

Background Note

ICT Applications and Cybersecurity

1 Overview and Context

Introduction to ICT Application and Cybersecurity in the Pacific

In the Pacific, unique rural topography and small populations spread throughout outer islands have been factors affecting the deployment of telecommunication infrastructure outside national capitals. As a result, very few people outside major cities are able to make a phone call, let alone access the Internet. Nearly all Internet users are located in capital cities and a handful of secondary urban areas, maintaining digital disparities across various demographics. Furthermore, due to vast distances, small markets, and the lack of economies of scale, improvements in network penetration are slow and expensive. Whereas users on main islands can be reached via fixed wireline and wireless cellular communication networks, those on outer islands and in remote rural areas typically rely on HF radio and costly satellite links to their capitals for both domestic and international communications.¹

Fortunately, the introduction of effective telecommunication, economic and social policies by local governments, coupled with recent ICT projects implemented by various international organizations and governments have resulted in a slow but steady progress in connectivity rates among Pacific Island Countries (PICs).

For instance, e-community projects such as women in Nauru and Fiji, who usually sell their home-made chutney by the roadside, have used the Internet to successfully market their products. Other factors that have contributed to the increased connectivity and ICT use include the establishment of tax-free zones for IT businesses, the introduction of Free and Open Source Software, USPNet equipment upgrades, etc. Additional and consistent implementation of ICTs will further assist these countries in strengthening governance, expanding distance learning, improving healthcare and creating a more fluid online trading platform.

The region's ICT sector is headed in the right direction, but much more needs to be done. Achieving the potential benefits of ICT applications in the areas such as health, education, government, and commerce, has as a prerequisite the development of a secure network, as well as reliable and interoperable applications and tools. This paper provides an overview of the status of ICT applications and cybersecurity in the Pacific Island Countries; describes selected ongoing projects and activities in ICT applications and cybersecurity in the region and concludes with a discussion of possible ways forward.

2 ICT Applications

2.1 ICT Applications in the Pacific Region

The level deployment of ICT applications in the Pacific islands is influenced by the interaction of multiple factors, as illustrated in Figure 1 below. Although generalizations are difficult due to the diversity in history, scale, level of development and problems affecting the different islands, PICs largely share common geographic and socio-economic characteristics, in particular their remoteness, isolation and scattered small populations. Understanding the current status of adoption and development of ICT applications across PICs requires an in-depth analysis of the performance of each country in a series of indicators of ICT access, institutional capacity and financial support that goes beyond the scope of this

¹ Tonga, for example, uses satellite connectivity to provide 1 Mbps connections to some of its islands. The satellite connection links to the mobile telephone network to provide GSM voice and data, as well as Internet services. For more information see: ITU (2008), *Asia-Pacific Telecommunication/ICT Indicators 2008*.

background paper. The following sections describe the current status of deployment of applications in the areas of e-Government, e-Commerce, e-Education, e-Health and e-Environment, highlighting some of the challenges faced and responses taken by PICs when implementing them in their territories.

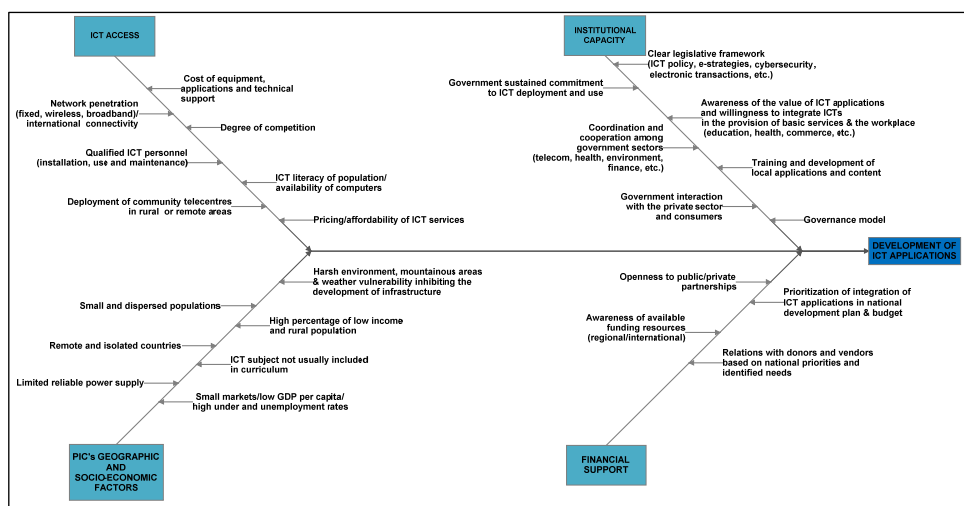


Figure 1. Factors contributing to current development of ICT applications in Pacific Island Countries

Source: ITU

1.1.1 e-Government

The introduction of e-Government has posed unique challenges and special opportunities for the PICs. The Pacific faces low level of penetration of telecommunication infrastructure and platforms, particularly of international fibre connectivity, which tend to result in broadband prices above the per capita income of their populations.² These challenges are compounded in some countries by relatively high levels of ICTs illiteracy, differences in governance and large disadvantages of scale and distance. However, there are equally exciting possibilities ICTs can bring about to improve productivity and quality of life through e-Government applications.

An analysis of the current state of e-Government in the region reveals that PICs are mostly still at an emerging stage of e-Government maturity. All countries and many government agencies have developed websites, but the complexity of the government IT services provided through them is limited, ranging from access to maps, statistics, payroll uses and tourism. Important features usually missing in their sites related to security and accessibility.³ According to the most recent UN e-Government Survey, Oceania's regional average of e-Government readiness had jumped from 0.2888 in 2005 to 0.4338 in 2008.⁴ However, a regional comparison, illustrated in Figure 2, shows that Oceania lags behind Europe (0.6490) and the Americas (0.4936), but surpasses the e-readiness of Africa (0.2739).

A comparison of scores and rankings among PICs, presented in Table 1, shows that in the last three years, the ranking of some Pacific countries have tended to decrease, but in general, their e-

² According to ITU's *Asia-Pacific Telecommunication/ICT Indicators Report 2008*, this is the case in Papua New Guinea, the Solomon Islands and Vanuatu.

³ Budden, John, *e-Government in the Pacific (An opportunity for Regional Synergies?)*, June 2005. Downloaded February 6, 2008 from: <http://www.apdip.net/projects/e-government/capblg/casestudies/Fiji-Budden.pdf>

⁴ UN Department of Social and Economic Affairs (DESA), *United Nations E-Government Survey 2008. From E-Government to Connected Governance, 2008*; <http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf>

Government performance has improved slightly since 2005. The reasons for this relative slow progress are many, including overall slow economic development, lack of infrastructure in rural areas, particularly access to electricity and telephones; lack of funds to develop e-Government; lack of senior computer skilled people and insufficient commitment of governments to develop more complex e-Government applications.

