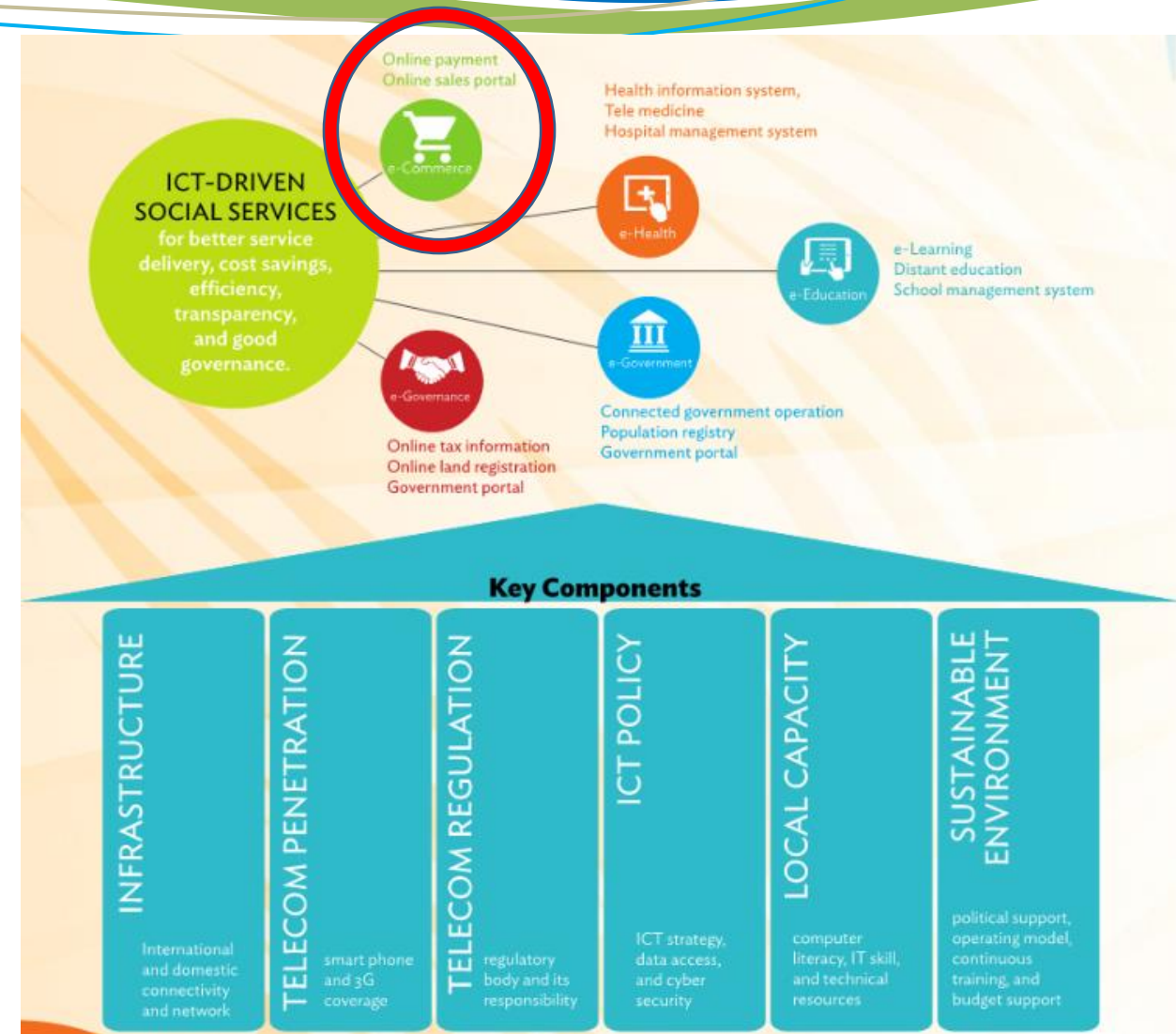


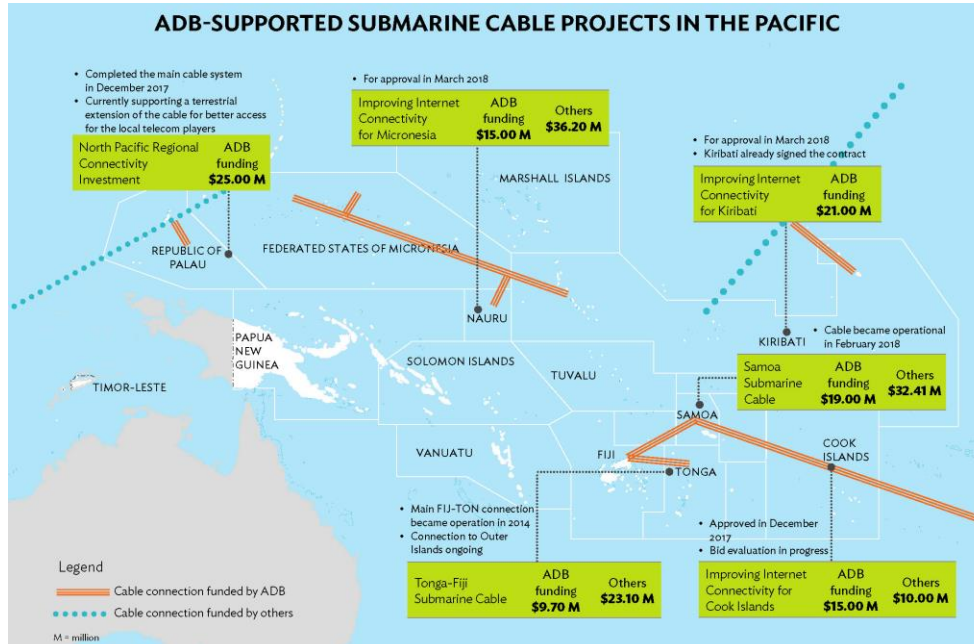
Introduction to E-Commerce Rule-Making

Key Areas of e-Commerce Regulation and the rules proposed therein:

Cybersecurity



Bridging the digital divide provides a pathway for digital vulnerability



- Affordability and access to information and communication technology
- E-payment availability and options
- Logistics and delivery infrastructure
- Digital skills/literacy training through smart devices and e-learning hubs
- Cooperation for better, effective, more efficient taxation policies and options
- Laws, rules, and regulations for data privacy and cybersecurity**



Cybersecurity by the Numbers (2021)

- Global Cybercrime Damages To Cost \$6 Trillion Annually
- Global Cybersecurity Spending \$1 Trillion Cumulatively From 2017-2021
- 3.5 Million Unfilled Cybersecurity Jobs Globally
- Ransomware Will Attack A Business Every 11 Seconds
- Ransomware Damage Costs Will Be \$20 Billion Annually

“The 5 Laws of Cybersecurity”



- ✓ Law 1: If there is a vulnerability, it will be exploited.
- ✓ Law 2: Everything is vulnerable in some way.
- ✓ Law 3: Humans can trust when they shouldn't.
- ✓ Law 4: With innovation comes opportunity for exploitation.
- ✓ Law 5: When in doubt, see Law 1.

