GLACY+

Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Bucharest, 15 October 2019

Report on the

Regional Conference on Cybercrime Strategies and Policies and features of the Budapest Convention for the Caribbean Community

12 – 14 June 2019, Santo Domingo, Dominican Republic

Jointly organised by the GLACY+ joint project of the Council of Europe and the European Union, the Ministry of Presidency of the Dominican Republic and CARICOM IMPACS

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Contents

Contact
Cybercrime Programme Office of the Council of Europe (C-PROC)
Tel +33-3-9021-4506
Email alexander.seger@coe.int

Contact
Cybercrime Programme Office of the Council of Europe (C-PROC)
Tel +33-3-9021-4506
Email alexander.seger@coe.int

1 The Conference on Cybercrime Strategies for countries in the Caribbean region

1.1 Background

The conference took place in Santo Domingo on June 12th to 14th 2019. Invitations were extended to all CARICOM member states, neighbouring countries and overseas territories (OT's) bordering the Caribbean region and the conference was part of CARICOM's effort to create a regional response to combating cybercrime.

The aim of the conference was to discuss what elements could be included in a cybercrime strategy and what the participating countries and territories saw as the most important elements to be included in an overall strategy at either the national or the regional level to establish an effective response to the growing threats of cybercrime.

Both, a cybercrime strategy and a cybersecurity strategy have for purpose to fight attacks against computer systems but they do differ: whereas a cybersecurity strategy will look at what can be done from a preventive perspective, often through technical means; a cybercrime strategy will look at how to address transgressions in cybersecurity from a legal perspective including the need to enact legislation to criminalize acts that compromise cybersecurity and to ensure that adequate capabilities are in place to enforce such cybercrime legislation.

1.2 The relationship between cybersecurity and cybercrime

Cyber*security* strategy can be compared to fighting burglary by installing locks on a front door and surveillance cameras, whereas a cyber*crime* strategy can be compared to ensuring that law enforcement has the capacity to catch the thieves if they commit a crime. It would be impossible for law enforcement to deal with theft if there was not adequate technical security such as strong front doors to protect valuables. However, security features alone will not prevent crime either, there's a need to be a legal sanction and not just technical protection to act as a deterrent to commit crimes.

1.2.1 Cybersecurity strategies to prevent cybercrime

A cybersecurity strategy aims to protect computer systems such as PCs, smartphones, and computer networks as well as the data they contain so that users can use them as intended and rely on their accuracy. Typical technical solutions to ensure the cyber security of computer systems and digital assets are passwords, firewalls, antivirus software, and encryption technology. Cybersecurity also encompasses organizational measures such as administrative structures and protocols that allow for expedited detection of problems to protect against further attacks and attacks against the information technology assets.

Cybersecurity is important in large computer systems in which many people rely such as those of an email provider or those which are part of a government system. Cybersecurity is even more important in those special computer systems that are considered part of critical information infrastructure. In addition to technical solutions and protections, cybersecurity also includes organizational means, establish incidence response capabilities, having a risk-based approach to priorities, develop contingency plans, foster research and development, establish baseline security measures, and address cybercrime. Cybersecurity legislation typically includes requirements for owners of computer systems to ensure adequate technical protection of those and can include

requirements to notify authorities' in case of a security incident and that employees have adequate training, keeping software up to date with the latest bug fixes, and using strong passwords and encryption technology to safeguard data. And while these security measures are important for large computer systems used by many users, they are also important for computer systems of any citizen as cybercriminals are also interested in attacking smaller computer systems, personal computer systems, because they can be equally profitable and create the same amount of damage if they can attack sufficiently large number of those.

1.2.2 Cybercrime strategies to ensure effective enforcement of cybercrime legislation

Even the best technical solutions have proven themselves over time to be insufficient to prevent attacks against computer systems. Cybersecurity is a moving target as cybercriminals are constantly developing new ways of attacking computers. Cybersecurity legislation, such as the European Union Network Information System (NIS) Directive, can improve cybersecurity by, in certain instances, making computer owners liable for providing an adequate level of cybersecurity on their information technology system. However, any cybersecurity expert can explain that even a cybersecurity protection that is *state of the art* on a computer system will not eradicate the risk of cybercrime.

As the first cybercrime laws were enacted in the 1980, we saw the commonality that they all addressed what is called the CIA offenses, attacks against the *confidentiality*, *integrity*, *accessibility* of computer systems. At the very minimum cybercrime law should criminalize attacks against these three properties of information technologies. Typically, cybercrime legislation can also address other types of crimes including crimes facilitated by computer systems such as online fraud, distribution of child pornography, and violations of intellectual property rights.

Cybercrime legislation benefits from including procedural measures for several reasons. The collection of electronic evidence is different from securing the more traditional types of evidence as electronic evidence is more volatile and could be deleted at the touch of a button – possibly without leaving a trace. Finally, as a 3rd element, cybercrime legislation also addresses the need for international cooperation as cybercrime almost per definition is a cross border crime where even in situations that both the victim and perpetrator are located in the same country is often the case that the evidence is located in a foreign country and measures need to be in place to be able to obtain the evidence from a foreign jurisdiction.

1.3 The historical context of the regional effort

1.3.1 HIPCAR project

CARICOM has for many years been engaged in assisting its member states in the fight against cybercrime including by looking at creating a policy framework in the area of ICT.

