Numéro 02 - Mai 2022

LE MAGAZINE DU CHEDS

Centre des Hautes Etudes de Défense et de Sécurité

CYBERSECURITE AU SENEGAL

Special Guest

CYBERSECURITE, CYBERGUERRE ET CYBERDEFENSE : Réponses pour un Etat souverain

Dr Papa GUEYE, Commissaire de Police

Directeur général de l'Ecole Nationale de Cybersécurité à Vocation Régionale

Extrait

Mot du Directeur général

Ce nouveau numéro du magazine du Centre des Hautes Etudes de Défense et de Sécurité (CHEDS) traite du thème de la cybersécurité dont l'actualité récente, à travers la crise russo-ukrainienne, nous rappelle la place de plus en plus importante qu'il occupe dans la sécurité des nations. En effet, les millions de « trolls » déversés dans le cyberespace les belligérants, via les médias sociaux, pour légitimer les buts politiques et gagner la bataille de l'opinion, la création d'armées numériques (IT ARMY Ukrain) mobilisant des milliers de volontaires, les attaques malveillantes des infrastructures numériques « en déni de service » (eau, énergie, alimentation, monétique etc.)

Général de brigade Mbaye CISSE,
Directeur général du CHEDS

Suivez nous sur nos différents réseaux pour rester informer

@cheds.senegal @CHEDS_ CHEDS officiel

cheds_officiel CHEDS SENEGAL +221 70 644 17 29

www.cheds.gouv.sn

SOMMAIRE

PÉSENTATION DU CHEDS

Établissement public à caractère administratif, créé le 03 janvier 2013 et placé sous la tutelle de l'État-major Particulier de la Présidence, le Centre des Hautes Etudes de Défense et de Sécurité (CHEDS) doit satisfaire les besoins de l'Etat en expertises sur des questions d'ordre stratégique liées à la protection des individus et des biens, à la politique étrangère, à la science, à la technologie et aux phénomènes économiques et sociaux.

Missions

Répondre aux attentes des décideurs politiques sur des problématiques d'ordre stratégique qui affectent le développement du pays ;

Participer à la formation de hauts cadres civils et des Forces de Défense et de Sécurité, par le renforcement des connaissances fondamentales en stratégie, l'appropriation des clés de compréhension de l'environnement géostratégique ainsi que des enjeux liés à la défense et à la sécurité ;

Constituer la documentation nécessaire à l'étude et la familiarisation aux questions relevant de ses missions et d'assurer la publication et la diffusion des études et des travaux d'ordre scientifique découlant de ses missions ;

Organiser ou de participer à l'organisation de colloques et de congrès internationaux similaires ;

Susciter et de promouvoir des travaux scientifiques se rapportant à sa mission ;

Fédérer la recherche et les études entreprises au sein d'universités et de centres de recherche sur des questions fondamentales relatives à la défense, la sécurité, la politique étrangère, la technologie, l'économie et les socio- cultures.

VISION

« Devenir une institution de référence sur les questions d'ordre stratégique liées à la défense, la sécurité et la paix en Afrique ».

Axes d'intervention :

Formation ;

Création d'espace d'échanges et de dialogue ;

Recherche-action ;

Appui-conseil.

LE MOT DU DIRECTEUR DU CHEDS

Général de brigade Mbaye CISSE
Directeur général du Centre des Hautes Études de Défense et de Sécurité - CHEDS

Ce nouveau numéro du magazine du Centre des Hautes Etudes de Défense et de Sécurité (CHEDS) traite du thème de la cybersécurité dont l'actualité récente, à travers la crise russo-ukrainienne, nous rappelle la place de plus en plus importante qu'elle occupe dans la sécurité des nations. En effet, les millions de « trolls » déversés dans le cyberespace par les belligérants, via les médias sociaux, pour légitimer les buts politiques et gagner la bataille de l'opinion, la création d'armées numériques (IT ARMY Ukrain) mobilisant des milliers de volontaires, les attaques malveillantes des infrastructures numériques « en déni de service » (eau, énergie, alimentation, monétique etc.), les brouillages des systèmes d'armes, les montages vidéos et autres manipulations expertes cybernétiques, ont fini de nous démontrer que le seul contrôle de l'espace physique n'est plus suffisant pour acter la victoire; cette dernière a besoin, pour prendre forme, d'un contrôle total de « l'espace virtuel ».

Comme l'indique son étymologie grecque Kubernêtikê (gouvernail) le cyber gouverne désormais nos vies, surtout en période de crise.

