2023

FORUM NATIONAL SUR LA GOUVERNANCE DE L'INTERNET AU BURKINA FASO

10ème édition

Thème :

Souveraineté numérique et cybersécurité au Burkina Faso

RAPPORT GENERAL

10ère édition

FORUM NATIONAL SUR LA GOUVERNANCE DE L'INTERNET AU BURKINA FASO

Thème :

Souveraineté numérique et cybersécurité au Burkina Faso

RAPPORT GENERAL

Novembre 2023

SOMMAIRE

AVANT-PROPOS 3

1. A PROPOS DE L'INITIATIVE POUR LA GOUVERNANCE DE L'INTERNET AU BURKINA FASO (IGF-BF) 4

2. PARTENAIRES DE LA 10ème EDITION DU FGI AU BURKINA FASO 5

3. CONTEXTE GENERAL DE LA SOUVERAINETE NUMERIQUE ET DE LA CYBERSECURITE AU BURKINA FASO 5

4. OBJECTIFS DU FORUM 6

5. DEROULEMENT DU FORUM 6

5.1. L'Ecole sur la Gouvernance de l'Internet (EGI) 6

5.2. Le forum public 7

6. RESUMES DES ECHANGES 10

6.1. Technologies émergentes et enjeux de la gouvernance de l'Internet 10

6.2. Souveraineté numérique du Burkina Faso : sur quels leviers actionner ? 12

6.3. Identification des ressources sur Internet : La fonction DNS 13

6.4. Les indicateurs de l'UNESCO sur l'universalité de l'internet 14

6.5. Cybersécurité : Quelles mesures de protection du cyberespace national burkinabè ? 15

6.6. Réseaux sociaux et comportement cybercitoyen : les dix conseils du CSC 16

6.7. Cybercriminalité : Retour d'expériences de la BCLCC au niveau national 17

6.8. Vie privée à l'ère des réseaux sociaux 19

7. POINTS CLES ET RECOMMANDATIONS DU FORUM 20

7.1. POINTS CLES 20

7.2. RECOMMANDATIONS ..... **Erreur ! Signet non défini.**

8. CONCLUSION 21

9. REMERCIEMENTS 22

AVANT-PROPOS

C'est avec un grand plaisir et un sens de responsabilité que nous présentons le rapport général du Forum national sur la gouvernance de l'Internet au Burkina Faso, axé sur le thème crucial de la "Souveraineté numérique et cybersécurité". Organisé dans un contexte où les défis liés à la sécurité numérique sont plus prégnants que jamais, ce forum a rassemblé des acteurs de divers horizons pour débattre, échanger et proposer des perspectives novatrices en vue de renforcer la posture du Burkina Faso dans le domaine de la cybernétique.

La question de la souveraineté numérique est devenue une préoccupation majeure pour les États, les entreprises et les citoyens. Dans un monde de plus en plus interconnecté, où les frontières numériques s'effacent, la protection des données, la gestion sécurisée des réseaux et la garantie de la confidentialité des informations sont des enjeux cruciaux pour la sécurité nationale et le développement socio-économique.

Durant ce forum organisé par l'Initiative pour la Gouvernance de l'Internet au Burkina Faso (IGF-BF), des experts, des décideurs politiques, des représentants du secteur privé et de la société civile ont partagé leurs connaissances, leurs expériences et leurs recommandations pour renforcer la souveraineté numérique du Burkina Faso. Les échanges fructueux et les débats constructifs ont permis d'identifier des pistes d'action et des orientations stratégiques pour relever les défis de la souveraineté en toute cybersécurité.

Ce rapport est le fruit de ces riches contributions. Il vise à synthétiser les idées émises, les propositions avancées et les solutions suggérées lors du forum. Il se veut un outil précieux pour les décideurs, les acteurs de la société civile, les entreprises et tous ceux engagés dans la promotion d'un espace numérique sécurisé et souverain pour le Burkina Faso.

Nous exprimons notre gratitude à tous les participants pour leur engagement et leur contribution à la réussite de cet événement. Nous espérons que les recommandations présentées dans ce rapport serviront de base solide pour des actions concrètes visant à renforcer la souveraineté numérique et la cybersécurité au Burkina Faso.

Bonne lecture et que ce document soit source d'inspiration et de mobilisation pour des initiatives futures visant à garantir un Internet sûr, ouvert et respectueux des droits de tous.

Bureau exécutif de l'Initiative pour la Gouvernance de l'Internet au Burkina Faso (IGF-BF)

1. A PROPOS DE L'INITIATIVE POUR LA GOUVERNANCE DE L'INTERNET AU BURKINA FASO (IGF-BF)

L'Association Initiative pour la Gouvernance de l'Internet au Burkina Faso (IGF-BF) est une Association Burkinabè à but non lucratif et apolitique, créée le 11 avril 2017. Régie par la Loi N°064-2015/CNT du 20 octobre 2015 relative à la liberté d'association au Burkina Faso, elle a été officiellement reconnue le 24 mai 2017 sous le récépissé de déclaration d'existence **N°00000173601.**

IGF-BF a été mise en place sous l'égide de l'organisation mondiale « Internet Governance Forum » (IGF) pour contribuer à l'harmonisation des positions du secteur public, du secteur privé et de la société civile sur le développement de l'accès et la gouvernance de l'Internet au Burkina Faso. A ce titre, elle poursuit naturellement la même vision que l'organisation mondiale IGF tout en supportant et adhérant à toutes ses initiatives.

- **Mission :**

IGF-BF a pour mission de fournir un cadre et une structure durable pour un Forum national qui engage l'ensemble des parties prenantes à savoir : Le secteur privé, le gouvernement, la société civile, les législateurs, le monde universitaire, les ligues des consommateurs et tout utilisateur dans un débat national stratégique sur la gouvernance de l'Internet. Cela afin d'assurer l'essor, le développement ouvert, l'évolution et l'utilisation de l'internet pour le bénéfice de toutes et tous à travers le Burkina Faso.

- **Objectif global :**

L'objectif global de IGF-BF, est d'assurer la promotion d'un Internet inclusif, participatif et au service du développement de l'ensemble des parties prenantes au Burkina Faso.

- **Objectifs spécifiques :**

Plus spécifiquement, elle souhaite :

- Réunir toutes les parties prenantes pour échanger et partager les expériences autour de la promotion de l'utilisation et du développement de l'internet au Burkina Faso ;
- Encourager et promouvoir les environnements réglementaires et les politiques favorisant l'accès, le service universel, la liberté d'expression sur internet et la diversité ;
- Promouvoir les bonnes pratiques sur internet, la sécurité, la protection de la vie privée, la protection des droits de l'homme sur internet, la lutte contre la cybercriminalité ;
- Encourager la participation des Burkinabè aux travaux de l' « Internet Governance Forum » au niveau Ouest africain, africain et mondial et favoriser une participation à tous les projets coopératifs, nationaux ou internationaux, de nature privée ou publique ;
- Favoriser la bonne gestion des ressources internet essentielles (adresses IP, passage de IPV4 à IPv6, serveurs racines, Points d'échange Internet, Registre des noms de domaine du Burkina (.bf), etc..) ;
- Servir de point focal pour les efforts communs de promotion de l'internet et de la gouvernance de l'internet en tant qu'outil de développement ;
- Promouvoir le traitement adéquat des langues nationales e locales Burkinabè sur Internet ;
- Susciter, préparer et participer à toutes réunions et conférences, groupe de travail et commissions formelles ou informelles, ainsi que tout ouvrage et publication, utilisant ou non les moyens électroniques, notamment internet, conformes à son objet social ;
- Entreprendre toutes activités allant dans le sens de la création d'un environnement favorable, de la démocratisation de l'accès et d'une manière générale visant à promouvoir Internet au Burkina Faso
- Dynamiser la coopération avec les partenaires nationaux et internationaux, publics et privés poursuivant le même but et les mêmes objectifs ;
- Protéger et informer les utilisateurs de l'internet au Burkina Faso sur leurs droits et devoirs.

- **Moyens d'action**

Pour se faire, les moyens d'action de l'association sont :

- L'organisation régulière d'un forum national sur la gouvernance de l'Internet au Burkina Faso incluant toutes les parties prenantes ;
- La participation régulière au forum régional ouest africain, africain et mondial sur la gouvernance de l'internet ;
- L'organisation et la participation à des colloques, forum, formations, réunions et rencontres au Burkina Faso ou à l'international ;
- La mise en place, la gestion et la participation à des groupes de travail, task force ;
- La réalisation d'études relatives à la gouvernance de l'Internet ;
- L'organisation de débats par voies électronique et physique ;
- Tout autre moyen concourant à l'objet de l'association.

