Cybersecurity Maturity in the Pacific Islands – Informing a Regional CERT Framework

Anthony Adams
Monash University
anthony.adams@monash.edu

Gillian Oliver
Monash University
gillian.oliver@monash.edu

Carsten Rudolph
Monash University
carsten.rudoph@monash.edu

Abstract

Cybersecurity acts as a strong influence on national governments' security, economic, physical and social interests. A common policy goal of governments is to protect their respective interests by supporting cybersecurity threat and attack response capabilities. Contemporary research addresses the use of multi-national CERT frameworks to improve national cybersecurity capability maturity and resilience, however little research has been conducted into the efficacy of such frameworks with Pacific Island nations. This research employs a qualitative interview technique to develop an inductive model for a regional Pacific Islands CERT framework. The research proposes a Pacific Islands regional model based on a network of affiliated national CERTs that operate independently and reflect their respective national interests, while collaborating on matters of shared interest, supported by regional partners providing targeted assistance to build national and regional cybersecurity capability maturity and resilience.

1. Introduction

Cybersecurity is recognized as a driver of national security and economic growth, with more than fifty nations having enacted national cybersecurity policies or strategies in the last decade [1]. A common goal of these national strategies is to protect nations' respective interests by implementing policy frameworks that provide resilient response capabilities to cyber threats and attacks which, in turn, protect their national defense, economic, physical and social infrastructure assets.

Pacific Island nations use independent policy approaches to support their respective domestic priorities (This research presents the Pacific Islands as a regional grouping of nations, containing Australia, Cook Islands, Federated States of Micronesia, Fiji, French Polynesia, Kiribati, Nauru, New Caledonia, New Zealand, Niue, Palau, Papua New Guinea, Republic of Marshall Islands, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu). Tonga, Samoa and Papua New Guinea currently support national policy frameworks, while Kiribati, Vanuatu and Fiji have emerging practices and awareness. Australia seeks to foster a Pacific Islands regional approach to national security through the Cyber Cooperation Program [2] which recognizes that in general, Pacific nations have varying, although relatively poor levels of cybersecurity readiness. The Australian approach recognizes that as a dominant regional partner, Australia's interests are active in all Pacific Island nations and are vulnerable to cybersecurity breaches and attacks, particularly in nations with relatively immature response capabilities, and that Australia has a significant role to play in improving capabilities across the region.

Over the last 30 years, many nations have developed Computer Emergency Response Teams ('CERTs') to provide cyber threat advisory and response capabilities. CERTs typically provide a mix of proactive and reactive response capabilities across different service domains, including Coordinating, Servicing, Thematic and Product [3]. The differing nature of these service domains leads to consideration of national governments' cybersecurity response priorities.

Contemporary practice highlights the importance of smaller nations focusing their limited CERT resources and expertise on specific areas of interest, while collaborating with other providers, to provide a full suite of services and capabilities. In the Pacific Island region, PacCERT was initiated in 2011 as a multi-national Pacific Island CERT, however it was suspended in December 2014 and has not been renewed. Subsequently, Tonga, Papua New Guinea and Samoa have established national CERTs; Samoa has grounded its CERT within a 5-year policy and strategic framework [4] that supports the prioritization of domestic and regional engagement and response capabilities.

URI: https://hdl.handle.net/10125/79999
978-0-9981331-5-7

While there is extensive academic research into the form and function of regional CERTs in densely populated, geographically proximate regions including Africa, Europe and NATO, relatively little focus has been given to the sparsely populated, geographically, ethnically and culturally disparate Pacific Island region.

Our research responded to the lack of academic focus on the use of multi-national CERTs within a Pacific Islands regional context, by examining the factors that influence the purpose, form and function of a regional threat response capability. To frame this research, we identified two competing perspectives relating to national and regional management of cybersecurity response capabilities – firstly, the "developed nation" view that nations should adopt global best practices to leverage their existing institutions and secondly, the "developing nation" view that existing institutions may not be in place and the national focus should be on building and reinforcing these institutions. We applied a developing nation perspective to examine the following research question: *How can cybersecurity threat response structures and practices across Pacific Island nations be leveraged to inform a regional Pacific CERT framework?*

Research outcomes included the identification of two semantic themes that influence the form and function of a regional CERT framework: firstly, developing nations will maximize their cybersecurity response capability using multi-national, regional CERTs and secondly, nations will seek to preserve their national interests in any regional framework. The research also identified four outcomes that help to enact the semantic themes. These are discussed at length in Sections 5 and 6.

