Asymmetrical Trusted Technology Networks in Developing Economies: A Case Study on Critical Infrastructure in Bhutan.

Pratima Pradhan, Bal Subba, Thinley Jamtsho, Ganga Ram Ghimiray & David M Cook

DOI: https://doi.org/10.17102/bjrd.rub.10.2.008

Abstract

Developing Nations are subject to amplified challenges in terms of the integration of technology, and the exposure to non-domestic opportunism from larger neighboring economies. These challenges are recognizable as asymmetrical differences between what is seen as the normative list of critical infrastructures, and the specialisms that can dominate an emerging economy with early maturity technology networks. This paper discusses the case of Bhutan and demonstrates the need for strengthened approaches to trusted networks to ensure the reliability and continuity of the Nation's critical infrastructures. The paper also links the importance of trusted information sharing networks as part of an overarching technology strategy that protects the Gross National Happiness of the nation.

Keywords – *Critical Infrastructure Protection, Trusted Information Sharing, Gross National Happiness, Trusted technology networks.*

Introduction

Securing national critical information infrastructure is imperative in the protection of any breakdown that could impact on the daily operation of a nation (Farouk, 2017). Critical information Infrastructure (CII) threats are more complex than before (C and IA, 2019). Man-made cyber threats can bring critical online services and businesses to a halt. Bhutan is an emerging nation that is rapidly developing technology for a range of services and provisions that represent its critical

infrastructure (Choejey, 2015; DrukREN, 2019).

Bhutan has received less attention from the modern threats of Cyber security and Informationwarfare than its larger neighbour India (Sulewski, 2013). The population is small, and the terrains are geographically prohibitive to competing nations. However, the critical infrastructures coordinated by the Royal Government of Bhutan are increasingly susceptible tothreats targeted towards the governance, management, continuity, supply, and resilience of thenation. These threats emerge in the form of varied and cross-disciplinary cyber security challenges (Choejey, 2018; Deibert, Rohozinski, Manchanda, Villeneuve, & Walton, 2009).

The 2018 annual report by the Bhutan Computer Incident Response Team (BCIRT) revealed the presence of crypto-mining and *The Onion Router* relay activities over the Government Intranet in addition to 230 other vulnerabilities (BCIRT, 2018). Further assessments showed threats to CI agencies like Bhutan Telecom, T-Bank, OAG, Thimphu Thromde (City Corporation) (Schmueli, 2010). Additional vulnerabilities have been reported in areas such asVISA card fraud (Business Bhutan, 2019), Facebook scams and privacy breaches in WeChat (Cheki, 2017). Such incidents represent the collective evidence of an emerging nation in termsof technology, ICT, and networked infrastructures. At the same time, many government services are digitally enabled (Cabinet Secretariat, 2015), and payment gateways for taxation and utility services such as power and water are available nationwide.

Bhutan has developed its digital capacity in online asset declaration, audit clearance, security clearance an,d e-Procurement Systems (MOIC, 2014). Banking and Finance incincludeternet banking and mobile apps usage, whilst the Power corporations of Bhutan rely on SCADA systems. These emerging changes represent potential risk scenarios that indicate the need for ra enewed assessment of Bhutan's critical information Infrastructure. In Bhutan, ICT depends on electricity, electricity on hydropower, hydropower on water resources, and water on climate conditions. Considering the inter-dependencies of critical infrastructures, there is a need for theidentification and distribution of

Critical infrastructure safeguard tactics and planned approaches.

Background

Bhutan is a landlocked country, with a constitutional monarchy and a modest population (National Statistics Bureau, 2018). It is a laggard nation in terms of its ICT progress yet is well positioned on the ICT development index compared to its immediate neighbors (ITU, 2017). Mobile telecommunications operators serving more than 730,000 mobile telephone subscribers (MIOC, 2018). The Government has established the national backbone infrastructure (Gewog) and runs a national intranet that connects agencies and offices such as the High-speed Education and Research Network (DrukREN, 2019) and the Bhutan Internet Exchange Point for handling local internet traffic (BtIX, 2019).