IGF-BF fonctionne autour d'une Assemblée générale, d'un bureau exécutif de 09 membres, d'un secrétariat exécutif et de commissariats aux comptes.

2. PARTENAIRES DE LA 10ème EDITION DU FGI AU BURKINA FASO

Cet événement a bénéficié des soutiens multiformes de plusieurs partenaires (personnes physiques et morales) qui militent pour une souveraineté numérique du pays et un comportement éthique et responsable sur Internet. Ce sont :

- Le Ministre de la Transition Digitale, des Postes et des Communications Électroniques (MTDPCE), assurant la présidence du Forum ;
- L'Autorité de régulation des Communications électroniques et des postes (ARCEP), parrain du Forum
- L'Assemblée Législative de Transition (ALT) du Burkina Faso, donatrice ;
- L'Association Burkinabè des Domaines Internet (ABDI) ;
- L'Association YAM-PUKI.

3. CONTEXTE GENERAL DE LA SOUVERAINETE NUMERIQUE ET DE LA CYBERSECURITE AU BURKINA FASO

Au Burkina Faso, comme dans de nombreux pays, la question de la souveraineté numérique et de la cybersécurité revêt une importance croissante, dictée par l'évolution rapide des technologies de l'information et de la communication dans divers domaines.

- **Infrastructures numériques et connectivité** : Le pays a connu une expansion significative des infrastructures numériques au cours des dernières années, avec une augmentation de l'accès à Internet et une croissance des utilisateurs de téléphones mobiles. Cependant, cette avancée s'accompagne de défis en termes de sécurité et de protection des données.
- **Défis de cybersécurité** : Comme ailleurs, le Burkina Faso fait face à des défis de cybersécurité, allant des attaques de logiciels malveillants aux cyberattaques ciblées contre des institutions publiques ou privées. Ces menaces mettent en péril la confidentialité des données, l'intégrité des systèmes et peuvent impacter la stabilité économique et sociale du pays.
- **Protection des données à caractère personnel et confidentialité** : La protection des données personnelles est une préoccupation majeure, notamment dans un contexte où la numérisation des services gouvernementaux et commerciaux s'accélère. Garantir la confidentialité des informations tout en favorisant l'innovation et le développement numérique représente un défi de taille.
- **Cadre réglementaire et gouvernance** : L'existence d'entité telles que l'ANSSI, la BCLCC, la CIL et le CSC contribue à la mise en place d'un cadre réglementaire solide et adapté aux réalités du numérique.
- **Formation et sensibilisation** : Renforcer les compétences dans le domaine de la cybersécurité, tant au niveau individuel qu'institutionnel, demeure crucial. Il en est de même pour la sensibilisation du public sur les bonnes pratiques en matière de sécurité informatique et la formation de professionnels spécialisés sont des axes prioritaires.
- **Coopération internationale** : Le Burkina Faso fournit des efforts pour participer aux initiatives régionales et internationales visant à renforcer la sécurité numérique et à lutter contre la cybercriminalité. Toutefois, cette participation reste en deçà des attentes des organisateurs de différents évènements tels que les Fora Ouest africain, africain et mondial sur la Gouvernance de l'Internet (IGF).

Le contexte actuel du Burkina et de la région du Sahel est marqué par la situation sécuritaire liée à l'hydre terroriste, la montée en puissance des réseaux sociaux avec des discours haineux et du cyber activisme, la hausse du nombre des cas d'escroqueries et de cybercriminalité,

etc. Le pays cherche donc à consolider sa souveraineté numérique en développant des politiques et des stratégies adaptées, tout en favorisant l'innovation et le développement économique dans un environnement numérique sécurisé.

Les axes de développement de la souveraineté numérique du Burkina Faso, les enjeux de la dépendance aux technologies étrangères et les initiatives visant à développer des solutions locales méritent d'être discutés de façon soutenue afin que les différentes parties prenantes puissent, non seulement, être éclairées mais aussi être sensibilisées sur l'ensemble de ces sujets.

Plusieurs questions nos interpellent :

- Quels sont les enjeux et les leviers d'une souveraineté numérique assumée ?
- Quels sont les droits et devoirs du citoyen sur Internet ?
- Quel est l'état actuel et les perspectives en matière de réglementation du cyber activisme ?
- Quels rôles les réseaux sociaux peuvent jouer pour la promotion du civisme ?

4. OBJECTIFS DU FORUM

Cette 10ème édition du Forum sur la gouvernance de l'Internet s'est voulu être un tremplin pour le pays, un cadre ouvert et inclusif pour recueillir les idées et favoriser les débats sur les enjeux de politiques publiques liées aux questions de souveraineté numérique et cybersécurité.

Les objectifs poursuivis par ce forum sont :

- Réunir l'ensemble des parties prenantes nationales autour du thème du forum afin d'engager un débat national autour de la thématique de l'édition ;
- Formuler des recommandations pertinentes pour le Burkina Faso et pour la sous-région ouest africaine relativement au thème du forum ;
- Sensibiliser et renforcer les capacités des parties prenantes sur la notion de Gouvernance de l'Internet et susciter l'intérêt du public sur le sujet ;
- Recenser les nouvelles questions et préoccupations liées à l'accès et à l'usage de l'Internet au Burkina Faso afin de les porter à l'attention des organes compétents.

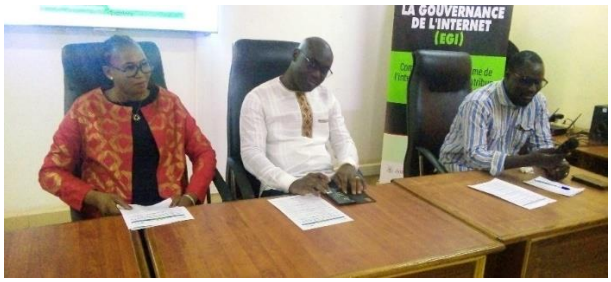
5. DEROULEMENT DU FORUM

La 10ème édition de forum national, tenu le 17 novembre 2023, a été précédé par la troisième édition de l'Ecole sur la gouvernance de l'Internet (EGI) dont la première session a été organisée à Ouagadougou du 08 au 10 novembre 2023 dans la salle de formation du siège de l'Association YAM-PUKRI.

5.1. L'Ecole sur la Gouvernance de l'Internet (EGI)

Organisée en prélude du Forum national, L'EGI a été une session de formation de trois (03) jours ayant regroupé trente-cinq (35) stagiaires dont l'âge varie entre 20 et 35 ans. Le thème de cette session était : Thème « ***Conception et mise en œuvre des principes, des normes, des règles, des procédures, des prises de décision et des programmes qui définissent l'évolution et l'utilisation de l'internet*** ».

Après la cérémonie d'ouverture en présence du président de l'Association YAM-PUKRI qui a hébergé cette formation à son siège, le programme des trois jours a débuté par la présentation et motivation des stagiaires.

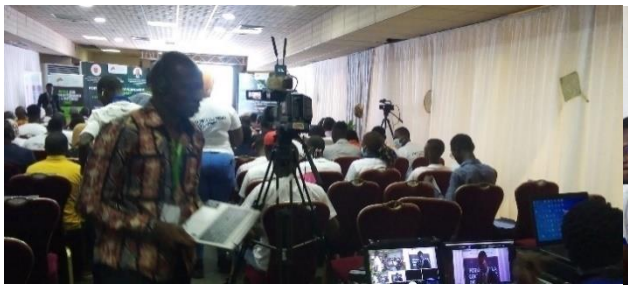
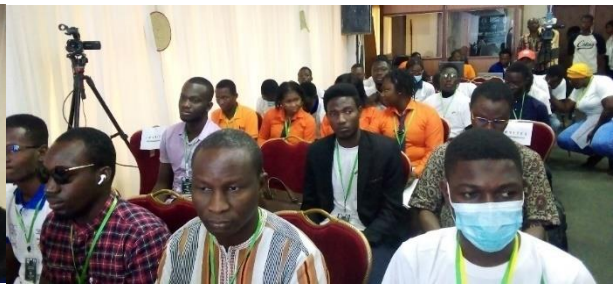


Cette formation, dispensée entièrement par des formateurs de IGF, a consisté à sensibiliser et renforcer les capacités des participants sur les questions essentielles de la gouvernance de l'Internet selon le programme ci-dessous :