2. Theoretical Background

2.1. Evolution of the Multi-National CERT

Defining a general CERT form and function provides a starting point for consideration of a regional Pacific Islands framework. Significantly, the "developed nation" worldview focuses on the development of individual CERTs in developed countries, whereas the "developing nation" worldview recognizes a shift in focus toward development of supranational, regional frameworks.

Contemporary (post-2010) academic literature provided an established general definition of CERT purposes, forms and functions however, consideration of a regional framework required discussion on how a combination of regional CERTs, developing nations, universities, commercial partners and "developed nation" neighbors could provide complementary services, across national borders [5] [6]. Implicit in the allocation of tasks between participants in a regional framework was recognition that CERTs are not homogeneous and that they differ in purpose and form [6]. As CERTS increasingly focus on delivery of specific tasks that respond to the objectives of their parent organization, the constituencies they serve and the urgency with which services must be provided [7], regional frameworks have evolved to include partners with complementary skills, to provide a full suite of proactive and reactive cyber threat responses.

This evolution led to a contemporary understanding that regional CERTS include a coordinated approach between multiple participants, each with different specializations, based on a blend of shared global and regional interests and local response capabilities [6] [8]. This broader understanding allowed the definition of a regional CERT to be extended to include a blend of transnational infrastructure spanning multiple countries and used by all actors, with subnational (i.e., Silicon Valley) and supranational (i.e., Pacific region) areas bounded by shared geographical, political and economic interests.

Literature identified the importance of small "developing" nations advancing their shared interests including trade, defense and the delivery of public services, through the development of cooperative institutions. Implicit within the use of cooperative institutions is the sharing of expertise across national boundaries [3] [7] [9]. The literature generally approached the sharing of expertise from a developed nations perspective [7], with the European Union and NATO used as examples of regional groupings with dense populations, geographic proximity and "developed nations" economies as the basis for a regional response. In contrast, the Pacific Islands region contains developing member nations with different cultural, ethnic, political and economic characteristics; they individually lack the critical mass to present their own interests globally [4] [9] and may leverage a pan-regional framework for the advancement of shared interests.

Consideration of regional frameworks was extended to the use of a network of distributed CERT functions across local and national jurisdictions [5] [10] [11]. In this general approach, independent local CERTs operate within national boundaries, with the regional CERT managing the decentralized, distributed response to incidents across different nations. This approach emphasized the need for CERTs to operate independently while also collaborating with specialized partners across industries, academia, and governments on matters of shared interest.

The literature generally approached the need for collaboration from a developed, rather than developing

nations' perspective. The developed nation's perspective emphasized leveraging existing global best practices, stable government and public institutions [8] as part of a regional framework. In contrast, the developing nation's perspective focused on the need to prioritize building and maintaining these societal foundations [8] as the basis for supporting a regional framework, with Pakistan [12] providing an example of an integrated national policy strategy involving government, academia, and the private sector. The Samoan policy approach [4] offered a "middle way" for developing nations, that prioritized the reinforcement of Samoa's national institutions and societal foundations, while also leveraging knowledge and resources from regional partners and developed nations.

2.2. Regional Approach to Delivering CERT Services

Implementing a regional CERT framework built on collaboration between specialized actors with intersecting interests, led to consideration of the most appropriate regional approach to providing a suite of complementary services.

While small states may use regional collaboration/partnerships to enhance their influence and interests, larger partners may be reluctant to provide support, with this reluctance contributing to a stifling of regional identity and norms [13]. The United States and European Union provide examples of larger powers resisting the need to subjugate their own national interests to those of a regional body. In both cases, the US and EU have argued that their partners should maintain their own national CERTs to protect their own, and by extension, the larger powers' interests. They have resisted establishing UN-level governance of the Internet through the International Telecommunications Union, warning against creating a 'prescriptive regulatory code for the world'. This unwillingness to provide reciprocal partnership, institutions and defining characteristics and capabilities may provide a key inhibitor to the successful function of a Pacific Islands regional CERT framework.

The literature did not explicitly consider a lack of developed nations' support in the Pacific Islands region, however it highlighted the reluctance of New Zealand as the second largest regional power and overall, net consumer of intelligence on a wide range of cybersecurity issues, to insert itself in a regional forum as a dominant partner [13]. Contrary to this approach, Australia retains ownership and management of most of its cybersecurity infrastructure with the private sector and uses regional engagement to provide opportunities to build and maintain economic relationships that advance the interests of both Australian (government and non-government) and regional participants [2] [14].

