Sarcouncil Journal of Multidisciplinary

ISSN(Online): 2945-3445

Volume- 05| Issue- 07| 2025

Review Article **Received:** 13-06-2025 | **Accepted:** 07-07-2025 | **Published:** 25-07-2025

Privilege Access Management as a Cornerstone of National Security: Protecting Critical Infrastructure and Government Systems

Salahuddin Syed
Independent Researcher, USA

Abstract: Modern cybersecurity challenges to national critical infrastructure indicate the futility of existing security models in the presence of professional nation-state groups and advanced persistent threat organizations. Privilege access management becomes a fundamental pillar of national security policy today, not limited to the traditional perimeter of enterprise security, but to cover infrastructure protection, government services, and classified information infrastructure. Full protection against state-sponsored cyber attacks that leverage privileged accounts to conduct a lateral movement and compromise systems The combination of advanced PAM technologies, such as zero-trust architectures, behavioral analytics, and threat detection by artificial intelligence, can offer comprehensive defense capabilities against state-sponsored cyberattacks that systematically target privileged accounts to access the lateral movement and compromise systems. Critical infrastructure sectors, such as energy, telecommunications, water, transportation, and healthcare, demand specific PAM implementations that can face the peculiar challenges of the convergence between information technology and operational technology and guarantee the resilience of the services through the active presence of a cyber incident. The PAM deployment efforts achieved successful results through intelligence community implementations, which have secured classified information assets in risk management efforts by implementing a multi-level security control, an insider threat mitigation effort, to gain comprehensive auditing capabilities to ensure that only the relevant access to sensitive material is granted according to the clearance level and the necessity of operations.

Keywords: Privilege Access Management, Critical Infrastructure Security, Nation-State Threats, Cybersecurity Defense, Intelligence Protection.

INTRODUCTION

This modern situation in cybersecurity demonstrates a dramatic increase in the number of threats posed to national critical infrastructure and the insidious process of utilizing more and more complex types of attack by highly developed enemies, whose actions cannot be effectively blocked using traditional security systems (America's Cyber Defense Agency). The nature of the threat environment has changed drastically as nation-state actors continue building capabilities that circumvent commonly used perimeter defenses to exploit the vulnerabilities available in privilege account management systems. Such superior persistent menace teams are exceptionally patient and clever in terms of remaining on networks long earlier than ever, traveling through privileges so as to gradually escalate mantles, and mapping key system architectures and then accomplishing most objectives (IBM Security, 2024).

Important facilities, such as energy generation plants, water treatment systems, telecommunications systems, and transport hubs, are under constant reconnaissance and are to be infiltrated by state-sponsored cyber units to gain permanent access to key elements of service delivery frameworks (America's Cyber Defense Agency). The interaction between operational technology systems and information technology systems has resulted in increased attack vulnerabilities that cannot be safely defended by conventional systems of cybersecurity systems. Inherited infrastructures based mainly on network segmentation and antivirus have been shown powerless to the adversaries that perform targeted attacks on the first stages of the network, where administrative credentials and privileged service accounts are accessed and utilized to provide lateral movement and the system breach (IBM Security, 2024).

The policy question that forms the basis of the research inquiry used in this analysis is based on the cognizance of how privileged access management is a crucial defense mechanism in the context of a total national security strategic plan. The modern history of cyber attacks shows that the privileged account is the most obvious way to achieve the strategic goals of causes such as the seizure of intelligence, disrupting infrastructure, or sabotaging operations. There are indicators that organizations using full-featured privilege access management solutions have much lower response times to complex threats, as well as the ability to detect abnormal administrator actions (America's Cyber Defense Agency).

This analysis provides the conclusion that privileged access management is not only a core part of the contemporary national security posture, but it now falls outside the historical enterprise security policy scope due to the need to protect

*Corresponding Author: Salahuddin Syed

DOI- https://doi.org/10.5281/zenodo.16419969

sovereign digital assets in addition to ensuring the resiliency of vital services. The examination reveals the various tactics employed by privileged access management to attract various strategic uses, such as the detection of threats, the containment of an incident, and the capabilities of forensic investigation that have not been met by other security controls. Across the critical infrastructure sectors, integration of end-to-end privilege access management builds defensive depth to make successful nation-state cyber operations highly complex and expensive (IBM Security, 2024).

