Establishment of Harmonized Policies for the ICT Market in the ACP Countries

Child Online Protection Assessment
Vanuatu

ICB4PAC

Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries

This document has been produced with the financial assistance of the European Union. The views expressed herein do not necessarily reflect the views of the European Union.

The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. The mention of specific companies or of certain products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned.

Please consider the environment before printing this report.

Acknowledgements

This report documents the achievements of the regional activities carried out under the ICB4PAC project "Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries", officially launched in Fiji in November 2009.

In response to both the challenges and the opportunities from information and communication technologies' (ICTs) contribution to political, social, economic and environmental development, the International Telecommunication Union (ITU) and the European Commission (EC) joined forces and signed an agreement aimed at providing "*Support for the Establishment of Harmonized Policies for the ICT market in the ACP*", as a component of the programme "ACP-Information and Communication Technologies (@CP-ICT)" within the framework of the 9th European Development Fund (EDF), i.e., ITU-EC-ACP project.

This global ITU-EC-ACP project is being implemented by ITU through three separate sub-projects customized to the specific needs of each region: the Pacific Island countries (ICB4PAC), the Caribbean (HIPCAR) and sub-Saharan Africa (HIPSSA).

The ICB4PAC focal points and the project coordinator provided guidance and support to the consultant, Prof Dr Marco Gercke, who conducted the basic assessment of the use of ICT in schools and Cybercrime threats students discovered.

ITU would like to especially thank the Ministry of Communications as well as the principals of the schools involved for their support. Without the active involvement of these stakeholders, it would not have been possible to produce a report such as this.

The activities have been implemented by Mr Wisit Atipayakoon, responsible for the coordination of the activities in the Pacific (ICB4PAC Project Coordinator), and Mr Sandro Bazzanella, responsible for the management of the whole project covering sub-Saharan Africa, Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms Reshmi Prasad, ICB4PAC Project Assistant, and of Ms Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried out under the overall direction of Mr Cosmas Zavazava, Chief, Project Support and Knowledge Management (PKM) Department. The document has further benefited from comments of the ITU Telecommunication Development Bureau's (BDT) ICT Applications and Regulatory Monitoring and Evaluation Division (RME). Support was provided by Mrs. Eun-Ju Kim, Regional Director for Asia and the Pacific. The team at ITU's Publication Composition Service was responsible for its publication.

Table of Contents

Executive Summary

This report is the first known study of child online protection (COP) in Vanuatu. While conducting this study, no information could be found on the Internet about COP in Vanuatu as well as most other small Pacific island countries. The only information found were studies about COP in New Zealand and Australia, where the situations in regard to penetration rate and bandwidth as well as cultural and legal framework are different. Therefore, this report provides new knowledge and information on COP.

This study was conducted through the global ITU-EC-ACP project. It is a new project jointly funded by the European Commission (EC) and the International Telecommunication Union (ITU) for Capacity Building and ICT Policy, Regulatory and Legislative Frameworks for Pacific Island Countries (ICB4PAC).

This report is an assessment and analysis of the present situation of COP in Vanuatu. Under the same project similar assessments have been carried out in Niue, Kiribati, Tonga and Tuvalu. The report gives a general background on COP, explains some of the main threats as well as strategies for prevention. This report concludes with an analysis of the findings and outlines policy implications that Vanuatu could consider.

The key driver for this report is to examine how students access the Internet and which risks they are facing. Taking into account that there is almost no data available regarding the number of victims of Cybercrime in Vanuatu, the report also helps to access the general situation with regards to Cybercrime victimization.

The assessment was carried out as a test only through a questionnaire with 14 multiple-choice questions. It was carried out in Central School. In total 294 students participated in the survey. In addition to carrying out the survey the students received basic trainings on Internet risks as well as protection strategies.

The assessment of the current situation related to COP and Cybercrime underlines that despite a comparably low Internet penetration rate of less than 10 per cent (based on World Bank Data), students in Vanuatu are intensively using the Internet. Almost 90 per cent of the students use the Internet with around 30 per cent of the students using the Internet daily. Facebook is among the most popular services with almost 50 per cent of the students using it.

Cybersecurity is a topic that the students are confronted with. Almost 60 per cent faced infection of ICT with malicious software. However, only 21 percent of the students reported that they use anti-virus software. When it comes to teaching security the school remains an important source of knowledge for students. One third of all students mentioned that they learned about Cybersecurity in school.

Students have been exposed to Cybercrime. Apart from computer viruses (see above) 15 per cent of the students in Vanuatu have been victim of Cyber bullying. Almost 10 per cent of students have been contacted by strangers online.

The questionnaire also contained a section dealing with illegal/inappropriate acts. Around 10 per cent of the students have stent mean/harmful messages which could be considered Cyber bullying. Around one third of the students tried or successfully broke into protected wireless networks.

The data collected through the survey enables the government of Vanuatu as well as schools in the country to better respond to the challenges of Child Online Protection.

- Knowledge about the services used by students allows the development of specific training courses that focus on those services that are most popular among students in Vanuatu. This will maximize the impact of such training. In order to avoid children becoming victims of security

incidents/crimes (such as infection with malicious software, cyber bullying and grooming) the training includes prevention measures related to these offences.

- The assessment clearly underlines that people in Vanuatu are affected by Cybercrime. Infecting a computer system with malicious software goes along with the alteration of data on the affected computer system. This is an activity that is widely considered to be illegal ("illegal data interference"). 121 students have reported such incidents and are consequently most likely victims of a crime. This does not correspond with number of Cybercrime investigations. One of the main reasons is that victims of Cybercrime tend not to report such crime. Non of the students indicated that they contacted the police when they have been confronted with a potential crime.

- Based on the current legislation the infection of a computer with a computer virus is not criminalized. It it is uncertain if other potentially harming activities such as solicitation of children ("grooming") and Cyber bullying are covered by applicable legal frameworks. This issue might require further investigations.

Due to the tremendous and generous support of the Principal of Central School, as well as the Prime Minister's Office via the Office of the Government Chief Information Officer and the Telecommunications and Radiocommunications Regulator, the entire assessment (distribution of the survey and collection of data) was carried out in less than three week. Taking into account the usefulness of the collected data the government may want to consider to carrying out a second more comprehensive assessment the includes more questions related to the way students assess the internet and what security incidents they were facing. With regard to the accuracy of the data a survey including more schools should be taken into consideration.