2.3. Projecting the National Interest in a Regional CERT

Small nations may lack the material resources available to advance their national interests beyond their domestic borders, in which case they will use regional forums and frameworks to project their national identity and behavioral norms, as a way of reinforcing their interests [13] [14], both domestically and regionally. In doing so, they will adopt one of 3 frameworks [13]: (1.) Small nations will form an alliance with the dominant regional power, on the basis that they cannot avoid the larger nation's influence in the region; (2.) Small nations will build liberal institutions across the region, as a way of coercing influence with neighbors, (3.) Small nations will assert their identity, values, and social norms in the region - nations tend to act in line with the identity and norms that they project within their region.

Framework 1 emphasizes the need for large regional members or partners to be actively involved in building a regional CERT framework; without their participation, other nations may lack the influence or resources to build a consensus outcome. Framework 2 implies that a country's national interest is enhanced where it can build and maintain liberal regional institutions. Framework 3 leads to the importance of developing a regional CERT identity that all member countries can identify with and endorse.

While small nations may seek to advance their national interests by collaborating with regional partners, they tend to rely on larger regional partners to provide leadership and resources [13]. This provides an apparent contradiction that sits at the heart of the regional CERT framework – as small nations seek material support from larger partners so they can build local capacity and hence, reduce their reliance on larger partners, they risk becoming beholden to the larger partners in exchange for said support. To avoid this contradiction, small nations will seek ways to retain sovereignty over their resources and assets, while also seeking targeted support [3].

Small nations may respond to this contradiction by reinforcing their national interest through a policy approach that targets an integrated domestic cybersecurity response capability, including local policy, institutions, and government structures [3] [15] [16]. Within this domestic context, the national CERT assumes additional significance as the government vehicle to build an integrated national capability. In doing so, the CERT assumes responsibility for protecting the national interest through underpinning national and economic security, the on-going operations

of a government, and the stability of critical infrastructure. This contradiction highlights the propensity of national governments to prioritize national security by protecting information infrastructure, before underpinning economic growth through a long term, strategic cybersecurity framework [3] [15] [16].

3. Methodology

This research employed a qualitative interview approach to gather and analyze personal narratives from cybersecurity practitioners in the Pacific Islands region. The research applied an emergent design strategy which allowed flexibility and adaptation in the line of inquiry, as the discussion and level of understanding deepened. The strategy used one to one, semi-structured interviews, allowing for open-ended enquiry and development of personal narratives as the source data for subsequent qualitative inquiry. The qualitative inquiry process was oriented towards identification and exploration of semantic themes, and the use of inductive logic to build general patterns of observations.

The research was conducted from within a social constructivist perspective, using naturalistic or qualitative methods to understand the participants' experiences and identify emerging factors that might define the participants' contextual realities. These methods included open questions that allow the participants to describe their perceived realities through personal narrative, and the researcher to interpret meaning based on their own personal and cultural experiences. Initial participants, as summarized in Table 1, included four cybersecurity practitioners in Tonga, Kiribati and supporting partners in the European Union.

Participants were invited to join one semi-structured, interview of 20 – 45 minutes duration. These interviews provided the source data for the subsequent content analysis. All interviews followed a similar protocol: participants were initially asked to describe their specific experience in the Pacific cybersecurity community, before progressing through 11 thematically sequenced questions organized in 4 sequential blocks, which allowed the participants to build a personal narrative through the discussion.

Interview transcripts were analyzed using a three-phase analysis process. Firstly, all self-contained thoughts that related to the interview protocols were annotated. Thoughts ranged from a phrase to a complete sentence or group of sentences. The only material excluded was content that did not relate to the interview, such as introductory small talk. Secondly, annotated thoughts were coded into emergent categories. The participants' lived experiences were used to guide the emerging themes and categories. Thirdly, the categories were grouped into two overarching semantic themes.

Table 1. Participants – nationality and Pacific CERT experience

Participant	Nationality	Pacific CERT experience
Participant 1	United Kingdom	Provides regional consultancy and advisory services
Participant 2	Switzerland	Provides regional training and capacity building
Participant 3	Tonga	Established and ran the Tonga CERT
Participant 4	Kiribati	Implements government cybersecurity policy

4. Findings

Analysis of the initial interview transcripts yielded 20 categories, grouped into two semantic themes: Firstly, the purpose, form and function of a Pacific Islands regional CERT, and secondly, the domestic imperative to preserve a country's national interest. Table 2 presents the relationship between the two semantic themes and categories and provides a reference point for the consideration of research and practice implications. Tables 3 and 4 present the semantic themes, associated categories and frequencies of occurrence.