This conference can be seen as a focus area of one of the important parts of the project CARICOM carried out in the years 2010 to 2012 called HIPCAR (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean). This project is part of the region’s efforts to develop the CARICOM Single Market & Economy (CSME).

The results of HIPCAR was the development off 6 model legislative texts including on cybercrime and interception of electronic communications. The others were:

- Access to Public Information (Freedom of Information)
- Privacy and Data Protection

- Electronic Commerce (Transactions),
- Electronic Commerce (Electronic Signatures and validity of transactions / Evidence)
- Cybercrime
- Interception of Electronic Communications.

1.3.2 Relationship to the Budapest Convention

The HIPCAR model legislation on cybercrime includes many of the provision of the Budapest Convention but in some areas this regional model law goes further than the international convention. An example of provisions in the HIPCAR model law which is not part of the Budapest Convention is the criminalization of sending out unsolicited email (spam). Legislation on spam varies around the globe and there is no harmonized approach (between opt-out and the stricter opt-in approaches for example, or variations in how an opt-in must be made to be valid) and therefore is not part of the global cybercrime convention as at this stage it would not be possible to set an international, globally accepted, standard.

However, there is nothing in the Budapest Convention that prevents countries or regions to legislate in areas beyond the substantive provisions after the said Convention, including in areas such as unsolicited electronic communications, identity theft, or cyberstalking. Indeed, several countries have criminalized the sending of spam emails and legislation has also been enacted at regional level such as in the European Union (Directive 2002/58 article 13), and a few countries have enacted legislation on identify theft (such as France, article 226-4-1 of the penal code).

The European Union has also realized that in the area of cybercrime, legislators need to consider the global dimension of cybercrime and as part of its legislation in the Directive on Cybercrime 2013/40 specifically makes reference to the Budapest Convention in the directive's premises 15. No country, no region can fight cybercrime by itself. The Internet spans to entire globe and for a victim of cybercrime it is more likely that the perpetrator is located outside of the victim's home country and hence the need for harmonized legislation on cybercrime that allows for a global action and cooperation on common cybercrime attacks.

2 The main issues that need to be addressed in a cybercrime strategy for the Caribbean region

During the conference, presentations were made as well as participant's discussions to identify elements needed in a cybercrime strategy adapted to the region. The sections below describes which areas had been discussed during the conference. The next section, section 3, will address the replies received from the delegates in more detail.

2.1 Legal framework on cybercrime and electronic evidence

It goes without saying, that legislation is a main pillar of a cybercrime strategy. More specifically cybercrime legislation that is sufficiently broad to cover both contemporary but also future, yet to be known types of cybercrimes and to do so in a technology agnostic manner so it continues to apply even as technologies change.

Currently not all the CARICOM member countries and territories have enacted legislation on the basis of the HIPCAR model law. One of the discussion points during the conference was to consider if it is sufficiently possible to have regional legislation on cybercrime, but that such legislation should be harmonized with the global community for efficient cooperation to be able to address today's risks. Cybercrime legislation in the CARICOM regional area should therefore at least cover the criminal offenses of the Budapest Convention. This will ensure that there is dual criminality for the most common types of cybercrime and will facilitate the international cooperation to address those crimes for which evidence will need to be sought abroad. But, should there be regional interest, the CARICOM countries and territories could also consider criminalizing specific crimes not included in the international convention and which could possibly address some specific cybercrimes that are a particular problem in the region. For this reason, the conference also focused on identifying what are the main cybercrime challenges in the region.

Legislation can also consider criminalizing specific types of cybercrime that have caused problems at a national or regional level to demonstrate legislator's willingness to address it. The purpose of an international legal instrument is not to have identical legislation across the globe, but to have harmonized legislation for cross-border, international, crimes that needed an international response. Indeed, the international legal instrument aims to criminalize behaviour that all countries across the globe can agree on, but it is not uncommon for countries to, in addition, criminalize specific types of facts for which however there is not an international consensus on the need for its criminalization.

An example of a common type of undesirable online behaviour which has not been addressed in the Budapest Convention is identity theft such as the creation of fake social media profiles. In 2011, France acted an identity theft law which criminalizes the creation of fake online profiles; no other European countries or any other countries have enacted similar legislation to the French fake online profiles' prohibition until today. Instead, other countries rely on more general laws such defamation and fraud to address the more egregious cases of identity theft. The Budapest Convention criminalizes computer related fraud and computer related forgery which could be used against a creator of a fake social media profile but only if someone acts on it for legal purposes (forgery) or if the criminal obtains an economic gain (fraud). Many countries consider that criminalizing the mere creation of a fake profile on the internet could result in an encroachment on free speech rights such as satire and pastiche. The French legislation has been limited to criminalizing identity theft when it is for the purpose of obstructing the tranquillity of a user, so limiting identity theft for harassment purposes. Nonetheless, the French legislation is still seen with scepticism in some countries as they believe that the French law could for example criminalize

the creation of a satirical social media profile of a politician or a well-known personality such as popular Twitter account of Fake Steve Jobs.

In the end, it should be considered if any legislation that is not an international standard is sufficiently important to alleviate the concerns of the citizens to counterbalance the risk that such specific legislation could cause. Other jurisdictions could be more hesitant to cooperate on cybercrime when dual incrimination is required because the requested country view the specific national law of the requesting country to go beyond what is criminal behaviour in the requested country.