“Cyber Crime Isn't About Computers: It's About Behavior”



Belief Emotion Behavior Habit

I'm not important and no one is looking for me.

I don't have anything anyone would want.

I can't stop them even if I wanted to.

**I'm important and thanks to automation,
they will find me.**

**I have Money. The bad guys will disrupt
my life until they get it.**

**I can drastically reduce the risk of
infection if I practice good cyber hygiene.**

Cybersecurity – Individual

- Individual
 - ✓ Education & Awareness
- Organizational
 - ✓ Policy
 - ✓ Operational
- National
 - ✓ Legal
 - ✓ Regulatory
 - ✓ National/Regional/International Security

Cyber Criminal Strategies & Digital Attacks

The image is a screenshot of the KnowBe4 website. At the top, the KnowBe4 logo is displayed with the tagline "Human error. Conquered." To the right of the logo are two navigation links: "PRODUCTS & SERVICES" and "FREE TOOLS". Below the navigation bar, the page is organized into three main columns of tools. The first column, "Phishing Tools", includes links for Phishing Security Test, Phishing Reply Test, Phish Alert Button, Second Chance, and Social Media Phishing Test. The second column, "Security Awareness Tools", includes Automated Security Awareness Program, Training Preview, Password Tools (Weak Password Test, Browser Password Inspector, Password Exposure Test, Breached Password Test, Multi-Factor Authentication Security Assessment), and Email Security Tools (Email Exposure Check Pro, Domain Spoof Test, Mailserver Assessment, Domain Doppelgänger). The third column, "Malware Tools", includes Ransomware Simulator Tool, USB Security Test, and Compliance Tools (Compliance Audit Readiness Assessment). On the right side of the page, there is a large promotional banner for the "Phishing Security Test". It features a graphic of a computer monitor displaying a "Phish-Prone Percentage" of 25% (labeled "Your Risk") and 1.6% (labeled "Industry Average"). Below the graphic, the text asks "What percentage of your users are Phish-prone™?" and includes a prominent orange button labeled "Phish Your Users". At the bottom of the page, there are two links: "All Free Tools" and "Featured Tool : MASA".

KnowBe4
Human error. Conquered.

PRODUCTS & SERVICES ▾ FREE TOOLS ▾

Phishing Tools

- Phishing Security Test
- Phishing Reply Test
- Phish Alert Button
- Second Chance
- Social Media Phishing Test

Security Awareness Tools

- Automated Security Awareness Program
- Training Preview
- Password Tools**
 - Weak Password Test
 - Browser Password Inspector
 - Password Exposure Test
 - Breached Password Test
 - Multi-Factor Authentication Security Assessment

Email Security Tools

- Email Exposure Check Pro
- Domain Spoof Test
- Mailserver Assessment
- Domain Doppelgänger

Malware Tools

- Ransomware Simulator Tool
- USB Security Test

Compliance Tools

- Compliance Audit Readiness Assessment

Phishing Security Test

Free Phishing Security Test Results

Phish-Prone Percentage

25% Your Risk

1.6% Industry Average

What percentage of your users are Phish-prone™?

Phish Your Users

[All Free Tools »](#) [Featured Tool : MASA »](#)

Cybercrime Strategies - Social Engineering

- **Social engineering**
 - ✓ is the art of manipulating, influencing, or deceiving you into taking some action that isn't in your own best interest or in the best interest of your organization.
 - ✓ The goal of social engineers is to obtain your trust, then exploit that relationship to coax you into either divulging sensitive information about yourself or your organization or giving them access to your network.

Cybercrime Strategies - Malware

- **Malware**

- ✓ stands for “malicious software,” an umbrella term for all the software out there that is being used by cybercriminals to spy on you and steal your information.
- ✓ Once your computer becomes infected, some malicious apps can log all of your keystrokes, including username and password.
- ✓ Some apps take over your computer and can even allow the hacker to turn on your webcam and spy on you or listen to your conversations.
- ✓ Malware attacks often result in data breaches, where a bad actor breaks into an organization’s network without their knowledge or consent. They steal data or information, which is then typically sold to other bad actors for a profit.

Cybercrime Strategies - Ransomware

- **Ransomware**

- ✓ Scrambles the data in computer files, making them unreadable. These "locked" files are then held hostage by the cybercriminals until a ransom is paid.
- ✓ This type of malware can paralyze your organization by spreading to all devices and files across your organization's network.
- ✓ Hackers increase the pressure on an organization in a variety of ways. A few examples include:
 - Threatening to increase the ransom amount if you do not pay quickly enough.
 - Threatening to sell the compromised data unless the ransom is paid.
- ✓ A ransomware attack can be devastating for an organization because of the loss of productivity, reputation, and large amounts of money needed to pay the ransom.

Common Digital Attacks - Phishing

- **Phishing** is the most common digital attack.
- Phishing is the process in which scammers try to trick you into giving out sensitive information or taking a potentially dangerous action, like clicking on a link or downloading an infected attachment. They do this using email disguised as contacts or organizations you trust so that you react without thinking first. For example, you receive an email that looks like it's coming from your IT department, telling you that there's a problem with your email account, and you need to reset your password.
- You are asked to click the link in the email.
- The link takes you to a password reset page with a password field, which is what the scammer is after. Once you enter your password, you've given entry into your account.
- The scammer now has access to your computer and can tunnel into your organization's network.
- The most effective way you can combat a phishing attempt is to be suspicious of all emails you receive containing links or attachments, especially messages that are unexpected.