The rapid development of different government e-Services signposts the ongoing need for a higher prioritization of oversight and scrutiny in terms of automation and digitization. A similar challenge faces the corporate sector. Recorded cyber-attacks include website defacements, SQL injections, botnets, and high impact DDOS attacks (BCIRT, 2018; Schmueli, 2010). These challenges are augmented by Bhutan's unique development philosophy involving Gross National Happiness which puts the Environment, Culture, Good governance and Sustainable development as the driving force for nation's progress (GNHC Centre Bhutan, 2019). The obstacles to citizen harmony alongside online processes, systems and technology are as persistent in Bhutan as in other countries (Pee & Kankanhalli, 2009). With a sharply escalated authority structure, the disclosure of official information to both public and private sectors is problematic for a small nation embracing the need for CI. Whilst some of the CI vulnerabilities are similar to the experiences of other nations, there remain a variety of starkly asymmetrical weaknesses that are specifically related to Bhutan and require a bespoke response that relies on both government input and non-government vendors, users, and stakeholders.

There is a need for a trusted sharing platform for circumstances where information is required to be shared between the organizations

quickly. The trusted network would not only provide direct and secure sharing of highly confidential information at critical points in time, but would also promote collaboration among private and public sectors while handling risk, enhancing services, and mutual growth of two or more organizations participating (DHS, 2018).

Literature Review

By comparison to other nations, Bhutan has diminutive military power yet boasts a hardened approach to dealing with natural disasters from glaciers, landslides, and earthquakes (Cooper, 2018). Despite this tough appearance of readiness, Bhutan is under increased pressure to reduce its cyber threat to its sovereignty, integrity, and national safety. Modern-day Bhutan is enormously dependent upon ICT to coordinate its CI against a growing number of aggregated challenges in the critical Information Infrastructure (CII). The over-arching protection described by the Bhutan's Information Communication and Media (ICM) Act is characterized by a likelihood of *"debilitating impact on national security, economy, public health, social welfare or safety*." (ICM Act, 2018).

The Bhutan ICM act states its capability to declare ICT and Media Infrastructure as critical through its use of centralized management of the systems and reinforces this through its legislation regarding illegal access and/or interception of CI (ICM Act, 2018), however, its internal policy and planning do not describe the important cross-agency sharing that would allow for better management and governance by means of the trusted sharing of information. Clearly, this is a challenge in terms of trust, governance, continuity, supply, and resilience. The CI of Bhutan states the need for sharing CI protection across networks but does not state a trusted network for that sharing except through a single centralized peak body (ICM Act, 2018). The ICM Act needs to allow for additional pathways for trusted information sharing that work in terms of "peer to peer" and "department to department" exchanges.

The nascent developing status of Bhutan's critical network security is reflected by the ITU e- Readiness study (ITU, 2012) and the 2016 cyber security readiness study which identified a lack of resilient ICT networks ISO standards (Roberts, 2016). Additional studies by

Choejey, (2018) and Yangden (2018) emphasized the need for increased CII for economic developmentand national security of assets. In other parts of the world small developing nations also identifywith similar challenges. In Ecuador, the mitigation of vulnerabilities and cyber threats has drawn suggestions of an Information Sharing Program to assist with the Financial sector (Catota, Morgan, & Sicker, 2018), whilst in Bangladesh (Satter and Hossain, 2016) the emphasis is focused on information coordination and communication systems. Both the studieshad similar recommendations while the approaches were different.

The common thread is the need to reinforce security resilience. Cook (2010) points to TrustedInformation Sharing Networks (TISNs) whilst Lu, (2018) suggests participation between public and private stakeholder groups as part of planned improvement measures in Chinese CI.Similarly, in Kuwait (Alsultanny, 2014), there is an identified need for joint approaches in reducing the threat of privacy breaches and unauthorized access. Other nation-state studies point to operator-driven interdependencies and the renewed emphasis on shared responsibilitiesin the analysis of cyber incidents (Canzani, Kaufmann & Lechner, 2017; Zareen, Akhlaq, Tariq, & Khalid, 2013). In Sri Lanka the SL Cert identifies the “knock-on” effect of vulnerability and interoperability where information is not shared between key stakeholders ofthe identified interdependencies (Sri Lanka Cert, 2018).