Jours	Modules	Formateurs
Jour 1 Mercredi 08/11/2023	Introduction à la Gouvernance de l'Internet	M. Drissa DEGNE
	Cartographie des enjeux, des acteurs et des forums de prise de décision de la gouvernance de l'Internet	M. Sidiki NANA
	Aspects liés à l'infrastructure de la gouvernance de l'Internet	M. Elysée G. KIEMDE
Jour 2 Jeudi 09/11/2023	Cyber sécurité et Gouvernance de l'Internet	M. Drissa DEGNE
	Aspects du développement de la gouvernance de l'internet	M. Romain TRAORE
	Aspect socioculturel de la gouvernance de l'Internet	M. Romain TRAORE
	Aspects juridiques de la gouvernance de l'Internet	M. Charles BAZIE
	Droits et Gouvernance de l'Internet	M. Charles BAZIE
Jour 3 Vendredi 10/11/2023	Acteurs de la gouvernance de l'Internet	M. Hermann OUEDRAOGO
	Stratégies pour une position régionale commune	M. Hermann OUEDRAOGO
	Travaux pratiques et exposés de groupes : Mise en situation, jeu de rôle des acteurs	M. Hermann OUEDRAOGO

5.2. Le forum public

Tenu le 17 novembre 2023, en mode hybride, virtuel sur Zoom et présentiel dans la salle B2 du Centre international de Conférences de Ouaga2000, à Ouagadougou, capitale du Burkina Faso, cette dixième édition du forum national sur la gouvernance de l'Internet au Burkina Faso avait pour thème central : « Souveraineté numérique et cybersécurité au Burkina Faso». Cet événement important destiné au grand public, a regroupé plus de cent soixante (160) participants provenant de toutes les couches sociales.

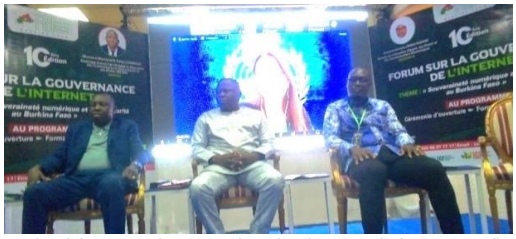
Ce forum a enregistré une grande participation et la présence effective des autorités aussi bien du Burkina Faso que d'autres pays qui ont toutes pris la parole pour encourager et exposer leurs points de vue sur le thème central. Ce sont :

- **Dr Aminata ZERBO/SABANE**, Ministre de la Transition Digitale, des Postes et des Communications Électroniques (MTDPCE) du Burkina Faso, présidente de la cérémonie ;

- **M. Patrice Wendlassida COMPAORE**, secrétaire exécutif de l'Autorité de régulation des Communications électroniques (ARCEP), parrain de la cérémonie ;
- **M. Kisito TRAORE**, Secrétaire général du MTDPCE ;
- **M. Michaël G. L. FOLANE**, Chargé de missions au MTDPCE ;
- Mesdames et Messieurs les Directeurs Généraux et centraux de l'administration publique ;
- Mesdames et Messieurs les représentants du secteur privé, de la société civile, des universités et instituts d'enseignement et de recherche, ...

Au titre des personnalités d'autres pays, on peut citer :

- **M. Alhamdou Ag ILYENE** : Ministre de la Communication et de l'Economie numérique de la **République du Mali** ;
- **M. Sidi Mohamed RALIOU** : Ministre de la Communication, des Postes et de l'Économie numérique de la **République du Niger** ;
- **Mme Anja GENGO**, Coordinatrice Global IGF, en ligne depuis Washington (Etats-Unis) ;
- **Mme Mary UDUMA**, coordonnatrice du WAIGF, en ligne depuis Abuja (Nigeria) ;
- **Amessimou KOSSI**, IGF Bénin ;
- **M. Abdeljalil BACHAR BONG**, IGF Tchad.



Présidium de la cérémonie d'ouverture : (de gauche à droite) M. Michaël FOLANE, Conseiller Technique représentant Mme le Ministre en charge de la Transition Digitale, -M. Patrice COMPAORE, secrétaire exécutif de ARCEP et M. Hermann OUEDRAOGO, Président de IGF-BF

Les trois (03) ministres de l'Alliance des Etats du Sahel (AES) en charge du Numérique

Dr Aminata ZERBO/SABANE, Ministre de la Transition Digitale, des Postes et des Communications Électroniques (MTDPCE) du **Burkina Faso**, Présidente de la cérémonie.

M. Sidi Mohamed RALIOU, Ministre de la Communication, des Postes et de l'Économie numérique / **Niger**

M. Alhamdou Ag ILYENE, Ministre de la Communication de l'Economie numérique / Mali

Mme Anja GENGO, Coordonnatrice Global IGF

M. Kisito TRAORE, SG du MTDPCE / **Burkina Faso**

Cette plénière s'est déroulée en 3 étapes : Une cérémonie officielle d'ouverture, deux panels suivis de questions - réponses et une cérémonie de clôture.

- **La cérémonie officielle d'ouverture.**

La cérémonie officielle d'ouverture des travaux a été marquée par 03 interventions :

- ***Mot de bienvenue du Président de IGF-BF*** : M. Hermann OUEDRAOGO a remercié les autorités pour leur présence effective à cette cérémonie qui témoigne de leur intérêt pour le thème de la souveraineté et la cybersécurité au Burkina Faso.

Après avoir expliqué la pertinence du thème, il a fait une mention spéciale aux partenaires ainsi que les parrains qui ont permis l'organisation de cet évènement.

- ***Allocution du parrain*** **:** Le parrain du Forum national, M. Wendlassida Patrice COMPAORE, Secrétaire exécutif de l'Autorité de régulation des Communications électroniques et des postes (ARCEP) s'est félicité du thème choisi qui entre droite en ligne avec a mission de son institution. Honoré de voir rassemblés des acteurs clés du secteur des technologies de l'information et de la communication, il a exhorté les participants à « façonner un avenir numérique inclusif, éthique et prospère pour notre nation..., en ces moments difficiles sur le plan sécuritaire. »
- ***Discours d'ouverture officielle de la présidente de la Cérémonie*** **:** Le discours de Mme le Ministre de la Transition Digitale, des postes et des communications électroniques a été lu par le Chargé de missions, M. Mickaël G. L. FOLANE. Dans son discours, la présidente de la cérémonie a tenu à relever l'importance du thème de ce forum consacré à la souveraineté numérique et cybersécurité. Précisant que « la souveraineté numérique est bien plus qu'une simple question de contrôle », la Ministre a indiqué que « Dans notre monde interconnecté et hautement numérisé, la question de la souveraineté numérique et de la cybersécurité est devenue un impératif national pour chaque État ». « Le Burkina Faso, conscient de ces enjeux, s'engage résolument à garantir une présence souveraine et sécurisée sur la scène numérique mondiale » a-t-elle confié.

- **Les panels de discussions**

De manière pratique, après la cérémonie d'ouverture officielle, deux panels ont été organisés autour de plusieurs sous thématiques en lien avec la question de souveraineté numérique et la cybersécurité au Burkina Faso (Cf. tableau ci-dessous).

PANELS	THEMATIQUES	PANELISTES	MODERATEURS
Panel 1	Enjeux et perspectives de la gouvernance de l'Internet : état des lieux des questions émergentes	**Secretariat Général /IGF-BF**: M. Drissa DEGNE	**Mme Emelie MAIGA/BARRO,** Spécialiste en transformation digitale en Direction Générale des Systèmes d'information du Ministère de l'Economie, des finances et de la prospective
	Souveraineté numérique du Burkina Faso : sur quels leviers actionner ?	**Représentant ARCEP** : M. Antoine YAMEOGO	
	Identification des ressources sur Internet : La fonction DNS	**Représentant ABDI** : M. Guy Edouard BOUDA	
	Indicateurs de l'UNESCO sur l'universalité de l'internet	**Représentant UNESCO** : M. Guy Hermann BAZEMO	
Panel 2	Cybersécurité : Quelles mesures de protection du cyberespace national burkinabè ?	**Représentant ANSSI** : M. Guestaba L. Arnaud SAVADOGO	**M. Ounteni T. Cyrille OUOBA**, Ingénieur de conception en génie Informatique et spécialiste en digitalisation, Promoteur de DIGTOUN (Site d'apprentissage des langues nationales par Internet)
	Réseaux sociaux et comportement cybercitoyen : les dix commandements du CSC	**Représentant du CSC** : Daniel BONZI	
	Cybercriminalité : Retour d'expériences au niveau national	**Représentant du BLCC** Moussa Christian ZONGO	
	Vie privée à l'ère des réseaux sociaux	**Représentant CIL** Mme Rasmata COMPAORÉ / TIENDREBEOGO	

- **La cérémonie de clôture**

La clôture du forum s'est déroulée en deux (02) étapes : la remise des attestations aux stagiaires de la 1ère session de la 3è édition de l'Ecole sur la gouvernance de l'Internet (EGI) et le mot de remerciement du Président IGF-BF.

