le cnam

Conservatoire National des Arts et Métiers

ÉCOLE DE GUERRE

Mémoire de Master 2 en Sciences Criminelles intitulé :

L'Impératif de la cyberdéfense au sein des armées ouest-africaines :

Menaces et dimensions sécuritaires.

(Focus sur G5 Sahel)

Commandant Ingénieur

Isselmou Beidy Messaoud

Mauritanie

Stagiaire à l'Ecole de Guerre de Paris 2017-2018

Directeur de mémoire : M. Philippe BAUMARD Professeur des universités, agrégé des facultés Conservatoire national des arts et métiers

DEDICACES

Je dédie ce modeste travail à ma mère et mon père. A mon épouse et à mes enfants.

A tous mes amis et camarades de la 25° Promotion de l'Ecole de guerre de Paris et les étudiants Master 2 criminologie au Conservatoire national des arts et métiers (CNAM).

Une dédicace spéciale est faite à l'ensemble de l'encadrement de l'Ecole de guerre (EdG) et du Conservatoire national des arts et métiers (CNAM) pour l'opportunité offerte et l'attention particulière au travail réalisé. Ce travail est aussi dédié à tous ceux qui, de près ou de loin, ont participé à son élaboration.

REMERCIEMENTS

En guise de témoignage et de reconnaissance, je remercie tous ceux qui de près ou de loin ont accepté de m'apporter leur soutien inestimable par l'orientation, l'aide et l'assistance faites à mon égard pendant les moments d'élaboration de ce travail :

- M. Philippe BAUMARD, Professeur des universités, agrégé des facultés Conservatoire national des arts et métiers Directeur de mémoire, de m'avoir encadré dans la rédaction du Mémoire, de m'avoir encouragé, guidé et soutenu tout au long de cette année universitaire 2017-2018.
- L'ensemble des professeurs et intervenants durant l'année scolaire 2017-2018 au profit du Master 2 criminologie
- Commandant de Vaisseaux François MAJOUFRE professeur de groupe à l'EdG
- Chef de Bataillon Henri HOURS mon binôme à l'EdG
- Mme Hapsatoue Dia, Secrétariat Master Criminologie/CNAM

Je témoigne tous mes remerciements, ma reconnaissance et ma gratitude à toutes les personnes ayant contribuées de près ou de loin, de par leur courtoisie et soutien ayant accepté de m'orienter et de m'apporter leur assistance et leur aide inestimable pendant tout le temps de préparation de ce mémoire.

Résumé:

*« We must **take change** by the **hand** or rest assuredly, **change** will **take us** by the **throat**» Winston Churchill, Homme d'état, Homme politique, Premier ministre du Royaume Uni (1874 - 1965).*

Cette citation de Churchill parait bien adaptée à la situation de nos armées ouest-africaines. Ces dernières sont confrontées au terrorisme qui peut muter et prendre plusieurs formes de menaces dont la menace cyber en plus de celle classique qui peut venir des personnes criminelles (hackers) ou organisations étatiques ou non. Ces armées doivent saisir l'opportunité « Alors mieux vaut prendre le changement par la main avant qu'il ne nous prenne par la gorge ». Autrement dit il est temps pour elles de prendre leurs responsabilités et affronter cette menace incontournable, en étroite collaboration avec nos partenaires européens si nécessaire.

Abstract :

*« We must **take change** by the **hand** or rest assuredly, **change** will **take us** by the **throat**» Winston Churchill,* Statesman, Politician, Prime Minister *(1874 - 1965).*

This quote from Winston Churchill suits well our West African Countries Armies that face terrorism which is susceptible of multiple kinds of threat such as cyber and classical form conducted by criminal individuals (hackers), state or non-state organizations. These armies ought to seize the opportunity “to make reliable changes before takes us by the throat”. In other words, it is time to play our role in order to counter such preordained and ubiquitous phenomenon that calls for a tremendous collaboration with our European partners.

Les idées ou opinions émises dans ce document ne peuvent en aucun cas être considérées comme l'expression d'une position officielle et n'engagent que la responsabilité de son auteur.

Introduction

« Les progrès des technologies numériques les rendent indispensables au fonctionnement de nos sociétés, de l'Etat comme de nos armées. Caractérisé par la multiplicité de ses acteurs, privés et publics, un faible encadrement juridique et la difficulté d'attribution des attaques, le cyberespace est générateur de vulnérabilités nouvelles, qui font de notre souveraineté numérique un enjeu prioritaire.» Cette synthèse cyberdéfense de la revue stratégique de défense et de sécurité nationale française du 17 octobre 2017 ; résume la complexité et l'opportunité du cyberespace qui se caractérise par la rapidité de l'innovation numérique et conduit inéluctablement à **décloisonner** davantage les domaines civil et militaire d'une part et inter-état d'autre part pour introduire plus d'agilité[1].

Ce mémoire a pour ambitions de décrire, comprendre et expliquer les menaces et dimensions sécuritaires dues à la criminalité cybernétique (Phénomènes de cyberattaques) et l'impératif de s'en prémunir ou au moins limiter les dégâts le plutôt possible tout en mutualisant les efforts de cyberdéfense civils et militaires dans la sous-région ouest africaine et notamment du G5 sahel.

La cyberdéfense représente un enjeu majeur pour les Armées. Aujourd'hui, toute opération militaire comporte un volet cyber. Au même titre que la terre, la mer et l'air, l'espace numérique constitue un milieu à part entière dont la défense est une nécessité permanente qui relève de la souveraineté nationale. Pénétration des réseaux à des fins d'espionnage, prise de contrôle à distance, destruction d'infrastructures vitales, les types de menaces sont nombreux et variés[2].

La cyberdéfense, sujet d'actualité dans nombre de pays et d'institutions, semble paradoxalement ignoré par les institutions militaires (voir étatiques) ouest-africaines.

A ce titre, ce modeste travail pourra être compléter à l'avenir et faire l'objet d'une étude académique plus élevé (dans un enchainement logique) au niveau d'un environnement plus approprié, plus riche et plus proche de la réalité africaine.

L'originalité de cette étude tient d'abord à l'absence d'études ou d'expertises dans le domaine de la cyberdéfense dans la sous-région et en particulier au sein des institutions militaires des différents pays concernés.

[1] Revue stratégique de la défense et de sécurité nationale françaises du 17 octobre 2017.
[2] http://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation

La cyberdéfense regroupe l'ensemble des activités conduites afin d'intervenir militairement ou non dans le cyberespace pour garantir l'effectivité de l'action des forces armées. C'est l'ensemble des outils, concepts et mécanismes de sécurité et les méthodes de gestion des risques en vue de protéger le cyber-environnement (dispositifs informatiques, infrastructures et applications, informations transmises et/ou stockées …), via la **cyber-sécurité** et à garantir l'assurance et la maintenance du cyber-environnement par rapport aux risques identifiés ou non[3]. La cyberdéfense est à différencier de la cybercriminalité qui correspond à l'ensemble des crimes et délits traditionnels ou nouveaux réalisés, via les réseaux numériques. La cyberdéfense englobe la lutte informatique défensive (LID) et la lutte informatique offensive (LIO), elle permet de défendre et d'attaquer des ensembles de réseaux et d'ordinateurs qui contrôlent un pays[4].

La cyberdéfense aujourd'hui au sein des armées en général et celles ouest-africaines en particulier parait un impératif incontournable dans un contexte de mondialisation imposé.