A second point to consider with regard to cybercrime legislation is that it must be of a sufficient abstract level so that it will endure over time and for being relevant even as the modus operandi of cybercriminals evolve. The basic cybercrime legislation which criminalizes attacks against the confidentiality, the integrity, and the accessibility of computer systems of the international legal instrument has stood the test of time and is applicable even to completely new types of cybercrime such as ransomware and business email compromise.

2.2 Capacity building for criminal justice authorities

With the enactment of cybercrime legislation there will be a need to provide information and training on the new laws to judges, prosecutors, and even attorneys. Not only because it is new legislation that may not be well known, but also because cybercrime is of a more technical nature such as financial crimes and the legal cases will rely on a different set of facts and circumstances then what most criminal justice authorities have been used to. Therefore, ensuring the expertise amongst the judiciary and legal community was a recurring suggestion when discussing the elements of a cybercrime strategy during the conference.

The capacity building should include elements such as having a standardized course to ensure a uniform training that does not depend on the interests and skills of the trainer. It should also include elements of basic training on information technology as not all judges and prosecutors have had a natural interest in learning about new information technology products, data storage devices, and communication technologies.

While there are many different types of cybercrime, the capacity building should focus on the most common or most problematic types of cybercrime in the country.

Finally, it was also discussed that the capacity building should address the many sources of possible evidence that can be sought in cases involving communications over information technology products. These could be elements such as what information can be obtained from social media profiles, what information is stored in a file's metadata, evidence in operating systems log files, tracing an email header, and many other types of evidence this can be gleaned from computing devices, but which are still not commonly used by prosecutors around the world.

As this type of training is highly specialized and not all of the CARICOM member states and territories may have the facilities to provide expert training, it could be considered to organize the capacity building at the regional level instead of at national level under the auspice of CARICOM.

2.3 The role of the private sector

The private sector such as Internet access providers, email providers, and other Internet service providers play an important role in fighting cybercrime for various reasons. Primarily because the service providers make use of technical measures to prevent cybercrime and by exchanging with them on successful cybercrimes, the private sector can improve their cybersecurity and the

technical measures to prevent further victimization using similar crimes when technical solutions exist that could help prevent them.

Secondly, cooperation with the private sector is important in order to collect evidence.

Indeed, a particular challenge of cybercrime is the layer of abstraction between the online identity which commits the crime and the natural person behind that identity who can be held liable for the crime in a court of law. Often the only way to identify the natural person behind the online identity is through information held by the private sector such as identifying the user of IP address or who created an online account.

In addition to providing the evidence between an online identity and the real-world identity, the private sector can also provide technical information about their products to explain what evidence may potentially be available to collect from their technology products. This type of technical information could be: for how long log files are stored; the structure of a file system used by the operating system; the possibility to restore deleted files from a storage media, etc.

Generally, Internet service providers are not required to retain specific electronic evidence with the exception of Internet access providers which may be subject to data retention legislation. Therefore, an investigator cannot expect to have a certain type of electronic evidence available as there is no regulatory framework mandating the safekeeping of certain types of electronic evidence. It is only by discussing with the private sector that the investigator will understand which electronic evidence may be available of use to their investigation.

This discussion with the private sector benefits from being an ongoing conversation to exchange ideas on what can be done to reduce the risk of crime by law enforcement and if the private sector could potentially change their policies to ensure more needed evidence is collected in respect of privacy legislation.

These conversations with the private sector can also be used to exchange ideas on the practicalities of obtaining electronic evidence through subpoenas or court orders including how to improve the speed at which service providers respond to such requests; and for criminal justice authorities to hear from service providers what can be done so that requests do not unnecessarily burden the service providers if it is not needed.

Service providers play their most relevant role in cybersecurity issues by improving technical security standards. However, their contributions to the criminal investigations are crucial. A cybercrime strategy should therefore also consider making the cooperation with the private sector as an integral part of the strategy including creating a permanent forum to organize regular meetings between the criminal justice authorities and the private sector to discuss matters of cybersecurity and cybercrime.

2.4 International cooperation

The international aspects of cybercrime are well known as crime committed over the internet is cross-border by nature. Moreover, often cyber criminals prefer to seek out victims in a different jurisdiction than where they reside in order to reduce the risk of being caught and evidence against them being readily available. Online services can be accessed globally as opposed to a national level so a cybercriminal can easily make use of a foreign online service to commit crimes.

It would be all but impossible to solve an online crime case without resorting to international cooperation. Still, one of the main obstacles to resolving cybercrime is exactly the challenges of international cooperation. In part because different legal systems and traditions can be obstacles to international cooperation without an international legal instrument to facilitate the cooperation.

Because international cooperation can be a challenge it should be a part of cybercrime strategy.

Mutual Legal Assistance Treaty procedures have come in disrepute in the internet age as they do not provide evidence sufficiently quick and are often so slow to use that evidence is lost before it can be secured through the legal process. They are also often tedious and laborious to complete so they may only be used exceptionally and in cases where the importance of the evidence is essential for the proper development of a judicial proceeding.

However, access to electronic evidence in any part of the world is increasingly necessary in a greater number of cases, including cases that are not *per se* cybercrime cases but for which the evidence, such as emails, log files, IP addresses are needed to adjudicate the matters including family law, commercial contracts, or public law.

Hence it is necessary to establish agile mechanisms to obtain e-evidence from any country of the world including the USA. The mechanisms for obtaining this e-evidence, and legal guarantees regarding the authenticity, integrity, and the respect of human rights lead to the discussion of improving international cooperation as an integral part of the cybercrime strategy.

