

Revista Sextante

ISSN : 2665-3923

Vol: 32 No: 01 (2025)

Cybersecurity Preparedness in Modern Defense Institutions: A Comparative Assessment

Thandiwe Mokoena-Larsson

Centre for Defence Cyber Policy and Resilience Studies, Johannesburg, South Africa

Article History

Received June, 12th, 2025

Accepted June, 13th, 2025

Published June, 14th, 2025



© 2025 The Authors. This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license

<https://creativecommons.org/licenses/by/4.0>

Abstract

Defense institutions depend on networked systems for command and control, logistics, communications, research and weapons support, which creates a large attack surface for state-sponsored, criminal and insider threats. This article presents a comparative assessment of cybersecurity preparedness in modern defense institutions. Drawing on cybersecurity frameworks, research on cyber conflict and deterrence, security engineering and resilience, it compares three stylised institutional models, namely centralised and mature, federated and service-based, and emerging and resource-constrained, across governance and policy, technical controls, workforce and training, incident response and supply chain security. The assessment indicates that preparedness depends on strong governance, risk-based and resilient technical architectures, a skilled workforce and learning culture, trusted partnerships and rehearsed response, and that supply chain security is the most difficult dimension in every model. Limitations include scarce comparable data, the simplification inherent in stylised models and difficulties in measuring preparedness. An illustrative figure summarises expected preparedness profiles of the three models.

Keywords: cybersecurity preparedness, defense institutions, cyber resilience, comparative assessment, supply chain security

INTRODUCTION

Defense institutions, including ministries of defense, armed services, intelligence and procurement agencies, military academies, research establishments and the industrial base that supports them, now depend on digital systems for almost every function. Command and control, logistics, personnel administration, communications, weapons and sensors, training and research all rely on networks and software. This dependence creates efficiency and capability, but it also creates a large and attractive attack surface for adversaries who seek to steal secrets, disrupt operations, degrade confidence or prepare for conflict (Kello, 2017). The cyber threat to defense is persistent and varied. State-sponsored actors conduct espionage and pre-position access to critical systems, criminal groups pursue ransomware and fraud

against institutions and their contractors, hacktivists seek publicity, and insiders may misuse access deliberately or inadvertently. The boundary between peacetime competition and armed conflict is blurred in cyberspace, and defense institutions must therefore be prepared to operate continuously under conditions of contest. Preparedness, the capacity to anticipate, withstand, respond to and recover from cyber incidents, has become a core component of national security. This article presents a comparative assessment of cybersecurity preparedness in modern defense institutions. It reviews conceptual foundations, the threat environment, a framework for comparing institutional models, and the dimensions of governance, technical controls, workforce, partnerships and response. It also considers limitations and directions for future work. The assessment is conceptual and integrative and does not rank particular countries, and the figure presented is an illustrative synthesis rather than a report of new empirical data.

Conceptual Foundations of Cybersecurity Preparedness:

Cybersecurity is commonly understood as the protection of information systems and the data and operations they support against unauthorised access, disruption and damage, and it is often described in terms of confidentiality, integrity and availability. For defense institutions, the three properties have distinct operational meaning: confidentiality protects secrets and intelligence, integrity ensures that commands, targeting data and logistics records are accurate, and availability ensures that systems function when needed. Attacks may target any of these, and a successful compromise of integrity may be more damaging than a loss of confidentiality because it undermines trust in information. Preparedness extends beyond prevention. A widely used national framework organises cybersecurity activities into five functions: identify, protect, detect, respond and recover, which together describe the lifecycle of risk management (National Institute of Standards and Technology, 2018). This structure emphasises that organisations should assume that some attacks will succeed and should invest not only in barriers but in the capacity to detect intrusions quickly and recover. The approach is relevant to defense institutions, although they face higher threat levels and stricter requirements than most civilian organisations. The concept of resilience is closely related. Researchers argue that for complex systems facing uncertain and evolving threats, risk management alone is insufficient and should be complemented by planning for the ability to absorb, recover from and adapt to disruption (Linkov et al., 2014). In defense, this suggests designing systems and procedures so that critical missions can continue in degraded conditions, with redundancy, manual fallback and rapid restoration. Preparedness is thus a property of people, processes and technology together, not of any single tool.