Destruction d'informations, corruption ou modification d'informations, vol, suppression ou perte d'informations, divulgation d'informations, interruption de services, les cybermenaces et les cyberattaques deviennent de plus en plus fréquentes, sophistiquées et dommageables. L'environnement cyber est complexe : des acteurs étatiques ou non peuvent utiliser les cyberattaques dans le cadre d'opérations militaires ou pour mener des actions de guerre hybride. De plus, la frontière entre cybercrimes et cyberattaques est souvent mince ; si les auteurs des attaques sont difficilement identifiables, leurs motivations peuvent l'être également. Le contrôle d'accès, l'authentification, la non-répudiation, la confidentialité des données, la sécurité des communications, l'intégrité des données, la disponibilité, le respect de la vie privée, sont autant de dimensions sécuritaires à garantir.

Afin de promouvoir ce qui est désormais appelé la cinquième dimension de l'action militaire, la mise en place d'une stratégie commune de lutte contre ce fléau et une vision partagée de la cyberdéfense, dans les armées ouest-africaines semble inévitable. Cela passe nécessairement par une réflexion approfondie et des actes

[3] http://data-scientix.com/cyberdefense-menaces-et-dimensions-de-securite-sujet-detude-pour-le-data-scientist/
[4] http://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation

concrets en vue d'harmoniser la législation et la réglementation, la mise en commun des moyens et outils physiques et virtuels de lutte (recherche et innovation), le renforcement des capacités et le partage de connaissances en matière de cybersécurité et de cybercriminalité pour pallier le retard préoccupant tant au niveau des états, qu'au niveau des armées.

Parce que leur connectivité est aujourd'hui accrue, le grand défi des armées ouest-africaines est désormais de préserver un parc informatique particulièrement vulnérable face aux cyberattaques de type APT (Advance Persistant Threats) pour lesquelles les traces de compromissions des systèmes d'information sont très discrètes. « L'Afrique est une source de cybercriminalité avec des foyers majeurs comme le Cameroun, le Sénégal, la Côte d'Ivoire ou le Benin. Les ordinateurs sont très peu sécurisés et le risque de piratage est omniprésent », constate Karim Ganame, fondateur burkinabé de la start-up Efficient Protection spécialisée en cybersécurité[5].

Face à une mondialisation dérégulée (sans ordre mondial) et une hyper connexion (objets connectés, Big Data) et au moment où les Américains, les Occidentaux et les Asiatiques posent les jalons technico-législatifs et mènent une cyberguerre à tous les niveaux que ça soit politique, économique ou militaire, l'Afrique malheureusement n'est pas au rendez-vous comme d'habitude. Les cyberattaques d'aujourd'hui, étant très variées, dangereuses et furtives (difficilement traçables), et étant donnée la nécessité de se coordonner avec de nombreux acteurs (étatiques ou non) pour les contrer. La dimension sécuritaire de la cyberdéfense doit faire de la mutualisation des moyens un préalable pour aboutir aux meilleures solutions et gérer les risques potentiels associés. D'autant plus que cette mutualisation s'inscrit dans la lutte **contre** *le terrorisme qui pourra à l'avenir utiliser ces moyens pour pallier d'éventuelles défaites tactiques sur le terrain.*

Pour une meilleure cohérence dans l'étude de ce sujet, nous allons dans un premier temps présenter la cyberdéfense et les cybermenaces ; dans un deuxième temps, nous évoquerons les enjeux et dimension sécuritaires, notamment au regard de la vulnérabilité des infrastructures et de la numérisation rapide des sociétés; dans un troisième temps, nous proposerons une solution à travers une approche globale

[5] http://www.jeuneafrique.com/398696/economie/acces-a-internet-continent-africain-entre-progres-inegalites/

inclusive basé sur la création d'une structure militaire du cyber chargée de la formation, la recherche et le développement des capacités en sécurité numérique aux profit des Etats et de leurs armées, l'amélioration du cadre juridique de l'information et le partenariat inter-états d'une part et avec nos partenaires d'autre part.

Chapitre 1 : La Cyberdéfense

La question de la cyberdéfense est d'actualité depuis les évènements survenus en Estonie en 2007. Pays pionnier de l'Union européenne (UE) en matière d'utilisation de l'Internet, l'Estonie - 1,3 million d'habitants, 46 % des foyers équipés - est devenue un cas d'école depuis que ses sites gouvernementaux, ses banques et ses médias ont subi une vague d'attaques cybernétiques, entre le 26 avril et le 18 mai. Au même moment, la république balte traversait une crise de ses relations avec la Russie, née du déplacement d'un monument à la gloire de l'armée soviétique à Tallinn[6]. Pour Linnar Viik, l'un des gourous estoniens de l'Internet, cité par *The Economist,* « *la mobilisation d'une telle armada informatique dépasse de très loin le stade de l'initiative individuelle, voire même mafieuse. Rien de tel ne peut se faire à cette échelle sans la coopération d'un Etat, et de plusieurs opérateurs télécoms*[7]*».*

De manière évidente cette affaire a relancé les débats, suscité des interrogations aux seins des autorités et des états-majors. Depuis nous assistons à la mise en place de nouvelles stratégies nationales qui s'accompagnent également de la création d'agences, d'unités de cyberdéfense et de cybersécurité[8]. Il ne s'agit plus uniquement de disposer d'outils de veille et d'alerte, mais de structures capables d'aller plus loin : mener des enquêtes, remonter aux sources être prêtes à l'action agressive, en temps de conflit, mais aussi de crise ou simplement de paix[9].

Nos armés sont chargées d'assurer et de garantir la défense de nos pays contre toutes les formes de menaces en tout temps et en toute circonstance et de faire respecter les lois et protéger les populations et leurs biens ; dans le cadre de leurs missions régaliennes et conventionnelles, elles se doivent d'assurer leur propre sécurité numérique et se donner les moyens humains et techniques nécessaires leur permettant également d'assurer celle des Etats dans un but de souveraineté nationale afin de leur garantir une résilience indispensable..

C'est dans ce cadre qu'aujourd'hui, les États-Unis, la Chine et, dans une moindre mesure peut être, les Russes et les Européens se préparent à la prochaine génération de conflits. Ce qui fait de la cyberdéfense un impératif majeur et prioritaire. D'autant plus qu'elle est principalement basée sur les systèmes de

[6] http://www.lemonde.fr/europe/article/2007/06/27/l-estonie-tire-les-lecons-des-cyberattaques-massives-lancees-contre-elle-pendant-la-crise-avec-la-russie_928568_3214.html#jgs4t1gOyvijRKF1.99
[7] http://www.01net.com/actualites/lestonie-denonce-les-cyber-attaques-terroristes-russes-350759.html
[8] NATO Cooperative Cyber Defence Centre of Excellence, établi en 2008
[9] Daniel Ventre, cyberattaque et cyberdéfense, hermes science Lavoisier § P. 96

détection d'intrusion (IDS), les scanners de vulnérabilités, antivirus ainsi que les systèmes de gestion et corrélation d'événements sécurité donc sur la SSI. Lorsqu'il s'agit de superviser un système informatique à grande échelle réparti sur plusieurs sites, il devient vite très difficile de corréler et analyser toutes les sources d'information disponibles en temps réel afin de détecter les anomalies et les incidents suffisamment vite pour réagir efficacement. Cette complexité est due à la quantité d'information générée[10] entre autres. A cela on peut ajouter la furtivité et l'agilité des attaquants (Hackers) qui ne cessent d'améliorer des techniques d'attaques sans cesse plus sophistiquées depuis 1972.

Pour comprendre ce phénomène de cyberdéfense il est indispensable de définir un certain nombre de termes techniques pour appréhender ses fondamentaux mais aussi et surtout comprendre les cybermenaces et cyberattaques qui conditionnent son évolution temporelle et technique, pour stopper ou atténuer leurs ampleurs.

