The National AI Cybersecurity Readiness Metric

31/03/2026

1. Overview

The National Ai Cybersecurity Readiness Metric (the Metric) enables nations to evaluate their existing AI cybersecurity readiness and provide an evidence base for future AI cybersecurity decision making. This tool meets growing demand from nations to better understand how they should manage AI cybersecurity risks and opportunities, and is informed by the GCSCC's extensive experience in benchmarking national cybersecurity capacity through the Cybersecurity Capacity Maturity Model for Nations (CMM).

The National AI Cybersecurity Readiness Metric is intended to support countries at all stages of readiness, whether they are actively implementing cybersecurity measures to address the risks associated with AI adoption, or are just beginning to explore how to integrate AI into their national strategies. Regardless of where a nation is positioned with regards to AI adoption, the Metric is designed to help nations prepare to defend themselves against the evolving threat landscape that they face.

The Metric is intended to be an adaptive tool that evolves alongside new developments in AI technologies and their influence on national cybersecurity capacities. This document presents the indicators of AI cybersecurity readiness identified across a 2-year research project. These indicators were developed through expert consultations with over 200 experts in AI and cybersecurity and three deployments in participating nations.

Section 2 provides definitions of common terminologies used within the Metric. Section 3 details the indicators of the Metric across 10 interconnected areas of AI cybersecurity readiness.

2. Terminology

The AI Cybersecurity Readiness Metric uses some general terms described below.

- **AI-related cybersecurity risks**: AI has the potential to impact on the "core" cybersecurity risk (illustrated in Figure 1). Developments in AI can impact on the risk to data and system confidentiality, integrity and availability: the traditional lens through which cyber-attack impact is viewed. AI may also introduce new challenges, such as the need for explainable and reliable AI models in cybersecurity applications. These risks include:
    - Risks posed by **AI-enabled threats**, where adversaries leverage AI to enhance cyber-attacks;
    - **Risks to the cybersecurity and cyber-resilience of AI-based systems**, which encompass vulnerabilities and cybersecurity challenges introduced through the adoption of AI.
- **AI-related broader risks**: Developments in AI are also creating broader risks that might be considered as outside the scope of these "core" cybersecurity risks and of current national cybersecurity strategies, but may have implications for national security and crime. These risks include AI-generated disinformation, the proliferation of increasingly advanced deepfake technologies, and the use of AI for large-scale data exploitation, which could lead to privacy violations or state-sponsored espionage, for example:
    - **AI-related cyber harms**: The negative consequences resulting from both AI-enabled threats (the malicious use of AI by threat actors) and risks to the cybersecurity and cyber-resilience of AI-based systems (vulnerabilities and failures in AI-based systems), including privacy violations, misinformation, financial losses, and operational disruptions.
    - **AI-related cybersecurity governance**: The frameworks, policies, and best practices being developed to manage AI-related cybersecurity risks, to ensure secure AI development, deployment, and oversight.
    - **AI-enabled cybercrimes**: The use of AI to enable cybercrime, such as automated hacking, and AI-generated phishing attacks. This incorporates cybercrimes resulting from both AI-enabled threats and risks to the cybersecurity and cyber-resilience of AI-based system.
    - **Broader AI-enabled crime**: The use of AI to enable broader digital crimes, such as deepfake scams, and sexually abusive deepfakes.

The Metric considers three key ways in which AI impacts on the cybersecurity considerations of nations: the impacts of developments in AI on the capabilities of threat actors; the risks from the growing adoption of AI; and the defensive opportunities to mitigate risk that AI might offer for the nation.

Threat:

- **AI-enabled threats**: Threats that leverage AI to enhance the speed, scale, and sophistication of cyber-attacks, including AI-assisted hacking, deepfake-based fraud, and automated social engineering.

Adoption:

- **Risks to the cybersecurity and cyber-resilience of AI-based systems**: The vulnerabilities and cybersecurity challenges associated with adopting AI, including adversarial attacks on AI models, data poisoning, and system compromise.

- **AI-system compromise**: The malign or benign manipulation or disruption of an AI system, which can impact on the system's outputs.

- **Vulnerabilities of AI systems**: The weaknesses in AI models and their supporting infrastructure, which can be exploited by attackers through methods such as adversarial inputs, data poisoning, or model-inversion attacks.