2.5 Specialized law enforcement training and forensics' capabilities

Part of a cybercrime strategy is to have a well-trained law enforcement to conduct investigations. Cybercrime raises the question of collecting and handling electronic evidence, but increasingly other types of crime investigations also benefits from law enforcement units that are able to make use of electronic evidence for their investigations.

2.5.1 Securing electronic evidence

Securing of electronic evidence such as acquiring devices, copying hard disks, analysing seized data, and having the capacity to extract evidence from a variety of hardware that may contain evidence of interest to the investigation often requires specialized training for investigators.

Securing electronic data and devices in a legally sound way will ensure the integrity and reliability of it as evidence.

2.5.2 Building a forensics' laboratory

Once a device has been seized for evidence purposes, it is necessary to have the capacity to analyse it in a specialized forensics' laboratory that has for purpose to ensure that the evidence is not modified and that tools are available to extract the evidence.

Often the forensics laboratory can be built at a low cost using free and open source software which can be important to ramp up capabilities quickly when budgets are low.

Examples of tools that can be used to build a forensics laboratory are:

Opensource software:

- The Sleuth Kit (TSK) & Autopsy: It is a software that incorporates the main and most important features that a forensic investigator needs in their day to day. Today, it is the most important open source tool that exists.
- Caine, Deft: There are Linux distributions (such as operating systems) that include an endless number of pre-installed programs for forensic analysis, for example, they already come with the TSK installed, software write blocking, cloning tools, triage (basic), hashes (md5sum; sha1sum ...) etc, it can be downloaded from the internet for free in an ISO file

- FTK Imager: to make forensic images of hard drives from Windows, it also allows dumping the RAM of a PC.

Commercial software:

- EnCase: a commercial tool that is used extensively by law enforcement for hard drives analysis.
- Axiom: software used to triage files for both Windows and MacOS as well as various smartphone operating systems
- UFED: specific tools dedicated to mobile telephone analysis.

2.5.3 Advanced capabilities

There are some areas of a specialized law enforcement capability that may not be necessary on a daily basis in the forensics' laboratory, but which could be considered to pull together at a regional level. This could for example be for malware (computer virus) analysis and reverse engineering of these which could be performed in highly specialized laboratory shared possibly amongst several countries in the region.

2.6 Prevention, public awareness and education

Several countries provided examples of successful public awareness campaigns that help citizens to identify risks and make them less likely to fall victim to cybercrime in the future.

A successful public awareness campaign should ideally be established in cooperation with local law enforcement who can provide information on which types of crimes are the most prevalent in the area, which has caused most victims. These campaigns have been effective not only for their preventive effect but also as they often lead to more crimes being reported by members of the public to law enforcement and should therefore ideally be part of a cybercrime strategy.

Examples of themes that can be included in an educational campaign are the most secure ways of using information technology such as allowing automatic updates, using complex passwords and multi-factor authentication, how to report unlawful activity such as child grooming, and possibly even basic internet etiquette for young people.

2.7 Reporting mechanisms

Cybercrime is unfortunately still a very under reported crime. In part this is caused by citizens feeling that law enforcement may not have the capacity to investigate crimes they are victim because of the technical nature of the crime. Secondly the cross-border nature may lead some citizens to feel that local law enforcement does not have the capacity to properly investigate the case in particular if the amounts lost are relatively minor and international cooperation is limited.

However, by having a tool for citizens to report cybercrime cases of which they are victim, it is ensured that law enforcement maintains a good overview of which crimes are being perpetrated in their jurisdiction as well as information on the nature of those crimes. This can be a powerful tool as, although most cybercrimes may not be sufficiently important to initiate international cooperation, by collecting victim reports and grouping together cases of similar nature, with similar perpetrators, it may well be possible that the minor cases can be coalesced into larger cases which are identified to have caused very important damages at an aggregated level.

Instead of dealing with one case where a citizen lost the equivalent to half a month of salary, which may not warrant an international investigation, through a common reporting mechanism many of the same case with the same perpetrator can be grouped into one larger case that will merit investigative efforts including lab analysis and international cooperation.

It could also be considered to have original reporting mechanism for example under the auspice of CARICOM IMPACS.

3 The presentations held during the conference

The presentations held by CARICOM, the Organization of American States, the United States Department of Justice, and the Council of Europe have been placed as annexes to this report.

4 Delegate presentations and questionnaire

During the conference the delegates were asked to make a short presentation on the current state of play in their countries and territories on cybercrime strategies; what types of cybercrimes were the most prevalent; and what they saw as priority areas for a cybercrime strategy.

Below is a description of the various replies provided and the actual replies to a questionnaire have been placed in the annex.

4.1 Anguilla

Anguilla currently does not have cybercrime legislation enacted but have been able to address certain cybercrimes through the laws on proceeds of crime. A cybercrime strategy has however been considered and a national plan is being dealt with by the H.E. Governor and Permanent Secretary responsible for Information Technology and Security. One of the considerations is to form an incident response team from the public sector.

The most common crimes they need to deal with are skimming which is dealt with proceeds of crime legislation; child pornography which can be addressed during the legislation on obscene publications; and cyberbullying which is not addressed through legislation, but which is usually dealt with through direct police interventions with the perpetrator.

