EL PACCTO 2.0

EU-LAC Partnership on justice and security

TECHNICAL ASSISTANCE ON THE ASSESSMENT OF THE EXISTING CYBERCRIME LAWS / ACTS IN CARIBBEAN COUNTRIES

Miriam Bahamonde Blanco
Blanca Sánchez-Blanco Mancera

CONTENT

INTRODUCTION TO THE REPORT AND OBJECTIVES OF THE ACTIVITY

The need to assess the legal framework of all Caribbean countries regarding cybercrime is essential to understand the legal instruments available and the criminal offenses provided for in each state. With the rapid digital transformation and growing dependence on information technologies, Caribbean states face a constantly evolving cyber threat landscape. The lack of harmonized legislation and effective regional cooperation mechanisms hampers the prevention, prosecution, and punishment of these crimes, highlighting the importance of establishing key recommendations for a future model cybercrime law.

In this context, a model cybercrime law would establish a unified legal framework that facilitates regional cooperation, strengthens law enforcement capabilities, and guarantees the effective protection of citizens and businesses. Harmonizing regulations among Caribbean countries would facilitate the extradition of cybercriminals, the transnational investigation of crimes, and the adoption of coordinated preventive measures. Furthermore, the implementation of appropriate sanctions and response protocols would help deter criminal activity in the digital environment, promoting a safer and more resilient cyberspace in the region.

Terms of reference for the EL PACCTO 2.0 activity C4.4.1.03.25, from which the previous paragraphs have been extracted, determine the following specific activity objectives:

- Examine and compare current cybercrime laws/act in Caribbean countries to identify differences, similarities, and best practices.
- Evaluate the alignment of these laws with international standards of Budapest Convention and II protocol, in Cybercrime, and United Nations Convention against Cybercrime.
- Identify legal gaps in key areas such as the classification of cybercrimes, including CSAM-related offenses, grooming, and related offenses and non-consensual dissemination of intimate images.
- Develop key principles for a future model cybercrime law/act, ensuring its applicability in the regional context.

BASIC PARAMETERS

- Countries covered: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Grenada, Guyana, Haiti, Jamaica, St. Kitts & Nevis, St. Lucia; St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.
- Main areas of legislation covered:
    - National legal framework from the countries covered coincidental, relative, related or enabling to the content of the articles 2 to 10 of the Budapest Convention.
    - National legal framework from the countries covered coincidental, relative, related or enabling to the content of the articles 6 to 16 of the UN Convention against Cybercrime.
- Initial sources of information:
    - 2019 Regional report developed under the Capacity Building on Cybercrime for CARIFORUM States initiative, implemented by CARICOM IMPACS.
    - CoE – Octopus Cybercrime Community "Country Wiki" tool.
    - National government repositories – where they exist.

MAIN FINDINGS

Criminal offences defined in the Budapest Convention form the legal foundation for addressing both traditional forms of cybercrime and the growing number of hybrid threats that involve digital technologies. The new United Nations Convention on Cybercrime, meanwhile, is a new instrument that is not yet in force, but whose provisions are worth considering for the purposes of this report. Given that it criminalizes two new types of conduct not included in the Budapest Convention (child grooming and the non-consensual dissemination of intimate images).

Country	Member of the Budapest Convention	UN Cybercrime Convention Signatories
Antigua and Barbuda	NO (invited to accede)	NO
The Bahamas	NO	NO
Barbados	NO	NO
Belize	NO	NO
Dominica	NO	NO
Grenada	YES	NO
Guyana	NO	NO
Haiti	NO	NO
Jamaica	NO	YES
Saint Kitts and Nevis	NO	NO
Saint Lucia	NO	NO
Saint Vincent and the Grenadines	NO	NO
Suriname	NO	NO
Trinidad and Tobago	NO (invited to accede)	NO

The following summary chart aims to present in a simple manner the current status of implementation /alignment of Articles 2 to 10 of the Budapest Convention and Articles 7 to 16 of the UN Convention against Cybercrime in the substantive criminal law across CARICOM Member States, pointing out main discrepancies or implementation gaps. The aim is to provide a clear and up-to-date overview of the region's alignment with the Conventions' core criminal law provisions.