An Approach to Trust and Interdependencies

This paper describes a novel perspective on the critical information infrastructure of Bhutan that calls for an understanding of CI asymmetry. This uneven apportioning of CI fortification is important to understand. This outlook presents a simple conceptual framework for the protection of Bhutan CII. It proposes a multi-layer approach to protecting critical information infrastructure (Izuakor, 2016) by identifying the sectors based on Bhutan’s national security goals and the likelihood of cyber threats impacting the CIIs. Such a framework for CII protection draws from Australian CI protection strategies and implementations, particularly theTrusted Information Sharing Network

(TISN). A conceptual framework to protect the CII would involve the creation of a trusted information sharing network of Bhutan, the BTISN.

Figure 1: Critical Information Infrastructure (Mattioli & Levy-Bencheton, 2014)

Mattioli & Levy-Bencheton (2014), described two approaches to identify CII within European Union Member states; those that are dependent on critical service approaches and those that focus on non-critical services (Figure 1). A Bhutan framework would work on a critical serservice-based approach to identify the CIIs. Kekete (2011), points to a framework of criticality that concentrates on a Pareto analysis of threats to interdependencies that incorporates time criticalities and quality issues (e.g.: the quality of water, food, air etc). By drawing from the COEC (2005) list of critical sectors and the Australian Government Trusted networks of criticalsector groups (TISN, 2019), it is possible to qualify the critical sectors of Bhutan and identify the significant risk-based interdependencies in terms of governance and resilience (CIC, 2019). A Trusted Information Sharing Network (TISN) is a non-competitive arrangement among businesses and governments to share information in order to build resilience (ibid, 2019) Australiahas been actively using a trusted sharing network for CI since 2003 (TISN, 2010).

An analysis and categorization of CIs in Bhutan showed the relationships between different critical infrastructure segments (Figure 2). The comparison and analysis were carried out on the basis of dependencies, linkages, vulnerabilities and shared exchanges of information. Rather than a uniform distribution between competing infrastructure segments, some areas were clearly more pronounced than others. Differences were clearly identifiable in terms of cross-dependent linkages, vulnerabilities, and expected rates of

development.

Recognizing the asymmetries that occur in an emerging nation's critical infrastructure is important in order to understand where and how to deploy further increased attention. Bhutan's framework has an additional feature that differs from the Australian model because it must also incorporate strategies that align with Bhutan's Gross National Happiness approach to government and society. The challenge for an authentic Bhutanese model is that whilst the Bhutan GNH approach clearly identifies issues such as climate resilience and sustainability, it is not clearly aligned with CIIs (GNHC, 2017a). In particular water, which is known as white gold in Bhutan (Woodruff, 2018), is vital for the economic stability and financial revenue in areas of hydropower, irrigation, health, and food (Royal Govt, Bhutan, 2018). Bhutan's Power Corporation (BPC) (2018) identifies the use of SCADA and SAP in terms of vulnerability to cyber-attacks (SAP News, 2009). This is an area of asymmetry that is unique to Bhutan in terms of size and scale (Figure 2). It highlights the need for trusted information sharing and draws attention to the need for an increased focus on an asymmetrical approach to hardening (Lewis, 2019).