Common Digital Attacks - Spear Phishing

- **Spear phishing** is a small, focused attack via email on a particular person or organization. The goal is to penetrate your organization's defenses.
- In this attack, the criminals invest time researching a specific target using social media and other open sources of information.
- Armed with this information, they send you a personalized message designed to trick you into taking an action that will put your organization at risk.
- Spear phishing attacks can be convincing but, just like in any phishing attack, you must take an action for it to be effective. One very common form of spear phishing targets top management—typically people who interact with your organization's CEO.
- A hacker impersonates your CEO and emails you with instructions to do something that could harm the organization.
- This tactic is called CEO fraud and is growing in popularity. It can even happen via phone with a fake voice message.

Common Digital Attacks - URL links

- You receive a link to a website in an email, but how can you be sure that it is secure?
- Review the link carefully.
- Hackers may disguise, misspell, or add extra characters to the link so that it looks like a trusted website.
- When in doubt, don't click on the link. Search for the website's actual domain using a search engine.
- If anything looks suspicious, check with IT/security team to confirm it is safe.
- <https://www.wto.org/> vs <https://www.wt0.org>
- <https://www.wto.org/> vs <https://www.wwto.org>
- Still a lot of unsecure Pacific government websites at “http” and not “https”!

Common Digital Attacks - Wireless Connections

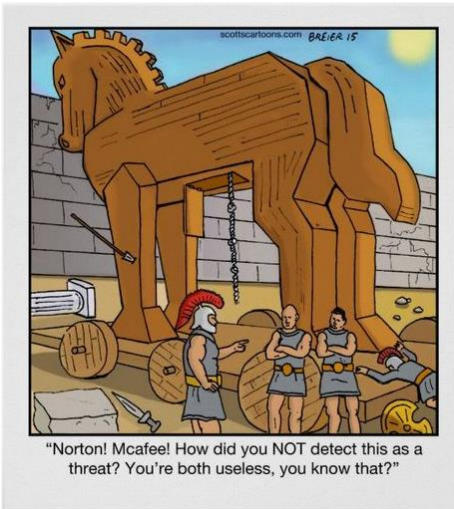
- Coffee shops, libraries, and even public parks seem to offer WiFi connections that can be conveniently used to access the organization's network and get work done.
- WiFi connections can be unsecure, and bad actors want to see what you are doing while online.
- Never connect to public WiFi unless you are using an organization approved VPN or Virtual Private Network. VPNs create a safe internet connection that shields your online activity from criminals.

Common Digital Attacks - Social Media sharing

- One of the biggest threats from social media is the abundance of shared information that can be used by social engineers to trick you or your coworker.
- Travel plans are an obvious example of information that you should never share online. Announcing that you won't be home is never a good idea.
- There are less obvious pieces of information that can put you and your organization at risk. Any type of sensitive information is like gold to hackers.
- Think about it from the perspective of a social engineer. Will the information you are about to post be useful in conning you or your coworker?
- Make sure you understand your organization's policy regarding sharing information on social media.

Common Digital Attacks - Fake Profiles

- Another effective trick that criminals use is to create a profile with a bunch of real or fake connections that all look very convincing.
- For instance, the profile could appear to be a headhunter who wants to talk to you about a career move, a potential romantic interest, or someone in your industry who wants you to speak at an upcoming conference.
- But fake profiles are a growing trend throughout social media—and are designed to trick you.
- So, take a close look at any requests that you receive.
- Some common aspects of a fake profile include model-quality or celebrity look-alike profile photos, an incomplete or generic profile, poor spelling and/or grammar, or a suspicious work history.
- Fake profiles will often lead you on for a while and then send you a link to click on in the message that seems to make sense in the context of the conversation.
- But this link leads to a site that is able to infect your device with malware.
- Now the hacker can begin to tunnel into your organization's network.



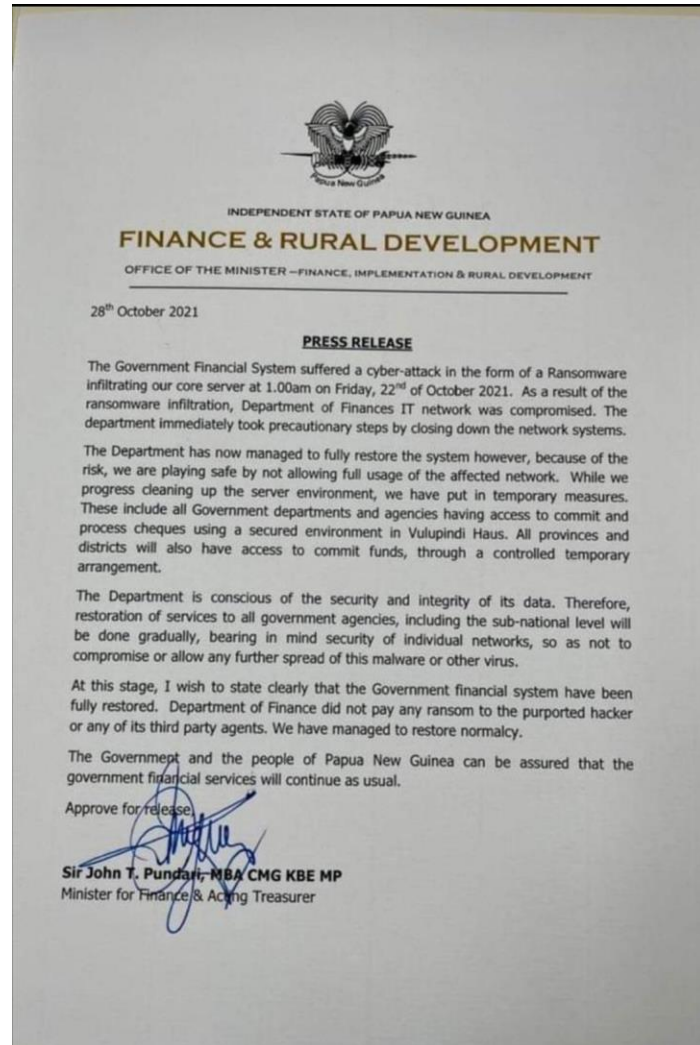
Common Digital Attacks - Trojans

- Trojan Horse
 - Powerful malware that hides itself on your computer and allows bad guys to run their software on your computer. For instance, Trojans send keylogger files back to the bad guys.
- Trojan Listener
 - A piece of malware that sits on the command-and-control server of a bad guy and waits for an infected computer to “call home” to it. It listens for the Trojan to call in.