1 Introduction

1.1 ICT as an opportunity for social development and economic growth

Properly engaged, ICT is a significant tool in the fight against poverty.[1] Through universality of access it can enable people in developing countries in general and especially remote islands get access to knowledge, information and government service as well as enabling a sustainable development and diversification of the economy. There is great hope that the Internet can in this regard become a facilitator for the economic development of Small Islands Developing States (SIDS).[2] Especially the tourism industry and the manufacturing of handcrafted goods can benefit from the global availability of their services and the reduction of costs for traditional marketing and commissions of travel agencies. The potential economic impact is highlighted in a World Bank Study from 2009 that observed that for developing countries every 10% increase in broadband penetration leads to up to 1.38% increase in GDP.[3]

1.2 Role of ICT in education

While in some areas ICT will need to prove that it can make an impact education is one of the areas where ICT has already proven to be successful.[4] Especially children benefit from this development. The Internet is used as technology to make available knowledge relevant for students. After decades of where institutions kept knowledge exclusively for students of the respective institution there is a trend of opening up. One example is the Harvard University, a famous university with high fees for registered students that decided to make online courses available for free.[5] This enables students in developing countries to get access to the same courses and material as students in the developed world. However, what is often forgotten is that this of course depends on the availability of Internet access and sufficient bandwidth in developing countries. Making video podcasts of lectures available for free is the one thing – students being able them to download large files is still a challenge in less and least developed countries. Connecting schools to the Internet and enabling students to access online sources has therefore become a key element of national ICT strategies in developing countries.

1.3 Risks of ICT for children

[1] With regard to the discussion about the impact of ICT on economic growth and access to knowledge in developing countries see: *Adam/Wood*, An Investigation of the Impact of Information and Communications Technology in Sub-Sahara Africa, Journal of Information Science, 1999, page 307-318; *Alabi*, Enpowering Socio-Economic Development in Africa Utilizing Information Technology, 1996; *Best/Maclay*, Community Internet Access in Rural Areas: Solving the Economic Sustainability Puzzle, published in The Global Information Technology Report 2001-2002, Chapter 8; Brown, Can ICTs Address the Needs of the Poor?, UNDP, 2001, available at: http://www.undp.org/dpa/choices/2001/june/j4e.pdf;

[2] Trends in Sustainable Development – Small Islands Developing States, United Nations, Department of Economic and Social Affairs, 2010.

[3] Wei Qiang CZ and Rossotto CM (2009) Economic Impacts of Broadband. In World Bank *2009 Information and Communications for Development 2009: Extending Reach and Increasing Impact*. Available at http://allafrica.com/sustainable/resources/view/00011823.pdf.

[4] *Camacho*, Evaluating the Impact of the Internet in Civil Society Organizations of Central America, Fundacion Acceso, 2001; *Elmer*, Education for All in the Information Age: The Potential of Information Technology for Improving Educational Access and Quality in Developing Countries, 1999; *Hawkins*, Ten Lessons for ICT and Education in the Developing World, in CID – The Global Information Technology Report 2001-2002, 2002, Chapter 4; *Ojedokun*, Distance Education and the New Information and Communications Technologies: An Analysis of Problems Facing a Developing Country, 1999; *Osin*, Computers in Education in Developing Countries:Why and How, World Bank Education and Technology Technical Note Series, Vol. 3, No. 1, 1998.

[5] Lewin, Harvard and M.I.T. Team Up to Offer Free Online Courses, The New York Times, 02.05.2012.

Just like the utilization of other technologies, or any action in real life the use of Internet services can go along with risks for children. Determining how big the risk is goes along with challenges. There is no evidence that children are exposed to more or more severe threats online than they are in the real world. However, it is important to underline that threats do existing – and most likely more important: The threats are different from threats in real life and so are very often other factors like for example who teaches the children security. In real life one of the threats to children is related to traffic. It will in general be the parents that are teaching children how to cross a road safely. With regard to the Internet the threats are different. Computer viruses, cyber bullying, "grooming" and access to illegal content are four examples of such threats.

- **Malicious Software / Computer Viruses**
  Computer viruses are malicious software that can cause harm to computer systems. There are currently more than one million known computer viruses and the number is growing with increasing speed.[6] The security company PandaLabs published even higher number. Based on their annual report for 2011 26 million new computer viruses have been identified in 2011.[7] These were in average 73.000 new computer viruses every single day in 2011. A viruses can be infect a computer in different ways (e.g. by opening an attachment of an e-mail or opening an infected website ("drive by infection") and no single anti-virus software can detect all computer viruses it requires a combination of experience and knowledge to know how to use protection measures to successfully protect against this threat. Children require training to be able to deal with this threat. It is important for children to be protected as there are viruses that can interfere with the privacy of children (for example by secretly activating the built-in video camera in notebooks).

- **Cyber Bullying**
  Many children today use social networks. Some social networks offer the possibility to register without providing real names. This enables members of the social network to leave threatening or defamatory messages on other member's website. A significant number of students have reported that they have been victim of such acts. "Cyber Bullying" is a term used to describe such acts, where the offender uses ICT to harm people in a deliberate and hostile manner. It is a social cruelty among adolescents.[8] Bullying is behaviour that was observed before the Internet was invented.[9] While it is true that students may also become victim of defamation outside the Internet, there are significant differences when this happens online. The first main difference is that offenders that act online can hide their identity.[10] Unlike in normal conflict situations in the real world children will in this case not know who the offender is. An anonymous posting has the potential to make the bullying feel more intimidating. In addition a posting distributed through popular social media sites has a far broader reach. The third difference is that offenders can continue the bullying online even after school hours. The possible impact of bullying and cyber bullying on victims is intensively discussed.[11] What is known is that some of the students that

[6] *Bidgoli*, MIS2, 2011, page 78

[7] PandaLabs, Annual Report, 2011, Summary, page 15.

[8] *Shariff/Hoff*, Cyber bullying: Clarfying Legal Boundaries for School Supervision in Cyberspace, International Journal for Cyber Criminology, Vol. 1, Iss. 1, 2007, page 76.

[9] *Donegan,* Bullying and Cyberbullying: History, Statistics, Law Prevention and Analysis, Elon Jounal of Undergraduate Reseach in Communications, Vol.3, No. 1, 2012, page 33 et seq.

[10] *Shariff/Hoff*, Cyber bullying: Clarfying Legal Boundaries for School Supervision in Cyberspace, International Journal for Cyber Criminology, Vol. 1, Iss. 1, 2007, page 77.

[11] See for example: Cyberbullying: Law and Policy. US Constitutional Rights Foundation, 2010; *Camodeca/Goossens/Gerwogt/Schuengel*, Bullying and Victimization Among School-age Children, Social Development, No. 11, 2002, page 332 et seq.

have been victim of cyber bullying have committed suicide[12] – although it is uncertain if cyber bullying alone led to the suicide.[13]

- **Solicitation of children for sexual purposes ("grooming")**
  The Internet offers the possibility of communicating with others without disclosing one's age or gender. This feature can be abused by offenders with inappropriate sexual interest in children to contact minors, establish a relationship and groom potential victims for sexual purposes.[14] The phenomenon is frequently called "grooming".[15] Just like cyber bullying the solicitation of children is no mere online crime but ICT in general and especially the anonymity of the Internet allows offenders to utilize new means of contacting children.[16] Some researches indicate that compared to the total number of cases of sexual abuse the number of Internet-initiated crimes are relatively small.[17] In many western countries the number of cases of online grooming raised during the last years.[18] One of the main differences between the offline and online world is the fact that safety measures that turned out to be effective in the real world like "be careful when you are approached by strangers that are much older than you" do not necessary reflect the reality in an online environment. It is in general not possible to determine the age of a person who starts a communication. Apart from this the process of establishing contact to previously unknown people is a rather usual behaviour on in social networks.[19]

- **Indecent material**
  Sexual-related content was among the first content to be commercially distributed over the Internet. Recent research has identified as many as 4.2 million pornographic websites that may be available on the Internet at any time.[20] Besides websites, pornographic material can be distributed through file-sharing systems[21] and instant messaging. Many of the websites are not only available for adults but also minors that access the Internet.