Cyber Threat Environment Facing Defense Institutions:

The threat environment for defense institutions is shaped by the strategic value of the information and capabilities they hold. State actors invest heavily in cyber espionage to acquire military technology, operational plans and intelligence, and may seek to establish persistent access in networks that could be exploited in a crisis. Debate exists about how decisive cyber operations are in war. Some analysts argue that the strategic effects of cyber operations are limited and that purely cyber war is unlikely (Rid, 2012), while others emphasise that cyber instruments are significant tools for espionage, coercion and the support of conventional operations (Kello, 2017). The best-known cases show both the potential and the limits of cyber operations. Analysis of a sophisticated operation against industrial control systems has suggested that such attacks require extensive intelligence, resources and expertise, and that their strategic benefit may be constrained by the difficulty of scaling and repeating them (Lindsay, 2013). For defense institutions, the significance lies less in any single event than in the existence of capable adversaries able to target critical systems, including those that are isolated from the internet, through supply chains, removable media or insiders. The attack surface has widened as defense systems become more networked. Weapons platforms, sensors and logistics systems incorporate commercial software and hardware, cloud services and remote maintenance, while military personnel use personal devices and social media. Operational technology, including control systems on ships, aircraft and bases, was often designed without security in mind. The result is a complex and heterogeneous environment in which vulnerabilities are numerous and the consequences of exploitation may be physical as well as informational.

Comparative Framework and Institutional Models:

A comparative assessment needs a framework that can accommodate diverse institutions without relying on country-specific details. This article distinguishes three stylised institutional models. The first is a centralised, mature model, in which a single authority sets policy, operates shared infrastructure, maintains specialised cyber forces and enforces standards across the defense enterprise. The second is a federated, service-based model, in which individual services or agencies retain considerable autonomy over their networks and security practices while coordinating through common policies. The third is an emerging, resource-constrained model, in which cyber capability is limited by funding, skills and legacy systems. The models are compared across five dimensions: governance and policy, technical controls, workforce and training, incident response, and supply chain security. Each dimension captures a distinct source of preparedness, and weakness in one can offset strength in another. Centralised models tend to achieve consistency and economies of scale but may be slower to adapt and risk creating single points of failure. Federated models offer

flexibility and closeness to operational needs but may suffer from inconsistent standards and gaps between organisational boundaries. Emerging models face structural limits that require prioritisation and external support.

Governance, Policy and Strategic Leadership:

Governance provides the foundation for preparedness. Effective defense institutions define clear responsibility for cybersecurity at senior levels, establish policies and standards that apply across the enterprise, allocate resources according to risk and hold leaders accountable for results. Without strong governance, technical investments may be fragmented and incompatible, and security may be treated as a technical matter for specialists rather than as a command responsibility. Leadership attention signals priority and shapes behaviour throughout the organisation. Risk management is the core governance process. Institutions need to identify critical assets and missions, assess threats and vulnerabilities, and decide which risks to accept, mitigate or transfer. In defense, this requires a clear understanding of mission dependencies, so that protection can be concentrated on the systems whose failure would most harm operations. Frameworks that organise risk activities into standard functions help to structure this work, but their value depends on adaptation to the institution's missions and on honest assessment rather than formal compliance (National Institute of Standards and Technology, 2018). Strategic leadership must also address the relationship between defensive and offensive cyber activities, legal authorities and the division of responsibilities among military, intelligence and civilian agencies. In many systems, ambiguity about who is responsible for protecting defense contractors, critical infrastructure and civilian networks on which the military depends creates gaps. Clarity of roles, supported by legislation and agreements, is therefore an element of preparedness, as are mechanisms for coordinating with allies and with national cybersecurity agencies.

Technical Controls and Architecture:

Technical controls translate policy into practice. They include network segmentation, access control, encryption, patching, monitoring, endpoint protection and secure configuration, and they are organised into architectures that determine how systems are connected and how trust is established. A systematic treatment of security engineering emphasises that security failures often arise from poor design, misaligned incentives and complex interactions rather than from the absence of any single control, and that a system should be designed with the assumption that components will fail or be attacked (Anderson, 2020). Contemporary architectural approaches reflect the recognition that perimeter defenses alone are inadequate. The zero trust model assumes that no user, device or network location should be trusted by default, and requires continuous verification of identity and authorisation for access to resources, with attention to minimising privileges and limiting lateral movement within networks (Rose et al., 2020). For defense institutions, which hold highly sensitive information and face determined adversaries, such approaches provide a framework for reducing the damage that follows from compromise, although they require substantial effort to implement in complex legacy environments. Understanding adversary behaviour improves defense. The intrusion kill chain model describes the stages through which an attacker progresses, from reconnaissance and delivery to exploitation, installation, command and control and actions on objectives, and suggests that defenders can disrupt attacks by detecting and interrupting any stage (Hutchins et al., 2011). Intelligence-driven defense uses knowledge of adversary tools and tactics to prioritise controls and to detect intrusions. Detection capabilities, including continuous monitoring and security operations centres, are particularly important because many intrusions go unnoticed for long periods.