Cybersecurity – Organizational Level

- Individual
 - ✓ Education & Awareness
- **Organizational**
 - ✓ **Policy**
 - ✓ **Operational**
- National
 - ✓ Legal
 - ✓ Regulatory
 - ✓ National/Regional/International Security

2021 PNG Ransomware Incident



- 22 Oct 2021: A cyberattack on Papua New Guinea's finance ministry briefly disrupted government payments and operations.
- Ransomware infiltrated and compromised a core server at the department of finance last week, hampering the government's access to foreign aid, its ability to pay cheques and carry out other basic functions in the midst of a spiralling Covid-19 surge.
- The platform controls budgeting and financing for the entire Papua New Guinea government.
- The department "did not pay any ransom to the purported hacker or any of its third party agents. We have managed to restore normalcy."
- "The department has now managed to fully restore the system, however, because of the risk, we are playing safe by not allowing full usage of the affected network".

2021 Papua New Guinea Ransomware Incident

- Jonathan Pryke, Director, Pacific Islands Program at The Lowy Institute
 - ✓ “The systems are so vulnerable already, and ...(partners) trying to come into this space and provide its own security and infrastructure. But the reality is I think the horse has bolted on this one,”
 - ✓ “The systems are so exposed anyway that you really have to start over from the bottom up and that would be a huge investment. But in the pantheon of ...(national) priorities, it’s nowhere near the top.”
- Ravin Prasad, CEO Cybernetic Global Intelligence
 - ✓ 85 % of organizations in PNG do not have formal cyber security policy/framework;
 - ✓ 90 % of organizations in PNG have not recently performed penetrations testing (cyber-attack simulation);
 - ✓ 86 % of organizations in PNG have not delivered cyber security training to all their staff;
 - ✓ 85 % of organizations in PNG do not have separate cyber security budget;
 - ✓ 92 % of organizations in PNG do not maintain a centralized register of cyber incident;
 - ✓ 90 % of organizations in PNG have not conducted a web application testing.

Source: [Papua New Guinea Hit by Ransomware Hackers With Millions in Aid Frozen - Bloomberg](#)



Source: [Cyber attack calls for tougher law – The National](#)

Government Response

- Minister for ICT Timothy Masiu called on the need to “escalate ICT to the strategic level in the Public Service” and underlined the need for “(...) appropriate mechanisms for enforcement of cyber security standards and a governance framework for ICT
- Held National ICT Summit [live on Facebook](#) in November 2021.
- In 2021, PNG became the first Pacific member of the Global Forum of Cyber Expertise ([GFCE](#)).
- Since then, assistance has been provided in preparing a Digital Government Bill which is currently with Cabinet for approval.
- Earlier in 2018, the Australian government had already agreed to fund the establishment of a Cyber Security Operations Centre in Port Moresby and a national Computer Emergency Response Team (CERT).
- Source: [Cybersecurity in the Pacific: Regional in Nature, Local in Practice | Pacific Online](#)

Some key questions for Executives, Board members & Government department heads

- WHEN was the last time you tested your IT infrastructure against cyber-attacks? Most critical being how secure is our organisation?
- HAVE we documented cyber security policies and procedures for our organisation?
- HAVE we performed risk assessment to detect internal and external threats?
- HOW frequently are we performing vulnerability assessment and penetration tests on our network to identify weaknesses/vulnerabilities in the network?
- DO we conduct web application assessment? Did you know compromised web applications lead to data breach?
- DO you have daily monitoring logs reports which confirms your organisation is not being attacked?
- DO we have a patch management policy within our business and how often is this managed and updated?
- DO you currently have mechanism to detect the vulnerabilities, are you fixing them on priority?
- WHAT preventive / detective controls have we implemented for data breaches?
- HAVE you implemented secure VPN for staff working remotely during the Covid-19?
- ARE we aware of all regulatory and non-regulatory cyber security compliances such as the international organisation for standardisation 27001?

Information Security – ISO/IEC 27001

- International standard on how to manage information security
- Details requirements for establishing, implementing, maintaining and continually improving an information security management system
- ISO/IEC 27001 requires that management:
 - ✓ Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
 - ✓ Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
 - ✓ Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.
- [ISO - ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements](#)

Organizational Cybersecurity

- Policies
 - ✓ Information Security
 - Considered as safeguarding three main objectives:
 - **Confidentiality**: Data and information assets must be confined to people who have authorized access and not disclosed to others
 - **Integrity**: Keeping the data intact, complete and accurate, and IT systems operational
 - **Availability**: An objective indicating that information or system is at disposal of authorized users when needed.
 - ✓ Acceptable Use of ICT
 - ✓ Social Media
 - Operational
 - ✓ ICT Operations
 - Cyber vigilance
 - Personnel
 - Hardware
 - Software
 - Network

Operational Cybersecurity – MITRE ATT&CK



- [MITRE ATT&CK](#) is a knowledge base of the methods that attackers use against enterprise systems, cloud apps, mobile devices, and industrial control systems.
- ATT&CK, which stands for Adversarial Tactics, Techniques, and Common Knowledge, can help you understand how cyber attackers think and work.
- ATT&CK is open and available to any person or organization for use at no charge.
- [What Is MITRE ATT&CK? - Cisco](#)

Cybersecurity – National Level

- Individual
 - ✓ Education & Awareness
- Organizational
 - ✓ Policy
 - ✓ Operational
- **National**
 - ✓ Legal
 - ✓ Regulatory
 - ✓ National/Regional/International

National CERTS & Regional Initiatives

- Computer Emergency Response Team (CERT)
 - ✓ [Tonga](#), [Vanuatu](#), [Papua New Guinea](#), [Samoa](#)
- Pacific Cyber Security Operational Network ([PaCSON](#))
 - ✓ Currently chaired by Tonga, operators and technicians from the Cook Islands, Fiji, Kiribati, Marshall Islands, Nauru, New Zealand, Niue, Palau, Papua New Guinea, Samoa, the Solomon Islands, Tokelau, Tonga, Tuvalu, and Vanuatu
 - ✓ Local Cyber Smart Pacific awareness campaigns ([Cyber UP Pacific](#))
 - ✓ Regional approach but country specific