This analysis is centered on privileged access management software in industries covering sectors that produce and distribute energy, water, and wastewater, telecommunications and information technology, transport networks, and healing delivery systems that are treated as critical infrastructures (America's Cyber Defense Agency). It will examine technical implementation and policy structures that should be used in successful privilege access management implementation at the national level. An economic second-order effect of poor privilege access management is not confined to the direct costs of an incident, but the second-order effect on people's confidence in systems, global competitiveness, and the national ability to withstand attempts at lasting cyber campaigns (IBM Security, 2024).

The systematic review of theoretical backgrounds related to privileged access management in the national security setting, effectiveness in state-sponsored threat scenarios provided in literature, and applicability to the security of the critical infrastructure, as well as implementation considerations of classified information systems, will be conducted in this study. The methodology will fuse technical evaluation of the privilege access management against the policy analysis of what is currently being done in the sphere of cybersecurity, especially focusing on the case studies of cyber attacks against national infrastructure reported.

Privilege Access Management in the National Security Context

The privileged access management concept relies on existing cybersecurity concepts used in the national security framework that focus on verification of identity, control of access, and constant monitoring of administrative activities. Modern privilege access management systems combine several authentication criteria and behavioral analysis strategies in order to create a full-scale security position that responds to emerging security threats (Almuhammadi, S., & Alsaleh, M. 2017). The theoretical foundations focus on the principle of least privilege; that is, access privileges are used under strict necessity and are regularly reassessed to avoid privilege creep. In current implementations, PAM solutions are integrating with more advanced technologies, such as machine learning and anomaly detection within systems, automated provisioning and deprovisioning solutions, and real-time monitoring of sessions, which give administrators granular insight into administration activity across a complex network environment.

The national security threat modeling frameworks divide adversaries along vectors of capability, intent, and access, and in specific detail, the threat toward privileged account credentials. Advanced persistent threat actors are shown as having an elaborate comprehension of enterprise network layouts and, in a quantitative way, exploit trust connections among interconnected systems in reaching tactical goals (Almuhammadi, S., & Alsaleh, M. 2017). The insider threat vectors are rather complex because authorized employees can have legal access to sensitive systems and have an ill intent, or have an impaired judgment because of external factors. Nation-state-sponsored groups are the most challenging type of enemy that can have both technical capabilities and many resources and tactical patience to launch their long-term campaigns against high-value targets (Harp, D. & Brown, B. G. 2016). Such threat actors regularly use multi-stage attack procedures involving reconnaissance, first entry, privilege escalation, horizontal movement, and lastly achieving goals.

The vulnerability process exposed critical infrastructure to systematically weak access management privileges that cut across sectors that are critical to national security and economic sustenance. In energy production plants, industrial control systems may have faculties of legacy authentication features, which lack the execution of modern security measures, leaving space open to attack extremely critical physical processes following compromised administrator accounts (Harp, D. & Brown, B. G. 2016). The telecommunications infrastructure owes this particular quality to being a good target, as higher access levels of visibility and data access controls with the corresponding privileges. The security controls, sometimes in conflict with operational efficiency requirements, represent special complications to healthcare systems since

Publisher: SARC Publisher

emergency situations can sometimes require priorities to be given to emergency access to critical systems. Transportation infrastructures, such as aviation air traffic control and marine transportation logistics, have interconnected platforms that any privilege elevation in one platform can possibly spread to other areas of operation (Almuhammadi, S., & Alsaleh, M. 2017).