Ainsi, la capacité des nations à circonscrire ce nouveau champ de bataille devient un impératif majeur de souveraineté. En plus de disposer des moyens de garantir l'intégrité physique de leur territoire, les nations ont besoin de se prémunir de toutes les vulnérabilités découlant de l'introduction massive du cyber dans leur quotidien. Ce nouvel univers, fruit de la mondialisation et de la révolution numérique en marche, dispose de sa propre grammaire et de son lexique terrifiant qui riment avec fake news, haking, doxing, ransomware, deep web, backdoor, botnet, phishing etc., qu'il faut apprivoiser, sous peine de couler sous le poids de ses combattants anonymes.

En attendant la parution prochaine des Dossiers du CHEDS, publication qui sera amplement consacrée à la problématique, ce numéro du magazine vous familiarise avec les enjeux, défis et perspectives de la cybersécurité qui interpellent tous les décideurs.

Bonne Lecture !

Dr Papa GUEYE, Commissaire de Police
Directeur général de l'Ecole Nationale de Cybersécurité à Vocation Régionale

CYBERSECURITE, CYBERGUERRE ET CYBERDEFENSE : Réponses pour un Etat souverain

« À défaut de temporiser les conflits géopolitiques, l'Internet semble au contraire les multiplier et les compliquer »[1]

Notre contribution, consistera d'abord, après une introduction, à aborder l'aspect stratégique du cyberespace. Ensuite, elle sera axée sur l'expression des rivalités et l'extension des conflits dans cet espace, et enfin, sur les réponses stratégiques à mettre en oeuvre dans un cadre global pour une souveraineté numérique.

1. INTRODUCTION

Le rayonnement du numérique conduit à s'interroger sur les conflits notés au niveau de l'internet en général et principalement au sujet de son contrôle et de sa régulation, de l'utilisation des réseaux à des fins criminelles, dans les rivalités politiques, les combats militaires, la guerre économique, le renseignement, la politique d'influence diplomatique et culturelle et le respect de la vie privée.

A l'analyse, on se rend compte que le digital s'est invité dans la défense et la sécurité, bouleversant, les dispositifs stratégiques, opératifs et tactiques. Cet outil de convergence et d'interdépendance généralisé, le cyber, a croisé de manière très puissante la sécurité et la défense. De cette union complexe[2] est née une nouvelle pensée stratégique qui change et/ou met à jour, celle, jadis, liée à la sécurité et la défense : le vocable de cyberstratégie est souvent utilisé pour traduire cette nouvelle évolution.

La cyberstratégie commande l'adoption de nouvelles règles de sécurité et de défense qui n'annihilent pas celles antérieures, lesquelles demeurent importantes. En termes clairs, ces nouvelles règles ne remettent pas en cause les fondamentaux classiques de la conduite de la guerre, de la gestion de la sécurité publique (maintien et rétablissement de l'ordre) et ceux liés à la défense de l'intégrité du territoire dans lesquels le nouvel élan trouve son inspiration.

Cette situation a poussé les États à adopter de nouvelles visions de politiques de sécurité et de défense, tournées vers la maitrise de l'information, de la sécurité et du durcissement des systèmes d'information surtout d'intérêts vitaux.

D'abord, l'action stratégique doit prendre en compte la capacitation des acteurs par la formation et la sélection de ressources humaines de qualité dans le but d'assurer la consolidation des acquis et la continuité des actions entreprises.

Ensuite, elle doit intégrer les conflits dans l'espace numérique, « le cyberespace »[3] et prendre en compte les agressions telles que l'espionnage, le sabotage et la subversion ainsi que la criminalité sous toutes ses formes.

---

[1] DOUZET, F.,"Internet géopolitise le monde," GéoProdig, portail d'information géographique, consulté le 22 mars 2022, http://geoprodig.cnrs.fr/items/show/87595.

[2] La complexité de cette union s'explique par le fait que le cyberespace sans frontières est difficile à cerner et que les acteurs de ce nouveau terrain de jeu géopolitique et géostratégique sont parfois incontrôlables.

[3] Par cyberespace, il faut comme un espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'internet, et par les données qui y sont traitées, in Journal officiel de la République française, n° 0219 du 19 septembre 2017.