Table 2. Relationship between the semantic themes and categories

Semantic Theme	General form	Observations
1 – Purpose, Form and Function of a Regional CERT	Tangible, action-based outcomes.	Categories 1-11 Participants described "how the CERT should work"
2 – Preserving the National Character	Abstract, behavioral-based outcomes	Categories 12-20 Participants described "why the CERT is important"

Categories 1-7 and 12-15 were consistent with the literature and tied the participant's narratives to the theoretical framework described in Section 2. The links between narratives and literature are summarized in Tables 2 and 3, with the implications for practice and further research discussed in Section 5. Categories 8-11 and 16-20 were not aligned with the literature and provided opportunities to extend the theoretical framework. These non-aligned findings included four specific challenges that act as disincentives for Pacific Island nations to commit to a regional framework (Categories 8-11), and five opportunities for national governments to reinforce their domestic interests within a regional framework (Categories 16-20). The challenges and opportunities were specific to the Pacific Island nations and reinforced the "developing nation" perspective on the importance of creating and stabilizing national institutions that then contribute to a regional framework.

Categories 8-10 were interdependent and reflected participants' frustration with the tendency for their teams to receive generic support from partners, without targeted and measurable outcomes. Participants discussed the need for a national CERT to monitor changes in its capability maturity, by measuring benefit outcomes from capability workshops and training (Category 8). Similarly, participants highlighted the importance of using increased capability maturity as an opportunity to assert national independence and reduce reliance on developed world partners for support and resources (Category 9). This was related to the participants' frustration at the general tendency of developed world partners to view the regional nations as a homogenous grouping without sufficient awareness of the cultural and ethnic differences between nations (Category 10). Participants also highlighted the lack of a regional legal framework (Category 11) that defined and protected their national interests, particularly with respect to the sharing of sensitive domestic information between member nations, as a critical inhibitor to a regional framework.

Categories 16-20 presented opportunities for member nations to strengthen their national institutions and interests through development and funding of strategic policies that target the development of local resources, industry and capability maturity and resilience.

Participants spoke about the critical need for national governments to move away from ad-hoc policy initiatives (Category 16) and an over-reliance on support from developed nations, towards framing domestic cybersecurity policies, and capability resilience and maturity within a strategic planning framework (Categories 17, 18, 19). Discussions identified the tendency for skilled local cybersecurity practitioners to seek better employment conditions and opportunities in developed regional nations, including Australia, New Zealand and the United States. In response, participants argued for national governments to prioritize spending towards sustainable, attractive domestic industries and employment opportunities (Categories 17, 18). Discussions also recognized the historical tendency for developing nations to rely on partner nations and organizations to contribute funding towards development of national infrastructure and identified opportunities for governments to assert their national identity and interests through targeted, strategic spending on domestic industry and infrastructure (Categories 16, 18, 19) and efforts to raise public awareness of the importance of their policy initiatives (Category 20).

5. Discussion

The research findings indicate that national CERT policies and practices can be leveraged to inform a regional framework, with the purpose, form and function being shaped by the domestic policy priorities of national governments, who can be expected to place their domestic priorities above those of the regional framework.

The two semantic themes provide important markers for consideration. While contemporary research applies a "developed nation" perspective to consideration of a regional framework supported by global practices, the participants challenge that perspective by identifying specific Pacific Island constraints, particularly around ongoing reliance on regional partners for provision of funding, skilled resources, infrastructure, and the development of sustainable national capability and resilience.

The findings identified four outcomes that enact the semantic themes, which are discussed in Section 6. Firstly, the regional CERT framework requires an affiliation of independent national CERTS, each serving their respective national interests, while collaborating on matters of shared impact. Secondly, regional partners have a critical role to play in providing support that targets national and regional capacity-building. Thirdly, regional partners' support should align with the policy priorities of the national governments. Finally, support for capacity building should be based on sound strategic and policy planning, with a focus on commercial investment opportunities and targeted domestic investment in resources (including people and skills), infrastructure and industry.

Table 3. Semantic Theme 1 – relationship with emergent categories and research/contribution