1.4 Child Online Protection (COP)

Taking into account the advantages that ICT offers children the process of connecting children to the Internet is widely recognized as desirable goal. However, it is equally widely recognized that in order to

[12] *O Cionnaith*, Third suicide in weeks linked to cyberbullying, Irish Examiner, 29.10.2012.

[13] *Hinduja/Patchin*, Bullying, Cyberbullying and Suicide, Arhcives of Suicide Research, 14(3), 206 et seq; Cyber-Bullying Overview, National White Collar Crime Center, Nov. 2010.

[14] See in this regard: *Powell*, Paedophiles, Child Abuse and the Internet, 2007; *Eneman/Gillespie/Stahl*, Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case, AISeL, 2010, available at: http://www.cse.dmu.ac.uk/~bstahl/index_html_files/2010_grooming_ICIS.pdf; Choo, Responding to online child sexual grooming: an industry perspective, Trends & Issues in crime and criminal justice, No. 379, July 2009, page 1.

[15] See: Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

[16] *Eneman/Gillespie/Stahl*, Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case, Thirty First International Conference on Information Systems, 2010, page 3.

[17] *Wolak/Finkelhor/Mitchell/Ybarra,* Online Predators and their Victims: Myths, Rality and Implications for Prevention and Treatment, American Psychologist, 63; page 111 et seq.

[18] Choo, Responding to online child sexual grooming: an industry perspective, Trends & Issues in crime and criminal justice, No. 379, July 2009, page 1.

[19] *Eneman/Gillespie/Stahl*, Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case, Thirty First International Conference on Information Systems, 2010, page 2.

[20] *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

[21] About a third of all files downloaded in file-sharing systems contained pornography. *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

maximize the advantages for the children it is important to control the risks. Consequently “Child Online Protection” (COP) has become an integral part of many initiatives of organizations that are active in the field of child protection. With the Child Online Protection initiative ITU has developed various tools in order to support the process of protecting children online. In this regard it is important to highlight that COP can not be limited to a single measure. A comprehensive COP strategy may combine various measures out of the following areas: technical measures, legal measures, organizational structures, capacity building and international cooperation. An introduction of COP measures can help to decrease the risks that children face online.

2 Assessment of Internet Usage and COP

2.1 Importance of an assessment and individualization of national strategies

In order to develop strategies/policies/legislation, design classes and training material for students or implement technical measures it is crucial to understand how children use ICT, what they know about security, how they learn about security, which risks they are exposed to and how far they themselves have been involved in illegal activities. Without such assessment the COP strategy might be based on wrong assumptions.

- **Individualized training**
  The likelihood of wrong assumptions as a consequence of a missing assessment can be demonstrated by referring to security training. One major Cybersecurity risk for Internet users is the infection of a computer system with malicious software that took place through an e-mail attachment. Consequently a lot of general Cybersecurity training focuses on the risks of e-mail attachments and how to prevent such infection. However, children, that use the Internet for communication purposes use e-mails way less frequent than adults and instead make use of instant messaging systems of social networks. This issue needs to be reflected when designing a Cybersecurity training for children. An assessment can ensure that the Cybersecurity training is tailored to the demands of children in the country.

- **Differences in Internet usage**
  In this regard it should be highlighted that despite the globalization of services like Facebook, with more than one billion users worldwide, the way how children use the Internet differs. The usage is depending on aspects like language, culture and bandwidth. Therefore Cybersecurity training courses designed for one country may require modifications when it is intended to be used them in another country. The results of the assessment can help the institutions responsible for the training to identify specifies of the country that might be relevant for the modification of existing training material.

- **Development of an individual legal framework**
  A lack of assessment may not only influence the development of training material but also the broader policy and legislation. Without an assessment policy and legislation may not reflect the reality of children in the country may not be reflected. One example is the criminalization of copyright violations. If it turns out that many students use copyright protected artwork within creative processes of discovering ICT (e.g. using a copyright protected song as background music for a video that they produce in school) the introduction of a criminalization of copyright violations without exemptions (e.g. based on the “fair use” principle) could lead to an unintended criminalization of a significant part of the society.

2.2 Importance of regular updates of the assessment

ICT is a highly dynamic area of technology. With new services being introduced on a regular basis the related Cybersecurity threat change. In order to be able to respond to such processes it is useful to carry out similar assessments on a regular basis. This could for example be supported by institutionalizing the assessment as part of the national Cybersecurity strategy/policy.

2.3 Assessment as part of the ICB4PAC methodology

2.3.1 HIPCAAR/HIPSSA/ICB4PAC

In order to support the development of ICT policy, legislation and capacities in ACP countries, ITU and EU decided to co-fund a project.[22] This project is part of the programme "ACP-Information and Communication Technologies" and the ninth European Development Fund. Taking into account different prior developments and priorities within the three regions, the project was sub-divided into three regional sub-programs. The Sub-Sahara Africa region was supported with the "Harmonization of ICT Policies in Sub-Sahara Africa" (HIPSSA). For the Caribbean countries the project "Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures" (HIPCAR) was implemented to promote the ICT sector in the Caribbean region.[23] Finally the Pacific countries received support within the project "Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries (ICB4PAC).

2.3.2 Methodology

All three projects were divided into two phases. During *phase one* a regional assessment of existing legislation and comparison with international best practices was carried out. Based on the assessment report and comparative law analysis model policies and model legislation was developed. During *phase two* the countries received support in the national transposition of the model policies and model legislation.

2.3.3 ICB4PAC

In parallel to the projects in Africa and the Caribbean, a project for Pacific countries was launched (ICB4PAC).[24] Upon request by the Pacific Island countries, the project provides capacity building related to ICT policies and regulations. It focuses on building human and institutional capacity in the field of ICT through training, education and knowledge sharing measures. Beneficiary countries are 15 Pacific Island countries.[25] Work areas covered are for example licensing and numbering, universal access, interconnection and cost modelling as well as cybercrime.

2.3.4 Assessment as part of the ICB4PAC project

[22] Details about the project and the funding are available at: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/

[23] For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html; ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 4.

[24] For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[25] Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

During phase 2 Pacific countries could request customized, individual support. Activities carried out in Pacific countries included capacity building for police, customs, judiciary, stakeholder consultations and support in drafting policy, legislation and regulation.

One component that is unique in the ICB4PAC in-country support is a demonstration of the advantages of a national assessment in relation to Cybersecurity through the process of carrying out a general assessment of the situation of Cybercrime in a the country as well as a more specific assessment of the use of ICT by students and their experiences in relation to the Cybersecurity/Cybercrime incidents.