C'est à la cérémonie de clôture du Forum que les 35 stagiaires ont reçu leurs attestations de formation des mains des autorités présentes, des panélistes ainsi que des partenaires de l'évènement. Une photo de famille des stagiaires a mis fin à cette séquence.

Satisfaits des connaissances acquises la semaine dernière au cours des trois (03) jours de formation, le porte-parole des stagiaires, a tenu magnifié l'organisation de cet évènement et à remercier IGF-BF pour l'opportunité qui leur a été offerte. Il a, au nom de ses promotionnaires, dit être prêt à servir d'ambassadeurs de la gouvernance de l'internet.

En réponse à cette doléance, le président de IGF-BF, a, dans son mot de clôture, invité les stagiaires à rejoindre les activités de IGF pour encore mieux apprendre afin d'être de bons ambassadeurs. Le président a terminé son intervention clôture par des remerciements renouvelés aux autorités administratives, aux parrains, aux panélistes, aux organisateurs et à tout le public pour la forte mobilisation et la participation active lors des débats.

6. RESUMES DES ECHANGES

Les échanges de ce forum ont été conduits autour de deux (02) panels, des interventions diverses, notamment celles des ministres en charge du numérique de l'Alliance des Etats du Sahel (AES), des experts du domaines et des questions réponses du grand public. Le résumé des échanges s'établit comme suit :

6.1. Technologies émergentes et enjeux de la gouvernance de l'Internet

La gouvernance de l'internet apparait depuis longtemps comme un mot-valise incluant différentes problématiques à la fois politique, culturelle et technique. Les questions qui y sont liées sont disparates. Depuis lors des enjeux historiques sont toujours de mise :

◎ Les enjeux historiques de la gouvernance de l'Internet

Au nombre des enjeux persistants depuis la création de l'Internet et sa gouvernance, on peut citer :

- La gestion des ressources critiques (l'administration des noms et adresses de l'internet y compris les systèmes de serveurs racines),
- La cybersécurité/Cybercriminalité,
- Les standards techniques,
- La diversité culturelle et linguistique,
- Les droits de propriété intellectuelle.

Outre les enjeux historiques de la gouvernance de l'internet, de nouveaux défis ont vu le jour grâce aux technologies émergentes qui façonnent l'internet et donc sa gouvernance.

◎ Les technologies émergentes

Outre les enjeux historiques de la gouvernance de l'internet, de nouveaux défis ont vu le jour grâce aux technologies émergentes qui façonnent l'internet et donc sa gouvernance. Ce sont entre autres :

- **L'intelligence artificielle** : L'IA soulève des questions sur l'automatisation des décisions en ligne, la responsabilité des algorithmes et les implications éthiques de l'utilisation de l'IA sur Internet. La gouvernance de l'IA est un enjeu clé en termes de « Pouvoir et responsabilité » concernant l'IA générative démocratisée. Comment l'IA générative va-t-elle changer les industries, à la fois positivement et négativement ?

- **Blockchain et cryptomonnaies** : La blockchain continuera à évoluer, non seulement pour les cryptomonnaies, mais aussi pour des cas d'utilisation tels que la gestion de la chaîne d'approvisionnement, la propriété intellectuelle et la sécurité des données. Les technologies de blockchain et les cryptomonnaies soulèvent des questions sur la régulation, la sécurité et la légitimité, ainsi que sur les possibilités de décentralisation de la gouvernance de l'Internet.

- **Cybersécurité renforcée** : La préoccupation majeure est la Gestion continue de l'exposition aux menaces (CTEM). Comment être en sécurité sachant que les cybermenaces continuent de s'intensifier, avec des attaques sophistiquées et des vulnérabilités croissantes. Bien que de nouvelles technologies telles que l'apprentissage automatique pour la détection des menaces et la sécurité quantique sont en développement, la gouvernance de l'Internet doit se concentrer sur des mesures de sécurité plus strictes et une coopération internationale renforcée.

- **Ingénierie des plates-formes de libre-service, Machine Customers, Machine Learning, IoT**, etc. Plus que l'IA, Les technologies d'Informatique quantique et Interface Homme-Machine apporteront plus de puissance pour la résolution des problèmes complexes. C'est par exemple la conception de logiciels tels que FactoryTalk pour des fabrications plus intelligentes. Les machines connectées (Une main d'œuvre connectée) deviennent de plus en plus intelligentes. Avec leur application dans la médecine, l'alimentation, … Comment concilier les comportements des clients humains et des machines (main d'œuvre) ?

◎ Les enjeux actuels de la gouvernance de l'internet

L'évolution de ces technologies émergentes soulève naturellement de nouveaux défis en matière de gouvernance de l'internet qui sont :

- **La désinformation en ligne** : La désinformation et la manipulation de l'opinion publique en ligne sont des problèmes majeurs. La gouvernance de l'Internet doit aborder la désinformation tout en préservant la liberté d'expression.

- **La protection de la vie privée et réglementation des données** : Les préoccupations liées à la vie privée et à la protection des données personnelles restent d'actualité, avec des lois de plus en plus strictes, qui influencent la gouvernance.

- **La géopolitique de l'Internet** : Les tensions géopolitiques, y compris la souveraineté des données et les politiques de censure, continuent d'influencer la gouvernance de l'Internet.

- **La neutralité du Net et gestion du trafic** : Les débats sur la neutralité du Net continuent, avec des questions sur la discrimination du trafic, la gestion

- **La durabilité et Green IT** : Il y'a lieu de protéger l'avenir par la mise en place de technologies durables pour réduire les impacts du numérique qui représente 4% des émissions de gaz à effet de serre dans le monde.

◎ Perspectives de de la gouvernance de l'Internet

Face à ces défis, il existe des perspectives encourageantes en termes de gouvernance pour un internet plus sûr et sécurisé. Il s'agit notamment de :

- L'élargissement de la connectivité à travers le monde,

- Les innovations technologiques en termes du durabilité (Green IT),
- Le renforcement de la cybersécurité,
- L'évolution des modèles économiques,
- Le renforcement de la gestion des ressources critiques par des structures dédiées,
- Le modèle de gouvernance multi-parties prenantes,
- Le renforcement de capacité des acteurs à travers les plateformes d'éducation et de sensibilisation.

6.2. Souveraineté numérique du Burkina Faso : sur quels leviers actionner ?

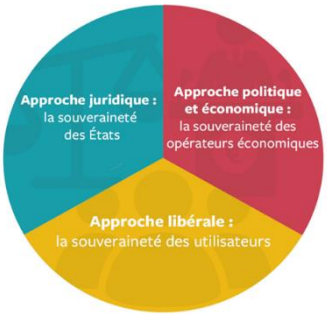
Définitions de la souveraineté numérique

La souveraineté numérique est l'application des principes de souveraineté au domaine des technologies de l'information et de la communication. A ce titre, elle englobe la capacité de l'Etat à :

- Maitriser les infrastructures numériques, c'est-à-dire réseaux, les centres de données et les systèmes d'information,
- Protéger les données, tant les données personnelles que les données sensibles,
- Développer ses propres technologies numériques afin de réduire sa dépendance aux technologies étrangères,
- Réguler le cyberespace afin de garantir la sécurité et la sûreté des infrastructures numériques et des systèmes d'information.

Approches et enjeux de la souveraineté numérique

La souveraineté numérique ne peut s'exercer sans considération des approches juridique, politique et économique et libérale.