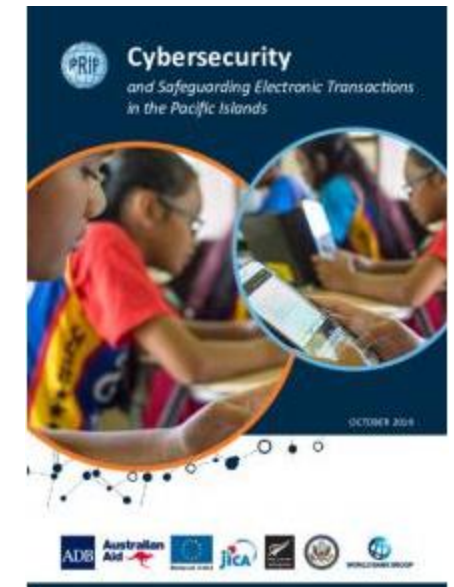


PaCSON
PACIFIC CYBER SECURITY OPERATIONAL NETWORK



National Cybersecurity – Legal & Regulatory Frameworks

Stage of development		None		Initial		Established		Sophisticated						
Country	CI	FJ	FSM	KI	RMI	NR	NU	PW	PNG	WS	SB	TO	TV	VU
Legal and regulatory frameworks														
Electronic transactions	I	E	N	N	N	N	N	N	N	E	N	N	N	E
Privacy, freedom of speech and other human rights online	I	I	I	I	E	I	N	I	I	I	I	N	I	I
Data protection	N	I	N	N	I	N	N	I	I	I	N	I	N	I
Digital authentication	I	N	N	N	I	N	N	N	I	I	N	I	N	N
ccTLD administration	E	E	E	E	I	E	E	E	I	E	I	I	E	I
Consumer protection	S	E	N	E	E	I	I	E	E	E	I	E	N	I
Intellectual property legislation	E	E	E	I	I	I	E	E	E	E	N	E	I	E
Access to information	E	E	N	I	I	I	N	E	N	I	N	I	I	E
Note: "Initial" means that the country is in the process of developing or implementing the concept measured and "Established" refers to a state where the relevant framework or concept is implemented and operates. Each of these ratings refers to the particular concept measured, and not the country's overall capacity to respond to cyber-risk.														



Source: [Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands | Pacific Regional Infrastructure Facility \(PRIF\) \(theprif.org\)](https://theprif.org/)

National Cybersecurity - Resilience

Stage of development			None			Initial			Established			Sophisticated		
Country	CI	FJ	FSM	KI	RMI	NR	NU	PW	PNG	WS	SB	TO	TV	VU
Resilience														
Cybercrime (substantive)	I	E	N	E	I	S	N	I	S	E	I	E	I	I
Cybercrime (child protection)	I	N	N	E	I	S	I	E	E	E	N	E	N	E
Cybercrime (procedural)	I	I	I	E	I	S	I	I	S	I	I	E	I	I
Law enforcement	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Prosecution	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Courts	I	I	I	I	I	I	I	I	I	I	I	I	I	I

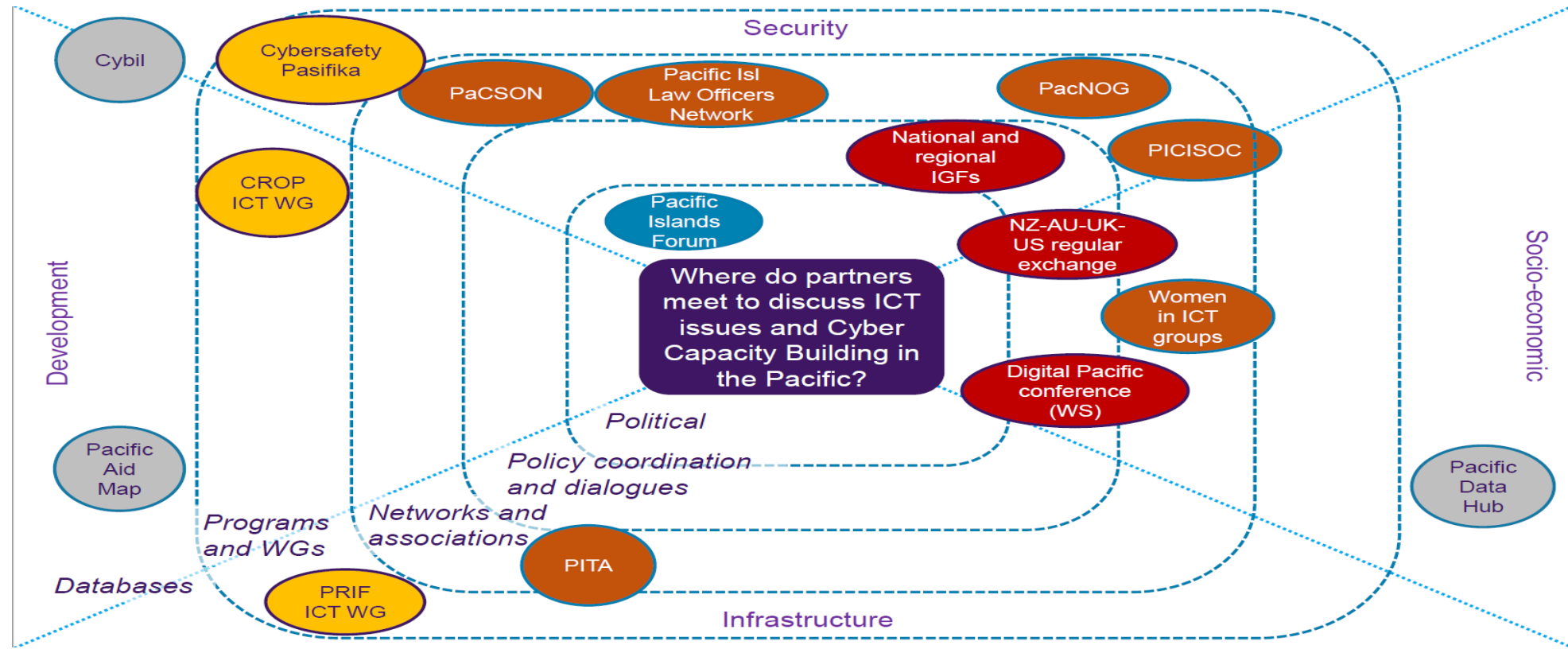
National Cybersecurity – Strategy & Governance, Security, Vigilance