Workforce, Training and Organisational Culture:

People are both the greatest vulnerability and the greatest asset in cybersecurity. Phishing, credential theft, poor password practices, misconfiguration and policy violations remain leading causes of compromise. Research on human error argues that it should be seen as a consequence of conditions in systems rather than solely as a failing of individuals, and that effective management addresses the error-producing conditions and strengthens defenses rather than relying on blame (Reason, 2000). Applied to cybersecurity, this implies that systems should be designed to make secure behaviour easy and insecure behaviour difficult. A skilled workforce is vital, yet defense institutions often compete with industry for scarce cybersecurity talent and struggle with retention. Preparedness requires sustainable pathways for recruitment, education and career development, including specialised cyber roles within the military, the use of reserve and civilian expertise, and partnerships with universities. Training should reach every user, since all personnel are part of the defense, and should be realistic, involving exercises and simulations that test responses under pressure and reveal weaknesses in procedures. Culture determines whether policies are followed. A culture that treats security as a shared responsibility, encourages the reporting of incidents and near misses without punishment, and values learning is more resilient than one that emphasises compliance and concealment. Hierarchical military cultures can impede the escalation of problems, so leaders should deliberately create channels for candid reporting. Education of commanders in the operational implications of cyber risk ensures that they can make informed decisions and treat cyber defense as an integral part of mission planning.

Supply Chain, Partnerships and Information Sharing:

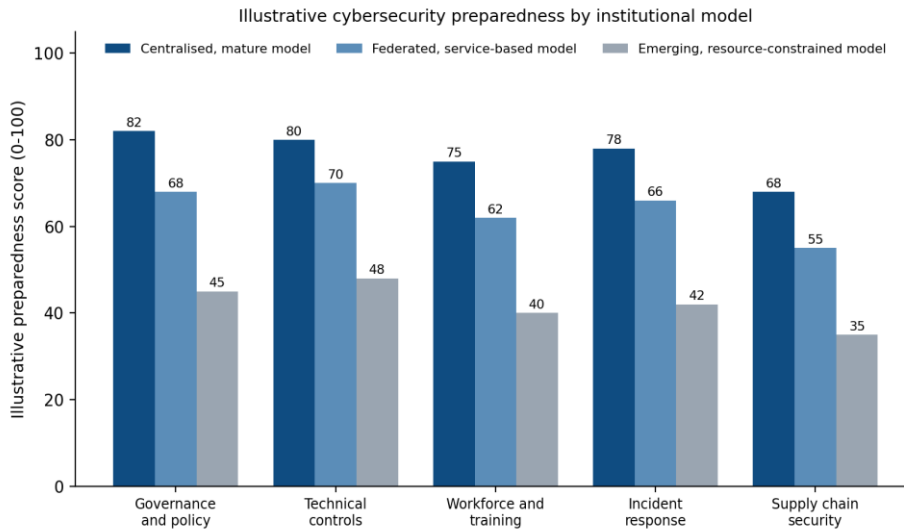
Defense institutions depend on extensive supply chains for hardware, software, services and components, and vulnerabilities in any of these can provide a route for adversaries. Suppliers may have weaker security than the institutions they serve, and compromise of a trusted vendor can give attackers access to many customers simultaneously. Counterfeit or tampered components, malicious code embedded in software updates and the exploitation of third-party remote access are among the risks. The difficulty of verifying the provenance and integrity of complex products makes supply chain security the most challenging dimension of preparedness. Effective responses combine contractual requirements, technical assurance and oversight. Institutions can require suppliers to meet security standards, conduct audits and testing, diversify sources for critical items, maintain trusted supplier lists and apply controls such as software bills of materials and code signing. Defense industrial base partners should be integrated into information-sharing and incident-reporting arrangements, with support for smaller firms that lack resources. These measures impose costs and may slow procurement, so risk-based prioritisation is necessary. Partnerships extend beyond suppliers. Sharing threat intelligence among defense organisations, national cybersecurity agencies, allies and industry improves early warning and enables collective defense, since many adversary operations target several organisations with similar tools. Barriers include classification, legal restrictions, concerns about attribution and exposure of weaknesses, and lack of trust. Trusted mechanisms, standardised formats and clear rules for handling shared information can reduce these barriers, and exercises with partners build interoperability for responding to joint threats.