Defence:

- **AI-enabled cybersecurity controls**: Technologies incorporating AI to strengthen cybersecurity by detecting, preventing, and responding to threats, including through automation, predictive analytics, and anomaly detection.

- **AI-related cybersecurity opportunities**: The broader ways, aside from technical controls, in which AI might enhance national cybersecurity capabilities, including by supporting threat-intelligence sharing, and improvements in cybersecurity education and awareness programmes.

Finally, the Metric also uses terms related to the provision of AI technology described below.

- **AI software**: The applications and algorithms that implement AI capabilities, such as machine-learning models, natural-language processing models, and computer-vision systems.

- **Training data**: The dataset used to teach an AI model how to recognise patterns, make predictions, or perform specific tasks during its learning phase.

- **Real-time data**: Continuously incoming data processed by an AI system during its operation, used as the basis for decision-making and adaptation in response to new information.

- **AI platforms**: The infrastructure and frameworks that enable the development, deployment, and management of AI applications, including cloud-based AI services

3. National AI Cybersecurity Readiness Metric

Area 1: National AI Cybersecurity Strategy and Governance

This area explores the country's capacity to assess AI cybersecurity risks as they are introduced into the national digital context and the incorporation of AI cybersecurity factors into strategic planning and decision making. This *area* also examines the extent of national stakeholder engagement in international AI cybersecurity debates and initiatives.

Readiness indicators of this *area*:

1. National AI-related cybersecurity risks and AI-related broader risks have been identified through comprehensive assessments of AI adoption, or planned adoption, within the economy and society.

2. The implications of these risks on strategic national priorities are understood, and actions have been taken to account for them where needed.

3. These risks formally inform the development, adaptation and implementation of the national policy and strategy stack related to AI cybersecurity.

4. The national policy and strategy stack related to AI cybersecurity considers the nuanced risks and opportunities of different local and international AI technologies and applications within different industries.

5. The development of the national policy and strategy stack related to AI cybersecurity has been informed by substantive consultations with relevant multidisciplinary stakeholders across sectors.

6. The resources required to deliver the objectives of the national policy and strategy stack related to AI cybersecurity have been allocated, including for the development of further capacities necessary for achieving the objectives.

7. A coordinated national governance structure exists that encompasses AI and cybersecurity, assigning clear roles and responsibilities to entities accountable for delivering the national policy and strategy stack related to AI cybersecurity.

8. The nation has considered its position in the international landscape (i.e. geopolitical context and supply chain) to develop its approach to national AI cybersecurity policies, and is engaging in international debates and forums to advance its vision and promote national AI agency (e.g. through cyber diplomacy and standards development).

Area 2: National Incident Prevention, Detection and Response

This *area* addresses the consideration of AI in national systems for cybersecurity incident response and crisis planning. This *area* incorporates assessment of the risks AI introduces to the national digital context, the changes to attack speed and scale, and the use of AI tools in cybersecurity incident prevention, detection, categorisation, and response.

Readiness indicators of this *area*:

9. Assessed national AI-related cybersecurity risks and AI-related broader risks have been incorporated within the scope of national incident response frameworks and plans.

10. The national systems for cybersecurity incident prevention, detection, categorisation, and response has the resources and updated capabilities to manage the risks of the AI cybersecurity landscape.

11. Consideration has been given to how AI-enabled tools might support cybersecurity incident prevention, detection, categorisation, and response, including within the national Computer Security Incident Response Teams (CSIRTs).

12. National crisis planning takes account of the AI-related cybersecurity risks and AI-related broader risks, and includes crisis coordination between key actors.

13. Cross sectoral information sharing, convening and learning is coordinated and encouraged to enhance efforts to prevent, detect, and respond to AI-related cybersecurity risks and broader risks.

Area 3: Legislation and Law Enforcement Capabilities

This *area* addresses the consideration of AI introduced components in cybercrime, cybersecurity and related frameworks and the capacity of law enforcement stakeholders to manage AI factors. This *area* also includes the adaptiveness of legal frameworks and stakeholders to AI related cybercrime developments.

Readiness indicators of this *area*:

14. Substantive and procedural cybercrime and cybersecurity legislation has been reviewed with respect to AI-enabled cybercrimes and broader AI-enabled crimes (i.e. deepfakes and accountability of autonomous systems) and has been adapted if determined to be necessary in the national legal context.