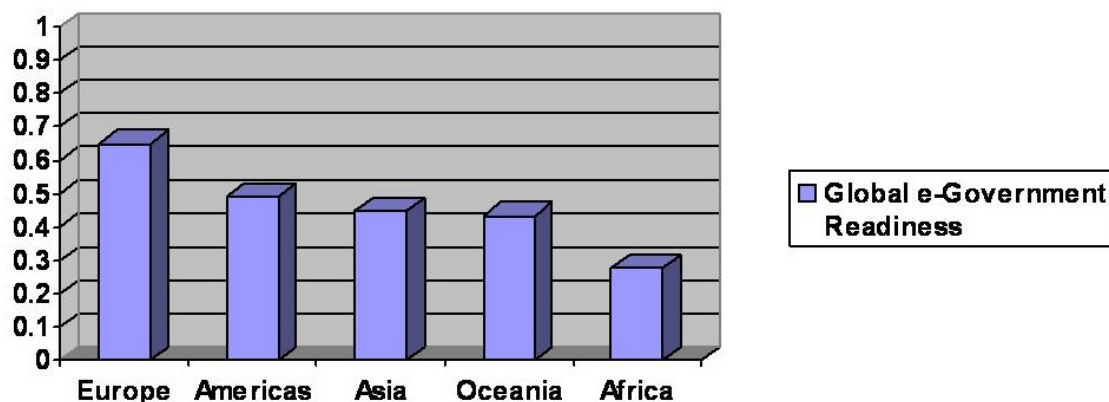


Figure 2. Global e-Government Readiness

Source: ITU from data published in UN Department of Social and Economic Affairs (DESA), *United Nations E-Government Survey 2008. From E-Government to Connected Governance, 2008;*
<http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf>

In order to close this gap, the PICs need to further focus on improving infrastructure, policies, capacity development, applications and content, which need to be in place in order to fully implement e-Government services. For some of the countries that have already begun to implement e-Government programs, they need to consider high-level tools of government service, such as publishing online e-decision-making; open web forums; e-consultation; and e-information..

Country	2008 Index	2005 Index	2008 Ranking	2005 Ranking
Fiji	0.4146	0.4081	105	81
Tonga	0.3950	0.3680	112	104
Samoa	0.3761	0.3977	115	91
Solomon Islands	0.2748	0.2669	147	140
Vanuatu	0.2510	0.1664	154	165
Papua New Guinea	0.2078	0.2539	166	142
Kirabati	--	--	--	--
Marshall Islands	--	0.0440	--	177
Micronesia	--	0.0532	--	176
Nauru	--	0.0357	--	179
Palau	--	0.0564	--	175
Tuvalu	--	0.0370	--	178
Region*	0.4338	0.2888	--	--
World	0.4514	0.4267	--	--

Table 1. e-Government Readiness ranking for Pacific Island Countries (2005, 2008)

Source: UN Department of Social and Economic Affairs (DESA), *United Nations E-Government Survey 2008. From E-Government to Connected Governance, p. 41;* <http://unpan1.un.org/intradoc/groups/public/documents/UN/UNPAN028607.pdf>

* **Note:** Regional rankings and scores include the values for Australia and New Zealand.

1.1.2 e-Commerce

The number of e-commerce activities remains small in the Pacific Islands because of the limited economy of scale, lack of access to internet service amongst potential customers, lack of familiarity with and trust in electronic transactions and high cost of connectivity. And yet some projects have already been implemented, such as Fiji's designated tax-free zones for IT businesses and online websites as purefiji.com. In addition, tourism thus far makes up a large portion of e-commerce transactions as numerous hotels and tours can be booked through company websites.

ITU has reported on the status of e-Commerce with "E-Business - A Technology Strategy for Developing Countries" (2000), followed by several workshops and study groups. One of their recommendations for developing regions, such as the Pacific islands, is to create a suitable legal framework and a functional ICT infrastructure, while opening their economies to much-needed foreign investment in the form of equity as well as joint venture capital. All of this would allow PICs to market electronically their natural resources or products in regional or global markets without the need to engage expensive intermediary services. There are innumerable benefits which flow from the electronic procurement and sale of goods and services.

1.1.3 e-Education

Many PICs experience numerous constraints in either implementing or maintaining an e-Education system that is in constant motion. The region has faced these issues head-on as a gradual growth of e-Education projects has occurred over the last several years. Such e-Education projects as AARNet,⁵ Samoa's SchoolNet⁶, Solomon Islands' PFNet⁷ and region wide projects such as the University of South Pacific's USPNet⁸ and the Pacific Open Learning Health Network (POLHN)⁹. All entail the enhancement of the educational and professional development experience in the Pacific island countries via open and distance learning.

Countries in the Pacific are encouraged to include e-Education and training in their national strategic plans so that more people attain skills and expertise in the area of ICT. This would mean developing and supporting a pathway that ensures and encourages ICT education and use among children, beginning from primary through to secondary school, and on to tertiary level. As is the worldwide trend, ICT is being increasingly utilized in most modern sectors and people need to have at least basic ICT literacy to ensure that they can find employment and live worthwhile lives. Therefore, it is crucial that students are taught at least basic ICT literacy in schools. There also needs to be a greater commitment by the governments of all the Pacific Islands countries to take control and leadership in the adoption and development of ICT in education. They need to commit themselves to the development of relevant infrastructure, purchasing hardware and training personnel.

Between 2005 and 2006, ITU helped establish multipurpose community telecentres (MCTs) in Samoa and the Solomon Islands, providing local communities, businesses and schools access points for voice communication and ICT services. Ten MCTs were established in the Samoan districts of Upolu and Savaii, while other ten were established in Honiara, Guadalcanal province, in Solomon Islands.

1.1.4 e-Health

The region has been exposed to several obstacles that have created a strong barrier to access and an imbalance of resources amongst the several PICs. A common problem in many countries is the lack of communication between relevant stakeholders, particularly between healthcare providers and health ministries and between the health and telecommunications sectors of Government. Also, technical

⁵ <http://www.aarnet.edu.au>

⁶ <http://www.adb.org/Documents/TACRs/SAM/36513-SAM-TCR.pdf>

⁷ <http://www.peoplefirst.net.sb>

⁸ <http://www.usp.ac.fj/index.php?id=6027>

⁹ <http://www.polhn.com>

barriers at national and regional/global levels, such as non-interopability of hardware, software and connectivity, as well as a lack of an accepted standard in e-Health applications currently exist. Another problem for the region is the shortage of financial resources for e-Health, which leads to limited ICT infrastructure in rural areas. A compounding factor is the shortage of manpower with appropriate skills, which is partly due to limited awareness of the potential of e-Health applications at the governmental level, as well as delays in the introduction of ICT and e-Health training courses in the curriculum of medical schools, institutes of technology and hospitals.