To facilitate the process different questionnaires were developed. Due to limited capacities and time the purpose of the assessment is not to get a response from all member of the target group but to get a significant number of responses to

- demonstrate the advantages of an assessment,
- enable reliable conclusions with regard to the subject matter, and
- utilize the information within the drafting of policy/legislation/regulation.

3 ICB4PAC Assessment in Vanuatu

During the ICB4PAC mission to Vanuatu (5-19 February 2013) an assessment of how students in Vanuatu already use ICT and their experiences was carried out. During the mission the ITU consultant shared some of the findings of other assessments that were carried within ICB4PAC in-country support missions. The office of the Regulator organized the distribution of questionnaires in school, the collection of the questionnaires as well as the conversion into an Excel file. It was agreed that the assessment should be combined with a capacity building workshop for the students. The assessment was undertaken on the basis of an adopted version of the ICB4PAC COP questionnaire (see Annex 1).

On 18th of February Ms Louisa Nasak from the office of the Regulators, Mr. Jackson Miake from Prime Ministers Office and the ITU consultant visited Central School and gave a capacity building lectures in relation to some of the most relevant Cybersecurity issues for children in Pacific countries (based upon the assessment in other Pacific islands). A total of 294 questionnaires were collected.

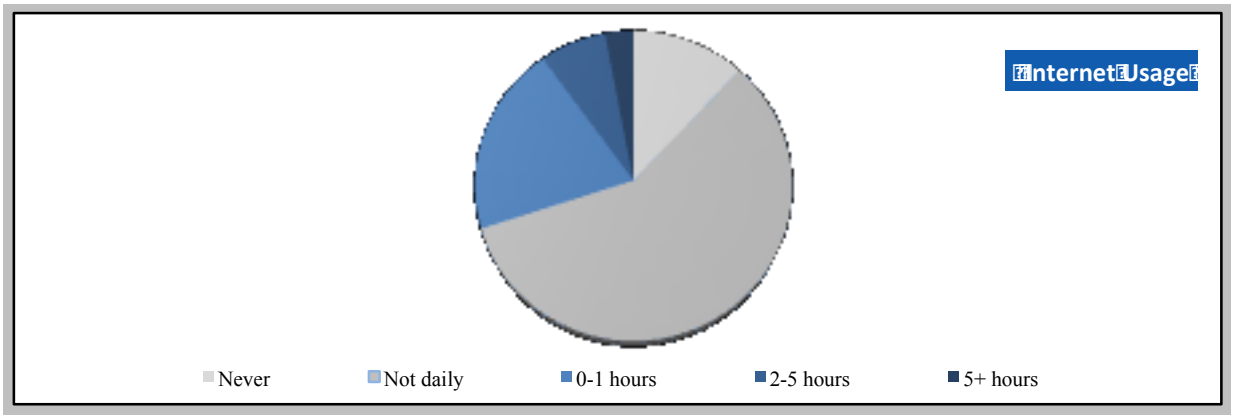
Section I

4 Assessment 1: Use of the Internet

The following overview summarizes the results of the assessment with regard to the use of the Internet as well as the services.

4.1 Internet usage

The assessment revealed that so far the majority of students do not use the Internet almost every day or even daily. Only a small percentage does not use the Internet at all.



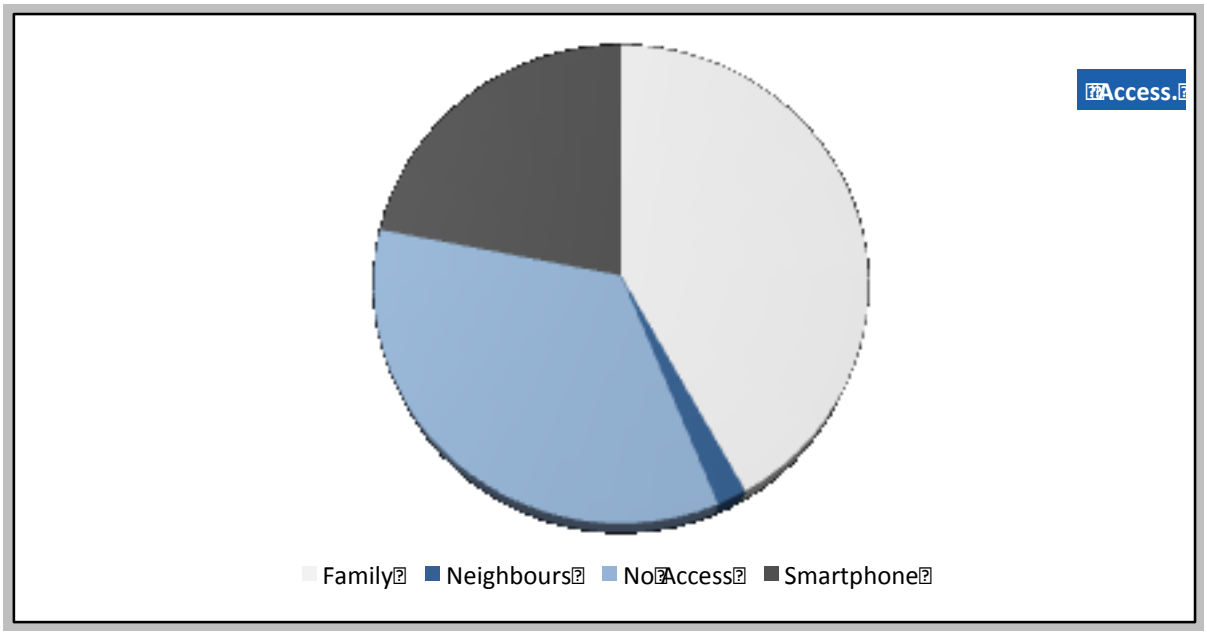
This is a major difference to many western countries where many students quite intensively use the Internet. This is also the case in some of the other Pacific island countries. One example is Niue, where a similar assessment took place. Compared to 66 per cent of the students in Niue, only 30 per cent of the students in Vanuatu use the Internet at least one hour a day.

Policy Implication:
In many countries of the world children between the ages of 10-18 are using the Internet quite intensively. This does not imply that daily use of the Internet is desirable or necessary. The results of the assessment however indicate that there is a chance for further improvements when it comes to enabling children to use the Internet.
The fact that not all students use the Internet daily might also have implications for the number victims of Cybercrime in the country. With an increasing number of people connected to the Internet the potential number of victims grows. An introduction of mandatory Cybersecurity training in schools within the next months could help to ensure that those students that do not yet use the Internet intensively will be well prepared with regard to self protection measures at the moment they get more active.

Bibliography

4.2 Internet access

With regard to the fact that the assessment was focussing on aspects of Child Online Protection and Cybersecurity/Cybercrime only few questions related to access to the Internet were included in the questionnaire. The assessment nevertheless revealed that almost half of the students do not have the possibility to access the Internet from home.