La lutte contre ces phénomènes doit s'inscrire dans le temps et doit faire l'objet d'une coordination tant entre les différentes armées de la sous-région qu'entre les différentes composantes participant à la défense des intérêts de la nation mais surtout en étroite collaboration avec le secteur privé et nos partenaires notamment occidentaux. Les attaques cybernétiques sont une forme d'agressions qui requière le concours de tous pour les vaincre par le déploiement des savoir-faire techniques et la mise en place de législations pour mieux appréhender et réprimer ce fléau.

[10] https://www.sstic.org/media/SSTIC2010/SSTIC-actes/CyberDefense/SSTIC2010-Article-CyberDefense-lagadec.pdf

a- Quelques définitions pour comprendre le phénomène

La définition de certains termes a pour objectif de mettre au clair des termes que certains utilisent sans connaitre le sens technique (surtout les non spécialistes).

Cyberespace : le cyberespace est un domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunication, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs de services en ligne.

Cyberdéfense : ensemble des activités conduites afin d'intervenir militairement ou non dans le cyberespace pour garantir l'effectivité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère. La cyberdéfense est à différencier de la cybercriminalité qui correspond à l'ensemble des crimes et délits traditionnels ou nouveaux réalisés, via les réseaux numériques.

Cyberattaques : acte malveillant de piratage informatique dans le cyberespace. Les cyberattaques peuvent être l'action d'une personne isolée, d'un groupe, d'un État. Elles incluent la désinformation, l'espionnage électronique qui pourrait affaiblir l'avantage compétitif d'une nation, la modification clandestine de données sensibles sur un champ de bataille ou la perturbation des infrastructures critiques d'un pays (eau, électricité, gaz, communication, réseaux commerciaux). La cyberdéfense du ministère vise à détecter et contrer les cyberattaques dont la cible et la finalité sont liées au ministère de la Défense.

Sécurité des systèmes d'information : ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Source[11]

[11] www.defense.gouv.fr

D'autres termes aussi ont une importance dans le dictionnaire cyber telle que :

La cyberguerre : Est avant tout un conflit dans lequel l'acteur étatique doit être présent. Ce type de conflit laisse la possibilité aux acteurs non étatiques d'intervenir. Elle n'est qu'une dimension de la guerre conventionnelle. Elle en est le prolongement, et ne saurait exister sans elle. Il ne saurait donc y avoir de cyberguerre sans conflit armé conventionnel ; les théories de Clausewitz s'appliquent à la cyberguerre qui peut être le prolongement du politique par d'autres moyens, persistance d'un brouillard de guerre, de frictions. Comme toute guerre elle implique le militaire, elle est faite d'ensembles d'opérations militaires, de nature défensive et offensive. Mais elle se distingue toutefois de la guerre conventionnelle car elle écarte le combattant humain au profit de la machine[12].

En pratique et techniquement parlant, l'exploitation du cyberespace à des fins offensive peut se baser sur trois niveaux d'accès constituant les trois couches de cet espace :

- La couche physique : les puces, les ordinateurs, câbles, réseaux, satellites, etc.… Les opérations envisageables consistent à couper les câbles de communication, détruire ou détourner les satellites de leurs trajectoires, cibler les bâtiments abritant les serveurs ou infrastructures de communication entre autres.
- La couche logicielle : applicative (code de données et des protocoles) permettant de créer, traiter ou manipuler les données. C'est ici le champ d'action des hackers (diffusion de malwares, intrusions dans les systèmes, perturbation du fonctionnement des systèmes industriels étatiques, civils ou militaires, vol de données, etc …)
- La couche psychocognitive : c'est le lieu de la guerre de l'information, les opérations y sont multiples ; défiguration de sites internet, exploitation des réseaux sociaux, propagande, désinformations « psyops »[13]

Il est à préciser que l'exploitation complexe de l'une ou l'autre de ces couches est susceptible d'entrainer des effets sur les autres. Cette complexité technologique

[12] Dictionnaire de la guerre et de la paix, sous la direction de Benoit Durieux, Jean-Baptiste jeangène Vilmer, Frédéric Ramel, § P. 337
[13] Dictionnaire de la guerre et de la paix, § P. 338/339

constitue un avantage permettant d'attaquer par surprise et de rester anonyme, elle constitue en revanche un défi majeur du faite de la difficulté de l'anticipation de ses effets et leurs risques collatéraux non maitrisables (interconnexion et interdépendance des réseaux). Ainsi la cyberattaque « stuxnet » lancée contre les systèmes industriels nucléaires iraniens par les Etats- unis et Israël, s'est-elle soldée par la diffusion accidentelle de malware dans des pays non visés, voire des alliés.

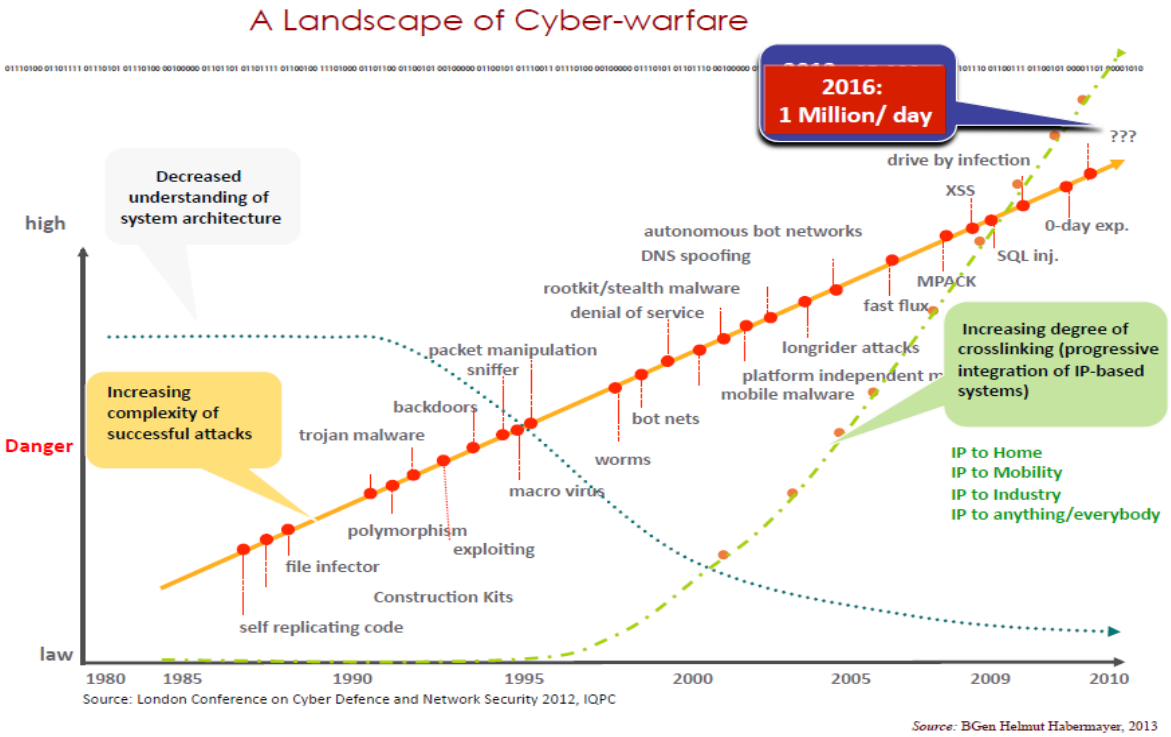
La question de la cybercriminalité se pose dans des nouvelles dimensions qui peuvent paraître par bien des aspects, inquiétantes. De simples outils trouvables facilement sur internet permettent à des néophytes de paralyser des sites web (exemple d'une attaque DDoS par exemple avec l'outil téléchargeable librement LOIC), de casser des mots de passe ou des clés wifi (avec un logiciel comme John The Ripper) facilitant l'intrusion à des données potentiellement sensibles ou de capturer et modifier des données à la volée (par la technique dite de network spoofer) transitant sur le réseau[14].