Les réseaux et les ordinateurs sont l'expression d'armes diverses[4] qui permettent d'atteindre le dispositif adverse et de le déstabiliser créant ainsi un désordre généralisé. De même, les terroristes utilisent de véritables outils d'endoctrinement rapide en ligne ainsi que des recettes pratiques qui peuvent permettre, parfois, de déjouer les dispositifs des plus grandes puissances. De plus, la guerre idéologique se mène sur les réseaux sociaux avec une masse importante de données qui constitue un nouveau pouvoir dont la maîtrise est nécessaire à l'exercice du pouvoir politique.

Enfin, le numérique est inscrit dans la gestion de la sécurité avec un aspect défensif appelé cybersécurité. L'absence de prise en compte de cette dernière fragilise les dispositifs de maintien de la sécurité intérieure et de l'ordre public constamment défiés par la criminalité, le désordre, les appels au soulèvement, et l'incitation à la haine.

En ce qui concerne la criminalité, qui se manifeste à travers l'intrusion illicite dans les systèmes, le vol, la destruction de données ou même tout acte criminel perpétré via les réseaux, l'enjeu est l'établissement de la preuve, devenue très difficile à cause de sa volatilité et de la nature transfrontalière des infractions. Ainsi, se pose la lancinante question de la coopération qui doit également s'adapter pour éviter les lenteurs préjudiciables à l'action de la justice.

L'objectif est d'accorder de l'intérêt à la forme et au contenu du cyberespace qui constitue un critère essentiel pour garantir la souveraineté d'un Etat, pour préserver la démocratie, la stabilité et la paix sociale.

Cette posture vis-à-vis du cyberespace est une condition substantielle pour tout État qui vise la résilience face aux menaces complexe et multiforme dans ce domaine. Le numérique sert à faire la guerre et même à la gagner[6]. Il contribue à asseoir la stabilité des pays. Dès lors, lorsqu'il est mal maitrisé, il peut conduire inéluctablement au chaos.

2. LE CYBERESPACE, UN DOMAINE STRATEGIQUE[6]

La transformation digitale a intégré les sociétés et les activités politique, économique et sociale. Elle est accompagnée d'une « informatique massive » avec une dimension stratégique et des enjeux multiples.

Le cyber a connu des évolutions avec son application dans divers domaines qui favorise l'usage de termes comme « e-réputation », « e-commerce », « e-gouv », « e-administration ». Cette nouvelle matrice conceptuelle s'est installée comme un centre d'intérêt majeur dans le champ de la sécurité défense et de la stratégie. Un bref rappel historique des cas d'agression cyber permet d'illustrer cette réalité. En novembre 1988, le « ver Morris » a déclenché la première cyberattaque reconnue et signalée, qui a infecté des machines ciblées, provoquant leur ralentissement et leur plantage pour favoriser la perpétration d'attaques par déni de service et/ou de subtilisation de données. Certains logiciels d'attaques sont conçus pour cibler des vulnérabilités non encore identifiées dans les systèmes informatiques[7].

Depuis le début de la guerre dans le Donbass en 2014, l'Ukraine est devenue la cible privilégiée des hackers russes, leur terrain d'entraînement favori.

Retrouvez l'intégralité en cliquant ci-dessous :

CYBERSECURITE, CYBERGUERRE ET CYBERDEFENSE : Réponses pour un Etat souverain

[4] Les armes informatiques s'articulent autour du vol de données à des fins de renseignement jusqu'à la prise de contrôle à distance d'un système d'arme. Avec les armes cyber, il est très possible de frapper des équipements informatiques matériels, des actifs immatériels tels que les données informatiques, logiciels à des fins de renseignement notamment, ou encore cibler les utilisateurs des moyens informatiques, neutraliser une défense anti-aérienne en piratant les radars, ou encore contrôler à distance les bâtiments des marines, par exemple.

[6] A. Lefébure, « Informatique communication et militaire », Réseaux, vol. 4, n° 17, 1986, p. 1.

[6] Pour plus de détails, voir le cyberespace, nouveau domaine de la pensée stratégique, collection Cyber stratégie dirigée par O. KEMPF, éd. Economica 2013,175 pages.

[7] Vulnérabilité non encore identifié ou vulnérabilité zero-day également orthographiée 0-day ou vulnérabilité du jour zéro1 est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu.

