CYBER SECURITY AND CYBERCRIME *ARUBA*

REGIONAL CONFERENCE: POLICIES AND STRATEGIES ON CYBERCRIME FOR THE CARIBBEAN COMMUNITY

12-14 JUNE 2019 SANTO DOMINGO, DOMINICAN REPUBLIC

Assistant Comissioner **Vanessa TJON KOCK**
Head of Investigation Unit & head of Special Unit, ARUBAN POLICE FORCE (KPA)

Ruthlyn LINDOR MSc.
Senior Strategic Analist, **NATIONAL CENTRAL BUREAU COUNTERTERRORISM, SECURITY AND INTERPOL (NCTVI)**

CONTENT

- Introduction
- Current structure cybercrime and cybersecurity in Aruba
- Steps already taken in the process of developing strategies and policies
  Cybersecurity
- Projected goals
  Action Plan
- Guiding principles
  Action plan
- Conclusion

INTRODUCTION

- Unfortunately, cybercrime offences are increasing in Aruba. This occurs on all levels with all its consequences for individuals, institutions, organizations and the State.
- Due to the rise of cybercrime and the increasing awareness of the importance of digital security in the context of national security, cybercrime and cyber security is prioritized in Aruba

CURRENT STRUCTURE CYBERCRIME IN ARUBA

The Aruban Police Force (KPA) is the law enforcement authority that responses to cybercrime offences

The KPA is responsible for maintaining law and order and safety in Aruba. The force consists of 3 parts, namely the general police services, the criminal investigation services and the special police services.

In total, the KPA has 550 employees, including 450 executives and 100 administrative staff.

- The judicial duties are mainly performed by the criminal investigation services. In view of the constantly changing demands (due to the technological and socio-economic developments), the KPA is constantly faced with increase challenges to restructure to cope with these demands
- The KPA is increasingly confronted with cybercrime offences such as skimming, ransomware, phishing, hacking and child pornography, but also classic offences involving computers such as fraud, extortion and swindle
- The number of incidents that are reported to the police is practically low, an average of 5 incidents per year to name a number
- We are aware that not all incidents are reported, at times to prevent image damage, out of shame or lack of knowledge
- We are also aware that cybercrime and cyber related crimes are sophisticating.

- As it is now regulated within the KPA, depending on the nature of the cyber offence, the case is dealt with by the KPA unit responsible for that type of crime. These units work independent of each other and there is therefore no coherence in approach and / or policy.
- Given the developments and challenges in this area, we aim to launch a Cyber Crime Unit soon. Together with our local and international partners, our main objective will be to work towards a situation where:
  - there is a clear national strategy and policy on cybercrime (prevention, protection, prosecution and partnership)
  - there are legal instruments/ criminal legislation available for effective response to cybercrime;
  - there is a dedicated Cybercrime Unit in the Force that is equipped with the necessary expertise in terms of personnel and resources;

CURRENT STRUCTURE CYBERSECURITY IN ARUBA

UNTIL RECENTLY, CYBER SECURITY WAS MAINLY CARRIED OUT BY THE SECURITY SERVICE OF ARUBA. THE SECURITY SERVICE DID THIS FROM ITS TASK WITH REGARD TO STATE SECURITY.

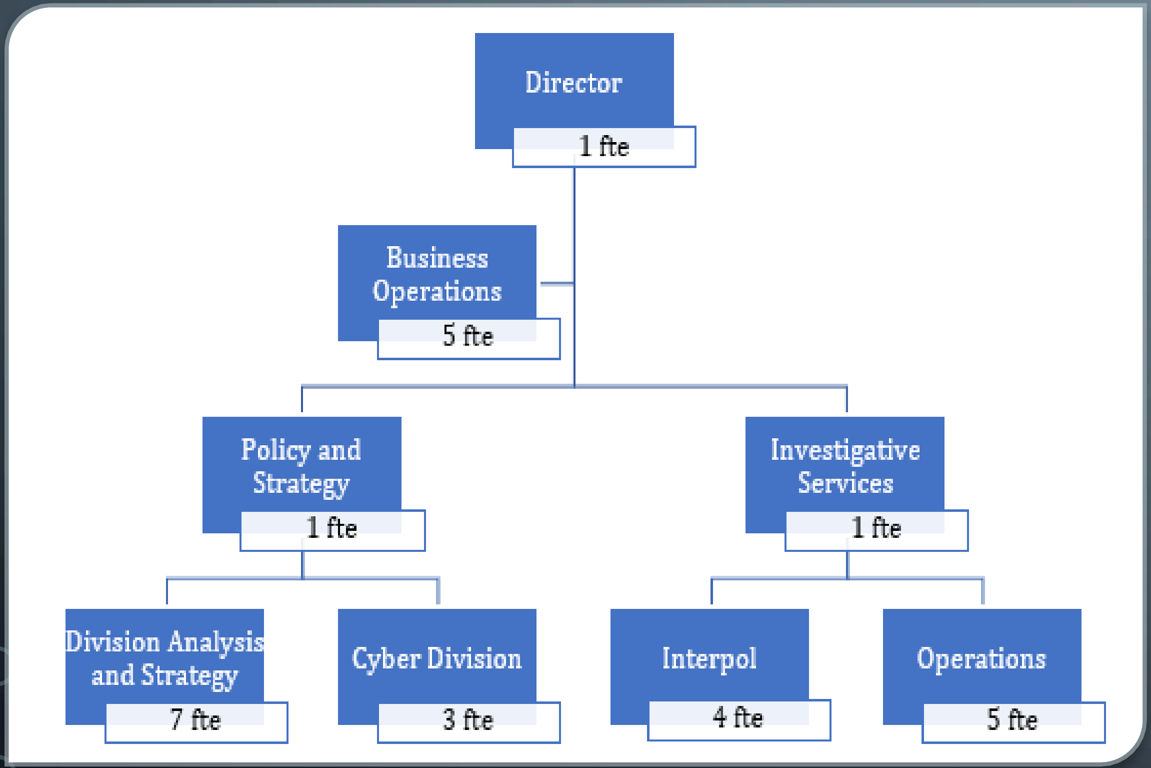
A GOVERNMENT SERVICE THAT HAD CYBER SECURITY AS ITS MAIN TASK DID NOT EXIST UNTIL RECENTLY.