	THEME and CATEGORY	Research/Contribution
	Theme - Purpose, Form and function of a regional CERT *(39 occurrences)*	
1	***Category*** - Define the national CERT function	Supports the argument that local CERTs should focus on delivering particular services only, by proposing that local CERTs actively choose to identify themselves in relation to selected, highly specialised capabilities [5] [10] [11] .
2	***Category*** - Larger countries' roles	Challenges the framework for smaller nations engaging with larger partners using their national identities as a negotiating asset [3], to argue that smaller nations with limited resources will in fact, engage with larger partners on the basis of the help and/or resources that they can receive.
3	***Category*** - National stand-alone CERTs	Categories 3, 4 and 5 reinforce the case for nations to maintain small, targeted, local CERTs that can collaborate in a network of neighboring CERTs that are similarly structured and equally reflective of their national interest [3] [5] [10] [11].
4	***Category*** - Pathway to a regional CERT	
5	***Category*** - Regional network of stand-alone CERTs	
6	***Category*** - Regional partners	Categories 6 and 7 reinforce the argument that regional partners have a significant role in helping smaller nations build their domestic cybersecurity response capability [3] [5] [10] [11] by positing that smaller nations cannot operate in isolation and require ongoing, material support from regional partners, whether government, academia or private sector.
7	***Category*** - Working in Partnership	
8	***Category*** - Challenge - Monitoring outcomes as a measure of maturity	*New contribution* - Highlights the importance of measuring business benefits, to monitor emerging capability maturity.
9	***Category*** - Challenge - Over-reliance on overseas partners	*New contribution* - Highlights the desire of nations to reduce their reliance on partners and neighbors, to assert national identity and interests.
10	***Category*** - Challenge - Partners' lack of cultural awareness	*New contribution* - Highlights the ineffectiveness of partners' support, where it fails to present ethnically and culturally appropriate content. Each nation in the region needs to be regarded as distinctly different.
11	***Category*** - Challenge - no regional legal framework	*New contribution* - Highlights the importance of a regional legal framework that provides a foundation for collaboration on areas of shared interest, while allowing nations to protect their identity, assets and infrastructure.

Table 4. Semantic Theme 2 – relationship with emergent categories and research/contribution

	Theme - Preserve the national interest *(17 occurrences)*	
12	***Category*** - Government expectations and priorities	Reinforces existing research that national governments will focus on driving a domestic agenda as the immediate priority [3] [15] [16]
13	***Category*** - Government manage the national interest	Reinforces existing research that governments project their national identity as a way of directing their national interest [13]
14	***Category*** - Government driver - drive the domestic agenda	Extends the argument that governments reinforce their national interest through an integrated domestic cybersecurity response capability [3] [15] [16], by suggesting that they do so to seek electoral appeal through projecting their preferred identity and behavioural norms to the domestic population.
15	***Category*** - Wishlist - national policy priority	Supports the argument [3] that national governments succeed where they offer a structured, well planned approach to developing an integrated cybersecurity response capability
16	***Category*** - Government lack of planning	*New contribution* - Highlights the tendency for Pacific Island national governments to make funding and policy decisions without adequate stragegic planning. Offers an opportunity for improved policy outcomes, through improved planning and a longer term, strategic view.
17	***Category*** - Government driver - capacity building with outside help	*New contribution* - Highlights the need for Pacific Island national governments to build capability maturity and resilience with the support of regional neighbors and partners.
18	***Category*** - Government driver - raising local maturity, resilience	*New contribution* - Extends Category 17, by highlighting the need for partners' support to target the building of domestic capabilty maturity.
19	***Category*** - Wishlist - national strategic planning and investment	*New contribution* - Highlights the desire of participants for their national governments to ground policy in robust, stragegic planning and funding considerations.
20	***Category*** - Wishlist - raising social awareness of cybersecurity	*New contribution* - Highlights the importance of natoinal governments increasing the general community awareness and engagement with cybersecurity policy.

5.1. Semantic Theme 1 – Purpose, Form and Function of a Regional CERT

Semantic Theme 1 contained the highest number of responses, with 70% of documented *thoughts*, across all *emergent categories*, suggesting that the participants thought broadly about the practical implications, issues and opportunities with respect to a regional CERT. Given that the participants were actively involved in the establishment, running or support of national and regional CERTs, the weighting of thoughts towards this theme was expected. Responses focused on tangible, action-based outcomes that described the mechanical aspects of a regional CERT framework.

Discussions focused on the role and impacts of smaller nations and smaller CERT teams. All participants recognized the need for a regional CERT framework as a vehicle for improving the cybersecurity response capability for Pacific Island nations, although they did so through the lens of a developing nation with small size and limited resources or capacity.

Category 1 supported the argument that local CERTs with limited resources should focus on delivering specific services [5] [10] [11], by proposing that those same CERTs can enhance their national identity by being recognized as a regional leader in selected response capabilities. Whereas the literature proposed an inward-looking approach based on sharing limited capacity and resources, participants emphasized an outward-looking approach that promoted the national capability in terms of high value functions with commercial appeal.

