Relever les defis juridiques de la CyberSecurité en AFRIQUE

Auguste Yankey, African Union Commission

African Union

RELEVER LES DEFIS JURIDIQUES DE LA CYBERSECURITÉ EN AFRIQUE

APERCU

I. QUELQUES CHIFFRES

II. POURQUOI LE CYBERSPACE EN AFRIQUE EST-IL PARTICULIEREMENT VULNÉRABLE?

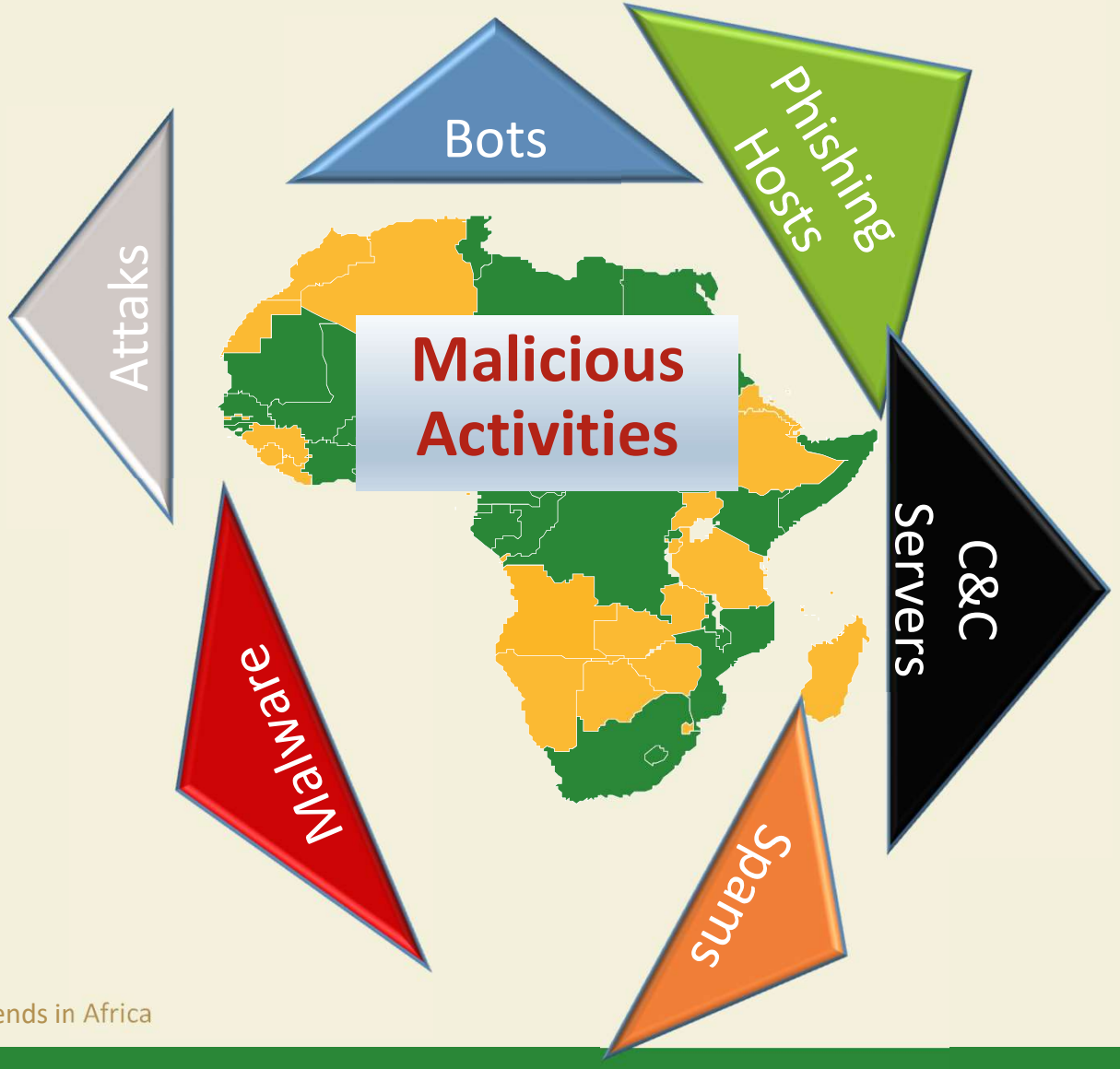
III. comment l'Union Africaine s'adresse-t-elle à cette vulnérabilité: LES INITIATIVES DE L'UA POUR RELEVER LE DEFIS DE LA CYBERSECURITE EN AFRIQUE