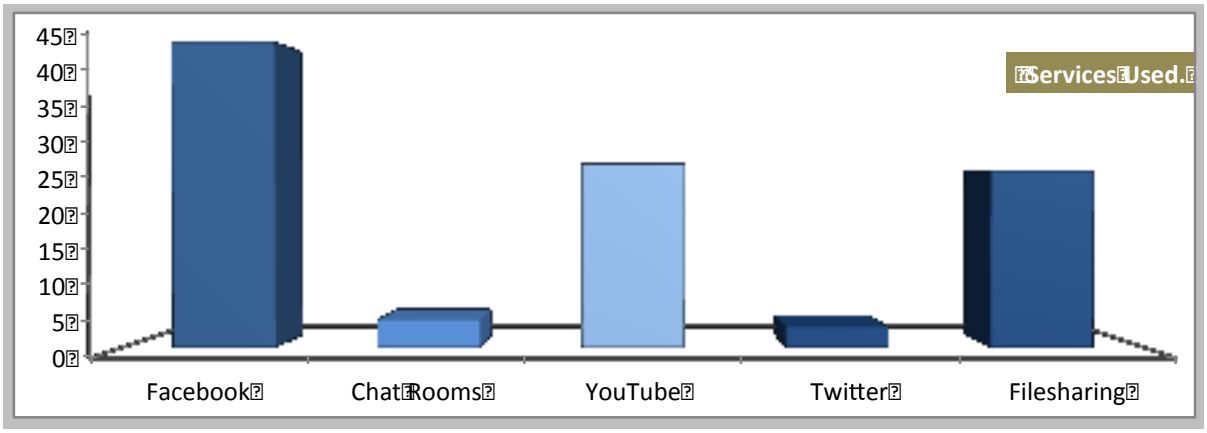


As shown from the responses of the students, one third of them simply do not have the possibility to access the Internet from home or through their neighbours. One of the reasons could be that they live in less developed or rural areas with no or restricted Internet connection. It could also be that their families are not technology affine or cannot afford to sign up for an Internet connection. This underlines the importance of further assessment.

Policy Implication:
Missing access to the Internet has security implications. It is certainly correct that while students are not online the risks of becoming victim of a Cybercrime decreases. The risk does not disappear as a computer could be infected by a computer virus that is on a flash drive. But a missing connection to the Internet (especially in combination with low bandwidth when connected) means that large updates for the operating system and anti-virus software, that are crucial self-protection measures, might not be available to those users.
The questionnaire was not designed to assess the ability of children to connect to the Internet in more detail. With regard to possible initiatives to connect rural areas or ensure that all school in Vanuatu have access to the Internet, a more detailed assessment could be helpful. It is possible that central access points in rural areas and an improvement on connectivity of schools could have a significant impact on connecting students.
One issue that could be further studied within a more complex assessment in Vanuatu in the near future could be questions like: Why do more 70 per cent of the students not use the Internet daily, would those children like to be able to have daily access, why would they want to access the Internet more often (school, communication with friends) and how/where they would like to access the Internet (mobile access, in school, at home).

4.3 Popular services

A deeper understanding of the services that students use is relevant for running the networks in the country/schools as well as the design of security measures.



The assessment shows that the students use similar services as students in other parts of the world do. Especially Facebook is popular among Students in Vanuatu. From a network operator perspective the fact that more than one quarter of the students that participated in the assessment reported that they used YouTube or other video site could be interesting. YouTube is a very popular website where users can watch all kinds of movies. The challenge for network operators in countries with low bandwidth is that the use of such websites goes along with significant download traffic. It is likely that the operator does already monitor the different services used with more sophisticated technical tools and has already implemented countermeasures. If not the implementation of such measures could be taken into consideration.

With regard to the design of Cybersecurity training for children the results of the assessment play a key role. There are various issues that could be discussed with children in relation to the two most popular services: Facebook and Chat Rooms:

- **Facebook**
  With regard to Facebook it could be useful for children to learn how to adjust the privacy settings to ensure that only invited friends can see their postings. Taking into account that a number of students in Vanuatu have already been confronted with cyber bullying, that also takes place on Facebook, awareness raising and response options could be discussed.

- **Chat Room**
  Unlike in other Pacific islands chat rooms do not seem to be very popular in Vanuatu. Such chat rooms and can be utilized in positive ways. However there are also some security implications if children use such chat rooms. In “online grooming” cases, where children were contacted by adults, that had an inappropriate sexual interest in children, the perpetrators often use chat

rooms to contact a child. Chat rooms are also used for defamation, the exchange of illegal content and bullying. Therefore awareness-raising with regard to the secure use of chat rooms for children could – despite the currently limited interest in such services - become a part of the Cybersecurity training in schools.

Policy Implication:
Children in Vanuatu – just like students in other parts of the world – use Internet services such as Facebook that offer great opportunities. However, those services have in the past also been utilized to victimize children. As pointed out above the safe usage of those services, that are particularly popular among students in Vanuatu, should be taken into consideration. In order to ensure that all students benefit from such training with updates at least once a year Cybersecurity training could be made a mandatory component of the curriculum. There is currently a discussion within some Pacific countries to make this part of the national Cybersecurity policy.
A second policy implication is the need from criminalizing offences victimizing children. If for example solicitation of children ("grooming") is not criminalized offenders from abroad could target children without the police being able to step in. Therefore a review of the current Cybercrime legislation should be taken into consideration in order to ensure that the police can act if children are at risk.
A significant number of students uses services that could be utilized to undertake copyright violations. It is possible that the students would even disrespect legislation if obeying the legislation leads to social pressure. One area where such process could be witnessed is copyright violations. Some children may experiment with technology, wish to try software even if they cant afford to buy it, download copyright protected artwork and maybe even combine their own artwork (for example a movie showing them dancing) with a copyright protected component (a background song for the movie) and make this publically available (for example on a video platform). In order to avoid a mass-criminalization the introduction of criminalization in the field of copyright protection should be undertaken in a mindful way. On possibility could be to limit the criminalization of acts on a commercial scale or implement an exclusion of criminal liability based on the "fair use" principle.