Categories 3, 4 and 5 reinforced the established argument that regional partners have a supporting role to play in providing resources and expertise to help smaller nations build their domestic response capability [5] [10] [11]. These arguments were observed in practice through government policy and strategy [2] [3]. The participants discussed the importance of support from a range of regional partners, including government, academia and the private sector. In all cases, participants identified the need for supporting partners to identify with larger regional nations or institutions – typically USA, Australia or New Zealand, with no consideration given to regional partner support provided by smaller nations with specialized areas of expertise. This contrasted with Category 2, where participants noted that with scarce resources and the impacts of the Covid-19 pandemic on fragile national economies, Pacific Island nations will seek support from many different organizations or nations. The difference in approaches may be explained by competing priorities – the imminent need for resource-scarce nations to obtain support from all possible partners, versus the ongoing need for resources (cash, people and expertise) from sustainable sources, typically larger regional neighbors.

Categories 8-11 identified four issues that may inhibit the willingness of Pacific Island nations to adopt a regional framework. These issues were specific to the Pacific Island nations and reflected their desire to retain a sense of sovereignty over their national identity, sensitive information and scarce resources, whilst also seeking material support from larger partners, to build capability maturity and resilience.

Departing from the contemporary argument that smaller nations require ongoing, material support from "developed" partners, the participants spoke about the need to progressively reduce reliance of regional partners, rather than remove said reliance altogether. This offered a pragmatic approach, based on the need for smaller nations to leverage regional partners to help build national self-reliance through strong societal foundations, before progressively reducing this reliance in a controlled manner. In a similarly pragmatic approach, participants highlighted the need for a regional CERT framework to be grounded in a legal framework that recognizes the participating nations' shared interests and objectives, whilst also supporting nations' rights to ownership and security of their sensitive information.

The inference arising from Categories 8-11 was that a regional framework needed to preserve and nurture participating nations' identities and sovereignty. This was expanded on in Semantic Theme 2.

5.2. Semantic Theme 2 – Preserving the National Character

Semantic Theme 2 contained the least number of responses, with 30% of documented thoughts, across all emergent categories. Responses focused on intangible, behavioral-based outcomes that described why the regional CERT was important and how it influenced governments' domestic policy and strategy considerations. With participants having worked with or within their national governments, several were hesitant to overtly criticize government policy. However, all participants discussed the extent to

which their respective government's policy and strategic approach to cybersecurity readiness reflected the national interest at the time.

Categories 12, 13, 14 and 15 extended the discussion on national governments' use of policy frameworks to project identity and behavioral norms [3] [13] [15] [16] by arguing that governments do so with a domestic policy agenda as the immediate priority. While literature identified the relationship between governments' perception of national identity and enactment of policy and strategy frameworks, it did not question why governments tie their policy platforms to a perceived national interest. In contrast, the participants argued that this relationship should be viewed through a domestic/electoral lens, with national governments prioritizing domestic political outcomes ahead of regional interests.

The findings reinforced the importance of smaller nations with relatively little bargaining or negotiating power, projecting their national character within regional forums as a way of affirming their independence to both domestic and regional audiences [13]. Categories 12 and 13 included discussions about the importance of governments being able to project a sense of sovereignty to their domestic populations, while at the same time accepting support from regional partners.

Categories 16, 17, 18, 19 and 20 introduced new contributions to the discussion, which provide opportunities for nations to strengthen their national interests and domestic policy outcomes, within a regional framework. They also reflected an emerging sense of national capability maturity (as noted in Categories 8, 9) by highlighting the need for improved strategic planning and policy alignment, as the basis for allocating funding to prioritized CERT policies. These Categories reinforced the persistent criticism that Pacific Island governments were prone to making rapid, ill-considered decisions to deploy a local CERT, without due consideration of the cost, resource and sovereignty impacts.

6. Implications for Research and Practice

The research considered the practical implications of applying the two semantic themes and four proposed outcomes, by tying the outcomes back to the respective emergent Categories. Underpinning this consideration was a conflict between the emerging sense of importance, urgency and commercial opportunities arising from a national cybersecurity response capability (Semantic Theme 1) and the lack of available skills, resourcing and capability resilience (Semantic Theme 2) - small nations may seek investment and support from larger neighbors to enhance their national interest through an improved response capability but in doing so, risk ceding sovereignty of national assets and infrastructure, and losing political support amongst their domestic audiences.

The interviews offered consistent agreement on the need for a regional CERT framework as a way of reinforcing national governments' response capabilities. While this outcome was consistent with the literature, the participants extended discussions into detailed consideration of the preferred purpose, form and function of a Pacific Islands framework. The proposed framework included a network of affiliated, independent national CERTs, with each specializing in CERT services that reflect their respective national interests, supported by a range of partners and neighboring nations who provide material resources that target capacity building at both national and regional levels.

