive best practices and resources.

These clearinghouses will eliminate fragmentation and stop redundant effort.

4.3.3 Joint Standards for Secure Innovation

Emerging technologies—particularly AI in cybersecurity—need shared guardrails. PPPs should jointly:

- Define fundamental security needs for artificial intelligence-based cybersecurity defense systems.
- Adopt audit procedures for black-box tools
- Create responsible innovation charters

This pillar connects back to your initial S.A.G.E.™ application in AI governance—developing a crosswalk between AI risk frameworks and cybersecurity ecosystems.

.

S.A.G.E.™ Implementation Blueprint

Pillar	Key Objectives	Example Application
Safety & Security	Federated threat intelligence, joint drills, secure R&D	U.S. JCDC, Israel CyberNet
Accountability & Ethics	Liability clarity, data ethics, transparent audits	EU NIS2, Singapore audit regimes
Global Governance	Harmonized laws, PPP clearinghouses, joint standards	ISO/ENISA/OECD-driven alignment
Engagement & Privacy	Inclusive stakeholder design, privacy-by-design	Singapore Masterplan, Israel academia model

4.5 The Strategic Value of S.A.G.E.™ in National Threat Management

Unlike fragmented public-private partnership approaches, S.A.G.E.™ is one unified governance model, implementable and adaptable, and allows policymakers to:

- Develop policy toolkits for every pillar
- Assess PPP maturity using pillar-specific KPIs
- Invest according to risk and inclusion gaps priority

Above all, the model makes PPPs exportable and scalable across borders. It balances the private sector energy with regulatory powers, and adds transparency, equity, and foresight to long-term national planning for cybersecurity.

5. Policy Implications and National Security Relevance

5.1 Reframing Cybersecurity as Shared Sovereignty

As boundaries between public and private digital spaces continue to erode, cybersecurity governance must move beyond conventional command-and-control models. Governments need to adopt shared sovereignty frameworks, under which private actors become institutionalized custodians of national security. It needs legal tools that:

- Define shared accountability
- Encourage active participation
- Protect private sector participants against inappropriate legal liability.

The S.A.G.E.™ system codifies this balance by distributing responsibility across four operational pillars, while still exercising national oversight.

5.2 Cybersecurity as a Public Good

Cybersecurity resilience generates good externalities: it protects not just individual companies but society as a whole. Just like public health or environmental protection, it merits public funding and government support. Governments should:

- Create public funding pools for PPP cybersecurity programs
- Address threat intelligence as a non-competitive national resource

- Enforce the "polluter pays" principle on reckless digital behavior

By defining cybersecurity as a public good, policymakers can defend more engaged interaction with industry without sacrificing market neutrality.

5.3 Regulatory Innovation and Agile Governance

Static rules cannot keep up with the evolving cyber threat environment. It is thus essential that regulatory agencies

- Create sandbox environments for testing the PPP model
- Establish multi-stakeholder forums for on-the-spot consultation
- Implement adaptive licensing for industries such as AI-based cybersecurity solutions

These adaptive structures complement the Global Governance and Engagement dimensions of the S.A.G.E.™ model well, enabling an efficient flexible mode of governance that is not over-constricting.

5.4 International Cyber Diplomacy and Norm-Setting

Lack of standardization at the international level for PPPs in cybersecurity is a matter of serious concern. Different data rules, definitions of key infrastructure, and disclosure obligations are barriers to transnational cooperation. Governments can, through regional platforms and multilateral organizations,

- Market S.A.G.E.™ as a meta-framework for PPP alignment
- Coordinate cross-border cyber incident exercises
- Establish regional Cyber PPP Hubs for knowledge and R&D sharing

The emergence of cyber partnerships like the EU's Cyber Solidarity Act or the Quad's Cybersecurity Partnership signals that cyber diplomacy is evolving and ready for more PPP incorporation.

6. Implementation Framework and Strategic Recommendations for S.A.G.E.™

In the effort to translate the S.A.G.E.™ framework from a conceptual model of governance to a productive tool of cybersecurity collaboration, operationalization processes, measurement, and contextualization processes need to be highlighted by countries. This section describes executable implementation strategies mapped against each pillar, then illustrating maturity metrics and interdisciplinary pathways.

