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.

COMPUTER EMERGENCY RESPONSE TEAM (CERT)

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.

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.

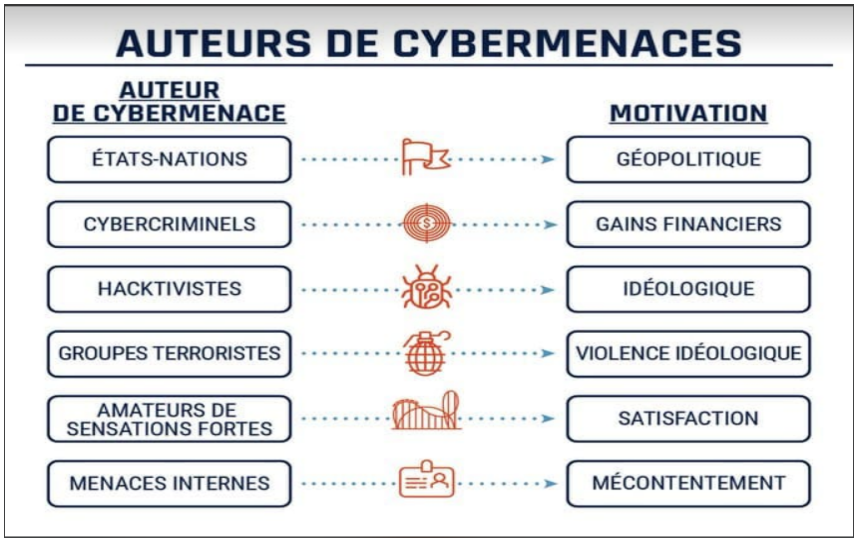
HACKERS

II. Comment diminuer le risque de ce phénomène ?

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.



PAYSAGE DE LA MENACE

III. La démocratisation de l'espace cyber est -elle adaptée à nos réalités politiques, sociales et culturelles ?

Pertinent questionnement particulièrement sur le continent Africain. Il est bien établi que la mondialisation et la globalisation sont des réalités dans les sociétés actuelles. Un mimétisme culturel et une uniformisation des sociétés sont en cours. Le Printemps Arabe est une illustration de ce phénomène. Partant de la Tunisie, le séisme de la liberté a ébranlé la plupart des régimes dans le nord du continent africain.

Dans un contexte de construction et de consolidation des institutions démocratiques, les équilibres sociaux demeurent fragiles sur le continent africain. L'édification des Etats en Afrique est un processus complexe. En effet, depuis le sommet de Baule, en 1990, l'idéal démocratique comme une valeur sociale intangible est devenue une réalité.

En outre, le cyberespace a renforcé l'accès à l'information et aux critères de bonne gouvernance. Aujourd'hui le citoyen est mieux informé sur la marche du monde grâce aux puissant supports des TIC, l'internet, les réseaux sociaux, YouTube. L'internet a aboli les distances. Il a permis l'accès aux informations en continue.

Par ailleurs, l'internet est une tribune de résonnance mondiale des luttes menées sur tous les fronts, dans le domaine politique et idéologique. Il est aussi un canal puissant d'endoctrinement, de fake news, de propagande, la liberté d'expression est difficilement conciliable avec la censure.

L'internet a favorisé une démocratisation de l'espace d'expression. Cependant, le contexte sécuritaire actuel nécessite des changements de paradigmes. La grande question est de savoir comment concilier les libertés fondamentales, la démocratie et la sécurité du citoyen. Le cyberespace est considéré comme étant un espace de liberté, qui bouleverse les critères classiques de la sécurité. Ainsi, cette interrogation constitue le défi majeur des décideurs politiques. Il est très difficile d'arrêter le progrès de la science et l'omniprésence des TIC. Il importe aux décideurs de trouver le juste équilibre, en mettant l'accent sur la formation, la sensibilisation, le cadre juridique en cas de violation dans cette ère numérique et de vitalité démocratique.

Enfin, il convient d'insister sur la nécessité pour les pouvoirs publics de prendre en compte la mutation majeure engendrée par le cyberespace : la fin du monopole des sources d'informations.

LA CYBERCRIMINALITE

IV. La cybersécurité menace-t-elle nos libertés ?

La cybersécurité est définie comme l'ensemble des outils techniques ou non techniques permettant à un Etat de résister à un évènement issu du cyberespace. Il n'est guère aisé de concilier les impératifs de la sécurité publique et la garantie des Droits de l'homme dans ce nouvel environnement géopolitique. Le cyberespace est devenu un lieu de confrontation, un front. Les Etats adoptent une stratégie nationale et un dispositif institutionnel de la cyber sécurité. Dans un monde marqué par la multiplicité et l'imbrication des menaces, la surveillance, la défense et la sécurité dans l'espace numérique posent aujourd'hui de nombreux défis.