A cybercrime and cybersecurity strategy should also be addressed to deal with cases of cyber fraud, malware and ransomware attacks and hacking in general.

The delegation proposes these objectives as a starting point for the cyber strategy development:

- Creating a response Unit
- Develop public/private partnership dealing with cybersecurity
- Sharing and implementing best practices
- Cooperating with UK and regional bodies
- Developing appropriate legislation to address cybercrime
- Education of public in relation to cybercrime and cybersecurity.

4.2 Antigua and Barbuda

An Electronic Crimes Act was enacted in 2013 which covers many types of cybercrimes as well as procedural measures. Substantive law measures include access and interference; sending offensive messages through communications services; identity theft; electronic forgery; electronic fraud; violation of privacy; misuse of encryption; child pornography; sensitive electronic system; electronic terrorism; harassment utilizing means of electronic system; false websites and spam; unauthorized access to code.

A cybercrime strategy is however still pending. The authorities rely on NCBs from Interpol for training and cooperation. They want to re-enact a Computer Emergency Response Team (CERT) that previously existed.

The delegation proposes the following objectives to improve the current status of the cyber strategy:

- Properly updating legislation related to cybercrime
- Establishing a body of specialized investigators in cybercrime/digital forensics
- Providing judicial education

- Raising public awareness
- Research and analytical units.

4.3 Aruba

Currently there is no comprehensive cybercrime legislation, but the delegates suggested ratifying the Budapest Convention. Additional suggestions were to create a National Taskforce and to develop national cybercrime strategies that would include the preparation of a Cybersecurity Threat Assessment; improve resilience; create an information sharing center; and establish a crisis management center.

A National Cyber Security Taskforce that combines public and private bodies and organizations is currently being developed. The Taskforce's main task is to develop the National Security Plan, which encompasses the cyber security and cybercrime strategies.

There are special units to deal with child pornography, but there is not cybercrime unit. There is no policy for cybercrime for the Aruba Police force.

Cybercrime was dealt by the Secret Service primarily in the past, but the National Central Bureau Counterterrorism, Safety and Interpol (NCTVI) has been recently founded to resume the task. There is a letter of intent to create a workgroup to deal with cybersecurity including a national cybersecurity plan.

The delegation proposes the following objectives to improve the current status of the cyber strategies:

4.4 Bahamas

Not questionnaire or comments were provided.

4.5 Barbados

Not questionnaire or comments were provided.

4.6 Belize

Belize does not have cybercrime legislation, but it is being worked on with the Attorney General to formulate the list of topics for cybercrime legislation and making definitions for those. Legislation on electronic evidence and personal data protection exist.

With the support of the Organisation of American States (OAS), a national cybersecurity strategy is being worked on and a framework for the legislation is being considered. There is no CERT, but there are ad-hoc CERTs.

The delegation proposes the following objectives for the development of the current cyber strategies:

- Continuing the journey in formulating the National Cybersecurity Strategy with the assistance of international partners
- Seeking assistance as required
- Continuing the participation in conferences and training
- Developing a "Big Brother" partnership helping another country in this effort.

4.7 Bermuda

There is a 1996's Computer Misuse Act, an electronic transactions act and an electronic communications act. Bermuda is looking at reviewing and updating those laws.

A cybersecurity working group working under Public-Private Partnership is established and engaged in broad consultation with the stakeholders.

The Commonwealth technology office helped with the formulation of the national strategy which was approved in October 2018 and includes a review of existing legislation, identification of a model framework and a gap analysis to identify deficiencies. The strategy also includes cybersecurity awareness and capacity building and improve international cooperation.

There is a cybersecurity committee, the setting up of a CERT is still pending.

The delegation proposes the following objectives for their cyber strategies:

- Their National Cybersecurity Strategy includes the identification of model legislation against which their existing legislation can be assessed to identify gaps and ensure alignment with international standards.
- This will include a revision of the following acts: Computer Misuse Act, Electronic Transaction Act, Telecommunications Act, Public Access to information Act (PATI), Personal Information Protection (PIPA), Promoting public awareness campaigns.
- Training and education to develop capabilities.

For the international dimension the following was proposed by the Bermuda delegation:

- International treaties and partnerships need to be established to facilitate information sharing, cooperation, and collaboration.
- Internal capabilities need to be established to meet international obligations.
- The need to work with international organizations (e.g., CoE, CARICOM, etc.) to establish cooperative partnerships for cybersecurity and cybercrime prevention.

4.8 British Virgin Islands

A Computer Misuse and Cybercrime Act was enacted in 2014 and draft legislation to amend it was introduced this year as for example the definition of computer is too narrow when today there is a broader range of devices that can communicate over the internet. The amendments seek to target also mobile devices and as a procedural measure to be able to obtain subscriber information from Telco companies. It will also target identity theft and malicious communications, or private and nude images without consent.

It is suggested that a national cybercrime strategy should address cyber bullying, use of electronic and mobile devices in the commission of crimes, human trafficking, child endangerment, defamation of character, identity theft, sharing of inappropriate content and hacking. Audiences to protect include the banking sector, school children, and senior citizens. The stakeholder of a strategy includes law enforcement, courts, ISPs, the telecom regulator and the financial services commission.

For the international dimension it is suggested to include international dimension by creating a global standard. Even in variations of policies, there will be uniformity and commonality due to adherence of global standards.

The delegation identifies the banking sector and primary education as areas that the cybercrime strategy should cover.