15. Legal entities (law enforcement, prosecution, courts) have been equipped with the skills and resources necessary to adapt their methods and process to deal with the complexity and volume of AI-enabled cybercrimes, and broader AI-enabled crimes.

16. Effective mechanisms are in place for victims of AI enabled cybercrimes and broader AI-enabled crimes to report issues to law enforcement.

17. Formal and informal cooperation frameworks enable relevant stakeholders in the nation to combat AI-enabled cybercrime and broader AI-enabled crimes, in manner aligned with international human rights principles.

18. Legal and regulatory entities have considered how to leverage AI to support their capabilities to deal with cybersecurity risks and cybercrime.

19. Broader legislative frameworks related to cybercrime and cybersecurity (i.e. data-protection legislation, consumer-protection legislation, intellectual-property legislation, and legislation for the protection of children online) have been reviewed with respect to AI, and have been adapted if determined to be necessary in the national legal context.

Area 4: Regulation and Related Legislative Frameworks

This area reviews the suitability of cybersecurity regulatory frameworks and the need to adapt these frameworks to account for new risks introduced by AI. This *area* analyses the impact of AI on cybersecurity provisions related to Critical National Infrastructure (CNI) and the capability of regulatory bodies to oversee secure AI adoption.

Readiness indicators of this *area*:

20. *Cybersecurity regulations, including cross-sector, sector specific and Critical National Infrastructure (CNI) regulations, have been reviewed through consultative processes to ensure they take account of AI-related cybersecurity risks in their deployment context.*

21. *Various regulations related to AI cybersecurity are aligned between different national regulatory bodies and there is comprehensive guidance on how regulations may be implemented.*

22. Consideration is given to whether the adoption of various AI technologies within the nation gives rise to new categories of CNI, which would be brought within the scope of CNI regulation and governance.

23. The security implications of AI data governance, cross border AI dependencies and market concentration have been considered, and regulations have been adapted if determined to be necessary.

24. Regulatory bodies have been equipped with the skills and resources needed to provide effective oversight and ensure compliance of AI-related cybersecurity standards risks within their remit.

Area 5: Cybersecurity Standards and Marketplace

This *area* studies the cybersecurity marketplace and standards frameworks for mitigating risks to and from AI systems. This *area* examines the developed or identification of these components and explores the capacity for AI cybersecurity research and innovation within the national context.

Readiness indicators of this *area*:

25. Standards and codes of practice are being developed or identified by national standards bodies and industry stakeholders to mitigate contextualised AI-related cybersecurity risks, including, for example, throughout the lifecycle of AI systems and organisational procurement processes.

26. Relevant technical and non-technical stakeholders are consulted in standards development and identification within the nation.

27. The cybersecurity marketplace provides solutions (e.g. products and consultancy services) to mitigate risks to the cybersecurity and cyber-resilience of AI-based systems and support the implementation of standards.

28. The cybersecurity marketplace provides effective solutions (e.g. products and consultancy services) that utilise AI-enabled cybersecurity controls where beneficial.

29. The domestic or international cyber-insurance markets provide organisations with insurance against losses resulting from AI-system compromise and AI-enabled threats.

30. Research and innovation into improving the cyber resilience of AI systems and mitigating against AI-enabled threats is being undertaken in the nation.

31. Research and innovation into developing and applying AI-enabled cybersecurity solutions is being undertaken in the nation.

Area 6: Organisational Practices

This *area* analyses organisational level of capacity (CNI and beyond) to protect against cybersecurity risks to and from AI. This *area* reviews the adoption of controls, processes and standards for ensuring the secure adoption of AI systems and mitigating AI-enabled threats.

Readiness indicators of this *area*:

32. Organisations are considering and using relevant standards, guidance and codes of practice to mitigate AI-related cybersecurity risks.

33. Organisations are implementing controls and processes beyond established standards for mitigating risks to the cybersecurity and cyber-resilience of AI-based systems they adopt, and AI-enabled threats.

34. Organisations consider the risks of shadow AI and have processes in place to identify and address these risks where relevant.

35. Organisations have put in place procurement processes to ensure the quality and security of the AI software and commercial AI products and tools they use.