The Pacific Open Learning Health Network (POLHN) —covering the Cook Islands, Fiji, Kiribati, Marshals Islands, Federated States of Micronesia, Palau, Samoa, Solomon Islands, Tonga and Vanuatu— is an excellent example of the cross-boundary use of e-Health in human resource development. The network aims to use e-Learning as a means to enhance continuing education and professional development, thus improving the quality and standards of practices of health professionals in the Pacific island countries.

Another example is the use of teleconsultations in Federated States of Micronesia. In the Pohnpei State, the use of teleconsultation has resulted in cost savings, enabled patients to have access to physicians and helped familiarize physicians with the use of ICTs. Before having Internet connection, approximately US\$1,500 per month was spent on telephone bills for outside consultations. With the Internet connection and the consultation web pages, costs have decreased to below US\$500 per month for consultations, a saving of US\$1,000 per month.¹⁰ Other e-Health projects to be implemented within the Pacific islands include the Pacific Basin Telehealth Initiative (PBTI), the Pacific Public Health Surveillance Network (PPHSN), Hawaii Telehealth Network Program and the Pilot Telehealth Project.

These accomplishments have pointed the region in the right direction but a lot more attention needs to be drawn from local and international parties. ITU's recent report, *Implementing e-Health in Developing Countries*¹¹ (September 2008) recommends that countries at the regional level need to collect and share technologies and strategies, as well as policies and standardization of norms. At the national level, ITU's report states how it is essential to have a comprehensive national vision on e-Health which takes into account financial and human resources, and a clear plan for implementation in a manner that promotes inter-operability using a global standard. In addition, public-private partnerships should be promoted with close communication between health, ICT and trade officials as well as those among health-care providers and between health-care providers and policy makers. The development of a strong policy and regulatory framework for balanced development and long-lasting implementation should also be implemented.

1.1.5 e-Environment

Historically, PICs have been concerned with direct climate monitoring (i.e. climate long range forecasting) and improvement applications due to their vulnerability to adverse weather patterns and their effects. Most PICs however do not have the capacity to undertake environmental research or act on the environmental data, information and knowledge that is available online and in each country. Many PICs lack sufficient information regarding climatic risks faced by their populations and how they could be mitigated or adapted to. Similarly, not all countries are making full use of ICTs for e-Environment.

These issues are slowly coming to light as numerous PICs and countries, such as the United States, have invested resources in order to monitor the Pacific's environment. As is the case with the other e-applications discussed, PICs show large disparities in the implementation of e-Environment with the rest

¹⁰ For more information see: <http://www.hinz.org.nz/journal-pdf/126>

¹¹ Available on the ITU website, at http://www.itu.int/ITU-D/cyb/app/docs/e-Health_prefinal_15092008.PDF

of the world due to the region's low exposure to high speed IP connectivity; low rural connectivity, and limited telecommunication infrastructure.

The region can become a global leader in environmental research if e-Environment applications significantly improve in the future. Organizations such as the International Telecommunication Union are analyzing the current status of e-Environment throughout the world and making concrete recommendations in order to support developing regions such as the Pacific islands. ITU's recent report, *ICT's for e-Environment: Guidelines for Developing Countries, with a Focus on Climate Change*¹² (September 2008) presents the results of research that demonstrate that ICTs can help to significantly reduce toxic emissions while concurrently increasing energy efficiency and reducing the use of natural resources. The report also discusses how the utilization of ICTs for e-Environment can save lives through natural disaster warning systems, monitor migratory patterns of marine life and accurately examine global warming trends and weather patterns.

1.1.6 ICT Applications for Disaster Management

ICT's, including space-based technologies, are key tools for assisting in all stages of disaster management activities, such as risk mapping, early warning and emergency communications, among others. In order to develop effective plans for disaster risk reduction and emergency preparedness, as well as to make fact-based decisions during disasters, Governments and communities need to be able to access, through affordable devices, information systems capable of combining information such as satellite imagery, aerial photography, topographic maps, and GIS, weather, and demographic data.

PICs stand to benefit from getting their researchers, civil servants, and community leaders involved in using and expressing requirements for the next versions of tools such as the Pacific Disaster Net (www.pacificdisaster.net), the Sentinel Asia (dmss.tksc.jaxa.jp/sentinel/) and other regional initiatives for information exchange. In this context, ESCAP is in the process of identifying and consulting relevant sub-regional and regional networks active in disaster management, as well as research institutions, national disaster management and ICT authorities and seeking their suggestions on modalities for the establishment of a network of networks on knowledge sharing and analysis for disaster management in the Asia Pacific Region. The establishment of this network would have the purpose of a) Facilitating the sharing of information, knowledge and expertise among various networks and initiatives covering and connecting various sectors, and b) Facilitating the access to a bank of knowledge and expertise shared by each member network and initiatives and experts and therefore opening new research and analysis opportunities for disaster management.

3 Cybersecurity

3.1 Introduction to Cybersecurity and Critical Information Infrastructure Protection (CIIP)

With the start of the 21st century, modern societies have a growing dependency on information and communication technologies (ICTs) that are globally networked. However, with this growing dependency, new threats to network and information security have emerged. There is a growing misuse of electronic networks for criminal purposes or for objectives that can adversely affect the integrity of national critical information infrastructures. To address these threats and to protect these infrastructures, a coordinated National Cybersecurity Strategy and Critical Information Infrastructure Protection (CIIP) programme is necessary.

As threats can originate anywhere around the globe, the scope of the problem is inherently international and the topic has entered the global political agenda.

¹² Available on ITU's website at <http://www.itu.int/ITU-D/cyb/app/docs/itu-icts-for-e-environment.pdf>

3.2 ITU Global Cybersecurity Agenda (GCA)

The legal, technical and institutional challenges posed by the issue of cybersecurity are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation. In this regard, the [World Summit on the Information Society \(WSIS\)](#) recognized the real and significant risks posed by inadequate cybersecurity and the proliferation of cybercrime. At the WSIS, world leaders and governments designated ITU to facilitate the implementation of [WSIS Action Line C5](#), Building confidence and security in the use of ICTs.