BIOGRAPHIE SUCCINTE DE L'INVITÉ

M. Papa GUEYE est Commissaire de police, Docteur en droit privé et Sciences criminelles. Il s'intéresse particulièrement aux questions liées au droit des TIC, à la cybersécurité et à la lutte contre la cybercriminalité notamment aux techniques d'investigations numérique, à la recherche, à l'innovation et à la prospective stratégique dans le domaine de la transformation digitale. Il a assuré plusieurs cours, ateliers et séminaires sur des thématiques liés aux problématiques de la criminalité émergente, à la sécurité contemporaine, à la géopolitique et à la géostratégie en rapport avec la cybersécurité et la défense.

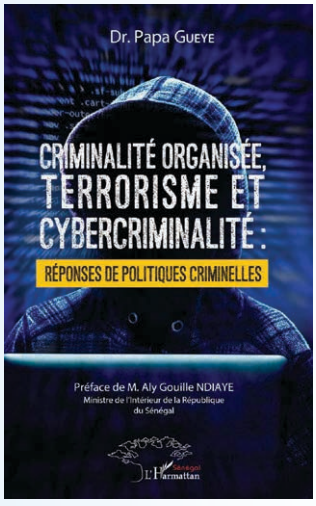
Dans le domaine de la lutte contre la cybercriminalité, le Docteur Papa GUEYE est fondateur de la Brigade spéciale de lutte contre la Cybercriminalité et de la Division spéciale de Cybersécurité, unités spécialisées qu'il a dirigées.

Ancien chef de Groupe de Recherches et d'Interpellation, de la Brigade Economique et Financière de la DIC et de la Division de la Police Technique et Scientifique de la Direction de la Police judicaire, il a participé à l'élucidation de plusieurs enquêtes et à l'exécution de commission rogatoire internationale dans des affaires ayant trait à la criminalité organisée et à la cybercriminalité.

Le docteur Papa GUEYE, expert formateur certifié, est membre de comités techniques Cyber et a participé des travaux d'expertise, de définition de stratégies de formation au profit des Forces de défense et de sécurité auprès d'instances (Interpol, Afripol, Francopol, Alliance de sécurité internationale, projet Glacy …..). Il est actuellement le Directeur général de l'Ecole nationale de Cybersécurité à Vocation Régionale créée par Son Excellence Monsieur Macky SALL, Président de la République en partenariat avec la France.

Dernier ouvrage :

CRIMINALITÉ ORGANISÉE, TERRORISME ET CYBERCRIMINALITÉ : RÉPONSES DE POLITIQUES CRIMINELLES



Ce livre étudie la problématique de la criminalité transfrontalière en Afrique de l'Ouest. L'auteur essaye de démontrer que le combat contre la criminalité transfrontalière organisée nécessite l'intégration d'une nouvelle approche de la question de la souveraineté des États, de surcroît, avec le développement du numérique. Il propose des réponses de politiques criminelles articulées autour de stratégies nationales et internationales, d'une part ; et des réponses dématérialisées notamment de cybersécurité, d'autre part.

Date de publication : 13 novembre 2018

Broché - format : 15,5 x 24 cm • 436 pages
ISBN : 978-2-343-14769-7
EAN13 : 9782343147697
EAN PDF : 9782140105272

Moustapha DIOUF,
Commissaire de Police principal,
Alumni Master Défense Sécurité et Paix
Promotion 2016-2017
Centre des Hautes Etudes de Défense et de Sécurité (CHEDS)

Cybercriminalité, l'affaire de tous ?

Pour vous, comment pourrait-on définir la Cybercriminalité ?

Si aujourd'hui les opportunités infinies du numérique ne sont plus à démontrer, dans leurs diverses dimensions politique, socioculturelle, économique et scientifique pour l'humanité qui en fait un bon usage, force est de reconnaitre l'ampleur et la gravité du risque numérique tant pour les organisations que pour les individus. Ainsi, le cyber espace a donné naissance à une nouvelle forme de criminalité appelée cybercriminalité ou encore criminalité informatique qui bouleverse les paradigmes classiques du droit criminel. C'est pourquoi, on en note une variété de définitions suivant les critères établis par chaque Etat, dont on pourra retenir quelques-unes ici :

- Selon le droit positif sénégalais, la cybercriminalité est toute infraction qui implique l'utilisation des technologies de l'information et de la communication ;
- Vincent Lemoine définit la cybercriminalité comme un ensemble d'atteintes aux biens et aux personnes commises via l'utilisation des nouvelles technologies ;
- Selon le Ministère de l'Intérieur français, la cybercriminalité concerne l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication en général, et en particulier sur les réseaux utilisant le protocole TCP-IP appelé communément internet ;
- Pour Stanislas de Maupeou, la cybercriminalité peut être définie comme des actes contrevenants aux traités internationaux et aux lois nationales utilisant les réseaux ou les systèmes d'information comme moyen de réalisation d'un délit ou d'un crime, ou ayant ces mêmes réseaux ou systèmes pour cible.