Enfin, les défis restent importants au sein même de l'institution militaire qui à long terme doit savoir comment intégrer les atouts technologiques de ce milieu dans la stratégie et la doctrine pour à la fois résister à son exploitation par l'ennemi ou l'exploiter nous-même à des fins offensives.

[14] rapport_final_juillet_2015, Master de cybersécurité, sous l'égide du CSFRS

b- **Un peu d'histoire :**

Le hacking (*hackers : pirates de la programmation qui agissent dans l'illégalité la plus complète pour pénétrer des réseaux privés, piller des informations ou mettre à sac des systèmes informatiques*[15]) est l'ancêtre de ce qui est aujourd'hui appelé cyber crime et qui a évolué pour prendre plusieurs forme dont cyber guerre, cyberespace, cyberdéfense ou cybercriminalité selon le niveau d'utilisation et où l'on se positionne. L'historique du hacking, depuis ses années pionnières au début des années 70, jusqu'aux mouvements cyber-libertaires et aux «start-ups» de cybersécurité des années 2010-2016, a systématiquement influencé les méthodes de cyberdéfense et de sécurité numérique. Les changements de culture organisationnelle et sociétale des activités de hacking et leur entrée progressive dans la sphère économique, puis la sphère de puissance des États nations[16] a bouleversé le référentiel jusque-là établi (les activités de cyber, et leur impact sur la société).



L'analyse du paysage cyber met en exergue un certain nombre de constats qui l'ont caractérisé au fil du temps, à savoir l'augmentation de la complexité des attaques

[15] Michel lallement, L'Âge du Faire. Hacking, travail, anarchie, Editions du Seuil, janvier 2015 §P02
[16] https://www.crimecnam.net/k2-user-groups/m-2/crm-210.html

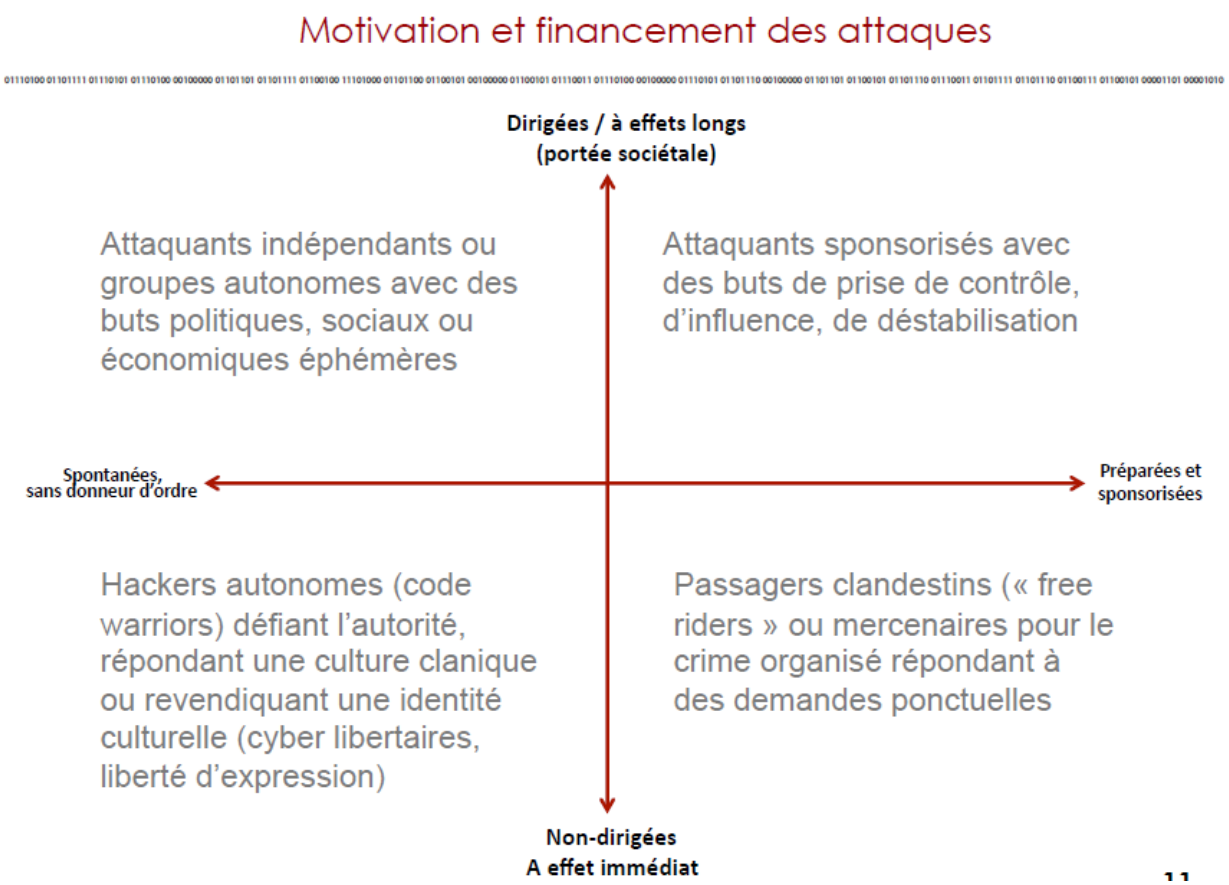
réussies (0-day exploit : *les failles dites « 0-day*[17]*» vulnérabilités d'un produit inconnu du fournisseur du produit ou ne possédant pas de correctif qui constituent des risques majeurs et permanents pour les systèmes d'information Ces failles peuvent se trouver dans n'importe quel code, qu'il s'agisse d'un logiciel classique, d'une application mobile, d'un composant web, d'un service en ligne et ainsi de suite. Des individus et des groupes cherchent ces failles pour les corriger mais aussi pour les exploiter. Parmi eux, il y a bien évidemment « les pirates » - hackers, crackers, ... mais également les agences de sécurité et de renseignement comme la NSA National Security Agency*) qui dépassent le million par jour depuis 2016 comme le montre la figure (Cf. *CRM 210 du CNAM: Introduction générale cybercriminalité, cybersécurité, cyberdéfense* (3C) qui résume de manière succincte l'évolution des 3C depuis 1972 à nos jours et dont on présente ici quelques illustrations pour mieux comprendre son évolution et sa mécanique).

La croissance des connexions et adressages IP (réticulation) ; « *l'internet a grossi jusqu'à interconnecter des milliards de machines et aujourd'hui, on ne comprend plus son comportement dans sa globalité*[18] », ce qui rend très difficile voire impossible de suivre la trace des attaques éventuelles et enfin par une diminution de la compréhension de l'architecture des systèmes en effet l'utilisateur est demandeur de convivialité, et les progrès de l'ergonomie des interfaces lui masquent la complexité du système - complexité dont il n'a d'ailleurs pas forcément conscience. Cette question est normalement logique et très importante dans un cadre purement criminologique pour savoir les réelles motivations des phénomènes, ce qui n'est pas forcément le cas des consommateurs simples.