In this regard, the ITU Secretary-General launched the [Global Cybersecurity Agenda](#)¹³ on 17 May 2007, alongside partners from governments, industry, regional and international organizations, academic and research institutions. The GCA is a global framework for dialogue and international cooperation to coordinate the international response to the growing challenges to cybersecurity and to enhance confidence and security in the information society. It builds on existing work, initiatives and partnerships with the objective of proposing global strategies to address today's challenges related to building confidence and security in the use of ICTs. Furthermore, the GCA has [seven main strategic goals](#)¹⁴, built on five work areas: 1) Legal Measures; 2) Technical and Procedural Measures; 3) Organizational Structures; 4) Capacity Building; and 5) International Cooperation.

3.3. Cybersecurity and CIIP

The goal of cybersecurity is to help protect organizations' and countries' assets and resources in organizational, human, financial, technical and information terms, allowing them to pursue their mission. The ultimate objective is to ensure that no lasting harm is done to them. This consists of reducing the likelihood that a threat materializes; limiting the resulting damage or malfunction; and ensuring that, following a security incident, normal operations can be restored within an acceptable time-frame and at an acceptable cost.

Considered as a system, telecommunication (both infrastructures and services) represents a security challenge that is largely analogous to the challenge of IT resources. The same technical, organizational and human constraints must be observed in attempting to meet that challenge. Protecting information while it is in transit is necessary; but this is far from sufficient in itself, for the degree of vulnerability increases, if anything, once information enters the processing and storage phase. Cybersecurity must therefore be viewed from an overarching perspective. Purely technical security solutions cannot compensate for the absence of coherent, rigorous management of security needs, measures, procedures and tools. A disorganized stampede to get security tools will hinder use, weigh down operations and impair the performance of IT systems. Proper IT security is a management issue, and the associated tools and services are linked to operational system administration.

Good stewardship of digital information assets, the distribution of non-tangible goods, the exploitation of content and the bridging of the digital divide are all examples of economic and social problems that cannot be addressed by looking only at the technological side of IT security. A response that takes into account the human, legal, economic and technological dimensions of the security needs of the digital infrastructure and of users can help to foster confidence and lead to economic growth that will benefit all of society.

3.3.1 Effective Critical Information Infrastructure Protection

¹³ <http://www.itu.int/osg/csd/cybersecurity/gca/>

¹⁴ <http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html>

Critical Information Infrastructure Protection (CIIP) is universally acknowledged as a vital component of national security policy. In order to protect their critical infrastructure, some countries have established sophisticated and comprehensive CIIP organizations and systems, involving governmental agencies from different ministries, with a variety of initiatives. Different facets of CIIP range from reducing vulnerabilities and fighting computer crime to defense against cyber-terrorism. Considering the variety of tasks affiliated with CIIP, the first step towards an effective and efficient CIIP organizational unit is to define its essential priorities and responsibilities. These essential tasks of CIIP are arranged in a “Four-Pillar Model” of CIIP¹⁵. The four pillars of this model include:

- i) **Prevention and early warning.** Prevention and early warning aim to reduce the number of information security breaches. A goal is to ensure that critical infrastructures “*are less vulnerable to disruptions, any impairment is short in duration and limited in scale, and services are readily restored when disruptions occur.*”
- ii) **Detection.** In close collaboration with technical experts from Computer Emergency and Response Teams (CERTs), the CIIP unit should identify new technical forms of attacks as soon as possible. Furthermore, non-technical analyses of the general risk situation are needed (e.g., information about the emergence of criminal organizations).
- iii) **Reaction.** Reaction includes the identification and correction of the causes of a disruption. Initially, the CIIP unit should provide technical help, and support to the targeted company. However, the CIIP unit cannot take on the management of incident response for these companies. The CIIP unit usually provides advice and guidance on how to tackle an incident, rather than offering complete solutions.
- iv) **Crisis management.** Minimizing the effects of any disruptions on society and the state has always been a major task of protection, so the CIIP unit must be embedded in the national crisis management structure. It should be well-positioned in order to have direct access to decision-makers, because a key function of the CIIP unit is to alert the responsible people and organizations. In case of a national crisis, the CIIP unit must be able to offer advice directly to the government.

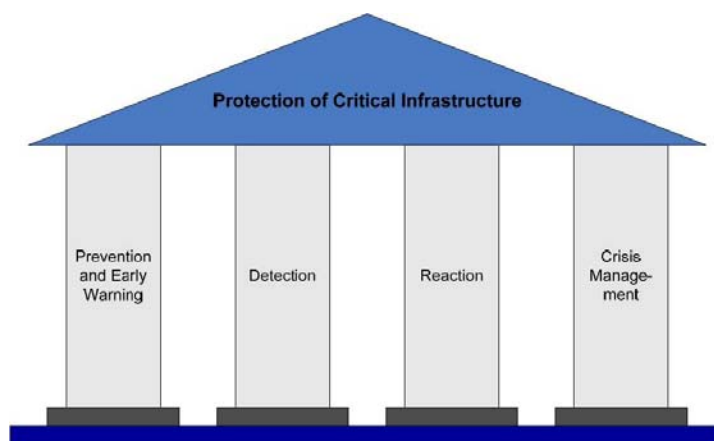


Figure 3. The Four Pillars of CIIP

Source: ITU and ETH Zurich: A Generic National Framework for Critical Information Infrastructure Protection (CIIP), 2007; <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf>

3.4. Cybersecurity and CIIP in the Context of the Pacific Island States

¹⁵ ITU and ETH Zurich: A Generic National Framework for Critical Information Infrastructure Protection (CIIP), 2007; <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf>

3.4.1 Overview of Cyber Legislation in the Pacific Islands States¹⁶

Cybersecurity presents problems for the world and obviously the small countries of the Pacific. It is a problem that needs to be addressed and addressed at the earliest possible date. It needs to be dealt with because of the general issues relating to state security; action is needed also to make way for the future and foreseeable developments in the area of globalization as it effects the movement of goods and persons. Increasingly these movements are subject to international exchange of information by cyber communication.

The Pacific Island countries and Small Island Developing States (SIDS) in general are faced with unique challenges posed by their small size and remoteness. This is also the case with regards to the special needs and cooperation models required for improving cybersecurity and related CIIP. Several cybersecurity initiatives are under way, like the Australian supported “*Anti-Spam Legislation Project*”, aimed a strengthening specifically spam legislation, enforcement and cooperation regimes in the Pacific Island States.