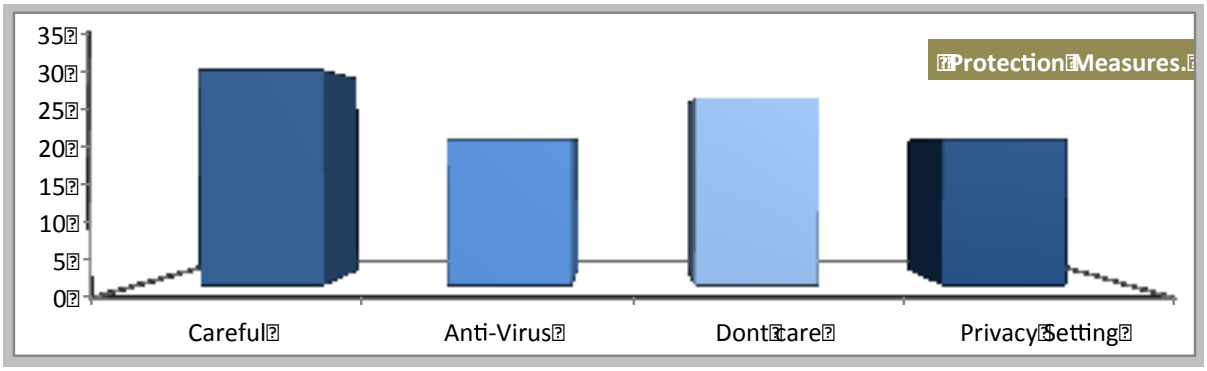
Section I

5 Assessment 2: Security

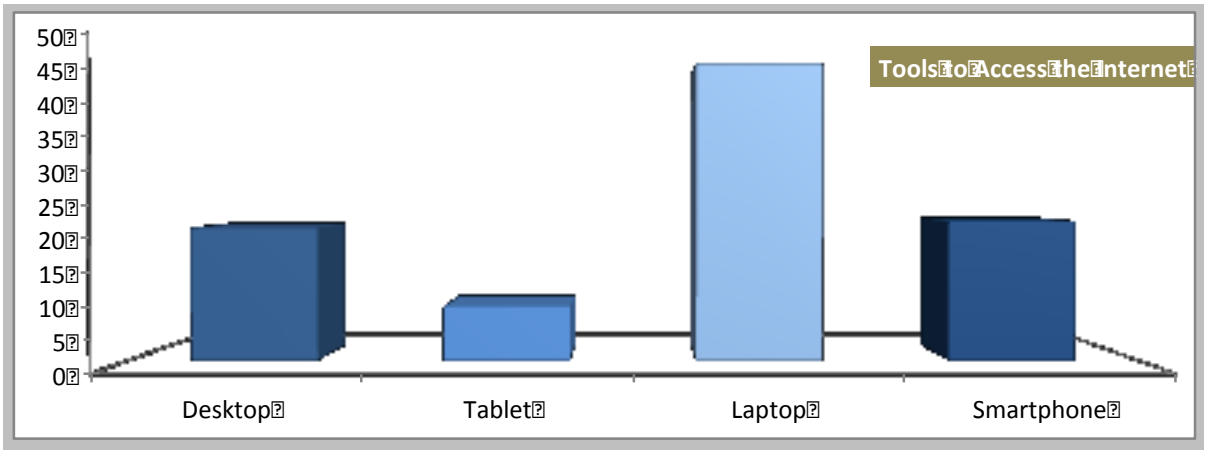
The following overview summarizes the results of the assessment with regard to security measures utilized by students as well as institutions involved in teaching security.

5.1 Security

Not all students are yet utilizing technical tools (anti-virus) to prevent Cybersecurity incidents. When it comes to teaching security schools play an important role.



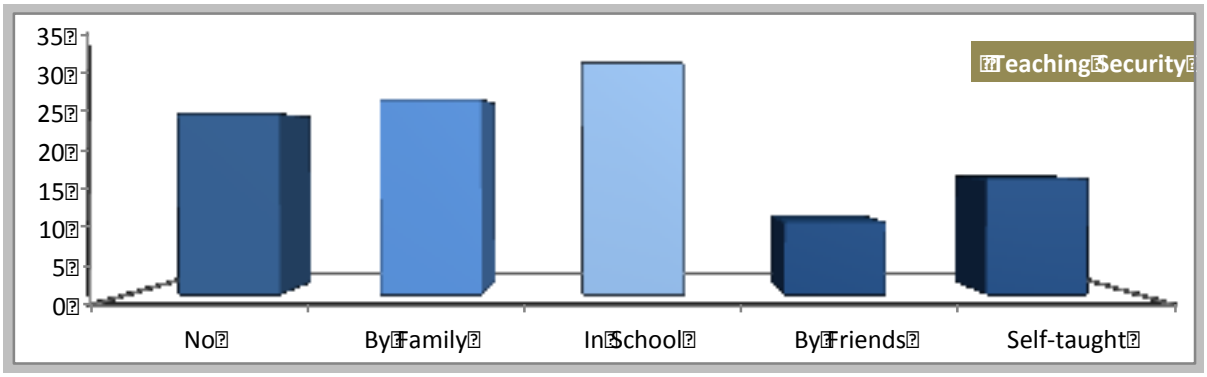
One measure in preventing Cybersecurity incidents is the utilization of technical tools (such as anti-virus software). The assessment shows that only 21 per cent of the students use anti-virus software. What on first sight looks like an alarming figure does not necessarily mean that the remaining 80 per cent are careless. While classic desktop computers and notebooks allow the installation of anti-virus software some closed systems like operation systems on smart phones and tablet pc do not enable the user to install anti-virus solutions. As especially younger Internet users make use of such tools it could explain the missing use of anti-virus software. However, the assessment also shows that tablet, PC's and smart phones are not that intensively used to access the Internet.



Most students use desktop computers and laptops. With regard to the importance of technical tools further assessments should be taken into consideration to identify the reasons for the missing use. There are various possible explanations that require clarification. It could for example be that the children are using computer systems that already have pre-installed measures that they are not aware of. Or the limited bandwidth combined with the necessity to download the large updates of anti-virus software hinders a wide usage in Vanuatu. Finally it could be a lack of awareness about the importance, the fact that several anti-virus tools are available for free or how to install and operate them.

5.2 Institutions teaching security

With regard to the possible need for capacity building and training schools could play a major role.



The assessment shows two facts. First of all schools are most likely at the moment the most important source of knowledge when it come to Cybersecurity. 32 per cent of the students reported that they were taught security in school. With regard to other, more traditional security concerns (like for example how to cross a road in heavy traffic) it is very often the family that provides the children the basic knowledge. When it comes to Cybersecurity it could be that the families do not have the capacity to take over the training. Identifying risks related to the use of the ICT requires specific knowledge. Even more challenging is the process of teaching users how to protect against such threats. Really difficult is finally to ensure that the knowledge transfer process takes place whenever important developments are on-going (such as the introduction of new services that go along with specific risks). Through schools it is possible to reach out to almost all people in Vanuatu between the age of 10 and 19. Such training could include lessons on how to get information about new risks after the students left school. This could lay the foundation for a more secure use of ICT of the next generations.

Policy Implication:
The assessment shows that there are existing structure in the country that partly already take over tasks related to Cybersecurity training and could play an even more important role in an institutionalized environment. This could be a bi-directional process where the institutions provide knowledge but at the same time repeat the assessment to ensure that the relevant stakeholders in the country have access to up-to-date information. Apart from schools there might be other institutions and stakeholders that could take over an important role like churches, religious leaders and chiefs.