Plusieurs enjeux de la souveraineté numérique peuvent être énumérés :

- ***Des enjeux stratégiques***
  - Il faut éviter la fuite des données à l'étranger ;
  - Il est important de conserver une capacité autonome d'appréciation, de décision et d'action ;
  - Il est indispensable de préserver la souveraineté nationale face aux nouvelles menaces générées par la numérisation croissante de la société.
- ***Des enjeux économiques***
  - Aucune société n'est à l'abri de l'espionnage scientifique, économique et commercial. La protection des entreprises et la confidentialité de leurs données sont donc essentielles. D'où l'importance de s'assurer que ces données restent hébergées sur le territoire national (soumises à la législation nationale) ;
  - La souveraineté numérique est aussi un moyen de lutter contre le rachat et l'utilisation des données à des fins commerciales et marketing, sans le consentement des personnes concernées.
- ***Des enjeux politiques***
  - La souveraineté numérique est un moyen pour l'administration et les institutions de redonner confiance aux citoyens, et de participer à leur protection ainsi qu'à la protection de leur vie privée et de leurs données personnelles ;
  - Elle doit également permettre la protection des infrastructures critiques.
- ***Des enjeux de sécurité nationale***

- Cybercriminalité, terrorisme, piratage, manipulation, sabotage, etc., aujourd'hui, la sécurité informatique est devenue un enjeu de sécurité nationale ;
- Les États, les entreprises et les citoyens sont, chaque jour, confrontés à des menaces majeures (usurpation d'identité, fraude sur les transactions monétiques, etc.) ;
- L'un des enjeux majeurs de la souveraineté numérique est donc de rendre le cyberespace plus sûr pour les citoyens comme pour les entreprises et l'État.

◎ **Leviers de souveraineté à actionner au Burkina Faso**

- ***Investir dans la sécurité informatique et former des professionnels de la cybersécurité***
  - Assurer la formation continue des professionnels de la cybersécurité ;
  - Investir dans des technologies de sécurités avancées pour renforcer la protection des infrastructures numériques ;
  - Sensibiliser les utilisateurs finaux à l'importance de la sécurité informatique et les former sur les pratiques de sécurité de base.
- ***Développer des infrastructures numériques Souveraines et des solutions numériques locales***
  - Investir dans des centres de données locaux, des réseaux de fibre optique, des systèmes de stockage de données, et autres éléments clés de l'infrastructure numérique ;
  - Développer des logiciels, des applications, des plateformes et des services qui répondent aux besoins locaux pour encourager l'innovation locale et stimuler l'économie numérique au Burkina Faso ;
  - Inciter les entreprises à choisir les hébergements locaux de leurs données.
- ***Promouvoir l'innovation et l'entrepreneuriat local pour valoriser la création de solutions numériques adaptées***
  - Soutenir l'innovation et l'entreprenariat local, en mettant en place des programmes de financement, des incubateurs d'entreprises et des centres de recherche et développement ;
  - En encourageant l'innovation et l'entreprenariat local, le Burkina Faso peut réduire la dépendance aux technologies étrangères et renforcer sa souveraineté numérique.
- ***Adopter des solutions numériques durables***
  - Investir dans des technologies numériques durables et économes en énergie par la vulgarisation des centrales solaires (ex. : centrale solaire de zagtouli) ;
  - La mutualisation des infrastructures (réseaux, stockage) ;
  - Adopter des politiques de traitement des déchets électroniques.

6.3. Identification des ressources sur Internet : La fonction DNS

◎ **Caractéristiques du nom de domaine**

- Un nom de domaine est un identifiant unique d'une ressource sur internet ;
- La ressource pouvant être une application, un site web, un ordinateur, un smartphone ;
- Le nom de domaine est utilisé pour éviter aux internautes d'avoir à retenir et utiliser des adresses constituées d'une série de chiffres et/ou de lettres complexes ;
- Un nom de domaine devient un élément essentiel de la politique des organisations et est donc un actif important.

◎ **Importance de la fonction DNS pour la souveraineté numérique**

- ***Le système des noms de domaine contribue à la sécurisation du cyberespace à travers ces fonctions :***
  - La construction et l'entretien d'un système de noms de domaine robuste et efficace (critères de sécurité : confidentialité, intégrité disponibilité et traçabilité),
  - L'identification précise des titulaires de noms de domaine (contacts administratifs, technique),
  - L'implémentation de DNSSEC par la signature et la validation,
  - Le filtrage DNS peut permettre de garder les logiciels malveillants ou logiciels malveillants en dehors des réseaux d'entreprises et en dehors d'appareils des utilisateurs. Il peut également contribuer à bloquer certains types d'attaques.
- ***Le système des noms de domaine contribue à la souveraineté numérique à travers :***
  - Le modèle de gouvernance multi-acteurs ;
  - L'opérationnalisation de projets structurants comme la migration vers IPV6, les points d'échanges, les Root Anycast.

◎ **Recommandations :**

- Utiliser exclusivement vos adresses e-mail professionnelles dans le cadre de vos correspondances de service,
- Exiger de vos partenaires une adresse email professionnelle pour vos échanges par messagerie électronique,
- Utiliser l'extension « .BF » pour vos sites web.

6.4. Les indicateurs de l'UNESCO sur l'universalité de l'internet

L'Internet est aujourd'hui le moyen de communication qui bouleverse sans cesse l'accès à l'information, les modes d'expression, ainsi que les nombreux aspects liés à la gouvernance et à la vie économique de tous ses utilisateurs où qu'ils se trouvent. Rendre l'Internet accessible à tous comporte toutefois de nombreux défis, au rang desquels figure la fracture numérique entre les pays développés, les pays en développement et les pays moins avancés, entre les zones urbaines et les zones rurales au sein d'un même pays, entre les personnes ayant des revenus plus élevés ou moins élevés et des niveaux plus élevés ou moins élevés d'éducation et de formation, et entre les femmes et les hommes.

Les opportunités et les risques continueront à croître en complexité et en taille, et ne manqueront pas d'influencer l'avenir vu l'évolution constante de la technologie, des services et des marchés de l'Internet. Il importe de comprendre et d'évaluer la complexité du développement de l'Internet et de son impact si nous entendons l'influencer efficacement et contribuer au mieux à la réalisation des objectifs de développement durable (ODD).

L'UNESCO s'est engagée de longue date dans ce programme, en soulignant le potentiel que renferme l'Internet dans le développement de sociétés du savoir fondées sur la liberté d'expression, l'accès universel à l'information et au savoir, le respect de la diversité culturelle et linguistique et la mise en place d'un programme d'éducation de qualité accessible à tous.

L'UNESCO a donc élaboré le concept d'Universalité de l'Internet en 2013, et adopté en 2015, dont le but est de mieux appréhender son évolution. En effet, l'intégration dans les politiques publiques des questions liées à l'Internet touche des thématiques telles que l'égalité, l'inclusion, les médias et le journalisme, la diversité culturelle, l'éducation de qualité pour tous et la défense des droits humains. Pour ce faire, l'UNESCO a élaboré les principes **DOAM-X**, à partir desquels les indicateurs sont mis en exergues.

◎ **Les principes DOAM X**

Le concept met en lumière quatre principes destinés à former les piliers de la croissance et de l'évolution de l'Internet, et souligne la nécessité de les renforcer à mesure que l'Internet s'immisce toujours plus dans toutes les dimensions de la vie.

D – l'Internet est fondé sur les Droits humains ;

O – il est Ouvert ;

A – il devrait être Accessible à tous ;

M – il est alimenté par la participation de Multiples acteurs.

Le cadre d'indicateurs de l'universalité de l'internet est structuré autour des quatre principes DOAM, auxquels s'ajoutent des indicateurs transversaux (X) qui abordent les questions du genre et les besoins spécifiques des enfants, le développement durable, la confiance et la sécurité ainsi que les aspects juridiques et éthiques de l'internet.

La version finale du cadre d'indicateurs de l'universalité de l'Internet comprend 303 indicateurs, dont 109 indicateurs fondamentaux, répartis en six catégories, 25 thèmes et 124 questions. Aux quatre catégories DOAM s'ajoutent 79 indicateurs transversaux qui abordent les questions d'égalité de genre et les besoins des enfants et des jeunes, le développement durable, la confiance et la sécurité, ainsi que les aspects juridiques et éthiques de l'Internet.

Le cadre est globalement structuré sur la base de cinq catégories, à savoir les quatre principes DOAM auxquels s'ajoute une catégorie d'indicateurs transversaux (X). Chacun des indicateurs DOAMX est subdivisé en thèmes. Les catégories D et A comptent six thèmes, les catégories O et X en comptent cinq, et la catégorie M, trois.

- **Les Indicateurs contextuels :**

IL existe par ailleurs des indicateurs contextuels qui sont :

- Indicateurs économiques
- Indicateurs démographiques
- Indicateurs du développement
- Indicateurs d'égalité
- Indicateurs de gouvernance
- Indicateurs de développement des TIC

Il faut reconnaître que les indicateurs de l'UNESCO sur l'Universalité de l'Internet visent à évaluer les niveaux de réalisation, dans chaque pays, des quatre principes DOAM identifiés comme essentiels à l'Universalité de l'Internet qui soutient un Internet fondé sur les Droits humains (D), qui est Ouvert (O), Accessible à tous (A) et nourri par la participation de Multiples acteurs (M).