The countries of the South Pacific have very little legislation specific to cybersecurity. Most countries would rely, if the issue were to arise in court, on their general criminal laws and particularly those relating to damage to property. There are also some provisions in legislation relating to civil aviation and broadcasting which could be called in aid. New Zealand, Australia, Kiribati and Tonga do have some specific legislation. In New Zealand the main rules are those now found in the Crimes Act 1961 sections 248-252; there are also some provisions in the anti-spam legislation. In Australia the main legislative provisions can be found in the Cybercrime Act 2001 and the Security Legislation Amendment (Terrorism) Act 2002. Kiribati provides for cybersecurity under Part VII (especially sections 64-69) of its Telecommunications Act 2004. Tonga has dedicated legislation in its Computer Crimes Act 2003. The Tongan legislation shows a clear influence of the European Convention on Cybersecurity. Provisions of that Convention are also reflected in the New Zealand statute. The Australian legislation covers the matters of the Convention but shows no evidence of direct influence from the Convention. The law of Kiribati follows a different pattern and reflects to a degree the Australian legislation.

Although the detail of the provisions varies, it is important to highlight that each of these countries has taken steps to address cybersecurity. As a general comment it can be stated that for the small Pacific countries it is likely that New Zealand legislation is likely to provide a better example than Australia simply because the New Zealand legislation is geared to the needs of a small non-federal state. Further the manner of presentation – the drafting style – of current New Zealand legislation is more accessible in countries where English is not the first language of administrators.

There is a significant amount of assistance available for Pacific administrators and legislators in the form of conventions, model laws, foreign precedents, and guidelines. Of particular relevance in this regard are documents emanating from the ITU, European institutions, and the Commonwealth¹⁷.

3.4.2 Overview of the Development of National Cybersecurity Policies and Strategies

Due to the changing nature of cyber-attacks over the years, countries have needed to modify their incident management and response strategies. As an example, online identity theft, the act of capturing via the internet another’s credentials and/or personal information with the intent to fraudulently reuse it for criminal purposes, is now one of the main threats to further deployment of e-Government and e-Business services, while state sponsored attacks and terrorism are slowly growing in magnitude. If people think things are bad now, experts indicate that things are very likely to get much worse, if no

¹⁶ Research paper prepared for the ITU Regional Cybersecurity Forum for Asia-Pacific held in Brasbane, 16-18 July 2008; <http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/angelo-cyber-legislation-in-the-pacific-brisbane-july-08.pdf>

¹⁷ <http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>

action is taken in this regard. With the use of applications such as Facebook, MySpace, peer to peer networking, etc. growing rapidly, most users do not know that they have been attacked or are under attack.

In obtaining agreement on the development of a national cybersecurity strategy it is important to create awareness at the national policy level about cybersecurity issues and the need for focused national action and increased regional and international cooperation in this regard. It is critical to ensure that all stakeholders, including the decision makers, understand that a national strategy to enhance cybersecurity is needed to reduce the risks and effects of both cyber and physical disruptions. In addition to this, any national strategy needs to be complemented with the participation in international efforts to promote national prevention of, preparation for, response to, and recovery from incidents.

In responding to overall growing number of threats, the role of a national Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs) or a national entity/center with this kind of responsibility is a very important part of a broader national cybersecurity strategy, especially in areas such as cooperation and coordination. The activities that a center with national responsibility can engage in range from monitoring and providing advice about threats and vulnerabilities, incident response and mitigation assistance for ongoing attacks to performing analysis of attacks and malware to understand the nature of the threat, and central coordination and collation of data in order to develop metrics on how the threat is changing. While the majority of countries in the Pacific have no integrated national ICT security policy at this point in time, in some countries there are a number of initiatives in place that are able to support the security requirements of government information technology network operations and the limited government portals that are used for financial and commercial information. With the discussions on plans to further increase online banking, online shopping, and other e-Commerce systems and applications, going beyond using the internet for sending e-mail alone, the governments will need to increase their attention on raising cybersecurity awareness, putting in place cyber legislation to criminalize the misuse of ICTs and establishing national frameworks and ensuring a coordinated regional approach to make best use of scarce resources and maximize impact and readiness.

3.4.3 Misuse of International Telecommunication Numbers in the Pacific

The hijacking and blocking of calls has a severe effect on the fragile economy of a small Pacific Island country which, due to its isolation, is totally reliant on telecommunications for trade. Moreover, blocking country code reduces inbound traffic, which directly affects the revenue of the operator and also makes it very difficult to establish roaming agreements with fellow GSMA members.

The World Telecommunication Standardization Assembly (WTSA) at its meeting in 2008 adopted and approved a new proposal from the Pacific Island countries¹⁸ pertaining to a certain type of telecommunication fraud that had been frequently occurring in the Pacific, more specifically the misuse of numbering resources on international telecommunication networks. The resulting WTSA-08 Resolution 61 deals with the "Misappropriation of international telecommunication numbering resources" (Johannesburg, 2008).¹⁹ The telecommunication fraud is commonly referred to as number hijacking in the region where calls to the Pacific Islands are diverted without the knowledge of the calling party, the called party or the domestic telecommunication operator. Papua New Guinea has also experienced this fraud in the past, however, in recent times the smaller neighboring Pacific Islands have been targeted because of their small volume in telecommunication traffic. Telephone number hijacking is fraudulent in nature. Not only does it give the Pacific Islands a bad reputation, it forces many international operators to stop calls going out to these Pacific Islands countries. Number hijacking also affects potential incomes for these countries and the social economic values that would have resulted from these calls. When a

¹⁸ See the PITA website for more information: <http://www.pita.org.fj>

¹⁹ Resolution 61: Misappropriation of international telecommunication numbering resources (Johannesburg, 2008); http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.61-2008-PDF-E.pdf

telephones number is hijacked, calls will not terminate in the Pacific Islands because some-one at the exchange, for fraudulent reasons, has filtered the calls away from the routing to the intended country.

Another similar fraud gives rise to GSM roaming International Revenue Share Fraud (IRSF) involving losses of hundreds of thousands of dollars. Other fraudsters filter the calls to porn sites without the knowledge of the home operator to collect the termination rate which in most cases translate to the value of millions of minutes. This has caused some operators to block calls to the Pacific Islands to avoid getting caught by the fraud. The blocking of country codes by international operators as a prevention control is an aggressive method which is contrary to existing ITU Recommendation (E.156) on blocking of country codes and stops all traffic to the affected country causing many other problems. This method fails to address the cause of this globally organized criminal activity and the perpetrators walk away undetected. The consequences of number hijacking is that that people make a telephone call to country whose number has been hijacked affecting all areas of social activity and trade such tourism.