6.1 National-Level Implementation Strategy

Governments need to implement S.A.G.E.™ on a phased basis according to the following structure:

Phase 1: Institutional Mapping and Legislative Alignment

- Conduct a PPP ecosystem audit to identify key stakeholders, legal vulnerabilities, and existing initiatives.
- Synchronize national cyber law, data protection regulations, and critical infrastructure requirements with each S.A.G.E.™ pillar.
- Determine duplicative or conflicting mandates among regulators, ministries, and industry associations.

Phase 2: Stakeholder Consultations and Framework Localization

- Involve public agencies, private sector companies, civil society, and research institutions in multi-round consultations.
- Make S.A.G.E.™ relevant to national context—for instance, highlighting "Accountability and Ethics" in high-risk industries such as finance and healthcare, or "Global Governance" in export-based economies.

Phase 3: Pilot Projects and Risk Modeling

- Initiate pilot PPPs under each of the pillars. For example:Security and Safety: Collaborative Security Operation Centers for utility grid companies.
- Engagement & Privacy: Privacy-enhancing technologies for threat-sharing portals
- Utilize simulations and cyber range testing to confirm resiliency and find integration issues.

Phase 4: National Integration and Capacity Building

- Expand successful pilots to national programs, with legal mandates, performance-based funding, and open participation.
- Support training and certification programs for public and private sector cybersecurity professionals that adopt S.A.G.E.™ principles.
- Incorporate PPP performance reviews into national digital risk planning and audit frameworks.

6.2 S.A.G.E.™ Public-Private Cybersecurity Partnership Maturity Model

To gauge S.A.G.E.™-based implementation growth and success, a Cybersecurity PPP Maturity Model can be used. There are five levels to this:

Maturity Level	Description	Characteristics
Level 1: Initial	Ad-hoc coordination, no formal agreements	Informal communication, reactive response only
Level 2: Structured	MOUs or legal mandates, limited sector scope	Incident reporting norms, baseline drills
Level 3: Integrated	Multi-sector coordination, shared infrastructure	Federated threat portals, cross-sector playbooks
Level 4: Strategic	Embedded in national security doctrine	Joint simulations, legal safe harbors, co-funded labs
Level 5: Harmonized	Regional/international PPP alignment	Cross-border agreements, global framework alignment (e.g., S.A.G.E.™)

6.3 Metrics for Continuous Assessment S.A.G.E.™ calls for outcomes-based instead of output-based measurements. Recommended Key Performance Indicators (KPIs) by pillar are:

Pillar	Example KPIs
Safety & Security	% of critical infrastructure participating in joint drills; MTTR (mean time to respond) across sectors
Accountability & Ethics	% of incident disclosures protected under liability shields; number of public-private audit reports published annually
Global Governance	Number of regulatory interoperability agreements; participation in transnational drills or clearinghouses
Engagement & Privacy	SME participation rate in national PPPs; number of privacy-by-design features implemented in joint systems

6.4 Sector-Specific Application Pathways

S.A.G.E.™ is adaptable to address the needs of high-priority sectors:

Finance

- Form legitimate PPP clusters with regulators, fintech institutions, and banking institutions.
- Implement real-time fraud intelligence systems with privacy filters (E&P).
- Encourage ethical algorithm auditing and resilience scoring (A&E).

Energy

- Incorporate OT/IT convergence simulation exercises into a safety-first framework (S&S).
- Share patch intelligence among operators with regional coordination (G.G.).

Healthcare

- Encourage cyber hygiene checks of public-private hospital networks (S&S).
- Require ethical management of medical data following incidents (A&E).

Telecommunications

- Use cross-sector authentication standards (S&S, G.G.).
- Work with civil society to counter disinformation threats (E&P).

6.5 Regional and International Paths of Implementation

The S.A.G.E.™ model can reach out to multilateral cooperation through:

6.5.1 Regional Adaptation

- **EU**: Implement S.A.G.E.™ into ENISA's long-term strategic plan along with NIS2 compliance protocols.
- ASEAN: Employ S.A.G.E.™ to coordinate varying levels of PPP maturity and overcome gaps in cybersecurity capacities.
- **African Union**: Incorporate into Smart Africa's digital infrastructure frameworks, emphasizing inclusive cyber protection.