6.5. Cybersécurité : Quelles mesures de protection du cyberespace national burkinabè ?

Le cyberespace est considéré comme ayant connu l'évolution la plus rapide de l'histoire de l'humanité. On ne saurait le réduire à l'internet puisque tous les réseaux interconnectés , publics ou privés et quel que soit le moyen de leur interconnexion (fils, fibres, ondes de proximité, ondes satellites) participent du cyberespace.

- **Définition, défis et enjeux de la cybersécurité**

La cybersécurité est l'ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes. Elle peut être également définie comme l'état recherché par un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées et des services connexes que ces systèmes offrent ou qu'ils rendent accessible.

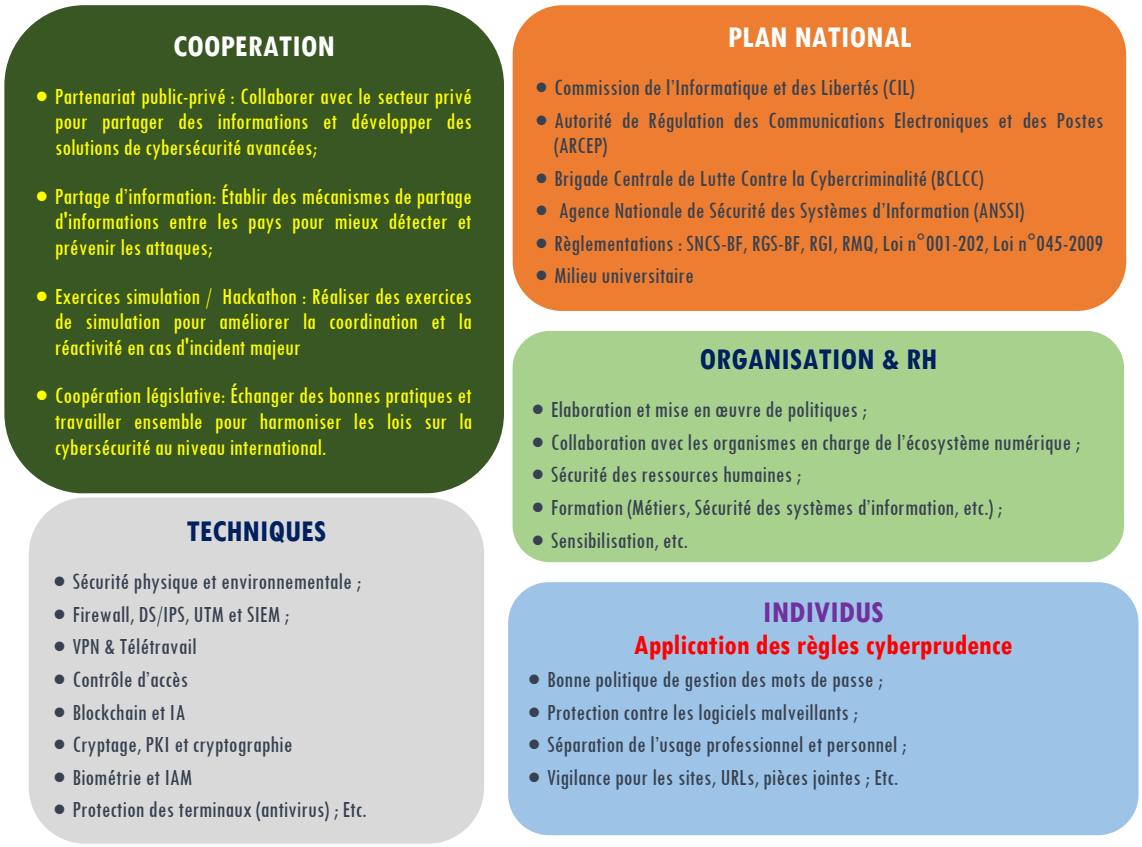
À ce niveau, il faut prendre en compte :

- Le gouvernement (joue un rôle crucial dans la protection du cyberespace national en établissant des politiques et des réglementations),

- Le secteur privé (les entreprises développent des solutions technologiques et mettent en place des mesures de sécurité pour lutter contre les cybermenaces),
- Les utilisateurs (sont également des acteurs importants, car leurs pratiques de sécurité en ligne peuvent avoir un impact significatif).
- Développement technologique : La rapidité des avancées technologiques crée de nouveaux défis pour la cybersécurité.
- Criminalité en ligne: Les cybercriminels sont constamment à la recherche de nouvelles façons de contourner les mesures de sécurité.
- Conflits géopolitiques: La cyberguerre est devenue une réalité, augmentant les risques pour la sécurité nationale.

◎ Mesures gouvernementales

Les mesures gouvernementales sont perceptibles à plusieurs plans :



◎ La cybersécurité est une responsabilité collective

La cybersécurité est un défi croissant dans notre société numérique. En continuant à renforcer nos défenses et à promouvoir la collaboration, nous pouvons protéger notre cyberespace national pour les générations futures.

Aussi, en mettant en place des mesures adéquates pour protéger notre cyberespace national, nous pouvons atténuer les risques et garantir la sécurité de nos individus, de nos organisations et de notre pays.

6.6. Réseaux sociaux et comportement cybercitoyen : les dix conseils du CSC

Il revient de façon récurrente qu'il y a une utilisation irresponsable des plateformes numériques d'une façon générale, dans les réseaux sociaux qui ont de nombreuses conséquences néfastes sur la vie de nos populations. Des individus continuent de publier

des contenus illicites qui se traduisent particulièrement par des manipulations massives : La mésinformation, la désinformation, la mal information, la propagande et le discours de haine en ligne. Pourtant, nul n'est censé ignorer la loi !

Cependant, il est à noter que très souvent cela dénote donc d'une ignorance des populations qui font généralement des publications sans forcément avoir une intention de nuire. La naïveté ou l'inconscience donc des utilisateurs pourraient donc justifier ces différents comportements. D'où la nécessité de mettre un accent particulier sur la sensibilisation à travers une bonne éducation aux médias et au numérique, pour promouvoir des attitudes cyber citoyennes.

Les dix conseils aux citoyens burkinabè pour des comportements responsables sur les réseaux sociaux et dans les émissions d'expression directe

1. Exprimons-nous toujours avec honnêteté. Parlons de ce dont nous avons été nous-mêmes témoin. Parlons des faits que nous connaissons vraiment.
2. Faisons preuve de bon sens et d'esprit critique quand nous recevons des informations sensationnelles surtout si elles émanent de personnes qui ne sont ni liées aux faits, ni professionnelles de l'information.
3. N'approuvons pas, ne relayons pas les messages graves quand nous ignorons la source, les vrais auteurs et leurs intentions, même si l'information nous paraît vraisemblable.
4. Évitons d'indexer une personne, une ethnie, une religion, un groupe spécifique quand il est question de faits graves qui pourraient provoquer des réactions violentes.
5. Évitons l'incitation à la haine, l'apologie de la violence, l'attisement des conflits et la stigmatisation des personnes en raison de leur origine, de leur race, de leur croyance.
6. N'agressons personne dans nos propos. Exprimons notre point de vue avec un effort d'argumentation, dans le respect et la courtoisie.
7. Avant de partager une image, une vidéo ou un audio, vérifions si elle est authentique, si sa source est crédible et si le sens qu'on lui donne à travers les réseaux sociaux correspond bien au contexte dans lequel l'élément a été enregistré.
8. Avant de publier, de partager, de liker ou de commenter, assurons-nous que le message transmis n'est pas interdit par la loi : les informations à caractère confidentiel ou personnel, les opérations sécuritaires, les données militaires, les messages de nature à démoraliser les forces combattantes…
9. Avant de partager, de liker ou de commenter, assurons-nous que le message transmis n'est pas incompatible avec nos convictions et nos ambitions personnelles.
10. Publions, partageons, likons, commentons les contenus qui contribuent au renforcement de la cohésion sociale et à la construction de la paix.

6.7. Cybercriminalité : Retour d'expériences de la BCLCC au niveau national

L'information a une valeur importante pour les particuliers, les entreprises, les États ; on parle aujourd'hui de « guerre de l'information ». Dans ce monde, chaque clic peut-être une opportunité pour un cybercriminel de :

- Gagner de l'argent ;
- Voler, de modifier ou de détruire les données ;
- Espionner des institutions ;
- Déstabiliser un pays, etc.