Their proposals regarding the cyber strategies:

- Updating policy framework of the existing legislation
- Creation of a cybercrime unit or division that focuses solely on this issue
- Training for relevant stakeholders
- Raising public awareness.

4.9 Cayman Islands

A Computer Misuse Act exists which addresses cybercrime, but the hope is to be able to implement a new cybercrime law pursuant to the conference. Cayman Islands already have strong data protection laws that are the equivalent to the European Union GDPR.

In 2015 they asked Interpol to review the Cayman Islands' cyber strategy, which resulted in a report with a number of suggestions including: establishing a national CERT, a national strategy, and reached out to UK to have a gap analysis on the law enforcement side. They identified the need of a digital forensics unit and that should soon be operational and supporting other countries in the Caribbean.

The delegation summarized the following targets of cyber strategies:

- Leverage the Budapest Convention to draft a new cyber law
- Amending Telecom licenses to provide mandatory compliance, data collection, cooperation with LEAs
- Reaching out to international bodies (CoE, OAS, CARICOM, etc.) to build channels for cooperation
- Developing public awareness campaigns.

4.10 Cuba

Cuban legislation protects the confidentiality of communications and against the classic computer crime offenses protecting the confidentiality, integrity, and accessibility of computer systems, but as a cybercrime strategy Cuba has primarily focused on prevention.

Legislation exists to address terrorism committed through computer system or the attack of computer systems for terrorism purposes.

4.11 Curaçao

Legislation exists including the offense of computer hacking but overall the cybercrime legislation could be more comprehensive.

A strategy has not been formulated yet though there are initiatives by the public prosecutor. The delegation finds that the cyber strategy should start by creating a cybersecurity strategy implemented with an action plan to do it.

4.12 Dominica

Not questionnaire or comments were provided.

4.13 Dominican Republic

The Dominican Republic ratified the Budapest Convention in 2013 and has put into force the "National Cybersecurity Strategy 2018-2021". This strategy is related to cybersecurity but includes

important elements for the fight against cyber criminality. Indeed, the first of its objectives is clearly related to cybercrime: "Strengthen legislative provisions that affect issues related to cybersecurity, and the capabilities of the Public Ministry and its auxiliary agencies to prosecute and the Judiciary to decide on cybercrimes and crimes."

The Dominican Republic also has a "Supplementary Action Plan on Cybercrime", with ambitious plans to strengthen cybercrime.

National police's specialized computer crime unit has existed for many years and has been active in supporting international cooperation.

4.14 Grenada

The Electronic Crimes Bill of 2013 includes a number of cybercrime offenses as well as a section on investigations and procedures and was, in part, modelled after the Budapest Convention.

A cybercrime strategy or framework has yet to be adopted but the delegation expressed interest in developing one for Grenada. The strategy should in addition to legislation cover public awareness, protection of critical infrastructure and having a process to monitor the implementation of the strategy. Grenada is looking into establishing a national CERT.

Law enforcement has a specialized cybercrime unit which can also conduct digital forensics and cooperates with Interpol. This has led to successful conviction, sentencing, using the cybercrime legislation.

4.15 Guyana

A cybercrime bill was enacted in 2016 covering many cybercrime offenses. Some of the most common experienced in Guyana have been phishing, website defacement, and malware. Prosecution of some of the crimes is difficult for their authorities. There is a need for more training and a more coherent updated legislation. There is also a need for first responders for police officers.

There is interest to create a forum to enhance government coordination to tackle cybercrime.

The delegation summarizes the following objectives as targets of cyber strategies:

- Safeguarding national interests
- Ensuring economic stability and business continuity
- Ensuring critical infrastructure and data are protected
- Safeguarding technological assets
- Ensuring citizens safety
- Encouraging business innovation and capitalize on economic gains from technological advancements.

4.16 Haiti

Not questionnaire or comments were provided.

4.17 Jamaica

There is no comprehensive law on cybercrime, but several laws deal in part with cybercrime offenses or regulated the admissibility of electronic evidence. Jamaica has enacted legislation on

electronic transactions, child pornography, and they created a law to address Advance Fee Fraud in 2013.

A website allows for the collection of victim reports without the need to have to file a report at the police station.

Jamaica had experienced different kinds of cybercrime activities, but the most recurring ones are malware infections and credit card skimming. Past cases have included money laundering with cryptocurrencies and child pornography from persons who have come to Jamaica from notably the United States. In Jamaica it is common to say that if a crime exists abroad, it will also be found in Jamaica.

4.18 Mexico

There is no specific cybercrime law but there are laws criminalizing child pornography, fraud, and theft of personal data. As Mexico is a federation of states, there are some variations in legislation and indeed some Mexican states have laws against online fraud. The main offenses experienced in Mexico are phishing, human trafficking, sexting, child pornography, attacks against banks, attacks against journalists, and fraud, including one case concerning of 110 million dollars against a Mexican bank.

A national strategy was developed in a council with the participation of several civil society and private enterprises. A government CERT exists as do a number of private CERTs.

CERT-MX functions at the government level with responsibilities for public institutions.

4.19 Montserrat

A draft Cybercrime Bill and Cybercrime Strategy document are currently being drafted and moreover Montserrat is considering legislation in the areas of data protection, electronic evidence, electronic filing, and electronic funds transfers.