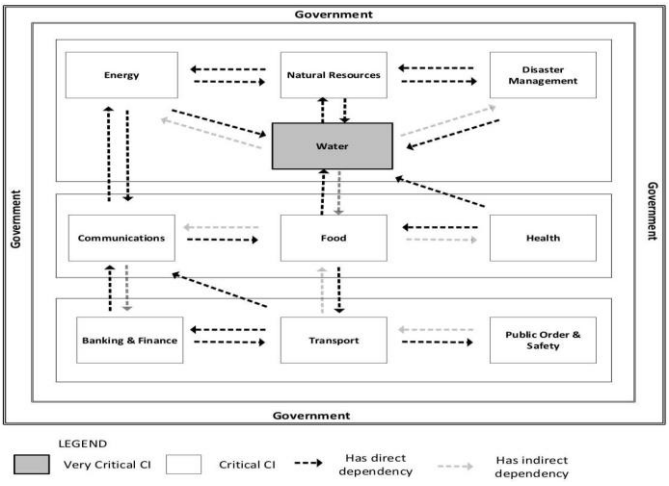

Figure 2: Bhutan's interdependencies of CI Infrastructure

CIIs can be dependent on other CIIs. In the case of energy, any disruption would eventually affect the North eastern regional quadrant of India where electricity supply is reliant upon Bhutan infrastructure. Similarly, the International Internet Gateway of Bhutan are drawn from India Internet providers. CII dependencies in Bhutan often incorporate dependencies in physical, logical, geographic, and cyber terms (Herrara and Maennel, 2019). Thus when individual areas of CI require hardening, the central decision processes must include some form of trusted information sharing that does not exclude commercial and individual groups that hold different and diverse perspectives based upon other characteristics outside of internal strategies (Lewis, 2019). Trusted Information Sharing can assist in the timely prevention and mitigation of known and unknown threats by incorporating a discrete protected set of exchanges that benefit Bhutan and its trusted stakeholders yet remains as private and confidential from the public domain (Dunn, 2007; Luiijf, Nieuwenhuijs, Klaver and van Eeten,2008).

This study found that the critical information infrastructures are either dependent on another CII or two or more CIIs are inter-dependent. In some scenarios one CII was indirectly dependent on the other CII. The study also identified that some of CII has inter-national dependencies. Energy disruptions affect North Eastern India whilst the International Internet Gateway of Bhutan relies on supply from India. Damage or disruption would affect the cyber security of the country drastically. Herrara & Maennel (2019), describe dependencies of CIIs as: physical, logical, geographic and cyber, which can be destroyed or disrupted by three types of failures: escalating, cascading and common cause. Bhutan coordinates interdependencies, direct dependencies and indirect dependencies in its critical sectors.

While applying the theory of dependencies, river water in Bhutan is the source for electricity production and directly depends upon favourable climatic conditions in terms of rainfall, snow, precipitations and climate change. The flora, fauna and the biodiversity of Bhutan is vital in contributing to the sustainable and free flowing supply of water. Disturbances on national watercycles can reduce the volume of water in rivers, and this has a flow-on effect on energy production in hydro-stations.

Similarly, the Bhutan fiber optic network is dependent on the Power transmission network. Thepower corporation uses the fiber optic network to create private network for Bhutan Power Corporation. The Geographical information of power transmission lines is important to managethe fiber optic network, and the security of fiber optic networks is important for uninterrupted power to the Network. These critical arrangements demonstrate the inter-dependencies of CIIs. Further instances of criticality can be conveyed through the Citizen Service portal, which has numerous public services online that are all hosted in the Government Data Centre (GDC). The security of this system is entirely dependent on the security and safety of the GDC. In return, GDC runs over the Government intranet, thus the criticality of secure and sound Government Intranet is profoundly vital. Since many sectors e-Services are integrated with banks for the payment. Any cyber-attacks in the banking sectors can have rippling effect on those services. The complicated relationships between CIIs are important to identify in order to recognize thegaps and develop resilience plans. Differences in terms of size, scale, and capability are important because they highlight areas that require additional response and target hardening toremain highly protected from outside attack. Small countries need to categorise their CIs in terms of asymmetrical differences because they will clearly show areas of greatest need.

