Submission: Protecting Critical Infrastructure and Systems of National Significance

Dr Brett van Niekerk[1], Dr Trishana Ramluckan[2], Mr Barend Pretorius[3]

[1.] Senior Lecturer, School of Mathematics, Statistics and Computer Science, University of KwaZulu-Natal, Westville, South Africa

[2.] Postdoctoral Research Fellow, School of Law, University of KwaZulu-Natal, Durban, South Africa

[3.] PhD Candidate, School of Management, IT and Governance, University of KwaZulu-Natal, Durban, South Africa

1. Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?

Some additional sectors that can be considered include:

Manufacturing: manufacturing could provide the necessary equipment, tools and supplies that are required for the maintenance and repairs that are used in other sectors.

Mining: this provides the raw materials for manufacturing, and also impacts on economic activity in terms of export. Impacting specific commodities could also impact international markets.

Chemical: certain chemical processing (for example, fertiliser production, production for cleaning products etc) could be targeted to cause local destruction due to failed processes.

Construction: This sector could provide the tools to recover from physical damage and/or destruction to other sectors (e.g. bridges and dams).

Sanitation and waste disposal: Severe disruption of sanitation and waste disposal could result in general decline of health, contamination of water, and a decline of morale.

Law enforcement and first responders: This is especially important as a disruption of first responders could be used as a 'force multiplier' in conjunction with other incidents (assuming intentional malicious actions).

Government: Local and national government is a critical sector as the provide the leadership and decision making, especially in times of crisis. A suggestion that the functioning of a government or an election has been subverted or compromised has a major impact in the trust and legitimacy of those in office.

National icons: This is one aspect that is not often considered. An attack on these (or destruction thereof) can be symbolic, but have an important psychological affect.

Another suggestion is that communication and the data and cloud could be combined. From the above, manufacturing, mining, and chemical sectors can be combined; as could government and law enforcement. In some cases a category of essential services could be used to encompass food, water, government, health, sanitation, and law enforcement and first responders.

2. Do you think the current definition of Critical Infrastructure is still fit for purpose?

The definition in the document considers a broad range that is sufficient. With the rise of influence operations and 'fake news', the psychological aspect could also be explicitly considered, or it could be incorporated into the social component. Perhaps national defence and national security can be combined.

3. **Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?**

These should be sufficient; however, there should be consideration for the consequences of *multiple* compromises. For instance, the compromise of a chemical plant resulting in fires and or toxic fumes (requiring evacuation) may be compounded in first responders are compromised simultaneously. Another example is the compromise of a health facility and surrounding traffic systems. The traffic backlog could affect the relocation of patients should that be required due to the health facility compromise.

4. **What are the common threats you routinely prepare for and those you have faced/experienced as a business?**

For the higher/tertiary education and transportation sectors, common threats include:

- Cyber-attacks (mainly cyber-crime and malware experienced)
- Disruptive and violent protests
- Severe weather conditions

In general, mismanagement and corruption has affected critical infrastructure operators, including electricity distribution and the viability of transportation and communication/broadcasting organisations.

5. **How should criticality be assessed to ensure the most important entities are covered by the framework?**

Type and severity of consequence, likelihood of compromise, as well as the time frame that the consequence will be realised should an incident occur. For instance, a compromise of electricity generation or distribution will have significant impact immediately. Education would probably be resilient to a disruption for a week or more.

6. **Which entities would you expect to be owners and operators of systems of national significance?**

Operators of electricity generation and distribution, critical pipelines, essential services (health, water, sanitation, first responders), and major transportation hubs (ports, airports, and railways).

7. **How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?**

In theory, the proposed TISN can support resilience through communication of best practices, training initiatives, knowledge sharing and collaboration, response coordination, and early warning of adverse events or attacks (for example, if an infrastructure experiences a cyber-attack, information can be distributed to aid others in preparing for the same or similar incidents). However, similar concepts to the TISN did not achieve success early on in the US for cyber-security, as there was resistance to the programme. In addition, when the South African Cybercrimes and Cybersecurity Bill was open for comment, there was strong resistance to the intelligence agencies having oversight. These cases are worth considering when engaging with stakeholders and attempting to achieve buy-in from them.

The TISN can be expanded to include allied nations, so international coordination and early warning can be achieved.

8. What might this new TISN model look like, and what entities should be included?

Sector-specific centres or hubs can be used to leverage off the commonalities within the sector, and a central co-ordinating centre to provide national and cross-sector support and communication.