Chaque année, de centaine de victimes de cybercriminalité sont enregistrées au Burkina et par le monde entier, liées aux piratages des SI, fuites d'informations, social engineering suivi d'escroqueries, ransomwares, etc.

La BCLCC enregistre en moyenne plus de 1500 plaintes par an depuis sa création en 2020.

◎ Qu'est-ce que la cybercriminalité ?

« La cybercriminalité est l'ensemble des infractions pénales en matière informatique ou aux moyens des technologies de l'information et de la communication » : *Code Pénal Burkinabè*

Selon l'ONU, la « cybercriminalité » constitut : « tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique »

◎ Les MENACES récurrentes dans le cyberespace

- Courriels: 679 millions de détections
- Fichiers: 8,2 millions de détections
- Web: 14,3 millions de détections

- ○ Piégeage des pièces jointes / liens
- ○ L'extorsion et l'escroquerie en ligne
- ○ Les campagnes d'escroquerie aux faux ordres de virement (ex : l'escroquerie à la sève de Moringa)
- ○ L'arnaque liée aux ventes et achats en ligne

◎ Les VULNERABILITES / CAUSES

- ○ Vulnérables des produits
  - Médias amovibles mal gérés ;
  - Accès depuis des installations tierces ;
  - Mots de passe par défaut ;
  - Mobilité des équipements non contrôlée ;
  - Sous-traitance non maîtrisée ; ...
- ○ Vulnérabilités humaines et organisationnelles
  - Humaine : manque de vigilance, de discipline, etc.
  - Organisationnelle :
    - Pas d'architecture fonctionnelle des SI ni de périmètre de sécurité défini;
    - Pas de processus métier;
    - Mauvaise gestion des droits;
    - Pas de plan de sauvegarde et de continuité d'activité;
    - Absence de plan de sensibilisation et de formation etc.

Statistiques

- ❑ **2020**: 556 plaintes, 32 personnes déférées, 1 109 323 606 préjudice financier;
- ❑ **2021:** 2 579 plaintes, 38 personnes déférées, 1 016 535 045 préjudice financier;
- ❑ **2022** : 3 028 plaintes, 33 personnes déférées, 1 108 382 906 préjudice financier.
- ❑2023… en cours

◎ Quelques signes d'alerte d'une arnaque pour les transactions en ligne:

- ○ Le prix de l'article ou du produit est trop bas par rapport au prix du marché ;
- ○ Le vendeur s'assure que vous n'êtes pas dans la même localité ;
- ○ Le vendeur exige un paiement électronique ;
- ○ Le vendeur évite le contact physique ;
- ○ Il répond très peu aux commentaires sous sa publication ;

◎ Quelques réflexes à développer en cas d'achat sur les réseaux sociaux :

- ○ Abstenez-vous de payer des articles ou services trop moins chers (risque d'escroquerie ou de payer un produit issu d'un délit) ;
- ○ Effectuez vos achats sur des plateformes sérieuses (sites de e-commerce ou pages connus et fiables) ;
- ○ Faites attention aux articles publiés via des profils ;
- ○ Lire les commentaires pour se faire une idée de la réputation du vendeur ;
- ○ Payez toujours à la livraison tant que cela est possible.

Mesures de prévention

- Verrouiller vos équipements par des codes;
- Chiffrer l'ensemble des informations aussi bien dans les équipements que sur les supports externes;
- Chiffrer des données stockées et/ou transitant sur les différentes plateformes en ligne ;
- Utiliser un VPN pour l'accès aux informations surtout en période de mobilité;
- Utiliser un outil d'authentification forte;
- Mettre en place une application de Management des ressources informatiques;
- Ne pas installer n'importe quelle application ou logiciel méconnu;
- Bien paramétrer ses plateformes et profils en ligne.

- Les autorités ne peuvent mettre fin à la cybercriminalité uniquement dans le cadre d'arrestations et de poursuites judiciaires;
- Face à aux défis du numérique, il est impératif de rappeler que la sécurité des SI est une responsabilité collective, tout utilisateur a un rôle à jouer pour sa protection et la protection de son entourage;
- Le partage d'expérience, la collaboration, la vigilance et la conformité aux réglementations en vigueur sont des éléments cruciaux pour renforcer notre posture de cybersécurité.

6.8. Vie privée à l'ère des réseaux sociaux

Notre monde de plus en plus connecté avec une utilisation généralisée d'internet et des réseaux sociaux facilitant la communication, le partage d'expériences et donc la collaboration. Toutefois, cette connectivité permet de savoir presque tout sur l'individu dans l'espace et dans le temps par la collecte et le traitement des données de cette personne. Ainsi, l'usage que l'on pourrait faire de ces technologies peut être attentatoire à nos droits fondamentaux.

L'enjeux principal est donc la protection des droits de l'individu dans l'environnement numérique.

Données à caractère personnel.

Ce sont toutes informations relatives à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un numéro d'identification, à un ou plusieurs éléments(s) propre (s) à son identité physique, physiologique génétique, psychique, culturelle, sociale, économique.

Avec l'apparition de l'internet, on distingue la « vie physique ou réelle » de la « vie numérique ».

Ainsi, on distingue l'IDENTITÉ NUMÉRIQUE (ensemble des informations /traces sur vous et qui sont sur internet /réseaux sociaux) de la REPUTATION NUMERIQUE (c'est la renommée que vous avez sur internet ou l'opinion que le public se fait sur une personne à partir des traces laissées sur internet)

Vie numérique :

Ensemble des activités menées dans l'espace virtuel qu'est internet et cette vie numérique s'articule autour des profils créés sur les RS , des contenus qui y sont diffusés.

Conseils pratiques.

- Bien configurer les paramètres des plateformes de réseaux sociaux (RS) pour préserver la confidentialité et la sécurité, utiliser des antivirus pour protéger vos terminaux de connexions.
- Ce qu'il faut savoir avant d'utiliser les RS : il n'y a pas d'anonymat parfait sur les RS. Tout internaute quel que soit le service qu'il utilise (RS), est traçable et peut être retrouvé via son adresse IP, il n'est pas anodin de publier une photo gênante de ses amis ou de soi-même car sa diffusion est incontrôlée, il faut donc éviter de publier des photos compromettantes de ses amis ou de soi-même,

- Il est très difficile, voire impossible de supprimer par la suite des informations, photos et images que vous publiez sur votre réseau social, il ne faut pas diffuser des images suggestives ou ridicules ni de séances webcam, elles peuvent être enregistrées et rediffusées, éviter d'étaler votre vie privée sur les RS,

NB : RÉFLÉCHIR AVANT DE PUBLIER : UN POST, UN COMMENTAIRE, UN TWEET OU UNE PHOTO INSTAGRAM UN PEU RIDICULE, PEUVENT SE RETROUVER DANS LE MOTEUR DE RECHERCHE ASSOCIÉ À TON NOM. UN TWEET PEUT-ETRE… REPRIS PAR LA PRESSE… OU RÉFÉRENCE DANS GOOGLE, FAIRE ATTENTION AUX PHOTOS, VÉRIFIER SES TRACES, RESPECTER LES AUTRES.

Telle une goutte d'eau dans l'océan, chaque donnée personnelle compte. Vos données sont le reflet de qui vous êtes alors, choisissez la transparence avec sagesse et préservez l'intégrité de votre identité numérique.

La toile est un monde virtuel à l'image du monde réel, il n'est pas nécessairement mieux fréquenté que certains endroits déconseillés de nos villes. Aussi, ce n'est pas parce qu'il y'a des accidents d'automobiles / moto que nous allons arrêter de rouler à moto ou en voiture. Il suffit d'observer le code et les règles de conduite.

Protéger sa vie privée sur internet et les RS est une responsabilité individuelle et non celle des promoteurs des RS.

AGISSEZ DONC SUR LE NET COMME VOUS ÊTES DANS LA VIE.