[17] ANSSI, Vulnerabilities 0`day, prévention et bonnes pratiques, http://www.ssi.gouv.fr/IMG/pdf/guide_vulnerabilites_0day.pdf

[18] Didier DANET et Amaêl CATTARUZZA, 2014, « la Cyberdéfense quel territoire, quel droit », Paris, Economica § P.43

le cnam

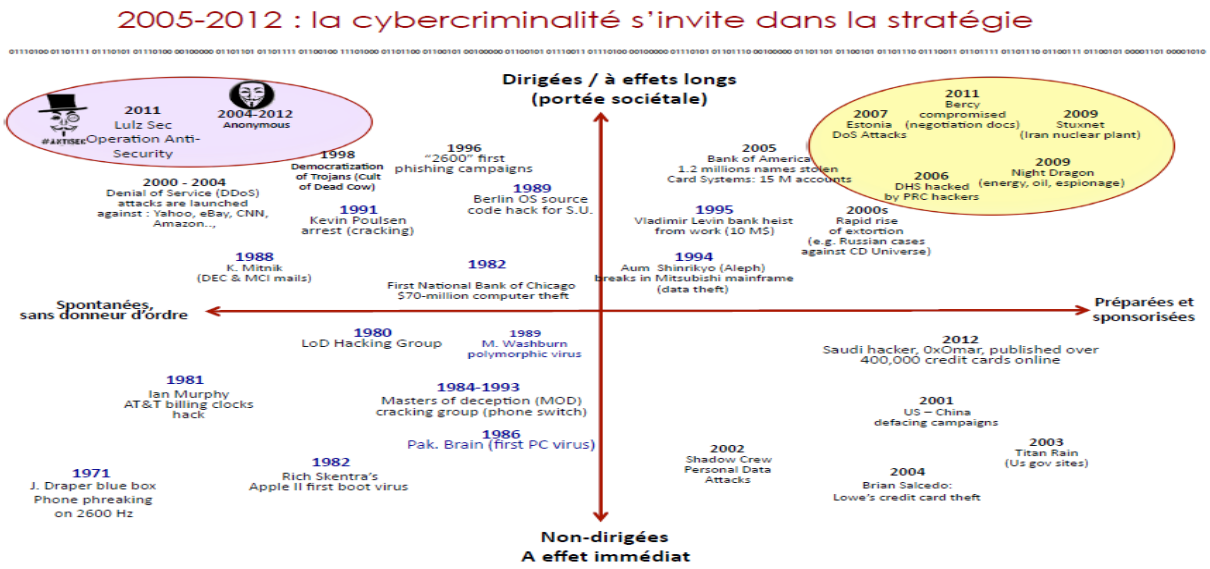


Sur un plan purement militaire, l'utilisation de l'information (cyberespace ou warfare) et la manipulation des connaissances aura pour but d'obtenir un avantage stratégique, pour tromper, faire de l'ombre ou détruire un adversaire ou un opposant, c'est aussi l'action par un État-nation de pénétrer les ordinateurs ou les réseaux d'une autre nation à fins de causer des dommages ou de la perturbation. Le Pentagone a officiellement reconnu le cyberespace comme une nouvelle composante de la guerre qui est devenu aussi critique pour les opérations militaires à l'image des composantes terre, mer, air et espace. (William J. Lynn, Sous-secrétaire à la Défense des États-Unis).

Historiquement, le hacking a passé par quelques étapes à savoir les années pionnières de 1972 à 1985 caractérisées par l'exploit d'individus talentueux cherchant de petits gains symboliques (LoD Hacking Group, Rich Skentra's Apple II first boot virus, …). Après cette période se fût la naissance du cyberespace durant les années 1990 avec une démocratisation des technologies de hacking, le développement des attaques à portée sociale et des sous-cultures organisées (Democratization of Trojans (Cult of Dead Cow), Kevin Poulsen arrest (cracking), …).

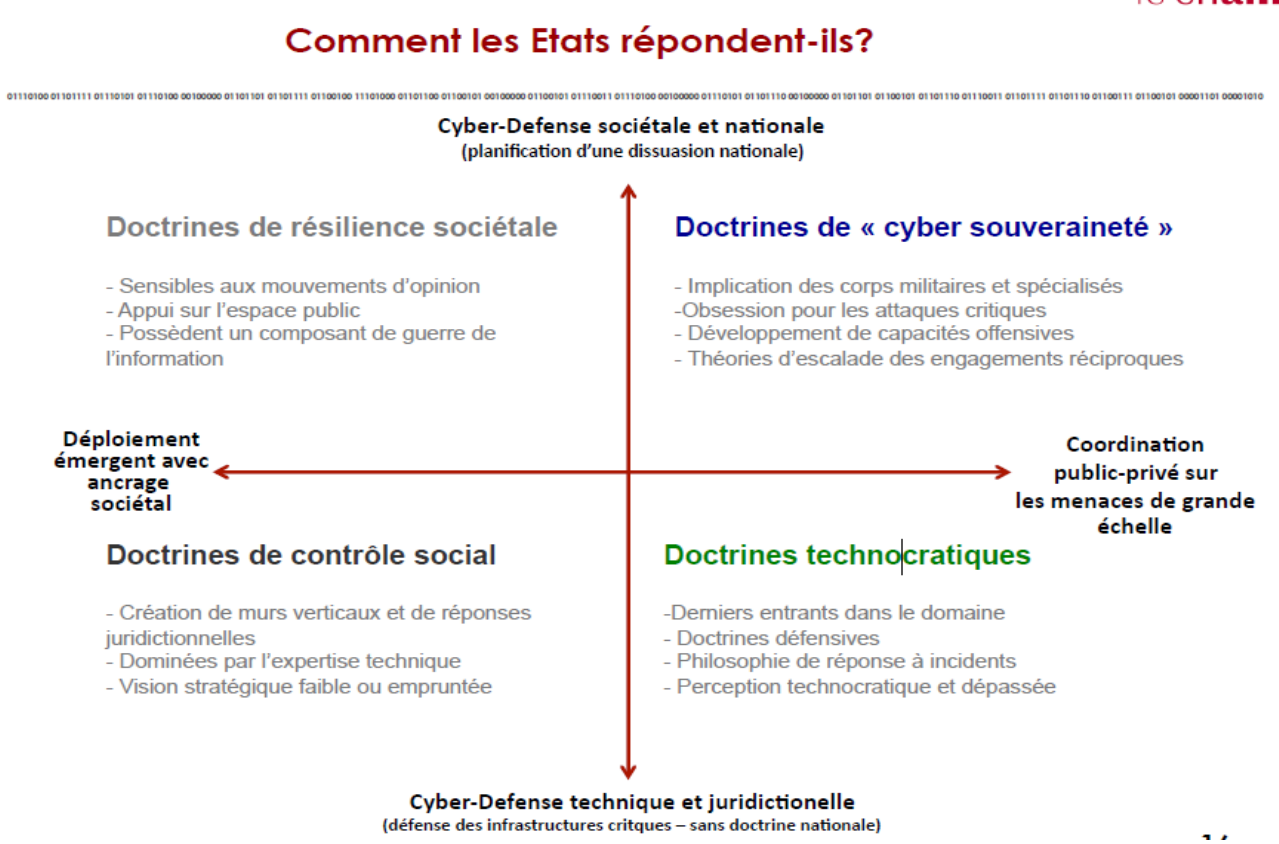
Ensuite, les années 2000 caractérisées par la monétisation du cyber-crime et les premières confrontations inter-états font leur apparition (Rapid rise of extortion (e.g. Russian cases against CD Universe), US – China defacing campaigns, Titan Rain (Us gov sites)).