Within the Pacific Islands framework, three broad drivers would frame national governments' cybersecurity policy formulation – preserving the national interest, domestic funding priorities and developing domestic capability maturity and resilience. These three drivers inform the governments' priorities for developing a cybersecurity response capability and provide regional partners with markers for the type of capacity building investment and support that will be required.

The implications of these findings are that firstly, regional partners have a critical role in providing support to a regional CERT framework, and secondly, support will be most effective when directed towards local and regional capacity building, and when framed by the governments' national policy drivers and priorities.

6.1 Outcome 1: Regional CERT | Network of affiliated national CERTs

A regional Pacific Islands CERT would consist of a network of affiliated national CERTs with a central body responsible for the coordination of communication, training and information sharing between participants (Categories 3, 4, 5).

Each national CERT would deliver selected cybersecurity response services that reflect the respective government's domestic policy and funding priorities (Category 1). The affiliated CERTs would collaborate on matters of shared interest and will share services within the regional framework where required (Categories 1, 2, 6, 7). The central body would facilitate collaboration, coordination and information sharing, using a mix of virtual conferencing

technologies and occasional shared, on-site meeting, to overcome geographical, time and cost constraints.

6.2 Outcome 2: Regional partners | Provide support for capacity building

Pacific Island national governments are likely to continue seeking material support from regional partners, including universities, Non-Government Organizations, commercial partners and larger "developed" nations (Category 2). This support will target the government's domestic priority areas for building and maturity of domestic cybersecurity service capacity (Category 19), improved strategic planning and policy making (Categories 16, 19), and creating a maturity model for current and emerging CERT practices and standards (Category 2).

Partners should be apolitical and should provide support based on a clearly planned strategy with measurable outcomes for each national government (Categories 15, 16, 19). Whilst governments will use the outcomes for domestic political priorities, partners should be distanced from such considerations.

Partners should not provide support for the development of equipment and infrastructure. Nations will seek to protect their sovereignty by retaining ownership of national assets and infrastructure (Category 13), while seeking support for knowledge-based capacity building.

6.3 Outcome 3: Regional partner | Provide support that targets national drivers

Regional partners' support would be expected to avoid a "one size fits all" approach and instead, provide culturally aligned resources, content and practices that supports the respective national governments' policy priorities, national interests and identity within the region (Categories 10, 12, 13, 14). Priority support areas are likely to include the provision of opportunities for commercial partnerships that position a national CERT as a compelling investment opportunity (Category 19), provision of education and job creation opportunities through sponsored places at universities and placements with regional cybersecurity service providers (Capabilities 17, 18) and building a brand differentiator that allows a national government to project itself as a specialist provider of defined CERT services (Categories 1, 13).

6.4 Outcome 4: National Governments | Support based on sound planning

Semantic Theme 2 emphasized the need for governments to establish detailed domestic planning, policy and funding priorities, prior to investing limited resources in a national or regional CERT (Categories 16, 19). Participants expressed consistent disappointment at the repeated delivery of cybersecurity policies and practices by Pacific Island national governments, based on inadequate planning and rapid, ill-informed decision making (Categories 16, 19), with the intention of projecting a particular policy stance to domestic audiences (Categories 13, 14). In response, regional partners will drive improved maturity in the decision-making process, by providing resources based on sound and transparent planning, including targeted funding, measurement of outcomes and benchmark returns on public and private investments.

7. Conclusions

The research confirmed that Pacific Island nations can leverage their respective domestic cybersecurity response capabilities to inform a regional CERT framework. The regional framework would be grounded in two semantic themes and four enabling outcomes. At the thematic level, the purpose, form and function of a regional framework would reflect the domestic policy considerations and priorities of the participating nations, while participating governments are likely to prioritize their national interests above those of the regional framework.

Pacific Island national governments and supporting partners would enable the framework, by enacting the four outcomes. Firstly, the regional CERT framework would include a network of affiliated, independent national CERTs, each servicing their respective national interests while collaborating on matters of shared impact. The regional framework would also include a central body, with responsibility for coordinating information, training and outcomes, between the member CERTs. Secondly, partners would provide targeted, strategic support that enables national and regional capability maturity and resilience. Thirdly, partners' support would target national government's domestic policy priorities and national interests. Finally, support would be grounded in targeted, responsible and strategic policy planning and funding.

