CYBERCRIMINALITE – CYBERPOLICE

FFGI 2019

I. INTRODUCTION

- Le développement contemporain des Technologies de l'Information et de la Communication (TIC) constitue un tournant majeur de la civilisation humaine.

  L'illustration la plus parfaite de l'essor des TIC est sans nul doute l'avènement du réseau Internet.

I. INTRODUCTION

- En Afrique et particulièrement au Burkina Faso, le passage de l'analogie au numérique a changé **profondément** la physionomie de la société traditionnelle qui s'est très vite transformée en une société de l'information.

I. INTRODUCTION

Mais, l'essor des réseaux numériques a entrainé l'apparition d'une nouvelle forme de criminalité charriée par les premières lueurs de la société africaine de l'information, appelée « cybercriminalité ».

II. DEFINITIONS

II. DEFINITION (S)

Aucune définition universelle de la cybercriminalité. La cybercriminalité apparaît comme une nébuleuse, par ses acteurs et ses procédés techniques essentiellement évolutifs. Elle demeure une réalité difficile à cerner par les dispositifs du droit matériel.

II. DEFINITION (S)

- La Convention sur la cybercriminalité, aussi connue comme la Convention de Budapest sur la cybercriminalité ou Convention de Budapest, est le premier traité international qui tente d'aborder les crimes informatiques et les crimes dans Internet en harmonisant certaines lois nationales, en améliorant les techniques d'enquêtes et en augmentant la coopération entre les nations.
- Elle fut établie le 23 novembre 2001 par le Conseil de l'Europe et ratifiée par 56 pays dont quatre pays d'Afrique (outre l'île Maurice, le Sénégal, le Maroc et le Ghana).

II. DEFINITION (S)

La Convention de l'Union Africaine (UA) sur la cybersécurité et la protection des données à caractère personnel – appelée aussi « Convention de Malabo » a été adoptée le 27 juin 2014. L'échéance des dernières signatures était fixée au 14 mars 2018. Or, force est constater que seuls 10 pays sur les 55 de l'Afrique ont signé cette convention (18 %) : Bénin, Tchad, Comores, Congo, Ghana, Guinée-Bissau, Mauritanie, Sierra Leone, São Tomé-et-Príncipe et Zambie. Et encore, seulement deux pays signataires – le Sénégal le 3 août 2016 et l'Ile Maurice le 6 mars 2018 – l'ont ratifiée pour que celle-ci entre en vigueur sur leur territoire national. (source Cio-mag, 2018)

II. DEFINITION (S)

- Pas de définition universelle du terme
- Néanmoins, il existe aujourd'hui plusieurs tentatives de définitions qui s'apparentent à la définition suivante :

« la cybercriminalité regroupe l'ensemble des infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau »

II. DEFINITION (S)

- La cybercriminalité regroupe deux (02) types d'infractions
  - **Les infractions spécifiques aux TIC** : cyberattaque , *cyberguerre(ou cyberterrorisme)*, etc.
  - **Les infractions facilitées par les TIC** : *cyberescroquerie*, blanchiment d'argent, contrefaçon, etc.

III. CONCEPT DE CYBERGUERRE

III. CONCEPT DE CYBERGUERRE

- Elle consiste en l'utilisation d'ordinateurs et de l'Internet pour mener une guerre dans le *cyberespace*
- Le réseau global est devenu un lieu de confrontation militaire majeur. L'utilisation de l'Internet permet de s'infiltrer rapidement dans tous les réseaux les plus sensibles du monde

III. CONCEPT DE CYBERGUERRE

- **L'espionnage politique et industriel** : des informations confidentielles qui ne sont pas correctement sécurisées peuvent être interceptées et modifiées, etc
- **L'arrêt ou le sabotage d'équipements** : les ordinateurs et les satellites permettant de coordonner des moyens de défense sont visés par ce type d'attaques
- **Les attaques d'infrastructures sensibles** : attaque des centrales électriques, distribution d'eau, communications, oléoducs, et moyens de transports