Offences	Illegal Access	Illegal interception	Interference with electronic data	Interference with an information and communication technology system	Non-consensual dissemination of intimate images
Art. Budapest	**2**	**3**	**4**	**5**	**-**
Art. Hanoi	**7**	**8**	**9**	**10**	**16**
Antigua & Barbuda	**YES***Electronic Crimes Act (2013)	**YES*:** covered.	**YES*:** covered.	**YES*:** covered	**YES***: covered
The Bahamas	**YES*:** covered. Computer Misuse Act 2003	**YES*:** covered.	**YES*:** covered.	**YES*:** covered.	**Not covered**
Barbados	**YES*:** Computer Misuse Act (2005).	**YES*:** covered**:**	**YES*:** covered	**YES*:** covered	**YES*:** CRIMINAL CODE AMENDMENT (NON-CONSENSUAL SHARING OF INTIMATE IMAGES) ACT 2021
Belize	**YES*:** Cybercrime Act 2020 .	**YES*:**covered	**PARTIALLY YES*:** only damages, not another interferences with electronic data)	**YES*:** covered	**YES *:** covered

Dominica	**NOT covered:** Not yet in-force cybercrime legislation (Electronic Crimes Bill 2013)	**NOT covered :** Not yet in-force cybercrime legislation (Electronic Crimes Bill 2013)	**NOT covered:** Not yet in-force cybercrime legislation (Electronic Crimes Bill 2013).	**Not covered:** Not yet in-force cybercrime legislation (Electronic Crimes Bill 2013)	**Not covered**
Grenada	**YES*:** Electronic Crimes Act (2013)	**YES*: Covered**	**YES*: Covered**.	**YES*: Covered**	**YES*: Covered**.
Guyana	**YES*:** Cybercrime Act 2018	**YES*: Covered**	**YES*: Covered**.	**YES*: Covered**.	**YES*: Covered**.
Haiti	**NOT cybercrime legislation**	**NOT cybercrime legislation**	**NOT cybercrime legislation**	**NOT cybercrime legislation**	**Not covered.**
Jamaica	**YES*:** Cybercrimes Act (2015).	**YES*: Covered**	**Partially Yes:**	**YES*: Covered**	**Not explicitly criminalized as standalone offence in the current legislation**
Saint Kitts & Nevis	**YES*:**. Electronic Crimes Act (2009; amended)	**YES*:** covered.	**YES*:** covered.	**YES*:** covered.	**Yes: Criminal Code Amendment 2021**
Saint Lucia	**YES*:** Computer misuse Act 2011	**YES*:** covered	**YES*:** covered	**YES*:** covered.	**Not covered**

Saint Vicent & The Grenadines	**YES*:** Misuse-of-devices criminalised in Cybercrime Act 2016.	**YES*:** covered.	**YES*:** covered.	**YES*:** covered.	**YES*:** covered.
Suriname*	**YES*:** Criminal Code 2015.	**YES*:** covered.	**YES*:** covered.	**YES*:** covered.	**Not covered**
Trinidad & Tobago	**PARTIAL:** Device misuse partly addressed in Computer Misuse Act (2000).	**YES*:** covered.	**YES*:** covered.	**YES*:** covered.	**Yes covered**

Offences	**Misuse of devices**	**Computer-related forgery**	**Computer-related fraud**	**Offences related to CSAM**	**Copyright infringement**	**Child grooming**
Art. Budapest	**6**	**7**	**8**	**9**	**10**	**-**
Art. Hanoi	**11**	**12**	**13**	**14**	**-**	**15**
Antigua & Barbuda	**PARTIAL:** Electronic Crimes	**YES*:** covered.	**YES*:** covered.	**YES*:** Online child sexual	**PARTIAL:** Copyright law	**YES*:** Child solicitation/luring

	Act 2013 criminalises misuse of encryption.			material criminalised.	(2003) does not explicitly address digital infringement.	online clearly criminalised.
The Bahamas	**PARTIAL:** Improper use of devices addressed indirectly in Computer Misuse Act (2003) by "Unauthorized use or interception of computer service".	**PARTIAL:** Forgery via computers is only implicitly included (CMA covers unauthorised modification / inauthentic data).	**PARTIAL–YES*:** Fraud offences can apply to electronic deception.	**YES/Indirectly:** provisions for child-pornography in Penal Code (publication or sale of blasphemous or obscene libel). CMA addresses illegal communications	**PARTIAL:** Copyright Act (infringement of rights of exclusive license) lacks explicit digital provisions.	**PARTIAL:** Grooming not separately defined though related exploitation offences exist.
Barbados	**YES*:** Computer Misuse Act (2005) contains illegal devices / interfering provisions.	**YES*:** CMA covers data alteration/deletion (forgery) in practice.	**PARTIAL:** CMA criminalises interference that can cause loss.	**YES*:** covered.	**PARTIAL:** Copyright law (1998) not adapted for online infringement.	**PARTIAL:** Grooming addressed in draft legislation but not fully in force.
Belize	**YES*:** Cybercrime Act 2020 includes unlawful device	**YES*:** Explicit computer-related forgery provisions.	**YES*:** Clear offence for electronic fraud.	**YES*:** Comprehensive online child	**PARTIAL–YES*:** Copyright law references digital works	**YES*:** Explicit offence of luring/soliciting a child through ICT.