Incident Response, Resilience and Deterrence:

Incident response determines how much damage an intrusion causes. Prepared institutions maintain plans that define roles, escalation paths, communication procedures and decision authorities; they have trained teams able to contain intrusions, preserve evidence, eradicate adversary presence and restore services; and they rehearse their plans through exercises. Speed matters, since the time between compromise and detection or containment strongly affects the extent of harm. Integration of cyber response with operational command ensures that decisions about continuing missions, switching to manual procedures or notifying partners are made with full awareness. Resilience requires that critical functions can continue in degraded conditions. Measures include redundancy of communications and data, offline backups, segmentation to limit the spread of attacks, manual fallback procedures and the capacity to operate without access to certain networks or to satellite services. Planning for recovery, including prioritised restoration of systems, is as important as prevention. Learning from incidents, through structured reviews and sharing of lessons, improves future preparedness and prevents repetition of failures. Preparedness also relates to deterrence. Analysts have debated how far deterrence concepts transfer to cyberspace, noting challenges of attribution, the variety of actors and the difficulty of signalling capability and resolve (Libicki, 2009). It has been argued that deterrence in cyberspace can operate through denial, by making attacks harder and less rewarding, as well as through punishment and entanglement (Nye, 2017). The balance between offence and defence is also contested, and depends on how one defines and measures advantage (Slayton, 2017). Strong defense contributes to deterrence by denial, although it cannot by itself guarantee security.

Challenges, Limitations and Future Directions:

Defense institutions face significant obstacles in improving cybersecurity preparedness. Legacy systems, long procurement cycles and the long service lives of platforms leave them dependent on technology that was not designed for the current threat environment. Skills shortages, budget constraints and competing priorities limit what can be achieved, and the speed of technological change makes any set of controls quickly outdated. Complexity of networks and organisations makes it difficult to maintain an accurate picture of assets and dependencies, and secrecy impedes learning across institutions. The comparative assessment itself has limits. Reliable, comparable data on the cybersecurity posture of defense institutions are scarce because of classification and sensitivity, and published information tends to describe policy intentions rather than actual capability. The three models discussed are simplifications, and real institutions combine features of each. Measuring preparedness is inherently difficult because the absence of detected incidents does not prove security, and metrics can encourage compliance behaviour that does not improve real protection. Conclusions should therefore be treated as provisional and tested against evidence as it becomes available. Future directions include greater adoption of zero trust and secure-by-design principles, increased automation and use of artificial intelligence in detection and response, with attention to the risks of adversarial manipulation, and stronger protection of operational technology and space and maritime systems. Investment in workforce development, exercises that integrate cyber with conventional operations, and trusted mechanisms for sharing intelligence with allies and industry will be critical. Researchers can contribute by developing better measures of preparedness, conducting comparative studies using declassified or anonymised data and examining how organisational models influence performance over time.



Summary:

Cybersecurity preparedness in defense institutions depends on the combined strength of governance, technical architecture, people, partnerships and response capability. A comparison of centralised, federated and resource-constrained institutional models suggests that centralised approaches offer consistency and economies of scale, federated approaches offer flexibility but risk uneven standards, and emerging models are limited by resources and legacy systems. Across all models, supply chain security is the weakest dimension, reflecting dependence on external suppliers and the difficulty of verifying complex products. Strengthening preparedness requires clear leadership and risk-based governance, modern architectures such as zero trust, intelligence-driven detection, investment in workforce and culture, trusted information sharing with allies and industry, and rehearsed incident response that supports resilience and contributes to deterrence by denial. The assessment is limited by scarce comparable data and the simplification of stylised models. Future work should develop better measures of preparedness, extend comparative research using anonymised data and examine the effects of automation, operational technology and new domains on defense cyber risk.

References:

- Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1), 80–106.
- Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
- Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation.
- Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3), 365–404.
- Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., et al. (2014). Changing the resilience paradigm. *Nature Climate Change*, 4, 407–409.
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity*, version 1.1. U.S. Department of Commerce.
- Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71.
- Reason, J. (2000). Human error: Models and management. *BMJ*, 320(7237), 768–770.
- Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5–32.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology.
- Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, 41(3), 72–109.