III. CONCEPT DE CYBERGUERRE

- **Quelques cas de cyberguerre :**
  - Les Etats-Unis ont lancé des cyberattaques contre des systèmes de lancement de missiles et un réseau d'espionnage iraniens, après la destruction par Téhéran d'un drone américain, ont rapporté des médias américains samedi 22 juin 2019.(sources L'Obs, publié le 23 juin 2019 à 09h35)
  - Fancy Bear et APT 28 (services de renseignement militaires russes) seraient à l'origine de l'attaque dont a été victime la chaîne d'information française TV5 en avril 2015. À un an des élections législatives.(sources judiciaires françaises)

III. CONCEPT DE CYBERGUERRE

- **Quelques cas de cyberguerre :**
  - En septembre 2010, l'Iran a été attaqué par le ver informatique *Stuxnet*, dont le but était d'infecter les systèmes des centrales nucléaires de Natanz et de Bouchehr, ralentissant d'un an leur mise au point. Selon Moscou, ce logiciel malveillant serait l'œuvre d'Israël et des États-Unis
  - En octobre 2007, un virus d'origine israélien s'attaqua aux systèmes de défense sol-air de la Syrie les rendant inopérants afin d'apporter aux chasseurs-bombardier de Tsahal plus de sécurité lors de leur attaque du réacteur nucléaire syrien d'al-Kibar

IV CYBERATTAQUE

IV. CONCEPT DE CYBERATTAQUE

C'est de réaliser un acte malveillant envers un dispositif informatique via une faille sur les systèmes d'exploitation en générale

IV. CONCEPT DE CYBERATTAQUE

le defacage de sites web (communément appelée defacing) exploite les

vulnérabilités d'un site web, le pirate et affiche un message ou une image ainsi que sa

signature.

IV. CONCEPT DE CYBERATTAQUE

- **formjacking**, l'attaque en vogue qui cible le e-commerce;
- **cryptojacking**;
- **Attack DDoS;**

IV. CONCEPT DE CYBERATTAQUE

Quelques cas de cyberattaque :

- En Aout 2019: une grosse centaine d'établissements de santé du groupe Ramsay ont été touchés par une cyberattaque jusqu'à contaminer l'ensemble de l'équipement informatique des hôpitaux. (source France 3)
- En Aout 2019: Les données personnelles piratées d'environ 90.000 clients allemands de MasterCard ont été publiées cette semaine sur un forum en ligne, dont des numéros de cartes de crédit, a rapporté la presse allemande, poussant MasterCard à suspendre la plateforme partenaire incriminée. (source journal 20minutes)

V CYBERESCROQUERIE

V. CYBERESCROQUERIE

- Il s'agit d'une forme d'escroquerie facilitée par l'usage des TIC
- Il existe plusieurs types de cyberescroquerie:
  - Le phishing ou hameçonnage
  - L'usurpation d'identité
  - Fausses Loteries
  - Webcam et chantage
  - La fraude via les services de Mobile Banking
  - La fraude liée a la téléphonie (phreaking):
  - Les fausses donations / lègues
  - Les fausses offre d'emploi, de stage, de bourse
  - Ventes et locations immobilières

V. CYBERESCROQUERIE

- **Le phishing ou hameçonnage** : consiste à faire usage de manœuvres frauduleuses, en vue de soutirer des informations personnelles de la victime qui seront utilisées à des fins malveillantes

V. CYBERESCROQUERIE

- **L'usurpation d'identité:** il s'agit d'utiliser l'identité d'une autre personne pour réaliser des actions frauduleuses.

Les réseaux sociaux sont le lieu en vogue où sévissent la plupart des usurpateurs

V. CYBERESCROQUERIE

- **Les fausses loteries** : il s'agit d'inventer sans cesse des promotions au nom de grandes firmes internationales, usurpant ainsi le nom et la marque. C'est ainsi qu'on retrouve souvent des loteries COCA-COLA, MICROSOFT, HEINEKEN etc. Surement un des types d'escroqueries les plus anciens et les plus répandus

V. CYBERESCROQUERIE

- **Webcam et chantage** : Résultant parfois de l'arnaque à l'amour, ce type de chantage est de plus en plus en vogue sur les réseaux sociaux et sites de rencontres. Les cybercriminels opèrent en soutirant de l'argent à leur proie, sous peine de divulguer des vidéos intimes captée sur Skype ou à caractère sexuel.