36. Organisations have considered the effectiveness of current cybersecurity controls in relation to emerging AI-related cybersecurity risks and updated their security processes and practices accordingly.

37. Formal and informal forums are available within the nation for organisations to share and receive information on AI-enabled threats, and on the vulnerabilities of AI systems, including with the national incident response body.

38. Organisations engage in international debates and forums on AI-related cybersecurity issues and frameworks.

39. Organisations governance structures ensure cybersecurity and AI teams, and technical and non-technical stakeholders, work collaboratively to adopt AI securely and advance organisational resilience.

Area 7: AI Cybersecurity Awareness and Behaviour

This *area* explores levels of awareness of AI's impact on cybersecurity risks and safe practices. This *area* looks at the broad culture of AI cybersecurity awareness amongst government agencies, industry, the general population, and media platforms.

Readiness indicators of this *area*:

40. There is awareness of how AI impacts on cybersecurity risks and broader risks amongst leaders and employees working in government agencies and private firms, including policy makers.

41. AI users in the general population are aware of AI-related cybersecurity risks.

42. Cybersecurity awareness-raising and AI-literacy programmes include information on AI-related cybersecurity risks that has been adapted to different segments of the population exposed to various types of risks.

43. Consideration has been given to how AI may be used to enhance the offering of cybersecurity awareness-raising programmes.

44.The organisational decision-making culture within organisations in the public and private sector ensure that leaders balance the benefits and security risks of AI when adopting AI technologies.

45. National mainstream media and social-media platforms cover issues related to AI-related cybersecurity risks and broader risks.

46. Safe practices for mitigating AI-related cybersecurity risks are being followed by the general population.

47. *The content of AI awareness raising programmes is informed by harms identified through incident monitoring and assessments of national AI-related cybersecurity risks to the general public and organisations.*

Area 8: Trust and Confidence in Digital Services

This *area* reviews levels of trust and confidence in e-commerce and e-government services utilising AI, as well as the impact of AI-enabled fake news and disinformation on users' trust and confidence in digital services in general (utilising AI or not). This *area* also explores the mechanisms to report AI-related cyber harms among Internet users.

Readiness indicators of this *area*:

48. Initiatives are in place to measure and mitigate the extent to which users' trust and confidence in digital services is being impacted by the rise of AI-enabled fake news and disinformation.

49. Internet users have trust and confidence in e-government and e-commerce services utilising AI.

50. The mechanisms that Internet users use to report cyber harms (such as online fraud, cyber-bullying, child abuse online, and privacy and security breaches) facilitate reporting of AI-related cyber harms, or new mechanisms have been established.

Area 9: Education and Professional Training

This *area* focuses on the availability of AI related cybersecurity education and training initiatives. This *area* includes an assessment of how both the risks and opportunities AI present to cybersecurity broadly are incorporated into these initiatives.

Readiness indicators of this *area*:

51. Tertiary educational programmes that cover AI-related cybersecurity risks and AI-related cybersecurity opportunities are available in the nation.

52. There is sufficient uptake of tertiary programmes that cover AI-related cybersecurity risks and AI-related cybersecurity opportunities to established a pool of skilled workers that meets workforce demands.

53. Foundational components of AI cybersecurity risks are covered at all educational levels.

54. Professional training programmes that cover AI-related cybersecurity risks and AI-related cybersecurity opportunities are available in the nation.

55. There is sufficient uptake of professional training programmes that cover AI-related cybersecurity risks and AI-related cybersecurity opportunities to established a pool of skilled workers that meets workforce demands.

56. Consideration has been given to how AI is used to enhance the offering of education programmes, and professional training programmes.

Area 10: Defence and Intelligence

This *area* considers national defence and intelligence stakeholders' capacity to assess and adapt to AI cybersecurity risks, as well as the strategic implications of AI on the nation-security establishment.

Readiness indicators of this *area*:

57. The cybersecurity risks associated with the development of AI as a component of national defence capability has been assessed, and if necessary, the cyber-defence strategy has been adapted to take account of these.

58. The defence and national-security establishments have considered how AI might be adopted as part of their cybersecurity strategies and capabilities, and have processes for keeping up-to-date with developments.

59. Collaboration between civil and defence entities on AI-related cybersecurity risks exists and has been formalised.