There is a need to have technical security controls with national security objectives in terms of integration of the principles of privilege access management in line with the nationwide accepted national security doctrines. Risk assessment approaches originally tailored to the national security domain focus on processes of identifying critical resources, conducting a threat vector analysis, and impact analysis processes that indicate suitable processes of security control choice and implementation strategies (Harp, D. & Brown, B. G. 2016). Privilege access management is naturally a built-in defense-in-depth strategy, an additional layer of protection on par with the current network perimeter controls, endpoint protection systems, and data classification schemes. The modern national security designs have understood that efficient control over access to privileges can offer necessary facilities in terms of detecting threats, responding during a crisis, forensic investigation, and continuity of business operations (Almuhammadi, S., & Alsaleh, M. 2017).

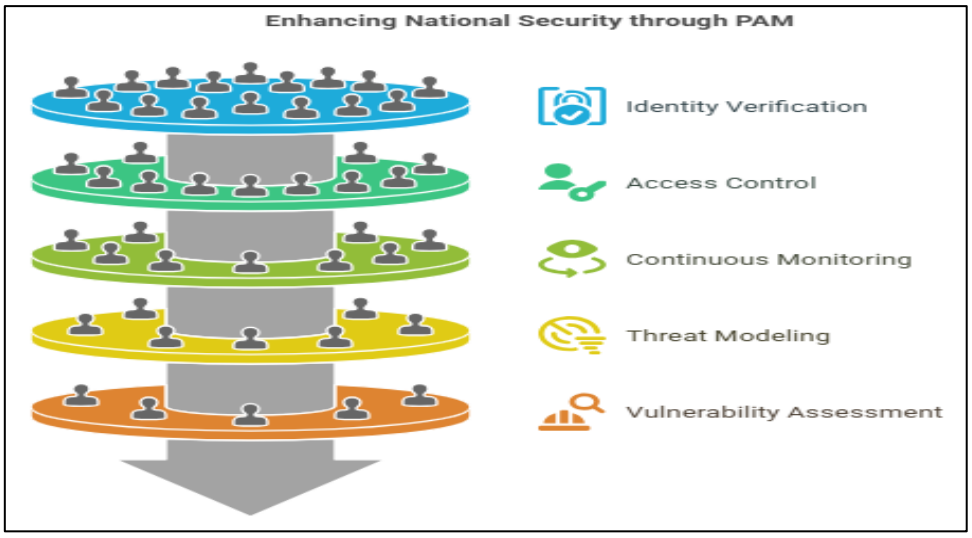

Fig 1: Enhancing National Security through PAM (Almuhammadi, S., & Alsaleh, M. 2017; Harp, D. & Brown, B. G. 2016)

Defending against State-Sponsored Cyberattacks

The modern nation-state cyber activity is characterized by growing sophistication in the application of more advanced forms of calculations and organized attack systems that are able to attack critical infrastructure and government systems. The study on the state-sponsored threat tactics demonstrates that there are organized methods that include not only automated reconnaissance solutions but also the human assets deployed to potential intelligence sources to identify privileged access points in the targeted bodies (Chen, P. *et al.*, 2014). Such advanced adversaries are using machine learning algorithms to study traffic patterns and system behaviour on networks so that they can isolate high-value administrative accounts, which offer the attacker the best avenue to accomplish their strategic objectives. Such advanced persistent threat campaigns incorporate cryptographic procedures and steganographic processes in ensuring concealed communications channels as they carry out extended infiltration missions on tough targets.

The systematic use of privileged accounts in government-controlled systems and those of critical infrastructure has a pattern similar to that used to target deeper weaknesses in traditional identity and access management systems. Elaborate mathematical models are used by the state-sponsored actor to streamline the attack pathways by utilizing complex network topologies and locating administrative accounts that offer maximum lateral movement capabilities and the least risk of detection (Chen, P. *et al.*, 2014). These adversaries employ advanced credential theft mechanisms through which they employ social tactics and engineering combined with technical executions to steal high-authorization

Publisher: SARC Publisher

credentials on service accounts and command-level user privileges. Advanced threat groups have specific proficiency in abuse of trust links involving connected systems and using the compromised privileged accounts to obtain access to the federated authentication systems and cloud-based infrastructure platforms (Nadeau, J. 2024).