	possession/production.			exploitation offences.	but lacks detailed cyber-infringement.	
Dominica	**NO:** Not yet in-force cybercrime legislation.	**NO:** No operative statute criminalising digital forgery.	**NO:** No explicit offence covering computer fraud.	**PARTIAL / NO:** Some sexual offences exist but no cyber component.	**NO:** Copyright offences exist but BC-style digital provisions absent.	**INDIRECTLY:** "Sexual grooming of a minor under sixteen years of age" covered but no by digital means.
Grenada	**YES*:** Electronic Crimes Act (2013) explicitly covers misuse-of-devices by Unauthorized access to code.	**YES*:** Digital forgery clearly defined.	**YES*:** Fraud committed by electronic means fully criminalised.	**YES*:** All major CSAM behaviours covered.	**PARTIAL:** Copyright Act (2011) partially aligns.	**YES*:** Child enticing/soliciting using technology criminalised.
Guyana	**YES*:** Cybercrime Act 2018 contains misuse-of-devices offences.	**YES*:** Computer-related forgery criminalised.	**YES*:** Fraud through digital means criminalised.	**YES*:** Comprehensive online child sexual exploitation offences.	**PARTIAL:** Infringement of copyright legislation not fully aligned with BC.	**YES*:** Act includes explicit child-luring offences using ICT.
Haiti	**NO / UNCLEAR:** No confirmed.	**NO / UNCLEAR:** No confirmed.	**NO / UNCLEAR:** No confirmed.	**PARTIAL / NO:** No confirmed.	**NO:** No confirmed.	**NO / UNCLEAR:** No confirmed.

Jamaica	**YES*:** Cybercrimes Act (2015) includes offences on misuse of devices.	**YES*:** Digital forgery criminalised.	**YES*:** Electronic fraud and deception criminalised.	**YES*:** Child Pornography (Prevention) Act (2009) fully criminalises CSAM.	**PARTIAL:** Copyright Act (1993) and amendment (2005) not updated for explicit digital criminalisation.	**PARTIAL:** Grooming addressed but no digital means mention.
Saint Kitts & Nevis	**YES*:**. Electronic Crimes Act (2009; amended) lists illegal devices / Unlawful disclosure of access code.	**YES*:** covered.	**YES*:** covered.	**YES*:** covered.	**PARTIAL:** Copyright enforced separately. Online infringement not specified.	**NOT FOUND**
Saint Lucia	**YES*:** Computer misuse / related statutes cover illegal devices and interference.	**PARTIAL:** Digital forgery not fully defined.	**YES*:** covered	**YES*:** covered.	**PARTIAL:** Copyright (Amendment) Act (2015) insufficiently digital-focused.	**NOT explicitly covered.**
Saint Vicent & The Grenadines	**YES*:** Misuse-of-devices criminalised in Cybercrime Act 2016.	**YES*:** covered.	**YES*:** covered.	**YES*:** covered.	**PARTIAL–YES*:** Copyright Act (2003) Some digital infringements	**NOT explicitly covered.**

					covered but lacks explicit cyber offence structure.	
Suriname*	**PARTIAL/YES*:** Criminal Code updates include some device misuse provisions.	**YES*:** covered.	**YES*:** covered.	**YES*:** covered.	**PARTIAL / UNCLEAR**	**PARTIAL** (amendment of the Penal Code in 2020)
Trinidad & Tobago	**PARTIAL:** Device misuse partly addressed in Computer Misuse Act (2000) and Cybercrime Bill.	**YES*:** covered.	**YES*:** covered.	**YES*:** covered.	**PARTIAL:** Copyright Act 1997 (Amended 5 of 2008) not modernised for digital offences.	**YES*:** Children's Act (2012) explicitly criminalises grooming/solicitation, including via ICT.

NOTE*: Although the offences are covered, definitions or penalties often diverge from Convention requirements, and the legal framework would require technical amendments to fully align with Budapest/Hanoi Conventions.

NOTE 2*: The sources on Suriname are in Dutch. The basic text has been translated using machine translation software to obtain a general idea of its content.

NOTE 3*: To provide a more comprehensive analysis, Annex 1 provides the full text of the legislation analyzed for each of the CARICOM countries.

CONCLUSIONS

1. Only Grenada is currently a party of the Budapest Convention against cybercrime (Grenada deposited its instrument of accession on 22 April 2024). In addition, Antigua and Barbuda and Trinidad and Tobago have been invited to accede (Antigua y Barbuda, by the Council of Europe decision of 24 September 2025 and Trinidad and Tobago is listed by the Council of Europe as a signatory/ "invited to accede" state from 2021 onward).