The Cybercrime strategy has as guiding principles: national leadership with political will for the policy; shared responsibilities public and private sector as well as the citizens; proportionality for risks and threats; international cooperation.

A cybercrime strategy should address breaches of the constitutional right to privacy; responsibilities of stakeholders; and training of the various stakeholders. But a strategy should also include incident management, collaboration, and legislation.

The main offenses are redistribution of pornography and cyberbullying.

However, Montserrat also explained: "A small island such as Montserrat, will benefit from collaboration among countries, both regionally and internationally. We simply do not have the resources, or infrastructure to be successful in our cyber related initiatives without the technical support, training and resources available from international organizations."

4.20 Puerto Rico

Currently there is no cybercrime legislation but the existing provisions of the criminal code addresses many of the crimes committed over the internet. The delegation of Puerto Rico expressed that they would like to implement specific cybercrime legislation as it is a type of crime that is increasing. The main offenses are identity theft, misuse of social media, child pornography, cyberbullying, extorsion on social media.

The delegation summarized the following objectives as targets of cyber strategies:

- More cooperation with neighbouring countries in the Caribbean
- More specific legislation for cybercrimes that covers all dimensions, and specific guide and prevention for these types of crimes
- Cooperation between entities to achieve an effective way to fight cybercrime
- Prevention and continuing education for cybercrimes.

4.21 Saint Kitts and Nevis

Cybercrime legislation was addressed in the 2009 Electronic Crimes Act and draft legislation is planned to address electronic evidence and electronic transactions.

Saint Kitts and Nevis stated that the following needs should be addressed in a cybercrime strategy: "public awareness for all to develop a cybersecurity culture, ongoing capacity building for Judiciary, Law Enforcement, Prosecutors, IT professionals including network specialist, software engineers and IT management, technical assistance for drafting the requisite Policies and Legislations, Legal Review of existing electronic crimes Act and Evidence Act and other related national legislations and drafting of amendments for cybercrime legislation and regulations, advise on required institutional and administration framework required."

The main offences are phishing, impersonation, use of mobile phones to carry out criminal activities, and misuse of social media.

4.22 Saint Lucia

Saint Lucia have implemented the computer misuse act, the evidence act and the electronic transactions act. The country is currently looking into establishing a national CERT. The main offences in this country are primarily related to social media.

In 2008 a taskforce from various ministries (public sector, customs) was organized. The role of the taskforce is to review legislation and policies. They have developed an acceptable use policy for the e-government services.

The delegation found that the work done so far by the National eGovernment Taskforce has laid to a great foundation for the future for managing the country's cybersecurity/crime environment, as well as the plan for establishing the CERT. The strategies are currently being developed and the delegation recommends engagement with critical public/private sector stakeholders should occur prior to the submission of the draft strategies.

The delegation identified these items as being of importance for a cybercrime strategy:

- Seek Technical assistance to develop a National Cybersecurity Strategy and Implementation Plan
- Public Awareness workshop for Government Officials, Private Sector including ISP, IXP and Financial Institutions Stakeholders
- Capacity Building in areas of Cybersecurity for IT Professionals, Ministry of Justice, Legal Affairs and Communications and Office of the Attorney General: including ISO 27001 Information Security Management, ISO 31000 Risk Management, Cybersafe Awareness within Government
- Establish a CERT focus on government then expand to schools and National level.

4.23 Saint Vincent and the Grenadines

The 2016 Cybercrime Act and the 2009 Electronic Transactions Act include provisions relevant for cybercrime and electronic evidence. A particularity of the legislation of Saint Vincent and the Grenadines is that it includes a provision on electronic harassment.

The main offences occurring in the country include the procurement of child pornography, skimming of electronic payment means, and cyber bullying.

The delegation identified the following objectives to improve the status of the cyber strategy:

- Raise public awareness on threats and how to avoid them
- Pass stringent laws to deal with cybercrimes, getting the private sector more involved (not just ISPs) in the sharing of information pertaining to cybercrime and cyber security.

4.24 Sint Marten

Cybercrime has not been enacted and instead ordinary criminal law such as provisions incriminating fraud are relied on to deal with cybercrime. The main offences are the skimming of credit cards and online fraud. Global security awareness is a big concern in this country.

For cybercrime related incidents which have implications at a national level the national security service will investigate them. There is currently no integrated strategy for cybercrime which may limit prosecution.

The delegation recommends the following points in order to improve the current cyber strategies:

- Shift in approach:
  - Cybercrime should no longer be seen as a problem of the IT department but rather a joint responsibility in society
  - There should be multiple levels in a cybercrime strategy: tactical, operational, and strategic level
  - IT/maintenance in the center, end user on one end, policy makers and legislation on the other but jointly responsible
  - weakest point breaks the chain of security
- Transposing the provisions of the Budapest Convention in national legislation
- Setting up awareness programs for the community but also managers, and country leaders.
- Look for ways and means to join local expertise and forces to come to one comprehensive national approach that should be compatible to regional and international visions.

4.25 Suriname

Suriname has developed a law on electronic transactions, but they have problems with the criminal proceedings. The main offences in the country are misuse of social media and skimming. There is an increased exposure to cybercrime and Suriname needs to protect their critical services.

A concept on a cybersecurity plan and the delegation summarized the most important aspects of a cybercrime plan as:

- The adoption of the National Cybersecurity strategic plan
- The official implementation of the working group of the SurCSIRT.

