

# Multidisciplinarity and Multistakeholderism for Cyber Resilience of Emerging Economies: Lessons from Cyber Challenges

Brett van Niekerk

Noelle van der Waag-Cowling

Trishana Ramluckan

# Introduction

- 
- WEF Davos 2022: *Digital resilience: Building the economies of tomorrow on a foundation of cybersecurity*
    - “Building global collaboration to combat cyberthreats”
    - “Partnerships in action”
  - Cybersecurity has multi-disciplinary aspects, and multiple stakeholders are essential for national and international cyber-resilience
    - This fact is often lost in national strategies and academic works, where the focus can be from a single disciplinary perspective
    - Cyber professionals need a good grounding in a variety of areas

# Introduction

- Cybersecurity competitions as experiential learning
- Provide a useful mechanism to appreciate the importance of the multidisciplinary and multistakeholder aspects to cybersecurity

*"You can't give her that!" she screamed. 'It's not safe!' IT'S A SWORD, said the Hogfather. THEY'RE NOT MEANT TO BE SAFE.*

*'She's a child!' shouted Crumley.*

*IT'S EDUCATIONAL.*

*'What if she cuts herself?'*

*THAT WILL BE AN IMPORTANT LESSON."*

*— Terry Pratchett, Hogfather*

# Cyber Security Competitions

- Capture the Flag
  - Jeopardy
  - Attack-defend
- Global Cyber Challenge (GCC 2.0 in 2021)
  - Strategy and Policy Track
  - CTF (IT and OT)
  - Innovation track
- Cyber 9/12 Strategy Challenge
  - Cape Town (2021)
  - Geneva (2022)
- Gamification solutions

# Technical Perspectives

- Capture the Flag
  - Very technical, sometimes arbitrary problems
  - Good for problems solving skills
  - Participants started trading answers
- GCC Strategy & Policy Track
  - What need to do is easy, how...not so much
  - Reliant on broader range of stakeholders
    - Big tech & ISPs to help filter
    - Vendor for patch
  - Focus became advisory, help desk and assisting with incident response


# Technical Perspectives

- Cyber 9/12
  - Single discipline teams missed major aspects of responding to the scenario
  - Solutions from multidisciplinary teams were more well-rounded
- Gamification solutions
  - Gamified table top exercise for cyber diplomacy and attribution
  - Differences in how key concepts were interpreted





# Strategy Perspectives

- 
- Significant Cyber Events
    - The speed and scale of propagation
    - The proliferation of threat actors
    - Contagion risk
  - Complexity of significant cyber events
    - Overwhelm a 'system of systems'
    - Cascading effects of systemic cyber incidents
  - Shift in focus from government or “regime” security to societal security and resilience

# Global South Strategy Perspectives

- Global South nations experience significant resource shortfalls
- National threat landscapes characterized by massive, single points of failure
- Lack of cyber maturity at the strategic – institutional and capability levels
- A robust national cyber event response capability is a key factor in mitigating resource shortfalls





# Strategy Perspectives

- Inter-dependencies within national cyber ecosystems
- A 'whole of nation' approach
- Requirement for frictionless integration of national capabilities and cross sectoral response
- Diversity is about diverse experiences, thoughts, abilities and perspectives
- Noticeable difficulties across competitions in the articulation and implementation of truly multi-stakeholder solutions



# Educational Perspectives

- Experiential learning to help bridge the technical and policy gap
  - Different disciplines learn to communicate and engage to produce holistic solutions
  - Challenges = interactive simulations, build 'muscle memory' and understanding amongst disciplines
- Challenges offer a number of different learning areas for cyber security students:
  - Mental/Emotional development
    - Stamina and commitment in pressure situations
    - Team Work
    - Agile thinking & ability to adapt and evolve



# Educational Perspectives

- Presentation and speaking skills
  - Identifying key issues and frontload them to decision makers
  - Preparation, succinct articulation
  - Successfully motivate and advocate chosen pathways/solutions based upon expertise and research
- Articulating Responses within set policy or legal parameters
- Focus on prioritization
- Emphasis of roles and responsibilities
- Risk Assessment
- Risk Tolerance
- Balancing and accepting risk

# Educational Perspectives

- Judges also have a learning curve in Cyber 9/12:
  - Have 2 minutes to assess participant proposals
  - Engaging with different disciplinary perspectives
- The experience provides simulated training for both participants and judges
- Using such challenges is useful for relevant stakeholders of government and critical infrastructure to learn to work together during a crisis with technology partners
- Palpable difference in the approach and priorities of judges from different regions

# Legal Perspectives

## Challenges with the legalities

- Why are the legalities important?
- The legal challenges presented the issues of legal compliance meets the real world
- The key element of attribution needs identification and reasonable evidence
- Complications as to which legal mechanisms are in place
  - Relevance of other nation's laws
  - Responses align to internal laws




# Legal Perspectives


- Offensive vs. defensive cyber legislation
- International laws that may apply
- Jurisdiction (cyber boundaries?) and legislation
- Treaties and conventions for collaborative alliances
- Legal remedies
- Creating this presentation resulted in discussion on interpreting points
  - Illustrates need for multidisciplinary competitions to facilitate a common understanding




# Relevance to Emerging Economies

- 
- Foster multistakeholder forums for cybersecurity
  - Whole-of-society approach:
    - Government
    - Big tech and key ISPs
    - Academia
    - Civil Society
  - Support participation in international working groups
  - Build multidisciplinary cybersecurity capacity
    - Encourage participation in international competitions (particularly for govt & critical infrastructure)
    - Partner with international organisations to host local competitions for capacity building
    - Conduct exercises with all stakeholders

# Relevance to Emerging Economies

- 
- Uniqueness of emerging economies
  - Emerging economies at higher risk from cyber attacks
  - Defensive, preventative mechanisms need to be established which cyber competitions allow for practical preparation
  - Treaties between countries with emerging economies
  - We were playing as a country with a mature cyber defence capability and found road blocks
    - How will an emerging economy perform?

# Conclusions

- 
- The nature and elements of cybersecurity
  - Multidisciplinary/ Multi-stakeholders
  - Raises the questions before the fact
  - Regional Institutions (e.g. AU, UNASUR & EU) - a stable and solid cyber capacity the capacities built to utilize cyberspace need to be secured- through practical competitions
  - International Public Private Partnerships involved in cyber competitions
    - Building knowledge
    - Knowledge transfer

# Thank you!

# Questions?

Brett van Niekerk: [brettv@dut.ac.za](mailto:brettv@dut.ac.za)

Noelle van der Waag-Cowling: [noelle@sun.ac.za](mailto:noelle@sun.ac.za)

Trishana Ramluckan: [ramluckant@ukzn.ac.za](mailto:ramluckant@ukzn.ac.za)