The research contributes to both theory and practice and informs audiences that are involved in the development of national CERT organizations and

practices, both within the Pacific Islands region and in the global cybersecurity community. As a contribution to theory, it provides a model for collaboration across a community of ethnically, culturally, economically and geographically diverse nations. From a practice perspective, the model links local and regional cybersecurity practitioners' narratives to the current literature, while also identifying a set of Pacific Island specific challenges and opportunities.

The research provides a foundation framework from which to further explore the semantic themes and enabling outcomes, however it is not without limitations. The approach was hampered by the global COVID-19 pandemic in 2020, with significant global restrictions on our ability to engage with participants in many Pacific Island nations. The low number of participants has resulted in a relatively small spread of views and experiences. This creates a bias towards those participants who spoke more extensively, and who provided more contextual data. In response, the research approach reflects a compromise, with cybersecurity practitioners engaged from developed nations, regional partners and practitioners with direct exposure to the Pacific region.

Follow-up research will extend the emerging discussion around the efficacy of a regional CERT framework with a developing nations perspective, to support the Pacific Islands region. It will include additional participants from a wider range of Pacific Island nations and regional partners. This will provide contrasting understandings of the regional CERT framework, from both developed and developing nations' perspectives, so that a deeper and more contextual analysis of the semantic themes and enablers can be conducted, with a greater plurality of views.

8. References

[1] CCDCOE, "Cybersecurity Strategy Documents", NATO, https://ccdcoe.org/strategies-policies.html, Accessed 27 April 2020.

[2] Australian Government, "Cyber Cooperation Program", Department of Foreign Affairs and Trade, https://www.dfat.gov.au/international-relations/themes/cyber-affairs/cyber-cooperation-program/Pages/cyber-cooperation-program, Accessed 28 April 2020.

[3] O. Hellwig, G. Quirchmayr, E. Huber, G. Goluch, F. Vock, and B. Pospisil, "Major Challenges in Structuring and Institutionalizing CERT-Communication", 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp.661-667.

[4] Ministry of Communication and Information Technology (MCIT), "Samoa National Cybersecurity Strategy 2016-2021", Government of Samoa, https://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf, 2016.

[5] J. Ferwerda, N. Choucri and S. Madnick, "Institutional foundations for cybersecurity: Current responses and new challenges (No. CISL-2009-003)". Alfred P Sloan School of Management, Cambridge MA, Composite Information Systems Lab, 2010.

[6] West-Brown, M.J., D. Stikvoort, K. Kossakowski, G. Killcrece, R. Ruefle and M. Zajicek, Handbook for Computer Security Incident Response Teams (CSIRTs), Carnegie Mellon University, Software Engineering Institute, 2003.

[7] O. Kruidhof, "Evolution of national and corporate CERTS - Trust, the key factor". In Best Practices in Computer Network Defense: Incident Detection and Response (M.E. Hathaway (Ed.)) IOS Press, 2014

[8] R. Slayton and B. Clarke, "Trusting infrastructure: The emergence of computer security incident response, 1989 – 2005", Technology and Culture 61(1), John Hopkins University Press, 2020, pp. 173-206.

[9] I. Z. Dlamini, B. Taute and J. Radebe, "Framework for an African policy towards creating cybersecurity awareness", Proceedings of the first IFIP TC9/TC11 South African Cybersecurity Awareness Workshop (SACSAW), Gaborne, Botswana, 12 May 2011

[10] S. Madnick, N. Choucri, S. Camina, E. Fogg, X. Li and W. Fan, "Explorations in Cyber International Relations (ECIR)-Data Dashboard Report# 1: CERT Data Sources and Prototype Dashboard System", MIT Sloan Research Paper 4754-09, 2009

[11] P.A. Yannakogeorgos, "Strategies for Resolving the Cyber Attribution Challenge (No. AU-AFRI-CP-1)", Air Force Research Institute, 2013

[12] Q. Ul Haq, "Cybersecurity and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan", International Journal of Computer Network and Information Security, 11(1), 2019, pp.62-69

[13] J. Burton, "Small states and cybersecurity", Political Science, 65 (2), 2013, pp. 216-238

[14] F. Smith and G. Ingram, "Organizing cybersecurity in Australia and beyond", Australian Journal of International Affairs, 71:6, 2017, pp. 642-660

[15] M. S. bin Hashim, "Malaysia's national cybersecurity policy: The country's cyber defence initiatives", in 2011 Second Worldwide Cybersecurity Summit (WCS), IEEE, 2011, pp. 1-7.

[16] S. Armenia, A. Cardazzone and C. Carlini, "Understanding security policies in the cyber warfare domain through system dynamics", Proceedings of 4th International Defense and Homeland Security Simulation Workshop, 2014