Quelles sont les typologies de cybercriminalité au Sénégal ?

On pourrait distinguer trois types ou catégories de cybercriminalité : la cybercriminalité individuelle (contre les personnes), la cybercriminalité contre la propriété et la cybercriminalité gouvernementale :

Cybercriminalité individuelle ou contre la personne

Elle implique une personne qui distribue des informations malveillantes ou illégales en ligne. Il peut s'agir de cyberharcèlement, de distribution de pornographie ou tout simplement de diffusion de données à caractère personnel.

Cybercriminalité contre la propriété

Il peut s'agir d'un cas réel où un criminel possède illégalement les coordonnées bancaires ou de carte de crédit d'une personne. Le pirate vole les coordonnés bancaires d'une personne pour avoir accès à des fonds, faire des achats en ligne ou lancer des arnaques par hameçonnage (phishing) afin d'inciter les gens à divulguer leurs informations. Il pourrait également utiliser un logiciel malveillant pour accéder à une page Web contenant des informations confidentielles.

Cybercriminalité gouvernementale

Cette catégorie est moins répandue, mais elle est la plus grave. Elle comprend le piratage de sites Web gouvernementaux, de sites militaires ou la diffusion de propagande. Ces criminels sont habituellement des terroristes ou des gouvernements ennemis d'autres pays. Ce type de cybercriminalité n'est pas encore répandue au Sénégal.

Quelle stratégie nationale développer pour une lutte efficace contre la cybercriminalité ?

Dans ce contexte où le Sénégal est engagé comme beaucoup d'autres pays dans la transition numérique avec une administration et une population, de plus en plus connectées, le développement d'une stratégie contribuerait à répondre efficacement aux enjeux de sécurité du numérique. Il pourrait s'agir de réfléchir plus spécifiquement sur les actions pouvant permettre de :

- Gérer les risques liés à la sécurité de notre système d'information (protections des installations informatiques et des données informatisées) ;
- Identifier les principales attaques et menaces sur la sécurité individuelle et celle des services ;
- Développer des techniques d'investigations numériques solides ;
- Renforcer les mécanismes opérationnels d'entraide judiciaire
- Promouvoir la coopération internationale dans un sens favorable à l'émergence d'une approche holistique de la lutte contre la cybercriminalité.

Que peut-on faire pour améliorer la prise de conscience générale des utilisateurs face à la cybercriminalité ?

Aujourd'hui, diverses infractions sont commises via internet et les réseaux et au moyen de technologies (pédopornographie, intrusion, escroquerie, fraude, injures, diffamation, diffusion de données à caractère personnel etc…).

Cela prouve que la prise de conscience des risques liés à la numérisation de la société reste insuffisante. Face à ce constat, la sensibilisation des masses, le renforcement de capacités des personnels des organisations publiques et privées restent des meilleurs moyens d'asseoir une prise de conscience générale des utilisateurs contre la cybercriminalité.

Sources :

Exposé des motifs de la loi n°2008-11 du 25 janvier 2008 portant sur la cybercriminalité,

Voir M. DIOUF, la Police nationale du Sénégal face au défi de la Cybersécurité, abis édition, 2019.

Consultez l'article en cliquant ci-dessous :

Cybercriminalité, l'affaire de tous ?

Lieutenant-colonel Ibrahima DIOUF
Inspecteur technique transmission informatique
Inspection Générale des Forces Armées (IGFA)
Spécialiste en cybersécurité-cyberdefense

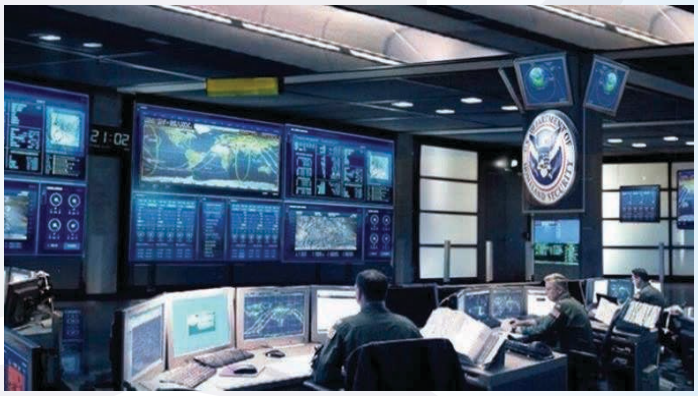
« Cybersécurité et démocratie. »