IV. CONCLUSION

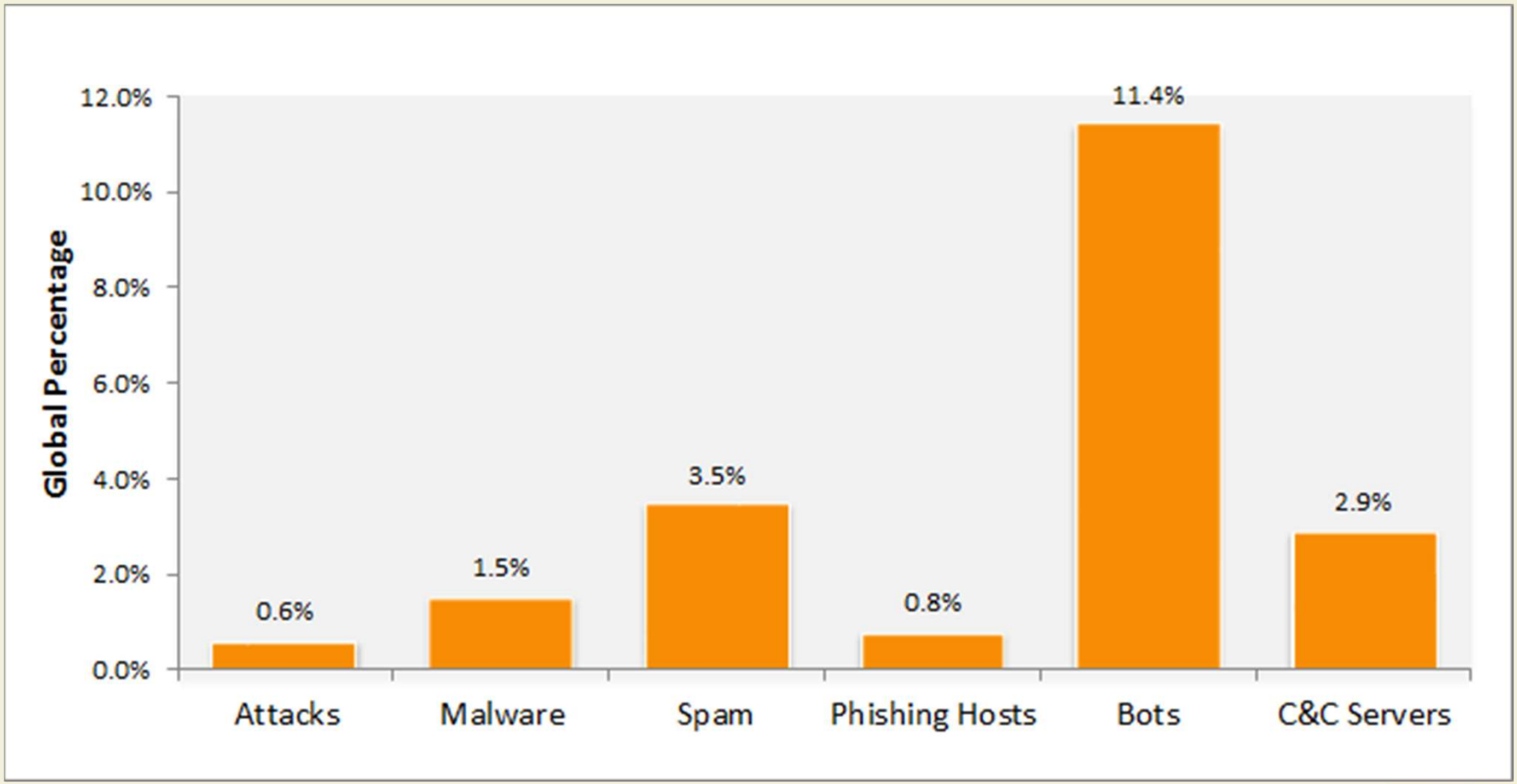
I: Quelques Chiffres

- **La Société de l'Information en Afrique: Manque de Base legale, source d'insecurité et d'inconfort**
  - **Economique** (Afrique reste le continent le plus rapide en terme de developpement de "mobile banking" and M-money Ex.. Orange Money, M-Pesa ...)
  - **Sociétal** Les experts en cybersécurité estiment que **80%** des PC sur le continent africain sont infectés par des virus et d'autres logiciels malveillants. Un rapport de Symantec révèle qu'en 2012, le nombre de cyberattaques ciblées en Afrique a **augmenté de 42%.**
  - **Infractions** (La cybercriminalité en Afrique croît plus vite que sur tout autre continent Ex. **4 pays parmi les 10** premiers pays avec une forte prévalence de la cybercriminalité sont Africains)
  - **L'Afrique est le continent le plus émergent en termes de développement des infrastructures et de concurrence sur le marché** ... mais aucune garantie de meilleurs services, accès et coûts sans des politiques et cadres règlementaires favorables