WITH THE INSTITUTIONALIZATION OF THE NATIONAL CENTRAL COUNTERTERRORISM, SECURITY AND INTERPOL (NCTVI) OFFICE IN 2018, CYBER SECURITY HAS BECOME ONE OF THE MAIN TASKS OF THE NCTVI.

THE NCTVI CONTRIBUTES TO THE SAFETY AND SOCIAL STABILITY OF ARUBA BY RECOGNIZING CYBER SECURITY THREATS AND BY STRENGTHENING THE RESILIENCE AND PROTECTION OF VITAL INTERESTS AGAINST THESE THREATS.

IN THIS CONTEXT, THE NCTVI HAS IN PARTICULAR A COORDINATING, POLICY-RELATED AND, WHERE NECESSARY, AN EXECUTIVE ROLE.

ORGANIZATIONAL CHART NCTVI- CYBER DIVISION



Director
1 fte

Business Operations
5 fte

Policy and Strategy
1 fte

Investigative Services
1 fte

Division Analysis and Strategy
7 fte

Cyber Division
3 fte

Interpol
4 fte

Operations
5 fte

- The Cyber Division consists of:
  - A head of Information and Expertise (Chief Information Officer)
  - IT Specialist
  - IT employee

TASK NCTVI- CYBER SECURITY

⚠ Identifying and indicating threats and risks in the area of cyber crime.

The realization of optimal crisis management and crisis communication in regard to cyber crime.

🔒 The development of policy and administrative reports regarding cyber security

STEPS ALREADY TAKEN IN THE PROCESS OF DEVELOPING STRATEGIES AND POLICIES - CYBERSECURITY

- On the initiative of the Security Service Aruba, various parties, - including the government, Airport Authority Aruba, utilities companies such as our telecom company SETAR, NGO's such as Aruba Hotel And Tourism Association and other entities such as TNO Caribbean (the Netherlands Organization for applied scientific research)- signed a letter of intent in 2016 to form an alliance in the field of cyber security.
- This public-private partnership aims to contribute to the protection of the vital interests of Aruba and to the strengthening of digital security and resilience in Aruba.

- The Minister of Justice set up a working group by ministerial order (MB) in 2018 with the task to form a National Cyber Security Task Force, consisting of parties from the public and private sectors.
- One of the main goals of this Task Force is to develop the National Cyber Security Plan Aruba.

PROJECTED GOALS- ACTION PLAN

- Develop a National Cyber Security Plan for Aruba.
- The following goals are being pursued with the implementation of the national plan:
  - strengthen cyber security on Aruba;
  - safe use of IT in Aruba;
  - further developing cyber skills by creating a partnership between the public and private sectors;
  - resilient vital sectors;
  - adequate response to crisis and / or incidents
  - Developing national cybercrime policy and strategies
  - Developing legal framework/ criminal legislation on cybercrime
  - Strengthen criminal justice capacities on cybercrime

- Preparation of Cyber Security threat assessment
- Creating coherence between the various initiatives and actions (coordination);
- Encourage parties to be accountable and to make capacity and / or resources available for cyber security (commitment);
- Establishing an Information Sharing Analysis Center (ISAC) This is a body in which information sharing and trust between the actors is central (trusted community);
- Develop the strategic policy frameworks with regard to cyber security in order to minimize potential threats and / or oblige companies to take minimal measures in the context of cyber security;
- Creating a crisis management and / or response system in the event of cyber attacks that can be quickly scaled up and deployed (response).
- Develop and introducing legal frameworks in regard to cybersecurity (such as introducing a reporting obligation and minimum security standards)
- Development of national policies or strategies on cybercrime and legal framework/ criminal legislation on cybercrime

GUIDING PRINCIPLES- ACTION PLAN

INTEGRATED APPROACH. PARTNERSHIP BETWEEN THE PUBLIC AND PRIVATE SECTORS IS ESSENTIAL;

THE PUBLIC ADMINISTRATION IS RESPONSIBLE FOR PUBLIC INTERESTS, WHILE THE PRIVATE SECTOR AND BUSINESS TAKE ON ACCOUNTABILITY FOR THEIR RESPONSIBILITIES. IN THIS CONTEXT, IT IS ALSO NOTED THAT EACH VITAL INFRASTRUCTURE IS RESPONSIBLE FOR THEIR OWN RESPONSE CAPACITY;

INFORMATION SHARING AND KNOWLEDGE DEVELOPMENT ARE CRUCIAL TO STRENGTHEN CYBER SECURITY. EXCHANGING EXPERIENCES AND KNOWLEDGE BETWEEN THE SECTORS SHOULD BE ENCOURAGED;

CYBER SECURITY MUST BE AN ESSENTIAL PART OF POLICY AND DAY-TO-DAY OPERATIONS WITHIN THE VITAL COMPANIES.

TO CONCLUDE

- This is a short presentation of Aruba regarding our process in developing strategies and policies on Cyber security and Crime we are honored to be attending the regional conference for the Caribbean community and looking forward to discussing on these matters with the participants in order to strengthen our competence in developing our national strategies and policies and international partnerships in regard to cyber crime and cybersecurity

Thank You