Stage of development		None			Initial			Established			Sophisticated			
Country	CI	FJ	FSM	KI	RMI	NR	NU	PW	PNG	WS	SB	TO	TV	VU
Strategy and governance														
National cybersecurity strategy	I	E	I	I	N	I	N	N	E	E	N	I	I	E
Governance	I	E	I	E	I	E	I	N	E	E	N	E	E	E
Security														
Institutions	I	I	I	I	I	I	I	N	E	E	N	E	I	E
Critical infrastructure	I	N	N	N	N	N	N	N	N	I	N	E	N	I
Vigilance														
Incident reporting	I	I	I	N	N	I	I	I	I	N	I	I	I	I
Domestic cooperation	I	E	N	I	N	E	N	N	I	E	N	I	N	I
International cooperation	E	I	I	I	I	E	I	I	I	I	I	E	I	E

PRIF Report Recommendations (2019)

- Regional
 - ✓ implementing cybersecurity and digital strategy in the region; preparing a legal framework;
 - ✓ building capacity at a regulatory, enforcement and technical
 - ✓ Improving cybersecurity safeguards for critical infrastructure; and
 - ✓ Increasing public awareness
- Country
 - ✓ develop cyber security strategies;
 - ✓ electronic transaction and digital authentication maturity is low or non-existent;
 - ✓ legislative support for the digital economy

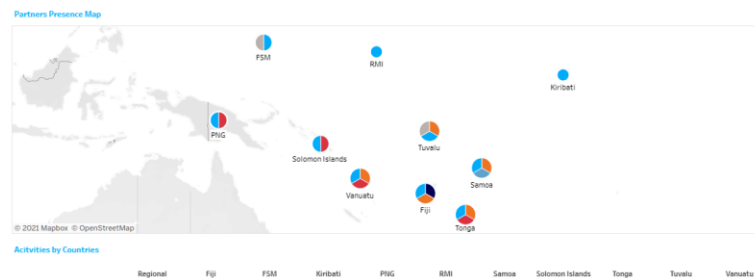
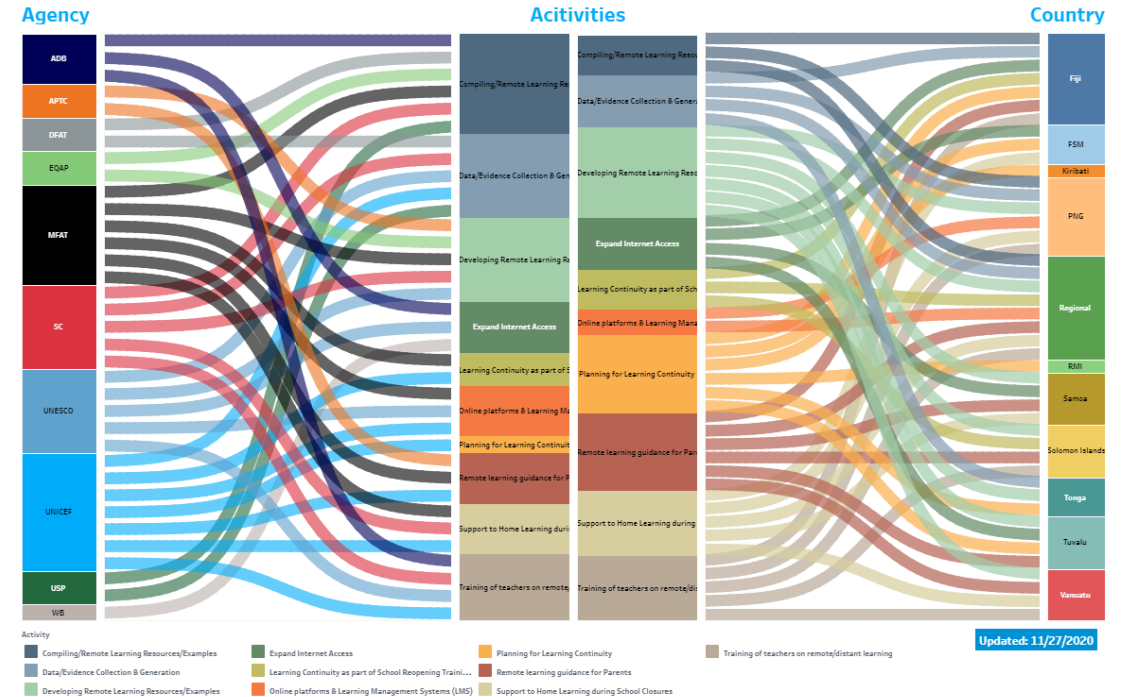
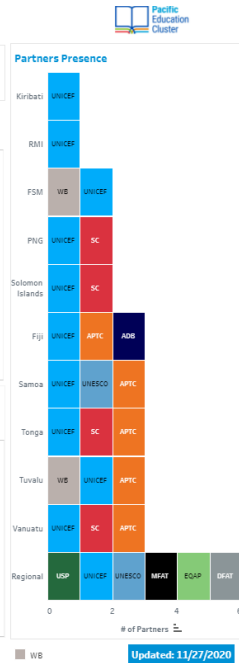
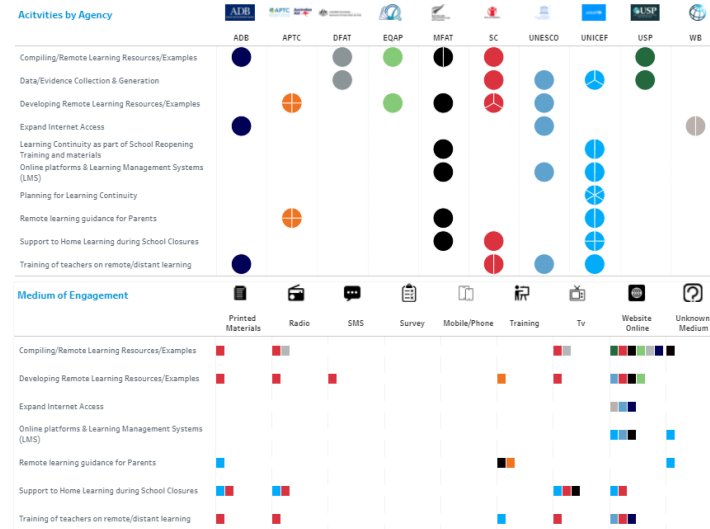
Many stakeholders, many forums, limited focus