Telemetrie Symantec: cyberactivité malveillante en Afrique



Activité malveillante originaire d'Afrique



Tableaux de données sur les activités malveillantes

Les 10 pays africains sources d'attaques

Pays	Rang africain	Pourcentage	Compteur d'incident
South Africa	1	**25%**	314,880
Egypt	2	**12%**	149,685
Kenya	3	**9%**	106,265
Nigeria	4	**7%**	89,100
Mauritius	5	**6%**	73,134
Algeria	6	**5%**	60,381
Seychelles	7	**4%**	45,661
Botswana	8	**3%**	37,880
Morocco	9	**3%**	34,464
Tunisia	10	**3%**	32,187

II: Pourquoi le Cyberspace en Afrique est-il Vulnérable?

- ✓ Faible niveau de sensibilisation à la cybersécurité
- ✓ Manque de financement approprié
- ✓ Absence de volonté du gouvernement et des autres parties prenantes de lutter contre la cybercriminalité
- ✓ compétences rares en cybersécurité

II: Pourquoi le Cyberspace en Afrique est-il Vulnérable?

Résultat de l'enquete sur les tendances de la cybersécurité et la cybercriminalité en Afrique

- Le processus a débuté en octobre 2015. Un lien sur l'enquête a été créé sur le site Web de la CUA et envoyé à tous les États membres de l'UA par les voies officielles ainsi que par le biais de la communauté technique.
- 32 pays ont fourni leur réponse, ce qui représente 60%

Stratégie nationale sur la cybersécurité	**08**
CERT National	**13**
Lois sur la protection des données à caractère personnelles	**14**
Lois sur la cybercriminalité	**12 (+ 12 partiellement)**
Campagne de sensibilisation, Education sur la cybersécurité	**13**

II: Pourquoi le Cyberspace en Afrique est-il Vulnérable?

L'état de la legislation en cybercriminalité en Afrique

Ayant une législation sur la cybercriminalité en place	Ayant une législation sur la cybercriminalité partiellement mise en place	Ayant des projets de loi	Aucune disposition légale spécifique sur la cybercriminalité en application
12	12	15	30
Botswana	Algeria	Burkina Faso	
Cameroon	Benin	Djibouti	
Cote d'Ivoire	Gambia	Ethiopia	
Ghana	Kenya	Guinea	
Mauritania	Madagascar	Lesotho	
Mauritius	Morocco	Mali	
Nigeria	Mozambique	Morocco	
Senegal	Rwanda	Namibia	
Tanzania	South Africa*	Niger	
Uganda	Sudan	South Africa	
Zambia	Tunisia	Swaziland	
Chad	Zimbabwe	Togo	
Guinée - Conakry		Tunisia	
		Zimbabwe	
		Kenya	

III: Les Initiatives de l'UA pour relever les défis de la Cyber sécurité en Afrique

S'attaquer à la cybersécurité fait appelle à **une volonté politique** claire de :

➔définir et de mettre en œuvre **une stratégie de développement de l'infrastructure et des services numériques** (services électroniques) et

➔d'élaborer **une stratégie de cybersécurité multidisciplinaire** cohérente, efficace et contrôlable

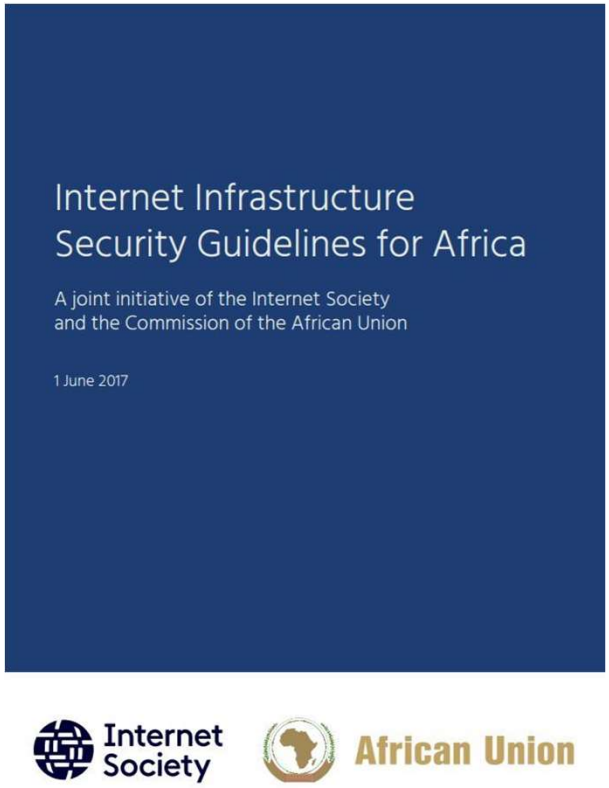
➔ d'entraide mutuelle par **une cooperation internationale** dans la lutte contre la cybercriminalité