The proposed Bhutanese *"Trusted Information Sharing Network"* is a group consisting of managerial or working level members from critical agencies of Bhutan such as Druk Holding and Investment (DHI), Gross Nation Happiness, and Ministry of Finance, Royal Monetary Authority, Financial CIRT(FiCRT), along with top Banks of Bhutan, Bhutan CIRT, e- Government Programme Management Offices among others. This group members from agencies who possesses high confidential information with regard to Critical Infrastructure andcyber-threats will bear the responsibility to share among other agencies who would benefit from the information.

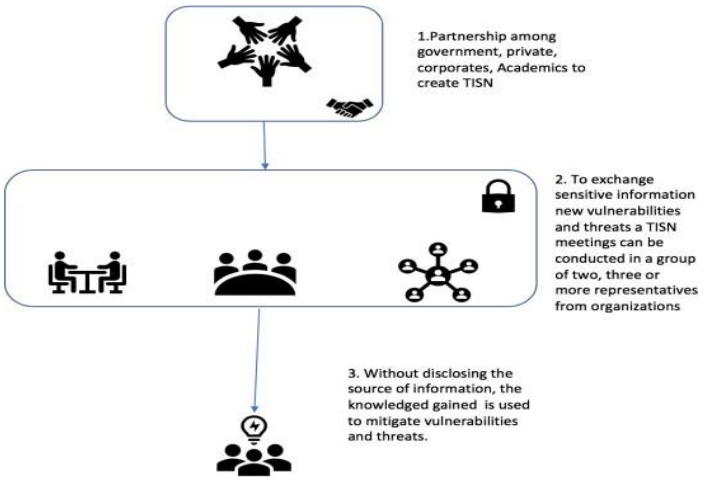

Figure 3: Typical proposed Trusted Information Sharing Mee

A trusted sharing network wou ld provide a secure environment to collaborate. Participating departments and groups would gain early warnings of cyber threats, the opportunity to learn from others' mistakes, and the chance to develop capacity in protecting their assets (National Cyber Security Centre, 2019). Such arrangements allow for rich exchanges of information under secure arrangements that protect the nation, its citizens, and its stakeholders (figure 3).

Conclusion

This study identifies two strategic areas for the future development and protection of critical infrastructure in Bhutan. The first is a re-evaluation of its critical sectors that takes into accounttheir differences, rather than their similarities. The second is that to continue on a path of development, Bhutan (and other nations of small size and unique geography) must develop new trusted networks that are inclusive of public and private enterprises.

The concept of trusted information sharing, whilst appropriate for most nation-states, isspecifically useful for Bhutan. The protection of critical information infrastructure is necessaryfor countries to prevent damage, destruction and disruption from multifaceted threats. The

cyberattacks of critical infrastructures in advanced nations like Estonia, Ukraine, USthe A, and even Sri Lanka demonstrate the value of CI protection of this kind. Bhutan, being a tiny nation,on the verge of graduating from LDC (Least Developed Countries) recognizes multiple vulnerabilities as it develops critical networks in energy, communications, and government.

For reliable technology progress, it is vital to identify the most critical infrastructures, study the underlying inter-dependencies and develop resilience critical infrastructures plan (Assaf, 2008). The creation of a Critical Infrastructure Protection Centre is an ideal approach towards coordinating the safety and security measures of Critical Information Infrastructure, however, Bhutan must also consider the value of public and private information sharing when organized through trusted sharing networks. The formation of trusted information sharing networks is likely to contribute significantly to the development of resilient and secure Critical InformationInfrastructures in Bhutan.

References

ADB, AusAID, JICA. (2013). *Country Diagnostic Studies: Bhutan Critical Development Constraint.*

Asian Development Bank, Australian Agency for International Development, and JapanInternational Cooperation Agency.

Alsultanny,Y. A. (2014). Assessment of E-Government Weak Points to Enhance Network Security. *International Journal of Information Science, 4*(1), 13-20.

Assaf, D. (2008, August 27). Models of critical information infrastructure protection. *International Journal of Critical Information Infrastructure Protection I, 2008*, 6-14.