Current privilege access management controls targeted at addressing the state-sponsored attack implement sophisticated analytical models that can perform threat evaluation and automated responses on demand. Zero-trust security structures do away with implied trust levels by using reinforcement procedures to ascertain access necessities against adaptive threat submissions and conduct profiles (Nadeau, J. 2024). Detection systems based on artificial intelligence use large volumes of authentication information and system actions to detect insidious abnormalities that signal the presence of an advanced threat actor within privileged account environments. By means of improving threat detection models with the help of machine learning algorithms, threat detection models are constantly optimized against newer forms of attacks, including the newest adversary strategies, offering responsive security states that dynamically adapt to the state-sponsored campaign strategy (Chen, P. *et al.*, 2014).

An in-depth investigation into state-sponsored intrusions documented in the literature has shown that there are patterns of exploitation that focus on under-secured privileged access management systems in important sectors of critical infrastructure. A study of significant government and infrastructure breaches evidences systematic insufficiencies in the capacity of administration to exercise account control and observatory capacities that allowed protracted presence of the adversary in sensitive settings (Nadeau, J. 2024). Improved privilege access management systems with high-performance cryptographic controls, behavioral analytics, and automated threat response offer the much-needed defensive controls against advanced nation-state attacks. It is shown that effective privilege access management systems can drastically decrease the dwell time of adversaries and restrict the extent of the effective state-sponsored activities in a wide-ranging manner due to higher visibility and control over management activities (Chen, P. *et al.*, 2014). Threat intelligence-fed and automated incident response-equipped advanced PAM solutions can help ensure the swift prevention of advanced threats before the organization can complete its primary missions.

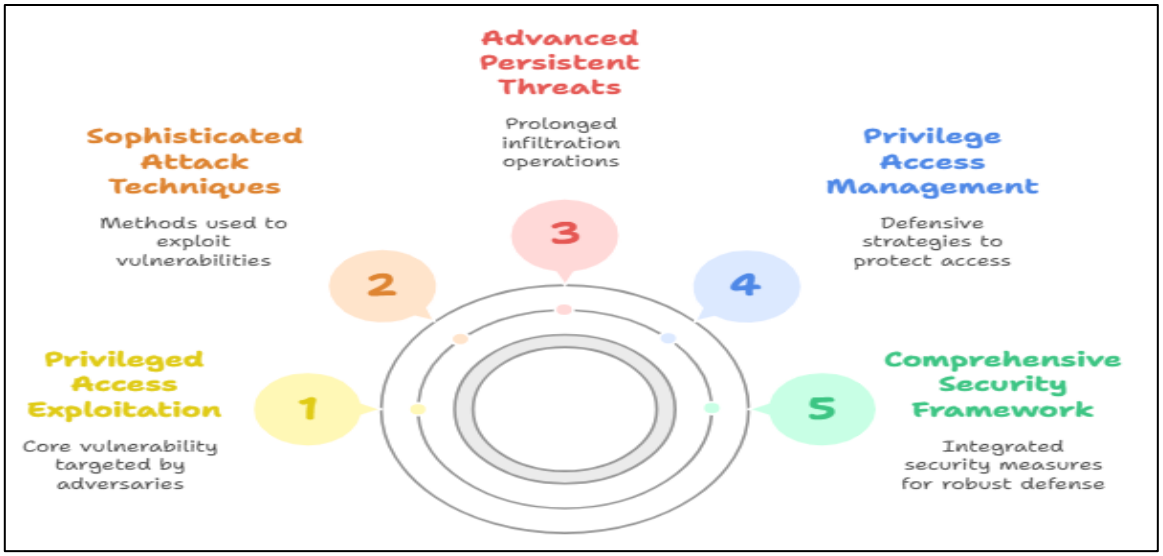

Fig 2: Cyber Security Threat Landscape (Chen, P. *et al.*, 2014; Nadeau, J. 2024)

SAFEGUARDING CRITICAL INFRASTRUCTURE

PAM's Role in Public Service Continuity

Critical infrastructure consists of closely related systems that deliver key facilities in various sectors, such as energy generation and distribution, water treatment and supply mechanisms, telecommunication systems, transportation channels, and health provision systems. Research studies have proved that these infrastructure sectors have an advanced interrelationship where culture in one sector may flow to several areas of services and form systematic weaknesses that can be exploited by the opponent by using specific privileged access breach (Lukas, L., & Hromada, M. 2011). Energy infrastructure is the underlying

Publisher: SARC Publisher

source upon which all the other important services run, and then there is the communications backbone that one can communicate on, thereby coordinating emergency response and other system management exercises. The transportation systems enable the transit of the people, tools, and materials needed to maintain the infrastructure and respond to any emergency situation, and the healthcare facilities can only be sustained with power, water, and communication during the time of crisis.