7. POINTS CLES ET RECOMMANDATIONS DU FORUM

7.1. Points clés

À travers les échanges animés, les débats constructifs et les partages d'expériences très enrichissantes lors de ce forum, nous pouvons retenir les éléments clés suivants :

- Les technologies émergentes telles que (i) l'IA générative, (ii) la blockchain et les cryptomonnaies, (ii) l'ingénierie des plateformes de libre-service incluant l'internet des objets (IoT) et les technologies homme-machine, suscitent de nouvelles questions en matière de gouvernance de l'internet.
- De ce fait, la gouvernance de l'internet doit donc demeurer participative et ne saurait être confinée à un seul secteur ou à une seule entité, mais requiert plutôt l'engagement coordonné et concerté de multiples parties prenantes, incluant les gouvernements, le secteur privé, la société civile, les techniciens, les universitaires et les utilisateurs finaux.
- L'application des principes de souveraineté au domaine des technologies de l'information et de la communication (souveraineté numérique) doit tenir compte des approches juridique, politico-économique et libérale.
- Pour assurer une souveraineté numérique au Burkina Faso, il faut actionner les leviers essentiels tels que :
  - Investissements dans la sécurité informatique et formation des professionnels de la cybersécurité ;
  - Développement d'infrastructures numériques souveraines et de solutions numériques locales ;
  - Promotion de l'innovation et l'entrepreneuriat local pour valoriser la création de solutions numériques adaptées ;
  - Adoption de solutions numériques durables.
- Les systèmes de noms de domaine contribuent non seulement à la sécurisation du cyberespace, mais aussi et surtout à la souveraineté numérique du pays. Leur bonne gestion favorise l'identification précise des titulaires des noms de domaine (contacts administratifs, technique) ainsi que le filtrage DNS pour contribuer à bloquer certains types d'attaques.
- Vu la complexité du développement de l'Internet et de son impact sur nos vies, l'UNESCO a mis au point le concept d'universalité de l'Internet basé sur les principes DOAM-X : (D) - l'Internet est fondé sur les Droits humains ; (O) – il est Ouvert ; (A) – il devrait être Accessible à tous ; (M) – il est alimenté par la participation de Multiples acteurs ; et (X)- il aborde des indicateurs transversaux sur les questions du genre et les besoins spécifiques des enfants, le développement durable, la confiance et la sécurité ainsi que les aspects juridiques et éthiques de l'internet.

- La cybersécurité est un défi croissant de notre société numérique. Elle est surtout une responsabilité collective. A ce titre, elle doit prendre en compte : Le gouvernement, le secteur privé, les utilisateurs, le développement technologique, la criminalité en ligne et les conflits géopolitiques.
- Au Burkina Faso, des efforts sont faits sur le plan institutionnel et juridique avec le fonctionnement effectif de l'ANSSI, la CIL, la BCLCC, le CSC et les outils règlementaires et juridiques tels : SNCS-BF, RGS-BF, RGI, RMQ, Loi n°001-202, Loi n°045-2009.
- Les autorités ne peuvent pas à elles seules, mettre fin à la cybercriminalité uniquement dans le cadre d'arrestations et de poursuites judiciaires. Tout utilisateur a un rôle à jouer pour sa protection et la protection de son entourage ;
- Les 10 conseils du CSC sont à juste titre, conçus pour aider les citoyens à avoir une identité et une réputation numérique responsables, car protéger sa vie privée sur internet et les réseaux sociaux est avant tout une responsabilité individuelle et non celle des promoteurs des plateformes.

7.2. Recommandations

Au terme de ce forum, nous recommandons :

1. **Coopération numérique** : Renforcer la coopération entre les pays membres de l'Alliance des Etats du Sahel (AES) en matière de gouvernance de l'Internet et de cybersécurité.
2. **Elaboration d'une cartographie** des métiers et des données en lien avec la souveraineté numérique du pays :
3. **Formation et sensibilisation :** Renforcer les programmes de formation en cybersécurité pour les professionnels du secteur et sensibiliser le grand public aux bonnes pratiques de sécurité en ligne. Dans ce cadre, il y'a lieu de renforcer le mécanisme de financement des structures de la société civile spécialisé dans la promotion d'un usage de l'internet.
4. **Collaboration public-privé :** Maintenir et renforcer la collaboration entre les acteurs publics et privés pour élaborer des politiques et des stratégies de cybersécurité plus efficaces, partager les informations sur les menaces, promouvoir les meilleures pratiques et investir dans des solutions de sécurité adaptées.
5. **Développement de centres d'excellence en cybersécurité :** Créer des centres d'excellence en cybersécurité pour la recherche, le développement et la formation spécialisée dans le domaine de la sécurité numérique. Investir dans la recherche et le développement de technologies et de solutions innovantes en cybersécurité, encourager les initiatives locales et soutenir les startups spécialisées dans ce domaine.
6. **Promotion de l'innovation et du contenu local :** Susciter et soutenir les innovations dans le domaine de la technologie tout en garantissant la sécurité des solutions développées, favorisant ainsi un écosystème numérique à contenu local sûr et dynamique.

8. CONCLUSION

La gouvernance de l'Internet est un domaine complexe qui implique des aspects techniques, politiques, économiques, sociaux et culturels. Elle demeure un domaine dynamique, et les perspectives évolueront au fil du temps en réponse aux défis et aux opportunités qui se présentent à travers les technologies émergentes. La coopération numérique et la réflexion continue sont essentielles pour aborder les défis liés aux technologies émergentes et assurer un Internet ouvert, sûr et équitable pour tous.

Cette coopération nécessite une collaboration entre les gouvernements, les organisations internationales, le secteur privé, la société civile et les utilisateurs finaux. C'est pourquoi Internet Governance Forum (IGF) facilite le dialogue et la coopération numérique pour aborder les enjeux liés à l'Internet, tels que la souveraineté numérique, la neutralité du réseau, la protection de la vie privée, la cybercriminalité et la gestion des noms de domaine et des adresses IP.

En matière de souveraineté numérique, l'équilibre entre la régulation pour assurer la sécurité et la protection des utilisateurs et la préservation de la liberté d'expression et de l'innovation reste un défi majeur pour la gouvernance de l'Internet à l'échelle mondiale, africaine et au niveau spécifique du Burkina Faso. Les décisions prises dans ce domaine ont un impact significatif sur la façon dont les gens utilisent, accèdent et interagissent avec l'Internet.

Cette 10è édition du Forum national sur la Gouvernance de l'Internet, a reconnu la pertinence du thème de souveraineté numérique et cybersécurité au Burkina Faso, au regard de la situation sécuritaire et géopolitique de la région du Sahel, confrontée à l'hydre terroriste. Les prises de décisions nécessitent une approche équilibrée et inclusive pour répondre aux besoins divers et changeants des utilisateurs.

Nous appelons à une meilleure éducation et sensibilisation des citoyens quant à l'utilisation sûre, responsable et éthique d'Internet. Les défis liés à la souveraineté et la cybersécurité ne peuvent pas être relevés seulement par le gouvernement. Il faut l'implication effective de l'ensemble des parties prenantes : société civile, secteur privé, universitaires, experts et utilisateurs.

9. REMERCIEMENTS

Nos sincères remerciements à :

- Le Président de l'Assemblée Législative de Transition (ALT) du Burkina Faso ;
- Le Ministre de la Transition Digitale, des Postes et des Communications Électroniques du Burkina Faso ;
- Le Ministre de la Communication, de l'Economie numérique et de la modernisation de l'Administration de la République du Mali ;
- Le Ministre de la Communication, des postes et de l'Economie numérique de la République du Niger ;
- Le Conseiller Spécial du Président du Faso en charge du digital ;
- Le Secrétaire exécutif de l'Autorité de Régulation des Communications Électroniques et des Postes du Burkina Faso (ARCEP) ;
- La Coordonnatrice au Secrétariat des Nation-Unis des Initiatives Régionales et Nationales pour la Gouvernance de l'Internet (IGF) ;
- La Coordinatrice du Forum Ouest Africain pour la Gouvernance de l'Internet (WAIGF) ;
- Les représentants de :
    - La Commission Nationale Burkinabè pour l'UNESCO ;
    - La Commission de l'Informatique et des Libertés (CIL) ;
    - L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) ;
    - Le Conseil Supérieur de la Communication (CSC) ;
    - La Brigade Centrale de Lutte Contre la Cybercriminalité (BCLCC) ;
    - L'Agence Nationale de Promotion des Technologies de l'Information et de Communication (ANPTIC) ;
    - L'Association Burkinabè des Domaines Internet (ABDI) ;
    - L'Association YAM-PUKRI ;
    - Les structures publiques, privées, ONG et associations présentes au Burkina Faso ;
- Les modérateurs des différents panels ;
- Les panélistes ;
- Les stagiaires de la 3ème édition de l'Ecole sur la Gouvernance de l'Internet (EGI) ;
- Tous les participants.