Bank of Bhutan Limited. (2018). *Annual Report 2017.* Thimphu: Bank of Bhutan.

Bhutan Computer Incident Response Team. (2018). Annual Report. Department of Information Technology & Telecom.

Bhutan Infocomm and Media Authority. (2018). *Bhutan Information Communication and Media Act*. Retrieved March 2019, from http://www.bicma.gov.bt/bicmanew/?page_id=31

Bhutan Power Corporation. (2018). *Annual Report 2017.* Thimphu: Bhutan Power Corporation Limited(BPC).

Bhutan Telecom Limited. (2017). About Us - Company Profile. Retrieved March 2019, from https://www.bt.bt/about-us/

BtIX. (2019). *Bhutan Internet Exchange*. Retrieved March 2019, from https://www.btix.bt/category/news/

Business Bhutan. (2019, March 27). Accounts Of International VISA Cardholders Of BoB Hacked. Retrieved from https://www.businessbhutan.bt:https://www.businessbhutan.bt/2019/03/27/accounts-of-international-visa-cardholders-of-bob-hackel

Cabinet Secretariat. (2015). G2C eServices. Retrieved March 2019, from https://www.citizenservices.gov.bt/home

Canzani, E., Kaufmann, H., & Lechner, U. (2017, November 22). An Operator-Driven Approach for Modeling Interdependencies in Critical Infrastructures Based on Critical Services and Sectors. In G. Harvarneanu, R. Setola, H. Nassopoulos, & S. Wolthusen, *Critical Information Infrastructures Security. CRITIS 2016* (Vol. 10242, pp. 308-320). Springer.

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018, March 15). Cybersecurity incident response capabilities in the Ecuadorian financial sector. *Journal of CyberSecurity*, 1-20.

Chatham House. (2019). *Chatham House Rule*. (The Royal Institute of International Affairs) Retrieved May 2019, from https://www.chathamhouse.org/chatham-house-rule

Cheki, K. (2017, July 4). *Hacking of WeChat accounts worry users in Bhutan*. Retrieved May 2019, from http://annx.asianews.network/content/hacking-wechat-accounts-worry-users-bhutan- 49747

Choejey, P. (2015). Cybersecurity Practices for E-Government: An Assessment in Bhutan. *The 10th International Conference on e-Business (iNCEB2015).* https://pdfs.semanticscholar.org/7fa0/82bd6407f3502933f89c27d2b5212ab971d1.pdf.

Choejey, P. (2018). *Cybersecurity Challenges and Practices: A Case Study of Bhutan.* Perth: Murdoch University.

Commission of the European Communities . (2005). *Green Paper on a European Programme for Critical Infrastructure Protection.* Brussels.

Cook, D. M. (2010). Mitigating Cyber-Threats Through Public-Private Partnerships: Low Cost Governance with HighImpact Returns. *International Cyber Resilience Conference.* Edith Cowan University.

Cooper, F. (2018). *Building Bhutanese Resilience Against Catalysmic Events (BRACE).* UK Research and Innovation. Retrieved from https://gtr.ukri.org/projects?ref=NE%2FP016219%2F1.

Corcoran, M. (2018). A system approach to risk assessment: assessing all hazards throughout the infrastructure life cycle. *System thinking for critical infrastructure resilience and security - OECD/ JRC Workshop.* Paris: OECD.

Critical Infrastructure Centre. (2019, May). *Risk Assessment*. Retrieved fromhttps://cicentre.gov.au/document/P50S012

Cybersecurity and Infrastructure Agency. (2019, May 20). About CISA. Retrieved from https://www.dhs.gov/cisa/about-cisa

Deibert, R., Rohozinski, R., Manchanda, A., Villeneuve, N., & Walton, G. (2009). *Investigating a cyberespionage network.*

Department of Homeland Security. (2018). *National Infrastructure Protection Plan*. Retrieved May 2019, from https://www.dhs.gov/cisa/national-infrastructure-protection-plan