Whereas current efforts to identify fraudulent operators have been futile due to commercial confidentialities within the international carriages, the new resolution will add as an important regulatory tool to identify fraudsters and hopefully mitigate the problem. The new ITU resolution among other measures, resolves to provide a mechanism to allow national regulators to request carriers to release routing information in cases of fraud, and to collaborate and share information on fraudulent activities related to misuse of international numbering resources and to consider sharing information about these activities. It is the first time that the Pacific Island countries have taken a proposal and presented it to the ITU and received adoption and approval. Such an initiative sets a precedent for the region to be involved more with the ITU as a means to improve the delivery of safe, secure and comprehensive telecommunication service to its people.

4 Ongoing Efforts

4.1 ICT Applications

4.1.1 [ITU] ICT Application Toolkits

Following its mandate to develop practical tools for Member States, ITU is currently developing ICT application toolkits that will provide policymakers principles and guidelines for the development and deployment of electronic applications and services in the areas of government, health and the environment. The toolkits are being developed as a series of modules that will cover different stages in the life-cycle of e-strategies, from needs assessment to implementation and evaluation.

The initial modules of the e-Government, e-Health and e-Environment toolkits, which address the process of needs and readiness assessment in each of these areas, are currently under development. The assessment and readiness module will support Member States in evaluating their current capacities, identifying needs and defining priorities so that their strategies for e-Government, e-Health and e-Environment match their needs and level of readiness. As part of the e-Environment toolkit, ITU is preparing an e-Environment Readiness Index (EERI), a tool to raise awareness on ICT-based approaches and management practices than can be used to achieve environmental sustainability.

The work on the different toolkits will be complemented by the collection of best practices in three areas, workshops and conferences to support Member States in the deployment of ICT applications, including mobile electronic applications, as well as direct assistance to the development and implementation of ICT application projects in response to country requests.

4.1.2 ICT Application Development Programme

Under the Doha Action Plan and within the framework of ITU Programme for Least Developed Countries (LDCs) and Small Islands Developing States (SIDS), ITU in 2008 signed a partnership agreement with the Servei de Telecomunicacions d'Àndorra (STA) to implement a Project for rural / outer island communications in the Pacific. The project aims to provide access to telecommunication/ICT services to Tonga, Marshall Islands, Papua New Guinea and Nauru through the Secretariat of the Pacific Community's (SPC) Pacific Rural Internet Connectivity System (PACRICS) initiative.

The project has established Multipurpose Telecommunity Centres (MTCs) in remote areas and/or outer islands of these four countries, and is being implemented in cooperation with the Secretariat of the Pacific Community (SPC). It has also received financial support from the Department of Broadband Communications, and the Digital Economy (DBCDE), Australian Government.

While providing basic access to telecommunications, the MTCs will also provide enhanced e-services such as e-Education, e-Health, e-Agriculture, etc. that help address the developmental needs of the local communities and the local institutions at an affordable cost. Therefore, the project aims to develop particular e-applications and local content (likely in local language as well) suitable to the specific needs of each community. A human capacity building programme will be specifically designed for particular communities and circumstances in order to ensure operations and maintenance of the centres in a sustainable manner. In particular, focus will be made on establishing a training-the-trainers programme.

ITU is currently pursuing a partnership with the **Carnegie Mellon University** for the cooperation in the University's Technology Consulting in the Global Community Programme (TCGC). In general, the partnership would enable Carnegie Mellon to recruit and select students to work with the ITU and Administrations in Pacific countries for a period of ten weeks beginning in late May or early June, 2009. The Student Consultants will work on site, in close collaboration with ITU and Administrations, to gain as broad understanding of the ICT problems and issues faced by these countries and recommend approaches and best practices that could ameliorate the identified problems.

In addition, ITU is strengthening the partnership with SPC through the organization of a "Training the Trainers Programme" in the Pacific. The programme aims to enhance human capacity of local communities in operating and maintaining telecentres, as well as developing applications deemed suitable for the local users.

4.1.3 [ITU-Private Sector Partners] ITU Global Telecentres Portal

The [ITU Global Telecentres Portal](http://www.itu.int/ITU-D/cyb/telecentres/portal-index.html)²⁰ was launched in 2008. The portal provides a one-stop-shop for telecentre activities, not simply providing a visualization tool for the telecentre community but also allowing interested communities to interact (e.g. via a forum), finding information about new developments in the field, new telecentres established in the regions, projects, etc. In addition, the Portal can be used as an enabler in order to stimulate the development of telecentres, providing for instance a gap analysis tool which can identify where new telecentres are most needed worldwide.

As such, the collaborative ITU Global Telecentres Portal can assist decision-makers and communicators in the Pacific Island Countries highlight what is done in the country, linking the mapping interface in the Portal with their own websites as well as with the telecentre.org community portal. As users look at a particular region and country they are able to look at information about a specific telecentre including its location, contact person, services offered, target audience, who is actually using the telecentre, etc. Such information may be critical in terms of sustainability of a telecentre, especially in instances where the telecentre users are reportedly different from the telecentre target audience.

²⁰ <http://www.itu.int/ITU-D/cyb/telecentres/portal-index.html>

4.1.4 One Laptop Per Child (OLPC) Oceania

The Pacific Rural Internet Connectivity System (PACRICS) together with the Oceania OLPC initiative is a package for rural and remote areas in the Pacific, addressing both the transport of information as well as its use for educational purposes - *'Every RICS site is an OLPC Hub'*.

OLPC Oceania describes OLPC activities in the Islands of the Pacific (excluding New Zealand and Australia). Ethnologically, the region includes sub-regions of Melanesia, Micronesia and Polynesia. Geographically, it includes thousands of coral atolls and volcanic islands with small populations, grouped in 26 island nations.

OLPC activities in the region are coordinated by the Secretariat of the Pacific Community (SPC), with Dr. Jimmie Rodgers as Director-General, with additional guidance from members of the Pacific Islands Forum Secretariat (PIFS), with Mr. John Budden as executive secretary. In consultation with governments, donor partners and other key stakeholders, OLPC and SPC have developed a concept note²¹ to deliver **"One Laptop per Pacific Child"** by 2015. OLPC Boston has gifted 5,000 laptops for seeding projects in the Pacific Islands. SPC is managing the rollout of projects in every PI and provides technical help, teacher/student/parent training and other assistance as needed to establish and run the projects. Countries under way and ready to proceed include: Cook Islands, Federated States of Micronesia, Kiribati, Nauru, New Caledonia, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu, and Vanuatu.