I. Comment appréciez-vous les dérives des utilisateurs dans l'espace cyber ?

Tout d'abord, je tiens à remercier les autorités du CHEDS de l'opportunité offerte, dans l'optique de contribuer à l'avènement d'une société de confiance numérique. Faire du CHEDS, un creuset de recherche militaire et universitaire, un pôle de compétence en cyber sécurité et la cyberdéfense, est une pertinente initiative du Directeur du CHEDS.

De plus, le projet d'élargissement de la cartographie de la formation par l'ouverture d'un Master spécialisé en Cyberdéfense devrait à terme renforcer l'expertise « Cyber Workforce Management » des hauts cadres de l'Etat. Le contexte géopolitique évolue, la cyberguerre entre la Russie et l'Ukraine en est une parfaite illustration. Dans l'architecture de la cyber sécurité nationale, ces cadres de haut niveau pourraient être les futurs Point focaux de la Cyber défense dans les ministères de souveraineté et aussi au sein des états-majors. Enfin, dans l'optique de gérer une situation de cyber crise majeure, il est crucial d'avoir des ressources humaines de qualité.

Pour revenir à la question, il est bien vrai que des dérives dans le cyberespace sont notées quasi quotidiennement. Ces dérives touchent tous les segments de la société notamment, au plan politique mais aussi dans le domaine religieux, un domaine très sensible pour des raisons de cohésion sociale. La perception d'anonymat sur l'internet gage d'impunité est très loin d'être avérée. Les instruments institutionnels mis en place par les autorités peuvent efficacement lutter contre ces dérives en cas de délit d'atteinte des sphères privées ou professionnelles, grâce aux moyens d'investigations numériques.



COMPUTER EMERGENCY RESPONSE TEAM (CERT)

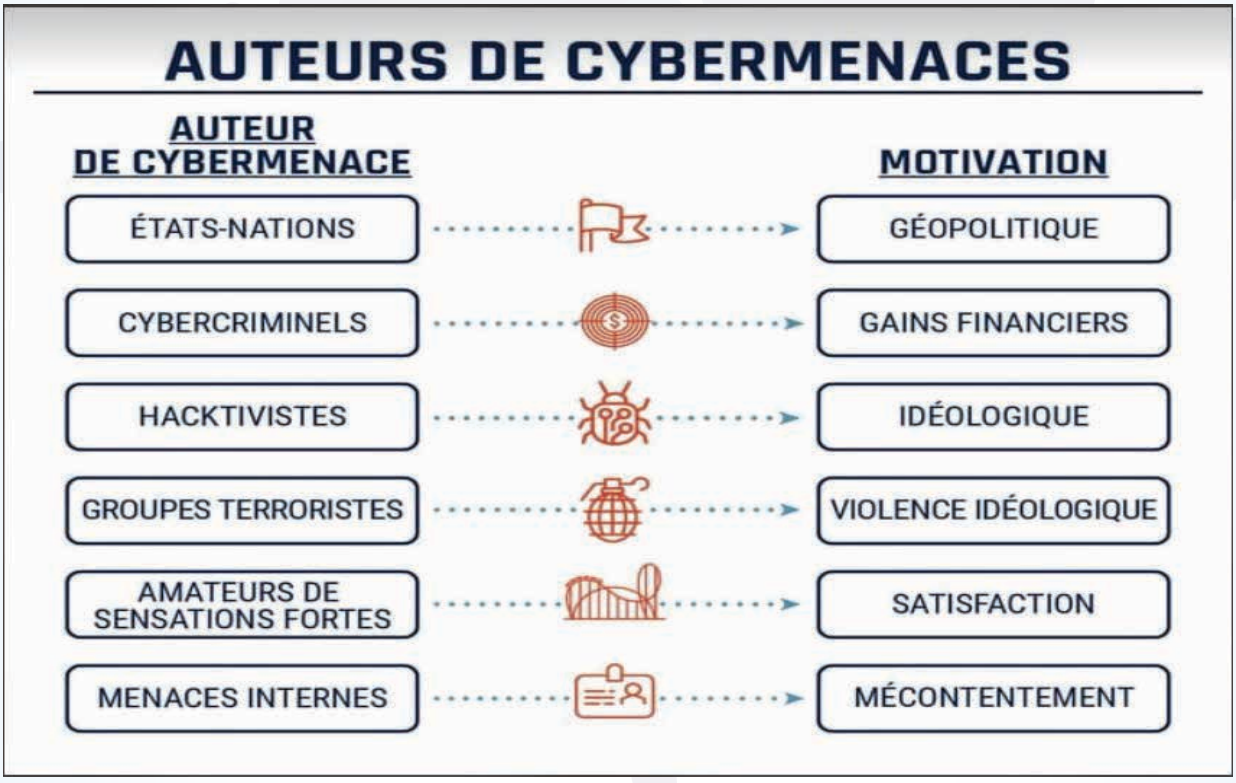
De par son impact planétaire, il s'avère utile de prendre en compte les aspects de la cyber menace qui bouleversent les repères traditionnels de la sécurité. Les conséquences économiques, politiques et stratégiques de ces nouvelles menaces sont potentiellement très déstabilisatrices pour les organisations et les États. Les utilisateurs finaux doivent être formés, sensibilisés pour un meilleur comportement responsable en ligne mais aussi les faire connaitre les peines encourues en cas de violation des règles établies.