Enfin, la période s'étalant de 2005-2012 où la cybercriminalité s'invite dans la stratégie avec l'apparition des Anonymous, des attaques visant des intérêts étatiques vitaux (Stuxnet en 2009 (Iran nuclear plant), Bercy compromised (negotiation docs) en 2011, Saudi hacker, 0xOmar, published over 400,000 credit cards online, etc …).



Face à ces nouvelles évolutions multiformes qui peuvent mettre en péril les centres névralgiques des états et dans un contexte où une attaque ciblée du système informatique peut porter un coup fatal à l'économie d'un pays ou endommager ses chaines de production vitales, des réactions étatiques basées sur des doctrines nouvelles ont vu le jour ; doctrines de résilience sociétale, doctrines de « cyber souveraineté », doctrines de contrôle social, doctrines technocratiques. Avec l'apparition de nouveaux vecteurs de référencement et d'appréciation dans le domaine cyber. La machine de la défense occidentale repose en majeure partie sur l'IP (cyberespace) qui constitue une vulnérabilité et une cible d'attaque capitale et probable. La figure suivante décrit clairement les réponses étatiques en matière de cyberdéfense face à ces nouveaux changements impliquant l'ensemble des moyens disponibles.

le cnam



Le Livre blanc français sur la Défense et la sécurité nationale de 2013 rappelle que la capacité de l'État à se protéger contre des attaques informatiques majeures constitue un enjeu de la souveraineté nationale. Il définit une doctrine nationale de réponse aux agressions informatiques majeures. La cyberdéfense militaire française s'inscrit pleinement dans le cadre de cette doctrine et vise à placer le combat numérique au service des opérations. Les armées doivent donc se doter des capacités défensives et offensives, adossées à de solides capacités de renseignement (numérique).

L'Afrique peut-elle se permettre de négliger les risques électroniques qui guettent ses entreprises et ses gouvernements ? La dernière attaque "Wannacry" est l'énième rappel que le continent n'est pas en marge des guerres numériques mondiales. Avec des dégâts répertoriés dans de nombreux pays, l'Afrique se confronte encore une fois, non pas sur son incapacité à se défendre, mais sur son inconscience des risques[19]. Un vieux proverbe français dit : « Le monde appartient à ceux qui se lèvent tôt.» autrement dit pour réaliser ses ambitions et réussir ses projets, il faut se mettre à l'œuvre sans attendre.

[19] https://afrique.latribune.fr/africa-tech/2017-05-18/cyber-securite-l-afrique-une-proie-facile-715875.html

c- Cybermenaces et les Cyberattaques

- **Cybermenaces :**

« La méfiance et la prudence sont les parents de la sécurité » ***Benjamin Franklin***

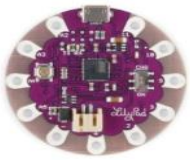
L'ANSSI dans son Guide n° 650 « *Menaces sur les systèmes informatiques* » de septembre 2006)[20] expose des méthodes globales d'attaque afin de porter atteinte à la sécurité des systèmes d'information :

• L'écoute ou l'interception de signaux, rendu plus facile par l'usage de transmission sans fils notamment via des hotspots wifi, 3 / 4G ou liaison radio.

• Le vol du matériel devenant problématique si les données ne sont pas cryptées.

• Le piégeage de logiciel par virus, malware, exploitation d'un défaut, rootkits (logiciel furtif permettant de pérenniser un accès à distance), trojans (cheval de Troie), RAT (Remote Access Trojan) est rendu plus facile par le nomadisme et la multiplicité des matériels,

• L'utilisation illicite de matériels notamment grâce à des *backdoors* (trappes) ouvertes par des logiciels ou laissé intentionnellement par le constructeur matériel ou tout simplement par la négligence des utilisateurs (facilitées par l'internet des objets, matériels électroniques open-source à bas coûts teensy, arduino, lilypad, raspberry pi) en plus des langages informatiques simples et l'échange de code open source.

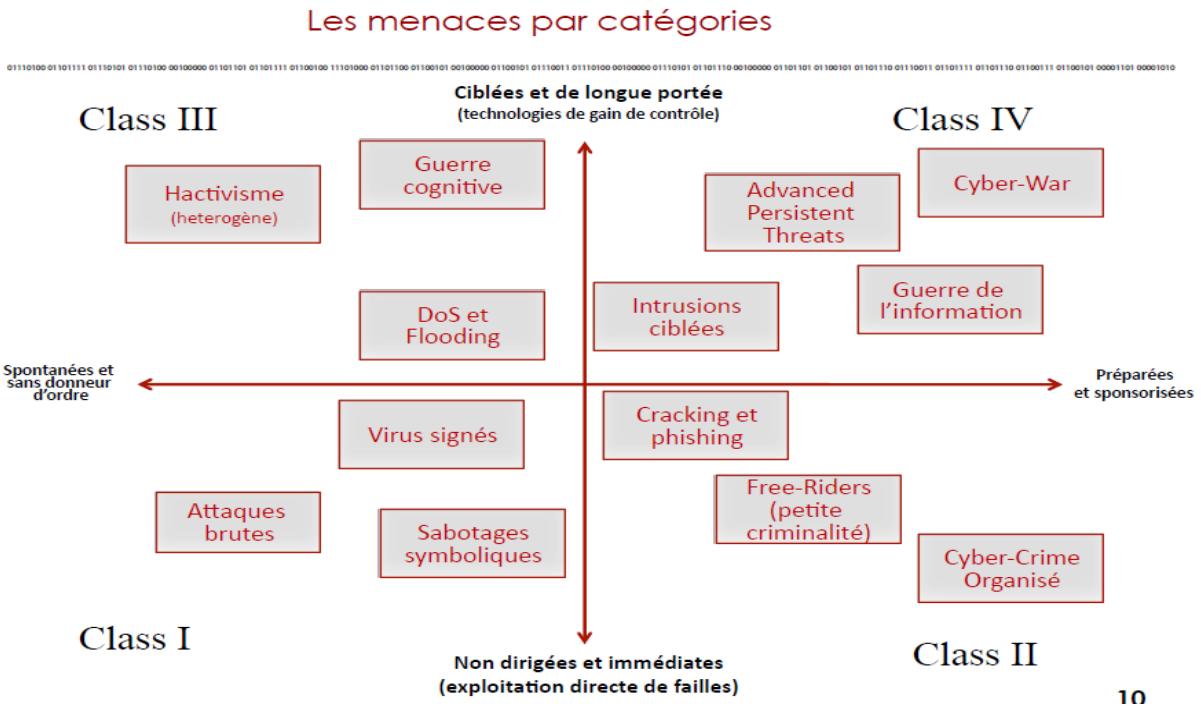




La visibilité et la compréhension des cybermenaces, leur classification et les outils pour y faire face sont la meilleure façon d'anticiper et de se préserver contre les cyber-agressions même si c'est un exercice objectivement difficile car la menace n'est pas un état stable, mais plutôt une succession particulièrement rapide d'états intermédiaires.

Selon qu'elle soit ciblée ou non, spontanée ou préparée et sponsorisée, la cybermenace peut être divisée en quatre classes décrites par la figure suivante.

[20]ANSSI, «Menace sur les Systèmes informatiques, Guide n°650, http://www.ssi.gouv.fr/IMG/pdf/Guide650-2006-09-12.pdf

le cnam



La classe IV est la plus dangereuse car elle comprend les menaces persistantes avancées qui sont furtives, continues et généralement préparées et ciblées. Mais il ne faut pas pour autant négliger les autres menaces.