Devex. (2019). *Druk Holding and Investments Limited - DHI*. Retrieved from https://www.devex.com/organizations/druk-holding-and-investments-limited-dhi-74470

DrukREN. (2019). *About*. Retrieved March 2019, from https://drukren.bt/about/

Dunn, M.A. (2007) Securing the digital age: the challenges of complexity for critical infrastructure protection and international relations theory. In *International relations and security in the digital age*, Edited by: Eriksson, Johan and Giacomello, Giampiero. 85–105. London: Routledge

Farouk, A. (2017). Critical Infrastructure Protection in Developing Countries. In R. C. Das, *Handbookof Research on Economic,*

Financial, and Industrial Impacts on Infrastructure Development. India: IGI Global.

Fekete, A. (2011). Common Criteria for the Assessment of Critical Infrastructure. *Int.J.Disaster RiskSci, 2*(1), 15-24.

Ghafir, I., Saleem, J., Hammoudeh, M., Hanan, F., Prenosil, V., Jaf, S., . . . Baker, T. (2018, October).

Security threats to critical Infrastructure: the human factor. *The Journal of Supercomputing,74*(10), 4986-5002.

GNHC. (2017a). *Strategic Program for Climate Resilience Under the Pilot Program for Climate Resilience.* Thimphu: Gross National Happiness Commission, Royal Government of Bhutan.

GNHC. (2017b). SUSTAINABLE DEVELOPMENT GOALS, TARGETS AND INDICATORS. Retrieved from www.gnhc.gov.bt: https://www.gnhc.gov.bt/en/wp-content/uploads/2017/05/SDGS-AND- INDICATORS.pdf

GNHC Centre Bhutan. (2019). The 4 pillars of GNH. Retrieved from http://www.gnhcentrebhutan.org/what-is-gnh/the-4-pillars-of-gnh/

Herrara, L. C., & Maennel, O. (2019, February). A comprehensive instrument for identifying critical information infrastructure services. *International Journal of Critical Infrastructure Protection,25*(2019), 50-61.

Humphrey, W. (2001, December 1). *Capability Maturity Model*. (The Data Group) Retrieved May 2019, from http://www.data-group.com.au/1-38-capability-maturity-model-cmm/

ITU. (2012). *Readiness Assessment for Establishing a National CIRT (Afghanistan, Bangladesh, Bhutan, Maldives and Nepal).* International Telecommunication Union.

ITU. (2017). *ICT Development Index 2017*. Retrieved March 2019, from http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017rank-tab

Izuakor, C. O. (2016). *Critical Infrastructure Asset Identifiction: A Multi-Critieria Decision System andAvaition case study.* University of Colorado Colorado Springs, Department of Computer Science. Mountain Scholar.

Lewis, T.G., (2019) Critical Infrastructure Protection in Homeland Security: Defending a networkednation, John Wiley and Sons,

Luiijf, E., Nieuwenhuijs, A., Klaverm M., van Eeten, M., and Cruz, E. (2008) Empirical Findings on Critical Infrastructure Dependencies in Europe. *International Workshop on Critical InformationInfrastructures Security CRITIS* 2008. pp 302 – 310.

Lu, X. (2018, May 22). Scoping critical information infrastructure in china. . *The Diplomat*.

Mattioli, R., & Levy-Bencheton, C. (2014). *Methodologies for the Identification of Critical Information Infrastructure assets and services.* European Union Agency for Network and Information Security. ENISA.

Ministry of Information and Communications. (2014). Bhutan eGovernment Master Plan. Thimphu,Bhutan.

Ministry of Information and Communications. (2018). *Annual Info-Comm and Transport StatisticalBulletin 9th Edition.* Planning and Policy Division. Thimphu: Ministry of Information and Communications.

National Cyber Security Centre. (2019). *CiSP-Cyber Security Information Sharing Partnership*. Retrieved from https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

National Land Commission. (2016). CGISC. Retrieved May 2019, from https://www.nlcs.gov.bt/?page_id=969

National Statistics Bureau. (2018). *2017 Population and Housing Census of Bhutan.* Thimphu: National Statistics Bureau of Bhutan.