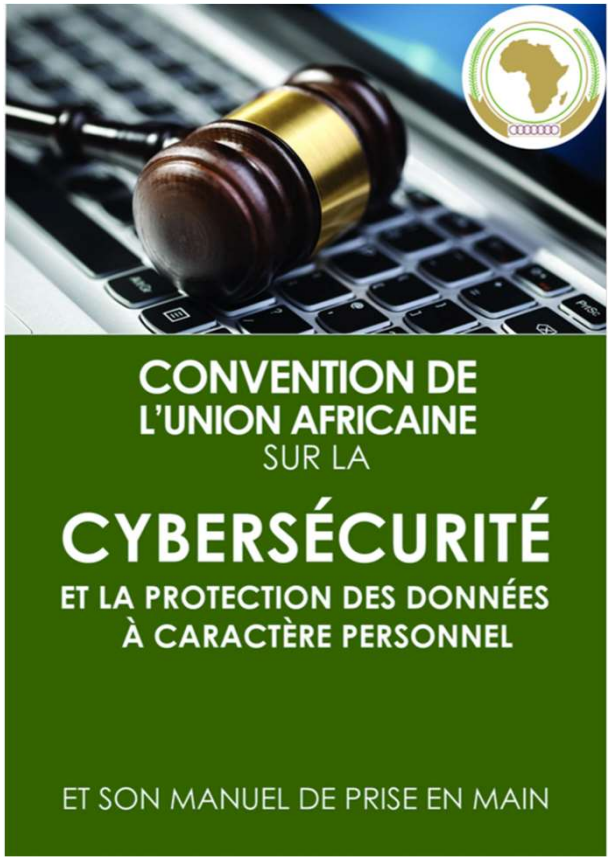
African Union

III: Les Initiatives de l'UA pour relever les défis de la Cyber sécurité en Afrique

UEMOA: ATELIER REGIONAL SUR LE COMMERCE ELECTRONIQUE
Ouagadougou, Burkina Faso, 9-11 octobre 2018

Ouagadougou, 9-11 Oct. 2018





https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

https://www.internetsociety.org/wp-content/uploads/2017/08/AfricanInternetInfrastructureSecurityGuidelines_May2017.pdf

https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

IV: Conclusion: Recommendations

➢ Regional (niveau de l'UA)

1. Former un comité de coordination et de collaboration de la cybersécurité à l'échelle continental
2. S'engager dans le renforcement des capacités et le partage des connaissances à un niveau panafricain

➢ Niveau National

1. Identifier et protéger l'infrastructure Internet critique
2. Faciliter l'échange d'informations par le biais de la structure multipartite nationale
3. Établir et renforcer les équipes nationales de réponse aux incidents de sécurité informatique (CSIRT)
4. Promouvoir la résilience de l'infrastructure Internet grâce aux points d'échange Internet (IXP)
5. Utiliser les institutions publiques pour donner l'exemple en matière de cybersécurité

IV: Conclusion: Recommendations

➢ Regional (niveau de l'UA)

1. Former un comité de coordination et de collaboration de la cybersécurité à l'échelle continental

2. S'engager dans le renforcement des capacités et le partage des connaissances à un niveau panafricain

IV: Conclusion: Recommendations

➢ Niveau National

1. Identifier et protéger l'infrastructure Internet critique
2. Faciliter l'échange d'informations par le biais de la structure multipartite nationale
3. Établir et renforcer les équipes nationales de réponse aux incidents de sécurité informatique (CSIRT)
4. Promouvoir la résilience de l'infrastructure Internet grâce aux points d'échange Internet (IXP)
5. Utiliser les institutions publiques pour donner l'exemple en matière de cybersécurité

➢ Au niveau FAI/Operateur

1. Établir une sécurité de base (solution technique)
2. Établir et maintenir la coopération et la collaboration

➢ Au niveau Organisationnel

1. Designer un Leader exécutif comme le Champion TIC de l'organisation pour insuffler **une culture de la cyber securité** au sein de l'organisation

➢ Niveau Cooperation Mondiale

1. Établir une forte coopération internationale et
2. Mettre en place une collaboration transfrontalière

***

MERCI POUR VOTRE ATTENTION

***

Auguste YANKEY (Mr.)
AU Commission
Email: yankeyka@africa-union.org
Website: www.AU.int