PRIF Cybersecurity Pacific Partner Platform (Education example)

Pacific Education Cluster Learning Continuity Mapping

The Pacific Education Cluster has conducted a mapping of activities and resources implemented by Pacific Education Cluster Partners and donors to support learning continuity in the face of school closures resulting from COVID-19 in the Pacific. This mapping provides a summary of the main activities being implemented in the region as currently reported and will be updated as new information and data is collected. If you wish to contribute and report the activities of your organisation please be in touch with the Pacific Education Cluster team at global@unicef.org



E-commerce Landscape in the Pacific

7 x Policy Areas



Regionalism, Regional Trade Agenda, and Strategic E-commerce Framework

Virtual Validation Workshop for
Pacific Regional E-commerce Strategy and Roadmap
21-23 July 2021



Addressing the Gender Dimension of E-commerce

Towards a Holistic Analytical and Policy Framework



eCommerce Legislation

Box 9: United Nations Conventions and Model Laws on Electronic Commerce

- **UNCITRAL Model Law on Electronic Commerce (1996)** establishes rules for the formation and validity of contracts concluded electronically and for the attribution and retention of data messages.
- **UNCITRAL Model Law on Electronic Signatures (2001)** establishes basic rules for assessing possible responsibilities and liabilities for the signatory, the relying party, and trusted third parties intervening in the signature process.
- **United Nations Convention on the Use of Electronic Communications in International Contracts (2005)**, building upon and updates the provisions of the two aforementioned Model Laws, contributes to enabling paperless trade by, among others: 1) validating the legal status of electronic transactions by setting general functional equivalence requirements of “writing”, “original” and “signature”; 2) preventing medium and technology discrimination; 3) enabling cross-border recognition of electronic signatures; 4) permitting the use of electronic means in alternative dispute resolution mechanisms.
- **Model Law on Electronic Transferable Records (2017)** aims to enable the legal use of electronic transferable records via all technologies and models, such as registries, tokens, and distributed ledgers both domestically and across borders on the principles of non-discrimination against the use of electronic means, functional equivalence and technology neutrality.

Source: United Nations Conventions and Model Laws on Electronic Commerce²⁴

Source: <https://uncitral.un.org/en/texts/ecommerce>

eCommerce Legislation: 4 different cyber laws

UNCTAD considers four (4) different cyber laws needed for E-commerce to develop harmoniously:

- **E-transactions:** E-transaction laws that recognise the legal equivalence between paper-based and electronic forms of exchange is considered a prerequisite for conducting commercial transactions online. Such laws have been adopted by 158 countries (81 percent), of which 68 are developing or transition economies and 30 are Least Developing Countries.
- **Data Protection and Privacy:** Data protection and privacy laws regulate the collection, use, and sharing of personal information to third parties without notice or consent of such individual (Data Subjects). 132 out of 194 countries (66 percent) had put in place legislation to secure the protection of data and privacy.
- **Cybercrime:** This area of law aims to address all forms of illegal acts, violations, and infringements committed online or through the Internet. 154 countries (79 percent) have enacted cybercrime legislation, with the highest adoption rate in Europe (93 percent). Asia and the Pacific has an adoption rate of 77 percent.
- **Online Consumer Protection:** This area of law protects and safeguards the economic interests of online consumers and empower them with free and informed choice, while also bestowing rights should any problems arise. Out of 134 countries for which data are available, 110 have adopted legislation on consumer protection related to E-commerce. It was not possible to obtain data in 55 countries, suggesting that online consumer protection is not being fully addressed.

Besides the above four main regulatory areas, UNCTAD eCommerce and Law Reform Programme also acknowledges relevance of legislation on underlying issues underpinning E-commerce, including Intellectual Property, Competition, and Taxation. As E-commerce expands to cover almost every aspect of trade and business, these areas of law will have increasing importance for countries to regulate cross-border transactions.

Source: UNCTAD Cyberlaw Tracker

eCommerce Legislation

Table 36: Recommendations on Legal and Regulatory Framework

Recommendations	Timeline
1. Draft or update E-transactions, consumer protection, privacy and data protection, and cybercrime legislation (based on regulatory gap analysis, and following best international practices), to meet E-commerce requirements.	Short-Medium

Summary of Adoption of E-Commerce Legislation Worldwide | UNCTAD

The UNCTAD Global Cyberlaw Tracker is the first ever global mapping of cyberlaws. It tracks the state of e-commerce legislation in the field of e-transactions, consumer protection, data protection/privacy and cybercrime adoption in the 194 UNCTAD member states. It indicates whether or not a given country has adopted legislation, or has a draft law pending adoption. In some instances where information about a country's legislation adoption was not readily available, 'no data' is indicated.

If you would like to update or amend your country's data, please fill in the [questionnaire](#) and forward your response to ICT4D@unctad.org.



Asia-Pacific (60 countries)

Countries with legislation

Electronic Transactions:
50 (83%)

Consumer Protection:
27 (45%)

Privacy and Data Protection:
34 (57%)

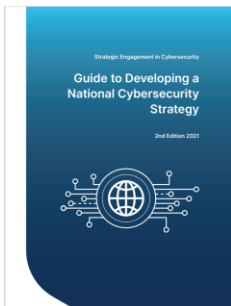
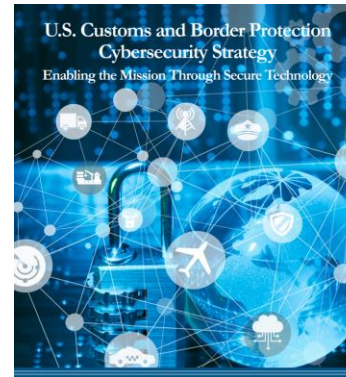
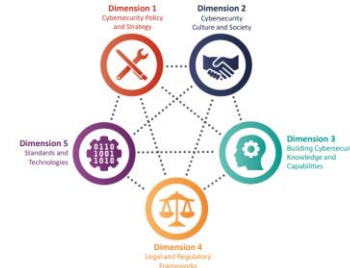
Cybercrime:
46 (77%)



The Dimensions of National Cybersecurity Capacity

The CMM considers cybersecurity to comprise five dimensions which together constitute the breadth of national capacity that a country requires to be effective in delivering cybersecurity:

1. Developing cybersecurity policy and strategy;
2. Encouraging responsible cybersecurity culture within society;
3. Building cybersecurity knowledge and capabilities;
4. Creating effective legal and regulatory frameworks; and
5. Controlling risks through standards and technologies.