Pee, L., & Kankanhalli, A. (2009). A model of organisational knowledge management maturity based on people, process, and technology. *Journal of Information & Knowledge Management, 08*(2),79-99.

Robert, T. (2016, July 25). Building Cyber-security Capacity in the Kingdom of Bhutan. (Global Cyber Security Capacity Centre) Retrieved April 2019, from https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/bhutan- cybersecurity-capacity-review-2015

Royal Government of Bhutan. (2018). *Country Statement.* United Nations.

SAP News. (2009, November 16). *Bhutan Runs SAP*. Retrieved May 2019, fromhttps://news.sap.com/india/2009/11/bhutan-runs-sap/

Satter, A., & Hossain, B. M. (2016). Vulnerabilities Assessment of Emerging Web- based Services in Developing Countries. *I.J. Information Engineering and Electronic Business, 5*, 1-8.

Schmueli, B. (2010). *Are Viruses clogging Bhutan's Information Highway*. Retrieved March 2019, from http://www.thimphutech.com: http://www.thimphutech.com/2010/08/are-viruses-clogging-bhutans.html

Sri Lanka CERT. (2018). *Information and Cyber Security Strategy of Sri Lanka.*

StatCounter. (2019). *Social Media Stats Bhutan*. Retrieved March 2019, from http://gs.statcounter.com/social-media-stats/all/bhutan/#monthly-201802-201902-bar

Sulewski, L. (2013). *A Geographic Modelling Framework for assessing critical infrastructure vulnerability: Energy Infrastructure Case Study*, (Doctoral Dissertation), Retrieved from: https://scholarcommons.sc.edu/etd/1305.

The TISN. (2019, April 20). *TISN*. Retrieved from tisn.gov.au: https://www.tisn.gov.au/Pages/default.aspx

TISN. (2010, March). TISN for Critical Infrastructure Resilience. *CIRNEWS for owners and operators of Critical Infrastructure, 7*(1).

Whitman, M. E., & Mattord, H. J. (2016). The Need for Security. In *Principles of Information Security* (Vol. Fifth Edition). Cengage Learning.

Woodruff, B. (2018, April 19). *'White Gold': Discovering Bhutan's Natural energy treasure*. Retrieved from https://abcnews.go.com/International/white-gold-discovering-bhutans-natural-energy- treasure/story?id=54532668

World Life Expectancy. (2017). *Bhutan: LIFE EXPECTANCY*. Retrieved March 2019, from https://www.worldlifeexpectancy.com/country-health-profile/bhutan

Yangden, K. (2018, October 19). *Technological Changes in Bhutan: Addressing Resulting Cyber Vulnerabilities October 19, 2018*. Retrieved March 2019, from Aviation Security International: https://www.asi-mag.com/technological-changes-in-bhutan-addressing-resulting-cyber- vulnerabilities/

Zareen, M. S., Akhlaq, M., Tariq , M., & Khalid, U. (2013). Cyber Secruity Challenges and Wayforward for Developing Countries. *2nd National Conference on Information Assurance (NCIA)*, (pp. 7-14). Islamabad, Pakistan.

About the authors

Pratima Pradhan, **Bal Kumar Subba**, **Thinley Jamtsho,** and **Ganga Ram Ghimiray** were Australia Awards recipients who had undergone the master's degree in Cyber Security at Edith Cowan University for the academic year 2018 to 2019. This research work was part of their academicwork. All four of them are now serving the Royal Government of Bhutan in different organizations.

Dr. David M Cook is a Lecturer at Edith Cowan University, School of Science since 2008 and a member of the ECU Security Research Institute. He is the Vice President of Australian Computer Society (ACS) – Academic Boards and a member of the Australian Centre for Cyber Security Excellence (ACCSE). Dr. David with all his enthusiasm supervised and guided this research work. He holds special regard for Bhutan and Bhutanese students.