The South African model for cybersecurity is a central Cyber-security Hub, with sector CSIRTS, and centres for the military, intelligence, and law enforcement. This appears to be somewhat align to the US ISAC concept.

Key functions should include:

- Response coordination
- Early warning and threat intelligence
- Training
- Best practice and knowledge sharing
- Collaboration

9. How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?

Conferences and workshops (preferably annual) to bring together practitioners (operators and vendors), academia, government, and civil society to engage and facilitate knowledge sharing.

Exercises to test decision-making and security/protection systems and processes; this will also aid in promoting coordination and create collegiality across sectors.

10. Are the principles-based outcomes sufficiently broad to consider all aspects of security risk across sectors you are familiar with?

They are. However, there needs to some explicit mention for skills development, education and training to ensure there are sufficiently capable human resources for implementation.

11. Do you think the security obligations strike the best balance between providing clear expectations and the ability to customise for sectoral needs?

In general they are, again skills development should be explicitly mentioned. The objectives appear ‘siloed’, and can maybe benefit from the concept of integrating the PSOs. For example, correlation of physical logs and network login information will aid in determining if there is a login where the account owner is not physical present. Personnel security can provide important information to both physical and cyber security: for example, a disgruntled employee who has resigned may be a threat, and that information will prepare the security functions for a possible incident.

12. Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?

We do not deal with Australian organisations to be able to comment.

13. What costs would organisations take on to meet these new obligations?

We do not deal with Australian organisations to be able to comment.

14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

We do not deal with Australian organisations to be able to comment.

15. Would the proposed regulatory model avoid duplication with existing oversight requirements?

We do not deal with Australian regulators to be able to comment. However, in some instances duplication may be beneficial to reinforce the importance of certain requirements, and to align them with other requirements.

16. The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?

Information that can be provided in the guidance and communications include: suggested best practices, processes, tools and templates, case studies, specific warnings and methods to address malware strains or emerging threats and technologies.

17. Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?

In South Africa, independent regulatory bodies are often created specifically for the purpose. This could be followed where no regulatory entity is in place.

18. What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?

Training and engagement to identify or develop and implement consistent tools and practices. There will be benefit for a general 'train the trainer' process, where the regulators are trained for their functions, and provided with best practice in providing the training and education solutions that can then be implemented within their sectors. Regulators will benefit from specific legal mandates to perform their duties and to enforce compliance.

19. How can Government better support critical infrastructure entities in managing their security risks?

High-level best practices, tools, templates, and processes that can be used and cascaded down into various sectors will be useful. This will allow for consistency and interoperability where collaboration and coordination is required amongst various sectors and responders.

20. In the AusCheck scheme, potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

That schemes should be implemented for other areas of critical infrastructure (assets of strategic national importance), in particular electricity generation and distribution, major water facilities, and first responders.

21. Do you have any other comments you would like to make regarding the PSO?

When considering security objectives, the alignment of specific activities to human rights, international laws and local laws should be considered.

22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

Table-top exercises and other technical cyber exercises will allow for the identification of vulnerabilities and mapping the attack surface, and proposed solutions to remediate vulnerabilities or mitigate the consequences of an incident.

A cooperative honeynet operation and cyber-intelligence centre will aid in the identification of threats, vulnerabilities, and remediating solutions.

Policies and procedures for the management of emerging technologies and the risks or vulnerabilities they introduce will be beneficial. A particular example is the Internet of Things (IoT); often organisations considered IoT only within defined projects, and do not consider the existing IoT devices within the organisation.

23. What information would you like to see shared with critical infrastructure by Government? What benefits would you expect from greater sharing?

National threat posture, any identified or emerging threats, any remediation information for known threats, indicators or compromise and techniques, tactics and procedures for threat actors.

Having a common framework, taxonomy, and protocols for information sharing will be important – the initial focus should be on establishing the information sharing capability.

24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

As we are not an Australian organisation, we would not actively participate in routine engagements in this regard. However, we would be willing to collaborate with Australian organisations through research and consulting if it is viable for South Africans to contribute.

25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

- Regular vulnerability scanning (monthly, and on any new system implementation or system change)
- Regular penetration testing (yearly, and on any new system implementation or system change)
- Table-top and red team / blue team exercises
- Cyber intelligence (cyber threat intelligence feeds, vendor alerts, open source intelligence such as SiloBreaker and Recorded Future)
- Bug bounty and responsible disclosure programmes (however these may be risky for critical infrastructure if not managed correctly)
- Regular and proactive risk management and audits of cyber security control implementations.