Figure 4. One Laptop per Child Computer Prototype

Source: One Laptop per Child, <http://laptop.org/en/laptop/index.shtml>

4.1.5 ESCAP Committee on Information and Communications Technology and Committee on Disaster Risk Reduction

During the first session of the ESCAP Committee on Information and Communications Technology, in November 2008, countries in the Asia Pacific region recommended that the ESCAP secretariat prioritize its activities, related to enhancing Pacific connectivity for improved ICT access by unconnected and underserved people. Those activities could include a study on viable options for deploying satellite technologies to geographically challenged countries in the region, particularly Pacific island developing countries. Additionally the committee called on the secretariat to further its initiatives in human resources and capacity-building as regards ICT policy development and applications, especially for countries with special needs, in the areas of ICT indicators, e-readiness, information security management, and such applications as e-commerce/e-business, e-government, e-tourism, e-health, e-literacy and e-agriculture.

²¹ http://wiki.laptop.org/images/c/c4/OLCP_Oceania_-_Concept_Note_-_Sep08.pdf

In March 2009, the Committee on Disaster Risk Reduction will be meeting for its first session in Bangkok, providing members and associate members including Small Island Developing Countries an unprecedented opportunity to establish a regional cooperation agenda addressing disaster management comprehensively, including through the use of ICT applications. Pacific States stand to benefit from a strong and unified participation in this Committee.

4.2 Cybersecurity

4.2.1 ITU Cybersecurity Work Programme Overview

To assist developing countries in cybersecurity, the ITU through its Telecommunication Development Sector (ITU-D) is involved in a number of activities. The ICT Applications and Cybersecurity Division (CYB)²² has the primary responsibility in ITU-D for supporting ongoing countries through their cybersecurity activities.

More specifically ITU-D is engaged in direct assistance to Member States on building national cybersecurity capabilities through a number of different activities. ITU-D is working on developing integrated national cybersecurity approaches to coordinate national efforts, including providing technical assistance through implementation of projects and capacity-building. In 2007 and 2008, some 8 Regional Forums on Cybersecurity have been organized by ITU-D to raise awareness and allow exchange of best practices and case studies²³.

In moving forward on its efforts ITU is working with partners from the public and private sectors on specific cybersecurity/Critical Information Infrastructure Protection (CIIP) development initiatives to assist developing countries in awareness and self-assessment, building and watch, warning and incident response capabilities. Some relevant deliverables in this regard include the [ITU National Cybersecurity/CIIP Self-Assessment Tool](#)²⁴ which aims to assist governments to enhance their cybersecurity and address CIIP requirements, the [ITU Botnet Mitigation Toolkit](#)²⁵, as well as toolkits on the establishment of CERTs/CSIRTs, and promoting a culture of cybersecurity²⁶.

Other ITU initiatives to assist developing countries include providing expertise and managerial support on activities related to cyber legislation (e.g. anti-spam legislative surveys, assessment activities of national cybercrime legislation and regional policies) and research into the financial and economic aspects of network security, malware and spam.

4.2.2 Feasibility Study on the Establishment of the PacificCERT

At the ITU Regional Cybersecurity Forum for Asia-Pacific & Seminar on the Economics of Cybersecurity held in Brisbane, Australia from the 15-18 July 2008²⁷, Senator Conroy (the Australian Federal Government Minister for Broadband Communications and the Digital Economy - DBCDE):

“... announced an initiative, a scoping study into the creation of a Computer Emergency Response Team in the Pacific. Computer Emergency Response Teams (CERTs) are a crucial aspect of a broader e-security strategy. CERTs can provide a coordinated approach to informing key stakeholders of the latest cyber-threats and assist in developing coordinated responses to these threats. Senator Conroy noted that the Department and the Attorney-General’s Department have held, over the past 12 months, a series of informal discussions with key stakeholders in the Pacific ICT community as the Departments have been keen to learn how best to support them to set up a Pacific-based CERT. The initial study, as

²² Contact CYB through the website <http://www.itu.int/ITU-D/cyb/> or by e-mail at cybmail@itu.int

²³ <http://www.itu.int/ITU-D/cyb/events/>

²⁴ <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html>

²⁵ <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html>

²⁶ <http://www.itu.int/ITU-D/cyb/cybersecurity/>

²⁷ ITU Regional Cybersecurity Forum for Asia-Pacific; <http://www.itu.int/ITU-D/cyb/events/2008/brisbane/index.html>

a ways to determine the best path forward for establishing a Pacific-based CERT, is a result of Australia's contributions to the ITU and collaboration with AusCERT."

The goal of the study is to assess the capability and readiness of likely stakeholders in the Pacific Islands to build a Pacific Island CERT based on an analysis of stakeholder attributes with relevance to the formation of a CERT for the region.

Based on the readiness assessment, it is envisaged that the report will give recommendations on a plan of action to either:

1. Create a Pacific Island CERT. In this case, the report will detail some recommendations on possible organisational models to adopt, the possible nature of the constituency, options for a CERT-stakeholder membership model and possible core services to be considered.
2. Enhance the capabilities of the likely stakeholders to a point where they are ready to create a Pacific Island CERT. In this case, the report will provide a suggested road-map for capacity-building in order to create the desired environment for the formation of a Pacific Island CERT. Possible capability enhancement activities may include the hosting of training courses for technical personnel or awareness raising seminars for members of the stakeholder community.

4.3 Harmonization of Legal Frameworks: Developing a Legal Foundation and Establishing Effective Enforcement²⁸

4.3.1 Understanding Cybercrime: A Guide for Developing Countries

Cybersecurity plays an important role in the ongoing development of information technology, as well as Internet services. Making the internet safer (and protecting internet users) has become integral to the development of new services as well as governmental policy. Deterring cybercrime is an integral component of a national cybersecurity/CIIP strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures.

The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively. As threats can originate anywhere around the globe, the challenges are inherently international in scope and it is desirable to harmonize legislative norms as much as possible to facilitate regional and international cooperation.

To assist countries in the region in understanding the links between cybersecurity, the building of confidence and security in the use of ICTs and cybercrime, ITU has developed, and is in the process of developing, a number of tools. One of these is the ITU guide dedicated to cybercrime titled "*Understanding Cybercrime: A Guide for Developing Countries*". The Guide can serve to assist in the assessment of the current legal framework and in the establishment of a sound legal foundation if this does not yet exist.

4.3.2 ITU Toolkit for Cybercrime Legislation

In addition to the guide, ITU, together with partners, is also working on a practical ITU Toolkit for Cybercrime Legislation. The toolkit aims to provide countries with practical instruments to conceptualize and implement a legal foundation and establish a legislative framework to criminalize the misuse of ICTs. The toolkit can provide countries with assistance in the establishment of a legislative framework

²⁸ See the website for more information on initiatives related to the harmonization of legal frameworks to criminalize the misuse of ICTs; <http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>

to deter cybercrime. Countries in the region that are interested in learning more about these ongoing cybersecurity related initiatives and possible assistance in this regard can contact ITU at cybmail@itu.int.