6.5.2 International Standards Setting and Coordination

Advocate S.A.G.E.™ as soft-law norm at international cybersecurity platforms (e.g., Munich Security Conference, UN OEWG on ICTs). • Encourage adoption by multi-stakeholder groups such as the G7, OECD, or Quad Cyber Group. • Ensure conformity with ISO/IEC 27110 on information sharing across sectors and cooperative structures for cyber defense

. **6.6 Strategic Enablers for Long-Term Success**

For S.A.G.E.™ to be more than a theoretical construct, several enablers must be institutionalized:

- **Political Commitment**: Governments must prioritize cybersecurity PPPs within national security doctrines and allocate sustained budgets.
- **Long-term Financing:** PPPs are usually unsuccessful because of short-termism. Long-term financing tied to resilience indicators is essential.
- **Public Trust Campaigns**: Public outreach programs—such as national cybersecurity awareness weeks—can help lower resistance to data-sharing programs and encourage civic cooperation.
- **Legal Modernization**: Current telecommunications, information technology, and liability laws require updating to reflect the modern dynamics of collaborative digital risk management. With strong policy intentions and intersectoral backing to back it, S.A.G.E.™ can evolve from a governance proposal to a global model of cybersecurity resilience.

Conclusion

Cybersecurity is no longer a domain that governments can safeguard in isolation. Since most digital infrastructure and innovation are in the private sector, public-private partnerships are not a choice—they are necessary. But today's global reality is that PPPs are generally hampered by legal uncertainty, trust deficits, regulatory fragmentation, and asymmetric operational readiness. This research paper has shown that although nations such as the United States, EU member states, India, Singapore, and Israel provide exemplary PPP models, they are still plagued by systemic misalignments. The suggested S.A.G.E.™ model provides a scalable, governance-led approach to institutionalizing PPPs as the pillars of national cybersecurity. By integrating Safety and Security, Accountability and Ethics, Global Governance, and Engagement and Privacy into policy and practice, nations can deploy an integrated, future-proofed cybersecurity ecosystem. Policymakers, business leaders, and civil society now need to work together, not just to share the cyber burden, but to collectively build the pillars of digital sovereignty and security for the future decades.

References

[1] World Economic Forum, “Why cybersecurity is a shared responsibility between governments and companies,” 2022. [Online]. Available: https://www.weforum.org/agenda/2022/06/public-private-cybersecurity-resilience/

[2] U.S. Department of Homeland Security, “Critical Infrastructure Security,” 2023. [Online]. Available: https://www.dhs.gov/topic/critical-infrastructure-security

[3] CISA, “Colonial Pipeline Ransomware Attack,” 2021. [Online]. Available: https://www.cisa.gov/news-events/news/colonial-pipeline-ransomware-attack

[4] CISA, “Joint Cyber Defense Collaborative (JCDC),” 2022. [Online]. Available: https://www.cisa.gov/jcdc

[5] European Commission, “The NIS2 Directive,” 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[6] The White House, “Executive Order on Improving the Nation’s Cybersecurity,” 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[7] Apache Software Foundation, “Log4j Security Vulnerabilities,” 2021. [Online]. Available: https://logging.apache.org/log4j/2.x/security.html

[8] Indian Computer Emergency Response Team (CERT-IN), “Cyber Security Drills,” 2023. [Online]. Available: https://www.cert-in.org.in/

[9] Cybersecurity and Infrastructure Security Agency (CISA), “About CISA,” 2023. [Online]. Available: https://www.cisa.gov/about

[10] National Council of ISACs, “Information Sharing and Analysis Centers,” 2023. [Online]. Available: https://www.nationalisacs.org/

[11] The White House, “Improving the Nation’s Cybersecurity Executive Order 14028,” 2021. [Online]. Available: https://www.whitehouse.gov

[12] European Union Agency for Cybersecurity (ENISA), “Cyber Europe,” 2023. [Online]. Available: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe

[13] Ministry of Electronics and IT, Government of India, “CERT-IN Mandate,” 2023. [Online]. Available: https://www.meity.gov.in

[14] CERT-IN, “Directions Under Section 70B of the Information Technology Act,” 2022. [Online]. Available: https://www.cert-in.org.in/

[15] Cyber Security Agency of Singapore (CSA), “Safer Cyberspace Masterplan 2020,” 2020. [Online]. Available: https://www.csa.gov.sg/News/Publications/masterplans

[16] Israel National Cyber Directorate (INCD), “CyberNet Overview,” 2022. [Online]. Available: https://www.gov.il/en/departments/general/cybernet