26. What are the barriers to owners and operators acting on information alerts from Government?

Lack of trust or scepticism, information overload, inadequate skills

27. What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?

A mix of real-world case studies and the lessons learnt and hypothetical examples with war-gamed responses and procedures. Flow diagrams for decision making, contact details, and any information on specific consequences or potential adverse effects related to certain response actions.

For specific sectors and organisations, information on the following should be provided (see ISACA CISM for more detail):

- Defined roles and responsibilities,
- Important contact information,
- System triage,

- Recovery time objectives,
- Recovery point objectives,
- Service delivery objectives, and
- Maximum tolerable outage.

28. What safeguards or assurances would you expect to see for information provided to Government?

Government should safeguard all information according to its own laws and procedures defined for the critical infrastructures.

29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

When dealing with actions against international actors, these situations and the allowable actions are covered by international law. Various studies and documents, such as the two *Tallinn Manuals*, assess and discuss these considerations. An extensive list of relevant documentation is provided at the end of this document.

30. Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

The Prime Minister and/or relevant minister, following the appropriate democratic process. Advice should be from the primary cyber-security and national security officials. A multi-stakeholder national cyber security advisory council (with representatives from the sectors, government, military, intelligence, law enforcement, academia, and civil society) should be implemented to provide input.

31. Who should oversee the Government's use of these powers?

A multi-stakeholder or parliamentary oversight committee, with representatives from with advisory council mentioned above.

32. If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?

Yes – the response will probably need to be dealt with on a case by case basis depending on the attack type as well as location. A challenge could be that the attack is emanating from a compromised third-party system. Should the perpetrators be identified in an allied nation, their law enforcement could assist with disrupting the attack. If the perpetrators are identified in a hostile nation, direct measures may be needed, aligned to international law in terms of necessity and proportionality.

33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

Immunity from local laws against cyber-attacks or cyber-crime, provided the actions they took were sanctioned. Should an official/officer take unsanctioned action (i.e. vigilantism or rogue actions) then they should be held to account based on the relevant laws.

34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?

Oversight at a national level as described above, with well-defined approval structures to ascertain if actions taken are sanctioned or not, with the necessary punishments clearly listed. These also need to be aligned to international law (see the documents provided at the end of the submission).

35. What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

Industry taking direct action may make them a target for further retaliation and escalation. Disproportionate responses, or accidental damage to another nation's critical infrastructure may bring negative reputational, political and /or economic impacts to Australia.

36. Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

Ideally, specific industry organisations should not be affected in terms of their risk management roles and responsibilities if they are already in place and adequate. Their specific processes that are already in place can feed up into sector and then national structures for risk management. If there are inadequate or immature processes in the industry, then they will be impacted in a positive way to bolster their existing processes.

Documents for further reading

NGO / regional / international organisation documents that can used to guide the strategy include:

- The Global Commission on the Stability of Cyberspace Final Report (https://cyberstability.org/report/)
- The *Paris Call for Trust and Security in Cyberspace* (https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433.pdf)
- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant reports
- The *Tallinn Manual* and *Tallinn Manual 2.0*
- The Budapest Convention (The Convention on Cybercrime of the Council of Europe (CETS No.185))
- The AU Convention on Cyber Security and Personal Data Protection
- The SADC Model Law on Computer Crime and Cybercrime
- ISACA CISM Manual.

National documents that can be used to inform the strategy include:

- Letter of 5 July 2019 from the Netherlands Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace; Appendix: International law in cyberspace (https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf)

- The French perspective on International Law Applied to Operations in Cyberspace (2019) (https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf)
- Cyber Security Strategy for Germany
- National Cyber Strategy of the United States of America (2018)
- Moteff, J.D. (2015, June 10), Critical Infrastructures: Background, Policy, and Implementation, Congressional Research Service, https://fas.org/sgp/crs/homesec/RL30153.pdf
- The South Africa Critical Infrastructure Protection Act (Act 8 of 2019)
- The South African Electronic Communications and Transactions Act (Act 25 of 2002)
- The South African Cybercrimes Bill (Bill 6 of 2017)
- The South African Protection of Personal Information Act (Act 4 of 2013)
- The South African National Cybersecurity Policy Framework
- The South African Terms of Reference for the National Cybersecurity Advisory Council (https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/NCAC-ToR-2017-Reappointment_V1.pdf)