HACKERS

II. Comment diminuer le risque de ce phénomène ?

En Le cyberespace apparaît comme un nouveau terrain potentiel de guerre, un champ de confrontation majeur dans tous les domaines qui implique aussi la sécurité des Etats et des Organisations. Il n'est guère facile de diminuer ce risque compte tenu des caractéristiques du cyberespace sur le plan technique. En effet, le cyberespace est l'interconnexion à l'échelle planétaire des réseaux et des services connexes. Le cyberespace est un espace sans frontière avec une multitude d'acteurs aux intérêts et objectifs divergents. La particularité du cyberespace est d'abolir les distances, les frontières nationales et l'anonymat qui favorise le sentiment d'impunité, ce qui est de loin de refléter la réalité. Les services spécialisés de la Gendarmerie ou de la Police peuvent retracer ou géolocaliser tout individu connecté pour des besoins d'enquêtes (preuves digitales) sur n'importe quels supports (mobile, PC, laptop, iphone). La sécurité des personnes et des biens est une prérogative des Forces de Défense et de Sécurité(FDS).

Le principe premier réside dans la formation, la sensibilisation continue des utilisateurs à tous les niveaux, à travers les instances d'éducation depuis l'école primaire, au sein des entreprises, des organisations et de l'administration, sans oublier l'indispensable contrôle parental. A ce niveau, il s'avère utile d'éduquer les internautes sur les bonnes pratiques en ligne, en conformité avec la loi mais aussi de respecter les règles relatives à la protection de la vie privée.



Retrouvez l'intégralité de l'article sur le lien suivant :

« Cybersécurité et démocratie. »

LES ACTIVITÉS DU CHEDS

« Population et prévention de l'extrémisme violent : vers une nouvelle dynamique du mandat des Forces de Défense et de Sécurité ? »

Table ronde publique en marge de la 7ème édition du Forum International de Dakar sur la Paix et la Sécurité en Afrique

En marge de la 7ème édition du Forum international de Dakar sur la Paix et la Sécurité, le Centre des Hautes Études de Défense et de Sécurité (CHEDS) en partenariat avec la Division Sécurité humaine du Département fédéral des Affaires Etrangères (DSH/DFAE) suisses, a organisé une table ronde publique, le mardi 08 décembre 2021, sur le thème : « Population et prévention de l'extrémisme violent : vers une nouvelle dynamique du mandat des Forces de Défense et de Sécurité (FDS) ? ».

Cette rencontre qui a enregistré la participation d'une centaine d'experts, avait pour objectif principal, d'offrir un espace de dialogue et de réflexion sur les principales mesures à prendre pour renforcer le rôle des FDS dans la prévention de l'extrémisme violent.

