Name: Glyrah Marie Mendina **Student Number: 23-058s**

Cyber Crime Law from All over the world

JAPAN	AUSTRALIA
SIMILARITIES (to Philippines)	
Both criminalize unauthorized computer access, cyberbullying, and data tampering. Both countries support public education on cybersecurity and promote awareness. Existence of a dedicated law: Japan’s Unauthorized Computer Access Law; Philippines’ RA 10175. Active participation in international collaboration against cybercrime.	Both countries criminalize unauthorized access, data interference, and computer-related fraud. Existence of a cybercrime law: Australia’s Cybercrime Act 2001 and the Philippines’ RA 10175 (Cybercrime Prevention Act of 2012). Both engage in international cooperation, working with entities like INTERPOL and ASEAN to combat cybercrime. Promotion of cybersecurity awareness through national programs.
DIFFERENCES (to Philippines)	
Japan’s enforcement is more technology-driven, using AI and analytics to monitor threats. The National Police Agency of Japan has a specialized cyber unit with advanced resources; Philippine agencies often have limited tools. Japan integrates cyber literacy in basic education, which is limited in the Philippines. Faster legal and procedural handling of cybercrime cases due to more streamlined systems.	Australia has a stronger and more updated cyber law framework, regularly amending laws based on new threats. The Australian Cyber Security Centre (ACSC) provides advanced threat detection and incident response capabilities; the Philippines’ systems are still evolving. Australia has a centralized national incident response center; the Philippines lacks a fully centralized system. Australia’s law enforcement has greater access to technology and training for cybercrime investigations.

JAPAN	AUSTRALIA
Best Practices Philippines can adapt	
Integrate cybersecurity lessons in school curriculums. Establish a centralized cybercrime intelligence center. Regular cyber drills and simulations for public institutions.	Real-time cyber threat response systems like those of the ACSC. Development of CERT (Computer Emergency Response Teams) for faster response. Strong public-private partnerships in cybersecurity management.
Best Practices they can adapt from us	
Grassroots-level digital awareness campaigns in multiple dialects. Programs like CyberSafePH, which are localized and community-oriented. Cost-effective approaches to outreach using social media influencers and youth organizations.	Barangay-level digital awareness campaigns. Use of community-led reporting systems for online scams and abuse. Leveraging youth digital volunteers in spreading cyber safety information.

REFERENCES:

- Republic Act No. 10175 – Cybercrime Prevention Act of 2012 (Philippines) https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/
- Cybercrime Act 2001 (Australia) https://www.legislation.gov.au/Details/C2004C01294
- Criminal Code Act 1995 – Part 10.7 (Australia) https://www.legislation.gov.au/Details/C2023C00330
- Australian Cyber Security Centre (ACSC) https://www.cyber.gov.au/
- Unauthorized Computer Access Law (Japan) https://www.japaneselawtranslation.go.jp/en/laws/view/2063
- National Police Agency (Japan) – Cybercrime Measures https://www.npa.go.jp/english/
- Department of Information and Communications Technology (DICT), Philippines – Cybersecurity https://dict.gov.ph/ictstatistics/cybersecurity/