V. CYBERESCROQUERIE

- **La fraude via les services de Mobile Banking**: L'arrivée des services de Mobile Banking, gérés par les opérateurs téléphoniques africains, a permis le développement de certaines pratiques frauduleuses, très populaires auprès des cyberdélinquants. En effet, ce type d'arnaque consiste, pour les cybercriminels, à s'attaquer au compte électronique des abonnés de services de Mobile Banking. Il s'agit d'une pratique courante très en vogue au Burkina Faso comme dans plusieurs pays africains

V. CYBERESCROQUERIE

- **La fraude liée a la téléphonie (phreaking)**: elle consiste à acquérir des informations personnelles en écoutant des conversations téléphoniques ou à l'appel de numéros surtaxés

V. CYBERESCROQUERIE

- **l'arnaque à l'amour**: le cybercriminel crée l'illusion d'une relation amoureuse passionnée avec sa victime et usant des sentiments, se fait remettre de l'argent
- **Les fausses donations / lègues** : le cybercriminel requiert l'aide de sa victime pour la réalisation d'une transaction financière ou du déblocage d'une fortune supposée, contre le paiement de commission très généreuses à sa victime
- **Les fausses offre d'emploi, de bourse :** le cybercriminel vous annonce qu'une société basée au Canada, aux États-Unis recrute plusieurs personnes de profils divers . Pour voir la belle affaire se réaliser, vous devrez avant tout, vous acquittez des frais relatifs à votre prise en charge, par Western Union ou Money gram
- **L'arnaque à l'achat-vente** : le cybercriminel entre en *pseudo contrat* « d'achat-vente » avec sa victime en utilisant une fausse identité ou émettant des faux documents. Ensuite, une fois la marchandise récupérée, aucun paiement n'est effectué

VI. CYBERPOLICE

VI. CYBERPOLICE

- **Sécurité des personnes et des biens dans l'espace virtuel**

Comme l'environnement physique, les espaces virtuels publics et privés (personnes et entreprises) doivent bénéficier d'un niveau de sécurité garantissant la confiance et la paix sociale.

- **Lutte contre le terrorisme**

Les aspects suivants sont chacun un défi à relever:

1. espace virtuel comme cible;
2. environnement de planification et de logistique;
3. environnement de communication et de propagande.

VI. CYBERPOLICE

La cybercriminalité pose un problème :

- ✓ d'atteinte à la sécurité publique ;
- ✓ d'atteinte aux institutions et à la sûreté de l'Etat ;
- ✓ d'atteinte à la vie privée ;
- ✓ d'atteinte à la propriété intellectuelle ;
- ✓ d'atteintes aux biens;
- ✓ d'atteintes aux mœurs.

VI. CYBERPOLICE

Établir infraction

- Échanges suspects,
- Éléments compromettants,
- Faux profils de réseau sociaux,
- Éventuellement, preuves de paiement.

- Faits dévoilés par la victime,
- Faits dévoilés lors de l'interpellation de suspects (pas de victimes). Comment accéder aux preuves (scène de crime) sans la coopération d'entreprises non locales?

Identifier

- Paramètre de création des profils et des identifiants,
- Identification des abonnés TIC (téléphones et IP),
- Documents d'identification utilisés lors des retraits.

- Le fournisseur du service coopère-t-il ou fournit-il une procédure claire d'accès aux informations?
- L'abonné (téléphone ou IP) est-il bien identifié?
- Les documents de retrait sont-ils accessibles et bons?

Localiser

- Analyse de facture détaillée (téléphones),
- Adresse géographique des l'IP utilisées pendant l'infraction,
- Adresse géographique des l'IP utilisées pendant la création ou l'utilisation du profil/identifiant,
- Caissier(e) / lieu de retrait des paiements.