4.4 Organizational Structures and Incident Management Capabilities

The Government of Malaysia has offered to make available the infrastructure and services of the International Multilateral Partnership Against Cyber-Terrorism (IMPACT) to meet the GCA goals in its five work areas. IMPACT and its state-of-the-art global headquarters in Cyberjaya, Kuala Lumpur, as one of the physical homes of ITU's GCA, is available to provide ITU's 191 Member States with facilities and resources to effectively address global threats to cybersecurity in order to assist ITU Member States in the region develop their cybersecurity and CIIP capacity and capabilities.

The collaboration between ITU and IMPACT is based on a Memorandum of Understanding (MoU) signed in 2008 by ITU Secretary-General, Dr Hamadoun Touré, and the Chairman of the IMPACT Management Board, Mr Mohammad Noor Amin. It seeks to build synergies to provide: 1) Real-time analysis, aggregation and dissemination of global cyber-threat information; 2) Early warning system and emergency response to global cyber-threats; and 3) Training and skills development on the technical, legal and policy aspects of cybersecurity. Under the terms of this MoU, the GCA is to be housed at the IMPACT Centre, while ITU will maintain a 'virtual showcase' in Geneva, Switzerland of the early warning system, crisis management and real-time analysis of global cyber-threats. IMPACT initiatives, such as the Global Response Centre, as well as training and skills development, security assurance, research, and international cooperation, are being conducted under the auspices of the GCA in order to further build security and confidence in the use of ICTs. Some further information on possible services Member States can request from ITU through IMPACT can be seen below.

Working with leading partners from governments, industry and academia, the centre can provide the global community with a constantly available, real-time "Network Early-Warning System" (NEWS) that will help identify threats and provide guidance on what measures to take. It can also provide ITU Member States with access to specialized tools and systems, including the recently-developed "Electronically Secure Collaborative Application Platform for Experts" (ESCAPE). This enables experts in different countries to pool resources and collaborate remotely within a secure environment, and it features a comprehensive and growing database of key resources around the world that can be called on to assist during times of crisis. To this end ITU contributes expertise from its research on cybersecurity as well as its experience with developing online collaborative platforms to the IMPACT team.

In collaboration with leading ICT companies and institutions, IMPACT also conducts briefings for representatives of ITU Member States. Many of IMPACT's key partners have already promised to make available their leading technical and research experts for a programme to keep governments abreast of threats to cybersecurity. ITU is actively working on contributing its existing experience in capacity-building and in developing policy frameworks to the initiative. Under ITU leadership, and together with such partners as United Nations agencies, Interpol, and the Organisation for Economic Co-operation and Development (OECD), the centre contributes to the formulation of new policies and the harmonization of national laws on cybersecurity, including online crime. The centre can provide advisory services to ITU Member States on policy and regulatory matters and will foster international cooperation through specific programmes such as coordinated emergency drills to respond to cyberattacks. See the IMPACT project website for more information: <http://www.itu.int/osg/csd/cybersecurity/gca/impact/>

4.5 The Child Online Protection (COP) Initiative

The Child Online Protection (COP) initiative has been created as an integral part of the Global Cybersecurity Agenda, in order to encourage collaboration with and between relevant partners to promote cybersecurity for the youngest users of the internet, and further facilitate international partnerships for the implementation of best practices. As a platform for global cooperation, ITU is coordinating the efforts involved in protecting children online in order to make them more effective and accessible. The United Nations Secretary-General Ban Ki-moon has fully endorsed the COP initiative and encourages all states to support it.

The key objectives of the COP are to: identify the risks for children and young people in cyberspace, create awareness of these risks through multiple channels, and develop tools to help governments, industry, educators and relevant organizations minimize the risks. It provides a basis for sharing knowledge and forging international partnerships to implement concrete measures to protect children and young people in cyberspace. ITU will be carrying out a national survey in order to find out what child online protection/safety programmes/projects are in place and also to determine specific country requirements. Activities on e-safety issues by a wide range of organizations will be studied and solicited in order to develop a common framework for the protection of children online. Reflecting ITU's firm commitment to child e-safety, ITU Secretary-General Dr Touré has declared that the theme for the 2009 World Telecommunication and Information Society Day (WTISD) is the protection of children in cyberspace. See the COP website for more information on how to participate: <http://www.itu.int/cop/>

5 The Way Forward

The large scale adoption and success of ICT applications depends greatly on the existence of clear guidelines, standards and, when possible, laws that address the issues of security and confidentiality of the data collected and transferred through the use of diverse electronic tools and technologies. Justified public trust on the electronic tools and the secured management of sensitive personal information records, particularly in the areas of e-Government and e-Health, is a prerequisite for extended use of these applications.

Infrastructure deployment, be it through community information centres like PACRICS, broadband or wireless connections, needs to go hand in hand with the development of local content that addresses the specific needs of the networked communities, giving the population access to educational programmes, health and agricultural information and business opportunities of their interest. A sustainable approach to the deployment and use of ICT applications also needs to include strategies to gradually overcome literacy and computer skill barriers faced by their users, to ensure that the potential benefits of ICTs are exploited to their maximum.

Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being. At the national level, this is a shared responsibility requiring coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national strategy for cybersecurity and critical information infrastructure protection requires a comprehensive approach. Collaboration between government, industry, private sector, and users is crucial when developing strategies to deal with cybersecurity threats that undermine confidence and trust in the online environment. Countries in the region are encouraged to take every opportunity for to come together to share experiences, and work towards their common objectives in promoting a culture of cybersecurity that will foster an inclusive, secure and global information society. The PacificCERT collaborative initiative is a good step in the right direction with regards to further building cybersecurity capacity in the region. As such Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs) and related dedicated national cybersecurity response centers are a crucial aspect of a broader cybersecurity/CIIP

strategy. The establishment of such a team/center can provide a coordinated approach to informing key stakeholders of the latest cyber-threats and assist in developing coordinated responses to these threats.

Discussions have taken place to date to better understand how the Pacific Island countries can best be supported in this regard and what kind of model would work best given the specific circumstances and challenges countries in the Pacific are faced with. When all countries, including countries in the Pacific region, are able to access computer incident prevention, response and mitigation strategies, they can respond in a timely manner to threats affecting or involving their telecommunications networks. However, to be noted is that the success of a CERT/CSIRT for the Pacific region will depend greatly upon agreed protocols and standards and a commitment by all participating nations to maintain and enforce them.