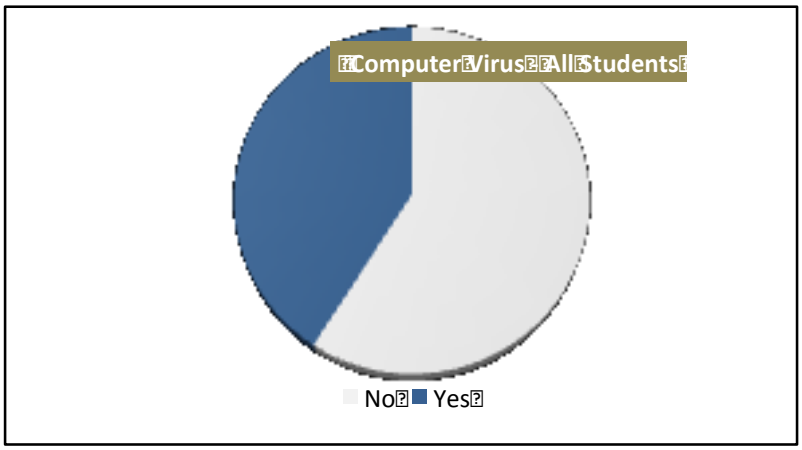
Section I

6 Assessment 3: Security incidents discovered

The following overview summarizes the results of the assessment with regard to security incidents that were discovered by students.

6.1 Computer Viruses

One of the main purposes of the assessment was to learn more about the situation of Cybersecurity/Cybercrime for students in Vanuatu. Students in Vanuatu have been exposed to different Cybersecurity incidents.



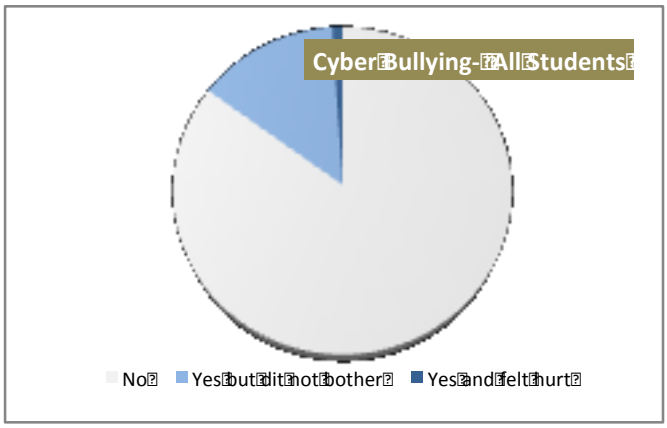
The assessment underlines that Cybercrimes do affect people in Vanuatu in general and more specific students. Around 40 per cent of all students that participated in the assessment have already experiences computer viruses. The introduction of a computer virus is a typical Cybercrime – although currently most likely not criminalized in Vanuatu.

Policy Implication:
The assessment underlines that Cybercrime is already affecting people in Vanuatu. Even students are among the victims of such crime. Computer viruses can be dangerous as their payload may go beyond slowing down computer systems and requiring a reinstallation of the operating systems. Some of the current computer viruses can secretly activate built-in microphones or cameras, record and transmit videos to the offender. Such potential threat is a concern for both users and their privacy as well the government and government secrets.
Although it is likely the offenders will in most cases not be acting from Vanuatu the ability of local authorities to take action depends on the existence of an effective legal framework. Such framework should especially include a response to those offences that are most relevant for people in Vanuatu. In addition the police needs to receive specialized training in investigating such crime.
The fact people are already affected underlines the importance of strengthening measure of crime prevention. Such measure, which could for example be included in a Cybersecurity policy, could include new way of distributing technical protection measures as well as institutionalizing training for students.

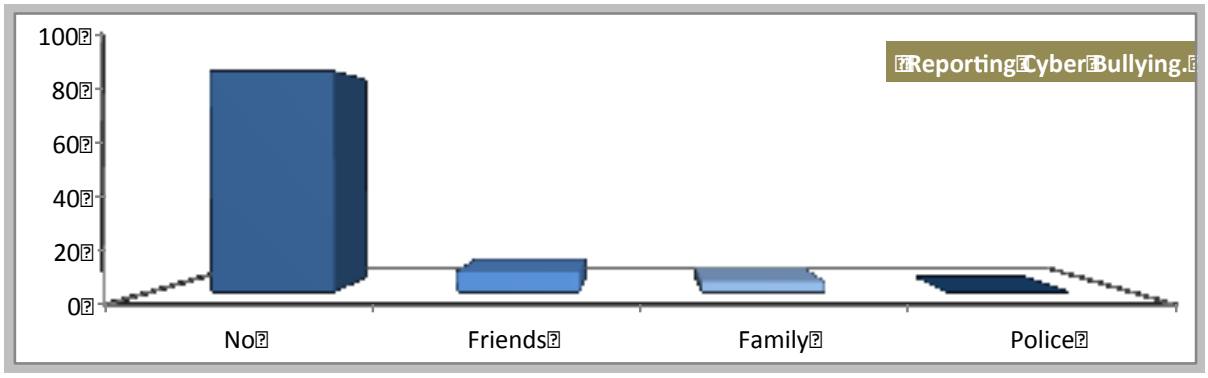
Bibliography

6.2 Cyber Bullying

The assessment did not only focus on Cybercrime incidents that are relevant for all kind of users, but also offences that are more specific to children. One example is cyber bullying. Students in Vanuatu are affected by this type of activity.



The assessment underlines that students in Vanuatu have been victims of cyber bullying. However, the number is lower than in other Pacific countries where similar assessments have been carried out. Around 15 cent of all students that participated in the assessment has been victimized. Less than 10 percent of the victims (3 students in total) felt hurt by what happened.

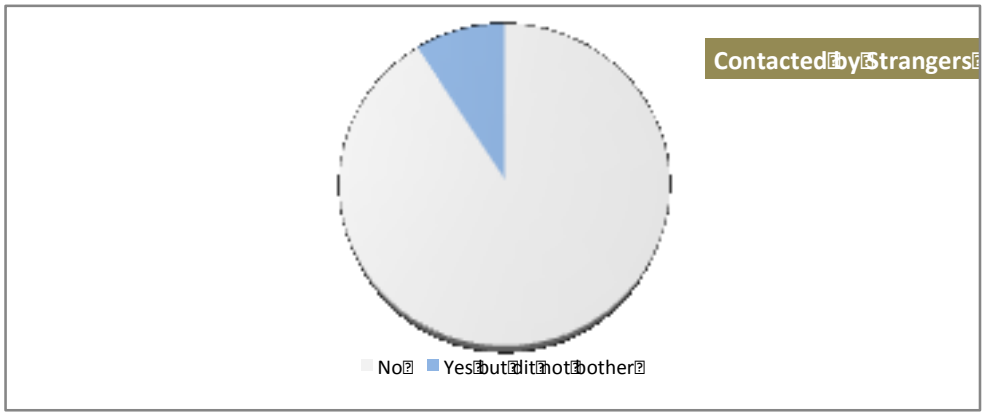


Further more the assessment underlined a trend that is known from other areas of Cybercrime: Victim do tend not to report the crimes to law enforcement authorities.

Policy Implication:
As explained in the introduction cyber bullying is a serious crime. The assessment highlights that students in Vanuatu have already been victimized. With regard to the fact that victims of cyber bullying often feel alone and do not speak other about the incident priority should be given to encourage students to report cyber bullying. At the same time it is important that at the institutions, that the crime could be reported to (for example teachers or police) are trained to deal with victims of such crime. This might require special skills and training.
It might also be required to verify if the current legislation in Vanuatu contain provisions that criminalize cyber bullying. If the offence is not criminalized in the country the ability of law enforcement to act is limited. To be able to deal with such cases may not only be necessary with regard to possible victims in the country. The assessment shows that some students have themselves been involved in cyber bullying.