Research documents that can be used to inform the strategy:

- Francois Delerue (2020), *Cyber Operations and International Law*, Cambridge University Press.
- Russel Buchan (2019), *Cyber Espionage and International Law*, Hart Publishing.
- Bobby Chesney (2020), *Chesney on Cybersecurity Law, Policy, and Institutions*, ver 3. https://ssrn.com/abstract=3547103
- Barend Pretorius and Brett van Niekerk (2020), “IIoT Security for the Transportation Infrastructure”, *Journal of Information Warfare* 19(3), pp. 50-67.
- Trishana Ramluckan (2020), “International Humanitarian Law and its Applicability to the South African Cyber Environment”, *Journal of Information Warfare*, vol. 19, no. 3, pp. 102-117.
- Trishana Ramluckan and Brett van Niekerk (2019) “International Humanitarian Law and Cyber-Influence Operations”, *Journal of Information Warfare*, vol. 18, no. 3, pp. 67-82.
- Brett van Niekerk (2019) “South Africa and the Cyber Security Dilemma”, *Journal of Information Warfare*, vol. 18, no. 2, pp. 96-116.
- Brett van Niekerk and Trishana Ramluckan (2019) “Economic Information Warfare: Feasibility and Legal Considerations for Cyber-Operations Targeting Commodity Value Chains”, *Journal of Information Warfare*, vol. 18, no. 2, pp. 31-48.
- Brett van Niekerk (2018) “The Cyber Security Dilemma: Considerations for Investigations in the Dark Web”, *Acta Criminologica* 31(3), Special Edition: Cybercrime, pp. 132-148.
- Brett van Niekerk, Barend Pretorius, Trishana Ramluckan and Harold Patrick (2018) “The Impact of IoT on Information Warfare”, in: Fields, Z. (ed.), *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, IGI: Hershey PA, pp. 141-164.
- Brett van Niekerk and Manoj Maharaj (2011) “Relevance of Information Warfare Models to Critical Infrastructure Protection,” *Scientia Militaria*, vol. 39, no. 2, pp. 99-122. Available online: http://scientiamilitaria.journals.ac.za/pub/article/view/114/147.

- Brett van Niekerk (2017) “Analysis of Cyber-Attacks against the Transportation Sector”, in: Korstanje, ME. (ed.), *Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities*, IGI: Hershey PA, pp. 68-91.
- Martha Grobler, Pierre Jacobs, and Brett van Niekerk (2017) “Cyber Security Centres for Threat Detection and Mitigation”, in: Korstanje, ME. (ed.), *Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities*, IGI: Hershey PA, pp. 22-52.
- Brett van Niekerk, Trishana Ramluckan and Daniel Ventre, (2020) “Assessment of the French and Dutch Perspectives on International Law and Cyber-Operations”, *Proceedings of the 19th European Conference on Cyber Warfare and Security* (ECCWS), 25-26 June, pp. 380-389.
- Tim Grant, Carien van ‘t Wout and Brett van Niekerk, (2020) “An Ontology for Cyber ISTAR in Offensive Cyber Operations”, *Proceedings of the 19th European Conference on Cyber Warfare and Security* (ECCWS), 25-26 June, pp. 117-125.
- Pierre Jacobs, Sebastiaan von Solms, Marthie, Grobler and Brett van Niekerk, (2019) “Towards a Framework for the Selection and Prioritisation of National Cybersecurity Functions”, *Proceedings of the 18th European Conference on Cyber Warfare and Security* (ECCWS), Coimbra, Portugal, 4-5 July, pp. 229-238.
- Brett van Niekerk and Trishana Ramluckan (2019) “A Legal Perspective of the Cyber Security Dilemma” *Proceedings of the 18th European Conference on Cyber Warfare and Security* (ECCWS), Coimbra, Portugal, 4-5 July, pp. 544-553.
- Brett van Niekerk, Trishana Ramluckan and Petrus Duvenage (2019) “An Analysis of Selected Cyber Intelligence Texts” *Proceedings of the 18th European Conference on Cyber Warfare and Security* (ECCWS), Coimbra, Portugal, 4-5 July, pp. 554-559.
- Barend Pretorius and Brett van Niekerk (2015) “Cyber-Security and Governance for ICS/SCADA in South Africa” *10th International Conference on Cyber Warfare and Security*, 24-25 March, South Africa, pp. 241-251.