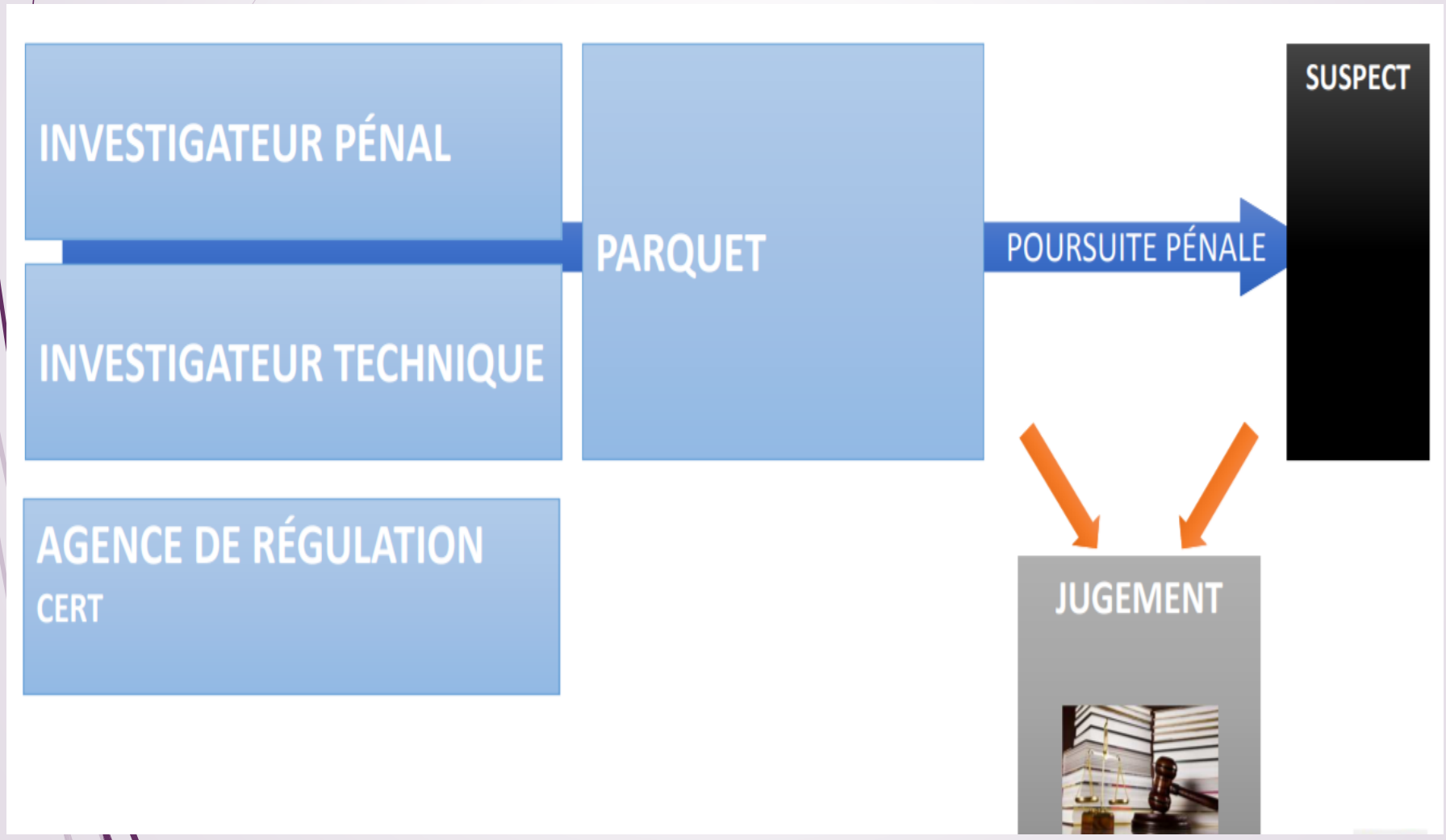
- Ces factures sont-elles accessibles et dans des délais raisonnables (numéros internationaux, opérateurs)?
- L'adresse IP a-t-elle une position géographique?
- L'adresse IP est-elle accessible? délivrée à un utilisateur unique à un moment donné?
- L'organisme de transfert d'argent coopère-t-il ou fourni-t-il une procédure claire?
- La caissier(e) / lieu de retrait est-il habituel ou ponctuel?

Interpeller

- Souricière,
- Patrouille,
- Convocation.

- Méthode de police classique,
- La population contribue-t-elle à la recherche de renseignement compte tenu du type de crime?