6.2 Contacted by Strangers

The assessment revealed that around 10 per cent of all students have already been contacted by strangers through ICT.



Being contacted by strangers does not mean that a crime was committed. Actually a lot of users are using ICT to get in contact with people that they did not know before. However, there are cases where offenders with an inappropriate sexual interest in children used ICT to get in contact with children. Only less than 10 per cent of the children were contacted by strangers (in total 28 children). This does not necessary mean that they have been victim of sexual solicitation (“grooming”) but that the Internet used to contact those children in a way that they felt inappropriate. To ensure that children do not become victim of sexual solicitation (“grooming”) information about this phenomenon, means to protect and ways to get help if it happens could become part of Cybersecurity training for children.

Bibliography

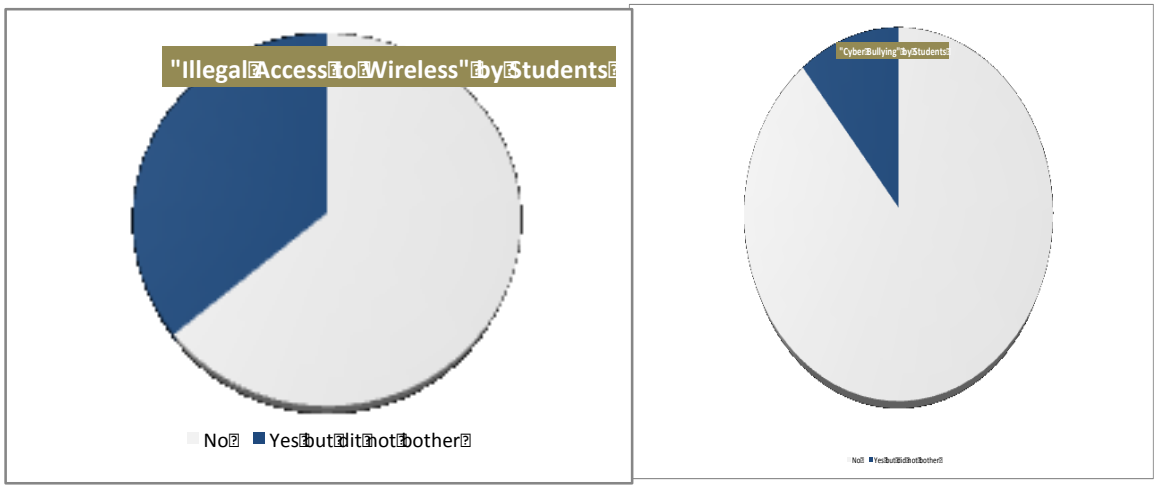
The number of children being contacted by strangers is lower than in other Pacific countries. One of the reasons could be that chat rooms, which are often used by offenders, are not that popular among students in Vanuatu.

Policy Implication:
Based on the assessment it is possible that children in Vanuatu have already been victim of grooming. Around 10 per cent of the students that participated in the assessment have already been contacted by strangers. In addition to including this subject matter in Cybersecurity training for students a more in-depth assessment could be carried to verify the background of those inappropriate contacts. Furthermore a review of the legislation could be taken into account to verify if solicitation of children is criminalized in Vanuatu.

Section I

7 Assessment 4: “Offences” committed by students

In addition to investigating in how far students in Vanuatu have already become victims of Cybercrime the assessment included questions to discover if students have been in activities that are criminalized in some countries. The two offences that were selected for the assessment were “illegal access to a computer system” and “cyber bullying”.



The assessment shows that some of the students have been involved in activities that are considered illegal in some countries of the world and are covered by international best practices with regard to the criminalization of Cybercrime. Around 35 per cent of the students have tried to break into a protected network and 10 per cent reported that they have left “mean” massages on other people’s online sites. In order to fully understand why the acts were committed further assessment is required. Based on the provided information it is not even possible to determine if these acts are criminalized by national law. One explanation for the acts of the students could be that some were not fully aware that their activity is inappropriate and maybe even criminalized. Within a Cybersecurity training more detailed information about illegal acts involving ICT) could be provided.

Policy Implication:
Compared to other parts of the world the Pacific is a rather peaceful place. It is most likely that most Cybercrimes will be committed by non-nationals from abroad. However, the assessment shows that if acts like attempted illegal access to a computer network and cyber bullying are criminalized some offenders might actually be locals. If there is an interest to exclude acts typically committed by minors that do not lead to any damage from criminal liability restrictions to criminalization could be included in the provisions. To ensure that such acts are not committed as a consequence of a lack of knowledge about the criminalization, information about the illegal acts in Vanuatu could be included in Cybersecurity training in schools.

Bibliography

Bibliography

Bidgoli, MIS2, 2011, page 78;

Camacho, Evaluating the Impact of the Internet in Civil Society Organizations of Central America, Fundacion Acceso, 2001;

Camodeca/Goossens/Gerwogt/Schuengel, Bullying and Victimization Among School-age Children, Social Development, No. 11, 2002, page 332 et seq.

Choo, Responding to online child sexual grooming: an industry perspective, Trends & Issues in crime and criminal justice, No. 379, July 2009, page 1

Donegan, Bullying and Cyberbullying: History, Statistics, Law Prevention and Analysis, Elon Jounal of Undergraduate Reseach in Communications, Vol.3, No. 1, 2012, page 33 et seq.

Elmer, Education for All in the Information Age: The Potential of Information Technology for Improving Educational Access and Quality in Developing Countries, 1999

Eneman/Gillespie/Stahl, Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case, AISeL, 2010
Hawkins, Ten Lessons for ICT and Education in the Developing World, in CID – The Global Information Technology Report 2001-2002, 2002, Chapter 4

Hinduja/Patchin, Bullying, Cyberbullying and Suicide, Arhcives of Suicide Research, 14(3), 206 et seq; Cyber-Bullying Overview, National White Collar Crime Center, Nov. 2010

Lewin, Harvard and M.I.T. Team Up to Offer Free Online Courses, The New York Times, 02.05.2012

O Cionnaith, Third suicide in weeks linked to cyberbullying, Irish Examiner, 29.10.2012

Ojedokun, Distance Education and the New Information and Communications Technologies: An Analysis of Problems Facing a Developing Country, 1999

Osin, Computers in Education in Developing Countries:Why and How, World Bank Education and Technology Technical Note Series, Vol. 3, No. 1, 1998

Powell, Paedophiles, Child Abuse and the Internet, 2007

Ropelato, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

Shariff/Hoff, Cyber bullying: Clarfying Legal Boundaries for School Supervision in Cyberspace, International Journal for Cyber Criminology, Vol. 1, Iss. 1, 2007, page 76.

Wolak/Finkelhor/Mitchell/Ybarra, Online Predators and their Victims: Myths, Rality and Implications for Prevention and Treatment, American Psychologist, 63; page 111 et seq.