Cela est d'autant plus difficile si l'on sait que des pays puissants et parfois alliés participent à la menace cyber. Ainsi, les militaires américains sont autorisés à « préparer » l'engagement futur en déployant des systèmes non agressifs en temps de paix afin de s'assurer de la viabilité des routes qui pourraient véhiculer des codes malveillants[21]. « *Le nouveau guide sur les cyber-opérations autorise les militaires à insérer des algorithmes informatiques dans les réseaux et les ordinateurs d'autres pays pour s'assurer de la viabilité des routes et des connexions. Ce travail s'inscrit dans le cadre d'un programme de surveillance et ne peut pas inclure de virus ou de vers qui pourraient être déclenchés plus tard. Toutefois, dans l'hypothèse d'un conflit ultérieur, les algorithmes auraient cartographié les voies permettant de conduire une véritable cyberattaque*»[22].

Les cybermenaces touchent désormais tous les secteurs : l'économie et les flux financiers (banques, escroquerie en ligne…), les données personnelles ou confidentielles sont souvent détournées pour être monnayées (réseaux sociaux), les objets connectés (ou transports intelligents) seront particulièrement visés dans les

[21] Bertrand BOYER, Cyberstratégie l'art de la guerre numérique nuvis,§P 166
[22] David A. Fulghum, Cyber-warfighting Rules Biginning To Emerge. Traduction de l'auteur.

années à venir et finalement les données militaires seront indéniablement parmi les futures cibles de choix et seront doublement ciblées soit par des groupes terroristes soit par des actions d'états concurrents ou ennemis. Ce qui nous impose de nous s'adapter continûment.

L'objectif de la cybermenace est de compromettre un système (un réseau interne) pour prendre son contrôle et permettre à un utilisateur externe d'accéder aux données sensibles, les extraire ou télécharger du code ou des programmes qui sont inactifs et attendent d'être déclenchés, prendre en charge des centaines, voire des milliers de ressources réseau pour contrôler la bande passante pour d'autres activités de piratage et en fin s'évader sans laisser de trace ni être déceler par la cible. Il est observé que les piratés sont devenus de plus en plus sophistiqués et peuvent être financés et parrainés par les États, ce qui explique l'utilisation de la «cyberguerre » qui semble augmenter à des fins spécifiques ou gain monétaire. En Afrique, un autre problème peut s'ajouter, grâce à la faiblesse des législations ainsi que le manque de conscience des problématiques liées au cyber, les hébergeurs de contenus situés en Afrique peuvent être relativement protégés des actions des forces de l'ordre. Un acteur non africain avisé pourrait très bien héberger quelques-uns de ses serveurs en Afrique, en profitant de vides juridiques pour fournir un service de location de serveur dit « Bullet-proof »[23] à l'image de l'immatriculation des bateaux battants pavillons.

[23] LA CRIMINALITÉ INFORMATIQUE AVANCÉE EN AFRIQUE, Auteurs : Jean-Jacques Alex, Gilles Chabannes, Pierre-Marie Léoutre, Ronan Mouchoux, Master M2

- **Cyberattaques :**

La cyberattaque se base essentiellement sur trois méthodes (Outils de cyberattaques) pour sa mise en œuvre à savoir :

Espionnage et violations de la sécurité nationale

Le cyber espionnage consiste à obtenir des secrets (informations confidentielles, sensibles ou classifiées) de particuliers, concurrents, rivaux, groupes, gouvernements et ennemis à des fins militaires, politiques ou économiques en utilisant des méthodes illégales d'exploitation sur Internet, réseaux, logiciels et / ou ordinateurs[24].

Le Sabotage

C'est le fait de rendre inopérant tout ou partie d'un système d'information d'une organisation via une attaque informatique. Le sabotage s'apparente à une « panne organisée », frappant tout ou partie des systèmes, selon le type d'atteinte recherchée, désorganisation durable ou non, médiatisée ou non, plus ou moins coûteuse à réparer. Pour y parvenir, les moyens d'attaques sont d'autant plus nombreux que les organisations ne sont pas toujours préparées à faire face à des actes de malveillance[25].

Les ordinateurs et les satellites qui coordonnent les activités sont des composants vulnérables et pourraient entraîner la perturbation d'autres équipements. L'électricité, l'eau, le carburant, les communications et l'infrastructure de transport peuvent tous être vulnérables à la perturbation.

Le Déni de service

En informatique, le déni de service (DoS) ou de déni de service distribué (DDoS) est un moyen de rendre une machine ou une ressource réseau indisponible à ses utilisateurs prévus. Les auteurs de DoS ciblent généralement des sites ou des services hébergés sur des serveurs Web de haut niveau tels que des banques, des passerelles de paiement par carte de crédit et même des serveurs racine.

L'attaque par déni de service est un grand classique du cyber-crime. Elle consiste à inonder le serveur d'un site Web de requêtes jusqu'à la paralysie ce qui entraîne

[24] Doc CNAM/CRM210 introduction générale au cyber
[25] https://www.ssi.gouv.fr/entreprise/principales-menaces/sabotage/

inévitablement un écran noir. Ou plus précisément une page d'erreur http 404, c'est-à-dire une fin de non-recevoir pour tout internaute désirant visiter ce site Internet.

Les attaques informatiques suivent toujours le même schéma cinq phases[26]:

1- Une phase de prise d'informations sur le système à attaquer : ciblage du système à attaquer par l'analyse des protocoles qui renvoie un certain nombre d'informations intéressantes sur le système cible (analyse de trafic réseau)pour identifier des vulnérabilités (mises à jours et correctifs non effectués). De nombreuses techniques combinées sont utilisées avec de plus en plus un ciblage des utilisateurs du système à l'aide des réseaux sociaux. Ainsi, la cyber-attaque de l'Elysée en mai 2012 a débuté via le réseau social Facebook.

2- Un gain d'accès : L'objectif est de s'introduire sur le système cible soit simplement quand le système n'est pas vraiment protégé (mot de passe « usine » non modifiés), par cassage de mots de passe par force brute, ou encore par l'introduction de cheval de Troie (trojans), malwares, à l'aide le plus souvent, de pièces jointes dans des Mails ou via des téléchargements (exemple du malware introduit par le FBI via le réseau TOR).

3- Une élévation de privilèges : (avec le plus souvent des fonctions d'administration) afin de prendre en main le système cible. Ceci n'est le plus souvent possible qu'au travers de l'exploitation de failles de systèmes d'exploitation et peut se faire en local sur le système ou à distance.

4- Un maintien de l'accès : Ce processus consiste à ouvrir des « portes dérobées » (backdoors) afin de revenir sur le système à n'importe quel moment. Ceci peut être utile lors d'attaques par « déni de service » ou d'envoi de Mails de grande ampleur (« pourriels ») nécessitant l'usage de milliers de machines zombie (on parle alors de botnet : robot + network). Il est à noter que certaines backdoors sont parfois installées par le fabricant lui-même (exemple sur Samsung Galaxy ou routeur DLink).

5- Nettoyage des traces : Après l'attaque, il est intéressant d'effacer les traces de son passage afin d'éviter d'être identifié d'une part et le cas échéant de pouvoir recommencer une attaque similaire dans le futur.

Nous devons sans cesse améliorer nos défenses pour lutter efficacement contre les pirates et, pour ce faire, connaître leurs méthodes peut être d'une aide précieuse indispensable.