Retrouvez la synthèse de la table ronde en cliquant sur le lien :

https://cheds.gouv.sn/wp-content/uploads/2022/01/Synthe%CC%80se-TR-PEV-FDD-07.12.2021.-V-Fr.pdf

LANCEMENT DU RAPPORT D'ÉVALUATION MOWIP SÉNÉGAL 2020-2021

En 2017, le gouvernement du Canada a lancé l'Initiative Elsie pour la participation des femmes aux opérations de paix. Elle vise à créer une base de connaissances solide et à développer des mesures innovantes pour favoriser cette participation. Dans ce cadre, le DCAF (le Centre pour la Gouvernance du Secteur de la Sécurité, Genève) a développé en partenariat avec l'Université Cornell et huits (08) partenaires nationaux la méthodologie MOWIP...**Lire plus**

Le rapport :

https://cheds.gouv.sn/wp-content/uploads/2022/03/Rapport-Senegal_Elsie_Francais.pdf

JOURNÉE INTERNATIONALE DE LA FEMME 2022

En l'honneur de son personnel féminin, le Centre des Hautes Études de Défense et de Sécurité (CHEDS) a organisé une matinée dédiée aux Femmes.

Le thème de la Journée internationale des droits de la Femme 2022 étant : « L'égalité aujourd'hui, pour un avenir durable », des rosiers ont été plantés dans les jardins du Centre par les femmes du CHEDS accompagnées du général de brigade Mbaye CISSÉ, le Directeur général. Un acte posé pour un appel à l'action climatique pour les femmes, par les femmes.

Le Général de brigade Mbaye CISSÉ a ainsi réitéré ses félicitations et encouragements à toutes les braves femmes faisant partie de la grande famille du CHEDS (femmes du personnel, auditrices, partenaires etc…).

LES ACTIVITÉS À VENIR

SÉMINAIRE DE PRÉPARATION DES FUTURS ATTACHÉS MILITAIRES

Le Centre des Hautes Etudes de Défense et de Sécurité (CHEDS) organisera, à l'Institut de Défense du Sénégal (IDS), du mardi 07 au vendredi 10 juin 2022, la session 2022 du Séminaire de préparation des futurs Attachés militaires, en partenariat avec l'Etat-Major général des Armées.

Le seminaire sera coordoné par le Colonel (er) A. WARDINI, sous la supervision du Directeur des formations. Le programme comporte une séance introductive, le 07 juin, un bloc «Environnement géopolitique global», le mercredi 08 juin et un bloc «L'Attaché militaire : un diplômate temporaire», les 09 et 10 juin.

Le cérémonie de clôture, prévue le vendredi 10 juin 2022 à partir de 15H00, sera présidée par le Président du Conseil d'Administration du CHEDS.

Vous pouvez avoir le programme prévisionnel en nous adressant un courriel à l'adresse suivante : infos@cheds.gouv.sn

LES ACTIVITÉS À VENIR

Organisation à Dakar, de séminaires sur l'implication des Forces de Défense et de Sécurité (FDS) dans la Prévention de 'Extrémisme violent

En partenariat avec la Division Sécurité Humane et Doits de l'Homme (DSDH) du Département Fédéral des Affaires Etrangères (DFAE) de Suisse, le Centre des Hautes Etudes de Défense et de Sécurité (CHEDS) organise, à Dakar, le 4eme Séminaire régional de Dakar sur 'implication des Forces de Défense et de Sécurité (FDS) dans la Prévention de 'Extrémisme violent, les 23, 24 et 25 mai 2022. Il sera suivi les 27 et 28 mai 2022, d'un séminaire national à la Résidence Le Ndiambour de Dakar.

QUATRIÈME SÉMINAIRE RÉGIONAL

« Le rôle des Forces de Défense et de Sécurité dans la prévention de l'extrémisme violent en Afrique :les cadres d'engagement»

23, 24, 25 mai 2022, Dakar. Sénégal

SEMINAIRE NATIONAL

Forces de Défense et de Sécurité et prévention de l'extrémisme au Sénégal dialogue sur les atouts, acquis, et opportunités

27 et 28 mai 2022, Dakar. Sénégal

Le rapport du troisème séminaire régional : «Forces de défense et de sécurité et acteurs politiques dans la prévention de l'extrémisme violent en Afrique : pourdes synergies opérationnelles ». :

https://cheds.gouv.sn/wp-content/uploads/2022/02/BAT-Rapport-3ieme-sem.pdf

CHEDS

Savoir - Excellence - Sécurité

Centre des Hautes Etudes de Défense et de Sécurité

Centre des Hautes Etudes de Défense et de Sécurité,

Boulevard de la Défense X Rue du Port,

BP : 4705 - Dakar – SENEGAL - Téléphone : 33 822 91 67

www.cheds.gouv.sn

Suivez nous sur nos différents réseaux pour rester informé

@cheds.senegal @CHEDS_ CHEDS officiel

cheds_officiel CHEDS SENEGAL +221 70 644 17 29