The connection of operational technology networks to information technology networks that are necessary in critical infrastructure development presents very special security issues that traditional approaches to privilege access management must deal with in very specific methods. ICS works with real-time demands and safety-decisive procedures that don't allow mainstream protection details of information technology without jeopardizing performances (Lukas, L., & Hromada, M. 2011). The network patterns supervisory control and data acquisition network networks employ a communication protocol that is highly optimized with the aspects of reliability and speed, but not security, which forms the attack vectors exploitable by the advanced adversary on those compromised administrative credentials. Traditional industrial systems commonly lack the means of computing involved in more sophisticated authentication systems, and safety requirements may forbid changes that can affect system availability or latency (U.S. 2014).

Privilege access management deployments in critical infrastructure settings should be deployed such that they do not result in disrupted service, in addition to ensuring the presence of end-to-end security controls to mitigate the impacts of sophisticated threat actors. High-order PAM systems include multiple authentication channels and built-in failover routines to guarantee that previously licensed members are in a position to take charge of critical frameworks if main access attributes are destroyed or inaccessible (U.S. 2014). Monitoring real-time systems offers an observable side of the activity of administrations in the spheres of operational technology and information technology, wherein the latency level might disturb the operations that are crucial to safety. Automatic session management features allow finer access controls to privileged access that still adhere to audit trails that are required to comply with regulations and a means to aid forensic analysis of a security incident occurrence (Lukas, L., & Hromada, M. 2011).

Privilege access management investments in the critical infrastructure sectors have sound economics in terms of cost-benefit associations when compared to the outcome of service failures. Failure of infrastructure has a cascading effect on the economy as it covers a range of sectors, commercial activities, manufacturing operations, and delivery of services by the government, which require the uninterrupted supply of essential services like utilities (U.S. 2014). Social impacts of critical infrastructure ramifications are endangering the lives of people, stopping healthcare services, and displacing whole communities so they can no longer use the big population centers over prolonged durations. The overall levels of privilege access management implementation hinder the risk mitigation levels, minimizing the likelihood of successful attacks on critical infrastructure, the impact thereof, and providing the facilitation of prompt remedying and service restoration after attacks have occurred (Lukas, L., & Hromada, M. 2011). Advanced PAM investments are also shown to have positive returns because of economic losses that PAM avoids and the ability to improve the resiliency of the system in the face of a changing threat landscape.

Table 1: Economic Impact Analysis of PAM Investment vs Infrastructure Disruption Consequences (Lukas, L., & Hromada, M. 2011; U.S. 2014)

Impact Category	Without PAM Implementation	With PAM Implementation	Risk Reduction	Cost-Benefit Ratio
Manufacturing Operations	Severe Disruption	Minimal Impact	85%	Positive
Commercial Activities	Extended Outages	Limited Interruption	75%	High
Public Services	Cascading Failures	Controlled Response	90%	Very High
Healthcare Delivery	Critical Interruptions	Maintained Operations	80%	Critical
Community	Large Population	Localized Effects	70%	Significant

Publisher: SARC Publisher

Displacement	Impact			

PROTECTING CLASSIFIED INFORMATION AND INTELLIGENCE ASSETS

Governmental systems of classification of information develop hierarchical structures according to which sensitive materials are classified by the possible harm they may cause to national security in the event of being disclosed to parties other than those authorized to access and use such materials. These systems of classification envisage various levels of classification, such as confidential, secret, and top-secret designations, and many other layers of compartmentalized access management to the extent that sharing of information depends on the specifications of operation and levels of clearances of the personnel, and so they cascade accordingly (Force, J. T., & Initiative, T. 2013). Department-specific access programs and sensitive compartmented information categories provide another level of protection to intelligence sources, methods, and continuing activities, where special security is added to the usual classification mechanism. The complexity of the contemporary classification systems also reflects the versatile character of the intelligence work and the necessity to secure a variety of types of sensitive information without losing the possibility to cooperate between a range of government bodies and even with the help of international partners (Blakley, B., & Heath, C. 2004).