4.26 Trinidad & Tobago

Legislation includes the Computer Misuse Act from 2000, the Data Protection Act, the Electronic Transaction Act, Interception of Communication Act, Fraud Act, as well as the Child Pornography and harassment act. The main offences are skimming, phishing and business email compromise.

Training has been received in cooperation with the United Sates, the OAS, and IMPACTS. The country members of the G7 24/7 Network managed by US Department of Justice.

A Cybercrime strategy should include the following elements according to the delegation:

- Collaboration amongst Government departments to formulate a plan to manage cybercrime
- The development or adjustment of cybercrime related legislation
- The adoption after evaluation of international cybercrime standards conventions
- The building of capacity of all required elements of cybercrime management
- Implementation of an awareness program on cybercrime.

4.27 Turks and Caicos Islands

Not questionnaire or comments were provided.

5 Guidelines and recommendations for countries in the Caribbean region to develop a cybercrime strategy

The conference laid out six initiatives that could be included in a cybercrime strategy and were presented in section 2 of this report. The various delegates pointed out different priorities, but any cybercrime strategy could consider all six of the initiatives discussed during the conference.

This section looks at particular recommendations for the unique situation of the Caribbean community as they were discussed during the conference.

5.1 Legislative efforts

As discussed in section one and section 2.1, one of the main topics of interest to the CARICOM countries and Overseas Territories (OT's) was how the international legal instrument, the Budapest Convention, would coexist with national legislation or with the regional initiative of the "Harmonization of ICT policies and legislation across the Caribbean" (HIPCAR).

However, during the conference it was explained that ratifying the Budapest Convention is not a hindrance to implementing national or regional legislation. Many Member States to the Budapest Convention have enacted cybercrime legislation beyond the list of incrimination in the Convention in such areas as spam, identity theft, or cyberbullying. The International Convention should not be seen as a legal instrument that harmonizes cybercrime legislation around the world, but instead it is an *ad minimum* legal protection in order to both serve as a model law and to facilitate international cooperation on cybercrime and electronic evidence. Regardless if national legislation is different amongst the member states of the Convention, all members will know that there is a minimum of cybercrime legislation and procedural measures in which the other members can rely on.

The choice is therefore not an either or between HIPCAR and Budapest Convention but in reality, the CARICOM countries and territories can choose both.

5.2 Regional cooperation

The participating countries and territories distinguished themselves by their diversity in terms of richness of culture, language, and economic size. But there are also numerous common traits and under the auspice of CARICOM it was discussed to which extent it may be beneficial to explore regional cooperation to fight cybercrime. There are several areas listed here below in which regional support may make sense.

5.2.1 Legislation

Legislation is an obvious choice as is already well on the way through the HIPCAR project. Enacting legislation is difficult, and in that, legislators must consider all different possibilities to be able to draft durable laws. Moreover, the international aspects of cybercrime are obvious and therefore enacting legislation that allows for international cooperation as it follows the standards of the Budapest Convention will allow the Caribbean Community to become part of the global group of countries and territories that cooperate on fighting crimes committed over the internet and crimes against computer systems.

5.2.2 Dialog with industry and private sector

There are advantages in seeking cooperation from the private sector in a joint effort of several countries in order to ensure the best possible sharing of knowledge amongst all the countries on

the types of evidence that can be obtained from Internet service providers. It will also help foster trust from the private companies as it would allow them to have a single point of contact that they trust to facilitate outreach to law enforcement in the various countries in the Caribbean.

5.2.3 Training and capacity building

Developing efficient courses for training on cybercrime capacity building consumes both time and resources. For a region like the Caribbean advantages can be drawn from developing modules for training jointly with most countries and territories.

5.2.3.1 Judiciary training

Although national laws and case law differs amongst countries and territories, having regional training for judges and prosecutors carries advantage that the individual costs can be brought down; often there will only be limited specialised training to a few judges which are the most likely to deal with cybercrime cases and therefore bring few judges from several different countries together as a group provides for more cost-efficient training. An added advantage is that participants to the training can exchange ideas and cases they or their colleagues have adjudicated and share the knowledge through the trainings.

5.2.3.2 LEA specialized training

As to judicial training, providing regional training for law enforcement can provide economies of scale on the cost of the training but will invariably also lead to exchanges amongst the practitioners on how to best manage cases, which type of evidence can be crucial, and where to look for evidence and so forth.

5.2.4 Forensics' laboratories

One of the more interesting ideas discussed during the meeting was possibly creating a joint forensics' lab that could be used by several countries and territories. The purpose would not only be to bring costs down of highly specialized lab with equipment that in individual countries or territories may not be used every day, but it is also sure to the high level of expertise that is available to all participating countries and territories.

5.2.5 Victim reporting mechanisms

Providing citizens with tools to report instances of cybercrime it's important to be able to effectively formulate a cybercrime strategy by having a better understanding of the crimes that are harming the citizens. The value of such a tool is great and also in the aggregated data which allows for a better statistical understanding of trends but also to group together similar victim reports to build larger, more important, criminal cases for investigation.

5.2.6 International cooperation

The Caribbean countries and territories are commonly associated with sunnier dispositions than cybercrime even though it is clear that cybercriminals strike in all countries as they often do know their victim's location when strike. To ensure the best possible cooperation internationally with law enforcement it can be an advantage to join a regional group. This helps foster trust which is essential for cooperation to get to know each other within the group and members can recommend each other for cooperation on joint or similar cases.