VI. CYBERPOLICE



VI. CYBERPOLICE

Les structures institutionnelles

- La justice
- DLCC
- Police Nationale
- Gendarmerie Nationale
- ARCEP
- CIL
- ANSSI

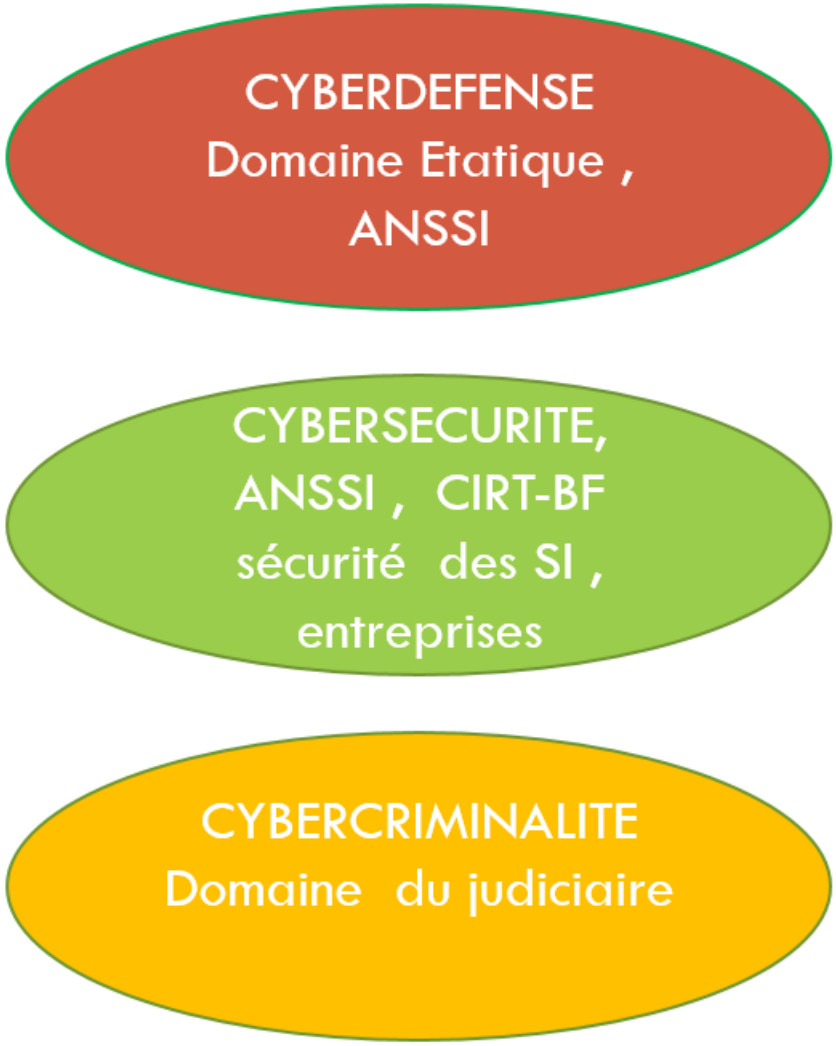
VI. CYBERPOLICE

Reforme des textes juridiques

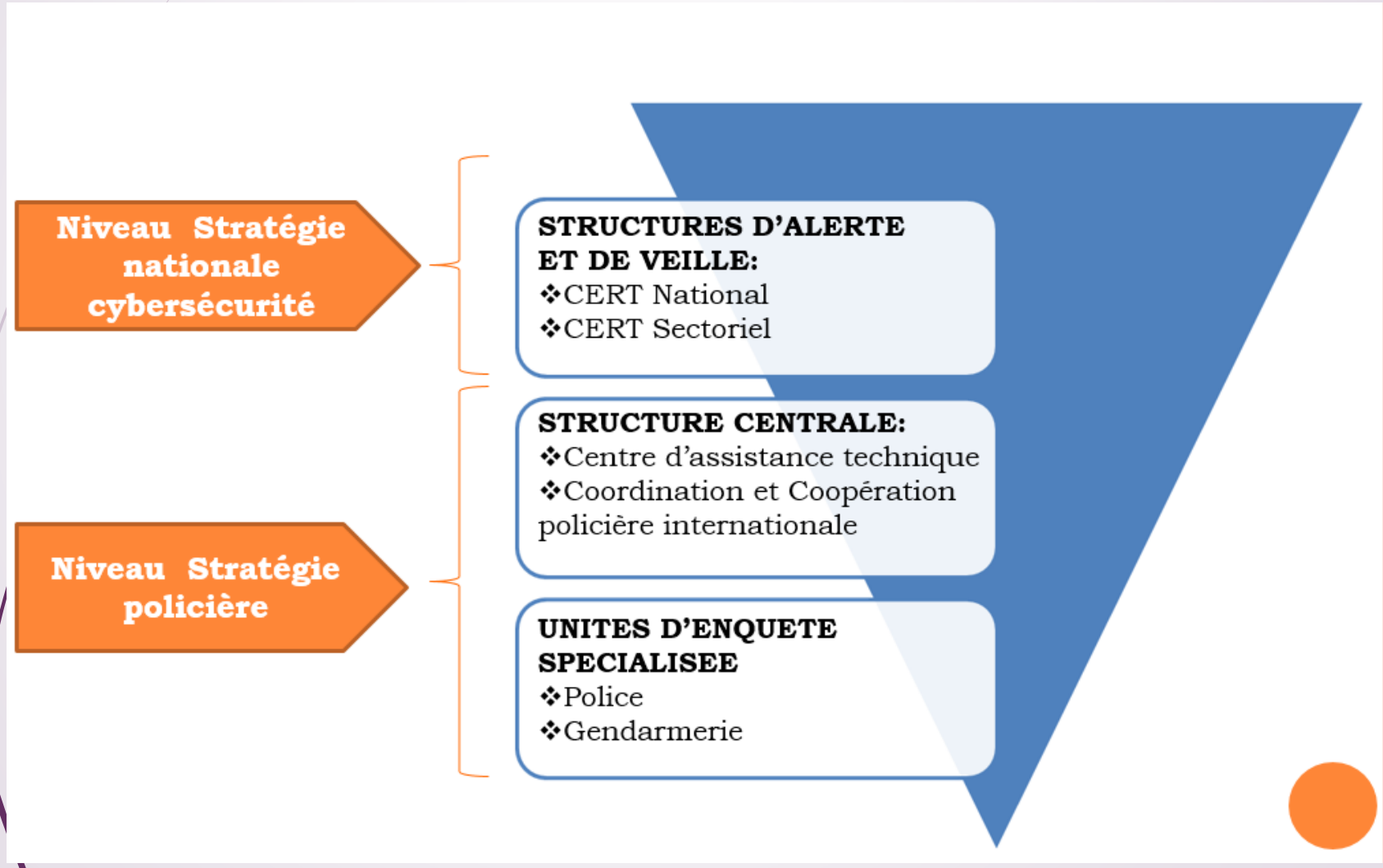
- Textes internes
  - ✓ Loi du 1er juin 2018 portant réglementation générale du renseignement au Burkina
  - ✓ Loi n°044-2019/an du 21 juin 2019 portant modification de la loi n°025-2018/an du 31 mai 2018 portant code pénal
  - ✓ Loi n°025-2018/an du 31 mai 2018 portant Code pénal
  - ✓ Loi n°040-2019/an du 29 mai 2019 portant code de procédure pénale
  - ✓ Loi n° 061-2008/AN du 27 novembre 2008 portant réglementation générale des réseaux services de communications électroniques au Burkina Faso
  - ✓ Loi n°010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel

VI. CYBERPOLICE

Reforme des acteurs



VI. CYBERPOLICE



VII. CONCLUSION

NECESSITE D'UNE REPONSE GLOBALE ET COORDONNEE

VII. CONCLUSION

- Les TIC sont facteurs de développement
- Leur expansion s'accompagne de nouveaux dangers
- La cybercriminalité est une menace réelle
- Elle pose de nombreux défis aux systèmes de sécurité et à la justice pénale
- L'adaptation des textes juridiques au plan sous-régional et international
- Consolidation des structures spécialisées
- L'acquisition de moyens d'investigations
- La sensibilisation

MERCI POUR VOTRE AIMABLE ATTENTION!