CYBER ATTAQUES EN TEMPS REELS

Les Etats sont conscients des risques sécuritaires et de la déstabilisation internationale qui peuvent découler de l'expansion et de la sophistication des Cyber attaques. En effet, une atteinte aux systèmes d'information essentiels (OIV) pourrait engendrer une crise majeure en cas de prise de contrôle ou de paralysie de secteurs vitaux de l'État. L'augmentation constante du niveau de sophistication et d'intensité des cyber-attaques a conduit la plupart des Etats à renforcer leur cyber résilience. Les nouvelles menaces liées à la cyber sécurité imposent des réponses adaptées et proportionnées, mais aussi respectueuses des libertés individuelles, car tout doit tout être encadré par la loi. Les Etats prennent des mesures d'anticipation et de prévention contre le cyber terrorisme, la cybercriminalité, les milieux maffieux, domaines où les Services Spécialisés de Renseignement jouent un rôle essentiel.

De plus, pendant les périodes d'élection ou de tension politique, des coupures ou des restrictions de l'internet sont notées dans certains pays. Ce qui freinent les activités des PME et startups. Ces mesures engendrent des pertes financières colossales pour les activités économiques. Les libertés ne sont pas menacées en règle générale, cependant la prise en compte des nouveaux défis sécuritaires implique une adaptation de la loi, qui découlerait de l'analyse des menaces. Cette situation conduit parfois à une restriction des libertés fondamentales pour des impératifs de sécurité publique. Ainsi, les décideurs à tous les niveaux sont confrontés à de nombreux défis à la fois politique, économique et démocratique, dans un contexte de risques sécuritaires accrus dans le cyber espace.

V. Comment concilier les libertés du citoyen avec les impératifs de cybersécurité ?

C'est le grand débat dans toutes les démocraties actuelles, particulièrement occidentales. L'épineuse question est de concilier la sécurité publique et les libertés fondamentales du citoyen. Les lois érigées afin de combattre les cyber menaces et le cyber terrorisme (écoute de masse et espionnage) génèrent systématiquement un débat autour de l'éthique et des atteintes à la liberté du citoyen. Cependant, la mission régalienne de l'Etat est d'assurer, le bon ordre, la sécurité des citoyens, essence même de la démocratie.

Par ailleurs, le cyberespace est devenu une tribune à résonnance planétaire de toutes les luttes menées dans le monde (politiques, sociales, idéologiques, religieuses), dans un contexte difficile d'édification de nos Etats fragiles et embryonnaires. Parallèlement, la liberté va de paire avec un certain esprit de responsabilité, afin d'éviter toute anarchie. C'est dire toute la difficulté des démocraties dans un contexte de lutte contre les menaces asymétriques, d'obédience djihadiste ou terroriste.

Il convient de noter lorsqu'il s'agit d'effectuer les opérations spéciales d'écoute, d'espionnage de certains milieux maffieux, dans une logique d'anticipation et de prévention d'attentats ou de cyber crimes, ces mesures se font en conformité avec la loi. Ainsi, toutes les enquêtes menées après les attentats survenus en France ont démontré le rôle des TIC, pendant la phase de coordination des actions terroristes, préludes aux attentats spectaculaires. De plus, le cyber espace constitue, pour ces cybers criminels, un lieu de recrutement, d'endoctrinement et de propagande. Dans ce cadre, le renforcement des capacités opérationnelles et des moyens techniques au sein des FDS est une nécessité qui permet de mener des investigations dans l'espace numérique sans frontière. Enfin, la coopération internationale des Agences de cyber sécurité dans le domaine judiciaire et le partage d'informations est une nécessité absolue.

BIBLIOGRAPHIE ET WEBOGRAPHIE :

Légende :
P.S.S.I.E : Politique de Sécurité des Systèmes d'information de l'Etat
SANS : Security Audit Network Système
ISC2 : International Information System Security Certification Consortium
CAMP : Cybersecurity Alliance for Mutual Progress
FIRST : Forum Incident Response Security Team
OIV : Organisme d'Importance Vitale
*CIIP : **C**ritical **I**nformation **I**nfrastructure **P**rotection*

- Expert meeting on cybersecurity in West Africa
- Joint Chiefs of Staff, Joint Vision 2010.la full spectrum dominance
- Atelier de partage des experts de la Corée du sud et du Ministère des télécommunications
- James Blackwell, « Revolution in military affairs », *Battlefield of the Future 21st Century*
- Monde International du 12/12/2016
- IMS course Fort Gordon USA
- www.anssi.fr
- www.usarmy.mil
- Projet de décret portant creation et fixant les régles d'organisation et de fonctionnement de l'Agence nationale de la cybersecurité et de la cyberdéfense (ANCC) du 04 juillet 2016

SOCIALNETLINKTV
Les coupures d'internet en Afrique , un paradoxe pour la démocratie et le développement socioéconomique
Justin Oumar BAMAH OSSOVI, Juriste-chercheur en cyber Droit

- **La mondialisation et les conséquences politiques du pluralisme négatif**
  David E. Apter
- **Revue internationale des sciences sociales 2007/2 (n° 192)**, pages 285 à 300