Privilege access management systems will be technically applied on classified systems, and this would necessitate special architectures that suit the specific needs of security systems without sacrificing performance within multiple security domains. The use of classified networks implies the presence of high classification needs, preventing unauthorized movement of data among security level demands, which would require solutions of PAM able to operate in the air-gapped environment and facilitating cross-domain information sharing protocols (Force, J. T., & Initiative, T. 2013). Many levels of security systems need to have the ability to authorize access in low resolutions and combine clearance levels and need-to-know restrictions so that individuals access only those classified materials that are needed to carry out approved functions. The sophisticated application of PAM includes cryptographic controls and secure credentials that guard against such advanced adversaries and also embrace intricate access patterns that are essential in deploying intelligence operations (Blakley, B., & Heath, C. 2004).

Mitigating insider threat in a classified environment is different because authorized users have the due access to sensitive systems and at the same time may have malicious motives or may have a corroded loyalty due to external influences or interests. Behavioral analytics systems continue to track user activity on classified networks to detect anomaly patterns that might be related to unauthorized access or data exfiltration activity (Force, J. T., & Initiative, T. 2013). Modern PAM systems have built-in capabilities of monitoring activities around privileged accounts and can create alerts once the events become different than the set baselines or are not performed based on the security measures. The controls on access rights can be designated automatically so as to inhibit or deny privileges on the fly before any harm is done by restricting access to classified materials (Blakley, B., & Heath, C. 2004).

Whether the application of privilege access management in the intelligence communities is successful or not, the first step towards addressing these issues in national security information protection continues to take place. The best practices have been put in place by the defense and intelligence organizations that highlight the significance of the completely auditable trails and session monitoring features that enable visibility of the activities involving all privileged accounts in the classified domains (Force, J. T., & Initiative, T. 2013). An effective PAM implementation has risk-based access controls that dynamically change the level of security that may be needed depending on the threat levels and the needs of the operations so that the missions can be done successfully and have proper security postures. The importance of having well-trained users and implementing policies to ensure OPSEC to keep efficient privilege access management programs in the classified settings cannot be overemphasized based on lessons learned via operational experience (Blakley, B., & Heath, C. 2004).