Among Caribbean countries, only Jamaica signed the Hanoi Convention on October 25, 2025 (its negotiators played a lead role in its development).

2. Most CARICOM states already have domestic cybercrime laws of varying vintage and alignment (for example, Antigua and Barbuda Electronic Crimes Act 2013; Jamaica Cybercrimes Act 2015; Guyana Cybercrime Act 2018; Belize Cybercrime Act 2020). As many states around the world, most CARICOM states have defined cybercrime offences (unauthorized access, data interference, fraud, child sexual offences, etc.) based on the substantive articles of the Convention, but statutes differ in scope, definitions, thresholds ("without right"), and requirements, leaving inconsistencies relative to Budapest standards. As more relevant, Dominica´s substantive law is missing or limited; Haiti presents a significant gap and needs a substantive cybercrime law; Trinidad and Tobago current law (Computer Misuse Act) is quite old (2000), prior to Budapest Convention. On the other hand, although refinement is still possible, Grenada is currently the most fully aligned state in the region with respect to substantive criminalization.

3. "Misuse of devices" is the most consistent regional gap. Many CARICOM laws criminalize unauthorized access and interference but do not adequately cover possession, distribution, or creation of malware, hacking tools, or access credentials and dual-use tools held "without right," as required. Some states criminalize possession of such tools only when used, rather than when held for the purpose of committing an offence.

4. Most CARICOM states criminalize online child sexual exploitation, but not always with all the Convention´s requirements. For instance, some CARICOM laws limit offences to "publication" rather than "making available."

Only approximately half of countries expressly provide for the criminalization of the non-consensual dissemination of private images; accordingly, consideration

should be given to encouraging its inclusion in the legal frameworks of all Member States, in line with the recently adopted United Nations Convention against Cybercrime.

5. Cyber-enabled copyright offences are inconsistently implemented. The main reason is that many CARICOM copyright laws were designed before digital distribution became widespread so some forms of online infringement may not be explicitly criminalized.

6. Some cybercrime bills in the region contain outdated terms or wording that may conflict with freedom of expression and privacy. For example, reference to “indecent” photos.

7. Grenada’s accession to Budapest Convention provides a model and a practical node for regional cooperation, but network effects (24/7 connectivity, mutual confidence in procedures) require several more accessions and domestic reforms to be effective region wide.

RECOMENDATIONS

1. Budapest Convention is primarily focused on criminalization of cyber-dependent crimes (e.g., illegal access, system interference, fraud, child sexual abuse material) and procedural tools to investigate them.

Grenada's accession to it, is a milestone as first CARICOM state to become a Party. Antigua and Barbuda and Trinidad and Tobago being invited is progress, but the rest of CARICOM remain non-parties.

The ratification of this treaty would be advisable for the countries of the Region, as Budapest investigative tools and international cooperation tools (24/7 contact points, harmonized MLA pathways, common standards for e-evidence) have been largely proven as extremely useful in combating cybercrime. Accession would reduce legal friction and unlock formal T-CY cooperation channels.

2. Hanoi Convention is more recent and still must reach a threshold number of ratifications to enter into force. As a UN instrument, it may carry a different kind of universality compared to the Council of Europe treaty (especially for states outside Europe). In Addition, beyond just criminalization, it places more emphasis on prevention, capacity building, and technical assistance, which could be interesting for CARICOM countries. Jamaica has already signed it and, given how involved it was in the negotiation, it is reasonable to assume that it has an interest in other states in the region doing the same. Regional alignment would facilitate cooperation.

3. As the region lacks a coherent, harmonized substantive framework, harmonization would be advisable as a first step for being part of Budapest/Hanoi conventions or, at least, to facilitate cooperation with current tools.

4. To achieve harmonization, it would be advisable to draft a model law for CARICOM countries. An ideal model law needs to be sufficiently flexible to be adapted (e.g., judicial level, terminology) to specific CARICOM legal systems (common law, civil law, hybrid) but grounded in international standards.

The law should focus on, among others, a clear criminalization of misuse of devices, update fraud/forgery provisions for digital context and harmonized/modernized child protection, non-consensual dissemination of private images and copyright offences.

In addition, careful drafting and human-rights safeguards are necessary if countries seek to align with Budapest standards. The UN convention defers a lot of the design of safeguards to domestic law, so also as part of ratifying the UN treaty, the model law should include strong domestic legal protections (e.g., judicial review, data protection) so that the agreement doesn't become a tool for abuse.

It would be advisable to work with regional stakeholders (judges, prosecutors, LEA, ministries…) during the drafting process.

ANNEXES

1. Comparative analysis of the full text of the different CARICOM Countries' legislation on Cybercrime to the Budapest and UN Conventions.

EL PACCTO 2.0

EU-LAC Partnership on justice and security