Selected Resources

- ITU, Guide to Developing a National Cybersecurity Strategy ([2nd Edition 2021](#))
- GFCE, Global Overview of Existing Cyber Capacity Assessment Tools [2021](#)
- UNCTAD, The Opportunity for Digital and E-commerce Payments in the Pacific Region ([2021](#))
- Global Cybersecurity Capacity Centre - Cybersecurity Capacity Maturity Model for Nations [2021](#)
- UNIDIR [Cyber Policy Portal](#)
- WB [Combatting Cybercrime Tools & Capacity Building](#)
- U.S. Customs and Border Protection Cybersecurity Strategy ([2016](#))
- [Cybersecurity Framework | NIST](#)

Cyber Tools, Publications

- UNIDIR – [Cyber Policy Portal](#)
- UNIDIR – [International Cyber Operations research paper series](#)
- GFCE – [Cybil Portal](#)
- GFCE, AU, EU, OAS – [Global Cyber Expertise Magazine](#)
- Chatham House – [International Security Programme research and publications](#)
- Chatham House – [Journal of Cyber Policy](#)
- GCSCC Oxford University – [Cyber Security Capacity Maturity Model for Nations](#)
- Diplo, GIP – [Digital Watch observatory](#)
- CSIS – [Global Cyber Strategies Index](#)
- NUPI – [Centre for Digitalisation and Cyber Security Studies research and publications](#)
- EUISS, GMF, SMV – [EU Cyber Direct's Cyber Diplomacy in the EU research and publications](#)
- CSIS – [Inside Cyber Diplomacy podcast series](#)
- NATO CCDCOE – [Strategy and Governance database](#)
- NATO CCDCOE – [Cyber Defence Library](#)
- NATO CCDCOE – [INCYDER database](#)
- NATO CCDCOE – [Cyber Law Toolkit](#)
- NATO CCDCOE – [Tallinn Manual](#)
- EUISS, GMF, SMV – [EU Cyber Direct Knowledge Hub](#)
- Government of Australia – [Cyber Affairs and Foreign Policy webinar series](#)
- C3SA – [Cybersecurity Capacity Maturity Model for African nations \(CMM\)](#)
- ITU – [Global Cybersecurity Index](#)
- ITU – [National Cybersecurity Strategies Repository](#)
- ITU – [Guide to developing a national cybersecurity strategy](#)
- CYRILLA Collaboration – [CYRILLA Global Digital Rights Law database](#)
- CSIS – [Cybersecurity and Technology research and publications](#)
- OCSC – [Cybersecurity Capacity Maturity Model for Nations \(CMM\)](#)
- ICT4Peace – [Cybersecurity High-Level policy briefings](#)
- Leiden University – [Hague Program for Cyber Norms research and publications](#)

Training Programs, Courses & Workshops

- UNITAR – [International Humanitarian Law and Cyber Warfare](#)
- UNITAR – [Digital and Cyber Diplomacy](#)
- Governments of AU, UK, CA, NL, NZ with UNITAR – [Women & International Security in Cyberspace Fellowship](#)
- NATO CCDCOE – [International Law of Cyber Operations](#)
- NATO CCDCOE – [Executive Cyber Seminar](#)
- ENISA – [National Cyber Security Strategies \(NCSS\) workshop](#)
- Global Diplomatic Forum – [Digital Diplomacy](#)
- Clingendael – [Cyber diplomacy training](#)
- Estonian MFA – [Tallinn Winter School of Cyber Diplomacy](#)
- ICT4Peace – [Cybersecurity Policy & Diplomacy Workshops](#)
- Norwich University – [Cyber Diplomacy](#)
- ANU – [Cyber Bootcamp Project](#)
- ESDC – [Cyberdiplomacy Tool for Strategic Security Policy](#)
- UNIDIR – [Disarmament Orientation Course](#) [Module 6 YT video]
- UNODA – [Online Cyberdiplomacy Training Course](#)
- OSCE – [Cyber/ICT security Confidence-Building Measures Course](#)
- Diplo – [Cybersecurity](#)
- Diplo – [Cybersecurity Diplomacy](#)
- SELA – [Specialisation Course on Cyber Diplomacy](#)
- UNSW Canberra at ADFA – [Master of Cyber Security, Strategy and Diplomacy](#)
- Governments of Australia and Denmark – [Cyber and Tech Retreat](#)
- INCIBE and OAS – [Cybersecurity Summer Boot Camp](#)

Requests for Information

- Requests for information may be sent to ADB through (i) the [online request form](#), (ii) [e-mail contact forms of staff](#), (iii) staff e-mail addresses, and (iv) mail or fax. Requests may be directed to ADB headquarters, a resident mission, a representative office, or any ADB department or office.
- ADB acknowledges requests within 7 calendar days of receipt and responds within 30 calendar days of receipt. It either provides the requested information or the reason(s) why the request has been denied, indicating the exception(s) to disclosure in the [Access to Information Policy \(AIP\)](#). The requester has the right to appeal denied requests in accordance with the appeals process.
- ADB will inform the requester if it uses the prerogative under paragraph 6 (positive override) or paragraph 7 (negative override) of the AIP. It will also notify the requester of any extension, if needed.
- For complex requests—which include seeking information from multiple sources and/or large numbers of documents, collecting information over multiple years, collating and correlating raw data, and providing findings—ADB may ask the requester for an extension to the deadline for responding.
- ADB is not required to comply with or respond to generic requests or any request that would require ADB to create, develop, or collate information or data that do not already exist or are not available in its records management system.
- It is also not required to respond to requests for information on the same subject from the same person, organization, or group if ADB has already provided such information after a previous request or has given reasons why it cannot provide the information.

Source: [Requests for Information | Asian Development Bank \(adb.org\)](#)