Publisher: SARC Publisher

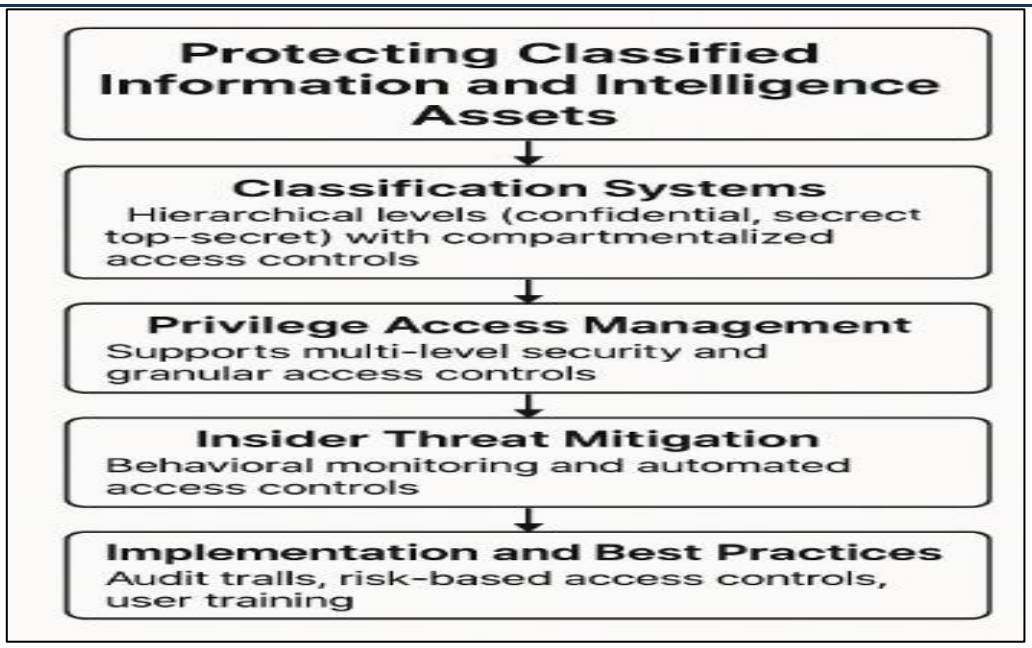

Fig 3: Securing Classified Information: Frameworks, Access Controls, and Threat Mitigation (Force, J. T., & Initiative, T. 2013; Blakley, B., & Heath, C. 2004)

CONCLUSION

The research findings developed in this study prove that privileged access management has become an essential pillar of the modern national security framework, and this is because it is playing a key role in protecting against advanced cyberattacks that aim at compromising the most sensitive government and infrastructure platforms. The application of extensive PAM frameworks in industries that constitute the national critical infrastructure not only builds defensive depth, making nation-state cyber operations much more complex and costly, but also assures the continuing provision of the most vital public services even under circumstances of national crisis. The changing nature of cybersecurity-related threats needs a national-level program of PAMs that builds on a unification of national security conditions through the common practices, information sharing windows, and linkages of incident responses between government units and with its industrial partners. Adaptive strategies of PAM in the future will involve artificial intelligence, quantum computing, and distributed systems, and will need to balance security operational effectiveness with the new demands of the business and technology changes. The ability to control access to privileges is no longer just a technical security measure, but an overall strategic safeguard of nations and their economies as well as the safety of their citizens in a more interconnected online world where technical experts across the malware industry relentlessly discover new modes of operation to attack privileged credentials and gain access to administrative routes.

REFERENCES

1. America's Cyber Defense Agency, "Critical Infrastructure Security and Resilience. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience
2. IBM Security "Cost of a Data Breach Report ". (2024) https://www.ibm.com/reports/data-breach
3. Almuhammadi, S., & Alsaleh, M. "Information security maturity model for NIST cyber security framework." *Computer Science & Information Technology (CS & IT)* 7.3 (2017): 51-62.
4. Harp, D. & Brown, B. G. "SANS 2016 State of ICS Security Survey," *SANS*, (2016). https://paper.vulsee.com/icsmaster/doc/%E5%9B%BD%E5%A4%96/ICS-2016-Belden-Survey.pdf
5. Chen, P., Desmet, L., & Huygens, C. "A study on advanced persistent threats." *IFIP international conference on communications and multimedia security*. Berlin, Heidelberg: *Springer Berlin Heidelberg*, (2014).
6. Nadeau, J. "New cybersecurity sheets from CISA and NSA: An overview," *IBM*, (2024).
7. Lukas, L., & Hromada, M. "Resilience as main part of protection of critical infrastructure." *International journal of mathematical models and methods in applied sciences* 5.6 (2011): 1135-1142.

Publisher: SARC Publisher

8. U.S. Department of Homeland Security, "Critical Infrastructure Security and Resilience." (2014): https://www.gps.gov/multimedia/presentations/2014/11/ICG/dhs.pdf
9. Force, J. T., & Initiative, T. "Security and privacy controls for federal information systems and organizations." *NIST Special Publication* 800.53 (2013): 8-13.
10. Blakley, B., & Heath, C. "Technical guide: Security design patterns." *The Open Group* (2004).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Syed, S. " Privilege Access Management as a Cornerstone of National Security: Protecting Critical Infrastructure and Government Systems." *Sarcouncil Journal of Multidisciplinary 5.7* (2025): pp 899-906.

Publisher: SARC Publisher