[26] rapport_final_juillet_2015, Master de cybersécurité, sous l'égide du CSFRS, Annexe 7

Durant la « Session Number C22 Introduction to Advanced Security Threats, Conference November 8th, 2011 » M. Bryan Kissinger, PhD, ISACA SF Fall a présenté l'évolution du paysage des menaces sécuritaires et la façon d'assurer l'avenir au vue de cette évolution. C'est sur cette étude que nous nous sommes basés pour décrire les types d'attaques les plus courantes et les méthodes pour limiter leurs impacts. Les attaquants sont multiples, protéiformes, variées et plus inventifs que jamais :

Campagnes de Spearphishing & Phishing:

Spearphishing est un mail spoofing ou fraude attachée à l'organisation spécifique des entreprises, en cherchant un accès non autorisé à des données confidentielles. Les tentatives d'hameçonnage ne sont généralement pas lancées par des pirates informatiques au hasard, mais sont plus susceptibles d'être menées par des auteurs pour obtenir des gains financiers, des secrets commerciaux ou des informations militaires. Les messages d'hameçonnage se retrouvent habituellement dans une entreprise ou un site Web bien connu avec une large base de membres, comme eBay ou PayPal.

Prévention : Éducation et sensibilisation des utilisateurs finaux à se méfier de tous les e-mails provenant de ces supposées "sources fiables".

Attaques de l'homme dans le milieu des appareils mobiles :

Elle permet de s'introduire dans des connexions indépendantes avec les victimes et de relayer les messages entre elles, en leur faisant croire qu'elles parlent directement entre elles en privée, alors qu'en fait toute la conversation est contrôlée par l'intrus qui doit être capable d'intercepter tous les messages entre les deux victimes et d'en injecter de nouveaux, ce qui est simple dans de nombreuses circonstances (par exemple, un attaquant à portée de réception d'un point d'accès Wi-Fi non crypté peut s'introduire en tant qu'homme - au milieu).

Prévention : authentification forte entre les hôtes, les infrastructures de clés publiques, les clés secrètes et l'examen de latence.

Ingénierie sociale :

Les attaques via les supports numériques ne concernent pas seulement l'usage de la

« **force brute** » (cassage de mots de passe ou de clés WiFi par exemple) mais reposent de manière beaucoup plus importante sur **l'ingénierie sociale**. Il s'agit d'utiliser les activités suspectes pour profiter de la sécurité physique détendue ou des contrôles non techniques. Les exemples incluent le surf sur l'épaule, le piggybacking, la benne à ordures et les « appels clients IT ».

Prévention : Appliquer des règles de sécurité physique et tester périodiquement l'adhésion de personnel aux politiques pour la protection des activités de routine impliquant des données sensibles

Réseaux de confiance des pays étrangers :
Des connexions à des adresses de localisation sont nécessaires pour empêcher un réseau de confiance de pénétrer dans les segments américains.

Prévention : Travailler avec les architectes réseau pour comprendre comment les segments de réseau à haut risque se connectent aux segments américains. Des réseaux séparés avec des connexions limitées sont la meilleure protection. La segmentation avec surveillance spéciale aidera à atténuer les risques. Contrôler minutieusement les employés étrangers à l'aide de vérifications des antécédents.

Menaces persistantes avancées (APT)
Attaques hautement sophistiquées ciblées, personnalisées, cryptées, morphing, plusieurs "agents" reconnaissance, "zero-day" et attaques réparties sur plusieurs mois.

Les APT sont utilisées dans les domaines de Criminalité, Terrorisme et Cyber Warfare et leur facture est lourde, 5,4 milliards de dollars perdus dans le cyber-vol de données et de fonds en 2010 (statistiques CNET) Citibank, Google, Intel, NY Power Grid et beaucoup d'autres ont été attaqués. Face aux APT, l'infrastructure de sécurité existante est considérée comme inadéquate, les signatures et approches heuristiques obsolètes, le déploiement distribué rend l'analyse comportementale actuelle inefficace. Les leaders de l'industrie sont unanimes pour de nouvelles solutions.

Assurer l'avenir - neutraliser les APT

La neutralisation des APT a besoin d'une "analyse accélérée" car leur concept s'apparentant à la "culture virale" dans le domaine médical, il faut donc des capacités permettant d'éliminer leur persistance et analyser les interactions d'application pour détecter les anomalies en circulation. Ces aptitudes doivent prendre en compte des aspects plus larges du trafic, analyse des communications décentralisées en développant des capacités pour chaque réseau.

Pour alléger les dépenses de protection contre les APT, qui sont exorbitantes (Le gouvernement américain prévoit des dépenses de 1,3 milliard de dollars pour l'APT en 2011 (Source : Market Research Media) et impactent negativement la sécurité de la conformité au profit de la protection des données (Forrester), des mesures s'imposent. Etre à jour en matière de protection, organiser des campagnes de sensibilisation à la sécurité, formation spéciale pour les super-utilisateurs et les développeurs internes, verrouiller les ports USB, contrôler et surveiller comment les supports portables sont utilisés. Mettre en place des d'outils de prévention des pertes de données, alerte systèmes et détection rapide et autres défenses actives pour atténuer l'impact des incidents[27].

Finalement beaucoup de menaces cyber qui constituent un enjeu sécuritaire qu'il convient de prendre en considération dans nos systèmes d'information.

[27] Session Number C22 Introduction to Advanced Security Threats, Bryan Kissinger,PhD, ISACA SF Fall Conference November 8th, 2011

Chapitre 2 : Les enjeux et dimension sécuritaires

« Le seul système informatique vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés. Même dans ces conditions, je ne parierai pas ma vie dessus. » ***Prof. Eugene Spafford, Purdue University.***

Les chiffres et les faits sont parlants ; en octobre 2012 vol en Caroline du Sud de 3,6 millions de numéros de sécurité sociale et 387 000 numéros de cartes de crédit / débit; près de 680% d'augmentation des violations de la cybersécurité au cours des six dernières années; 42 887 incidents impliquant la perte ou le vol de données (2011); les coûts de propriété intellectuelle pour les sociétés américaines s'est levé à 250 milliards de dollars (2012); la cybercriminalité mondiale quant à elle s'élève à 114 milliards de dollars par an; la part des cybercriminels en Russie est d'environ 1,8 milliard (2011); Une fois volé d'un compte bancaire unique en Russie: 14,8 millions de dollars; McAfee estime que 1 trillion de dollars ont été dépensés à l'échelle mondiale dans le cadre de mesures correctives[28].

En 2017, entre mai et juin, des cyberattaques par ransomware (Wannacry et NotPetya) ont touché plusieurs infrastructures critiques (secteurs bancaire, énergie, transport, etc.) dans plus de 150 pays dans le monde. Ces attaques ont frappé l'Ukraine, la Russie et se sont propagées par la suite à d'autres pays comme la France et les Etats-Unis. Ces Ransomwares visent les systèmes Windows et semblent exploiter des vulnérabilités identifiées et déjà détectées et exploitées par la NSA. A l'opposé de «WannaCry » qui crypte l'ensemble des fichiers, « NotPetya » redémarre les machines infectées, encrypte la MFT « Master File Table » et rend inopérable le MBR «Master Boot Record » ; empêchant ainsi les machines infectées de démarrer. En outre les statistiques ont démontré que parmi les dix pays les plus visés en nombre d'attaque par des hackers, quatre sont en Afrique, le Kenya, le Nigeria, l'Afrique du Sud et l'Égypte. *«L'un des principaux défis technologiques auxquels sont confrontées les entreprises en Afrique est la cybersécurité, explique le* Chief Executive Officer *(CEO) de* BIRGER*., Jacques Harel. D'où le lancement d'un*

28 Documentation CNAM ; introduction générale, cybercriminalité, cybersécurité, cyberdéfense, auteur : Philippe BAUMARD professeur des universites, agrege des facultés conservatoire national des arts et métiers,

centre de cyberdéfense, en partenariat avec Symantec, pour fournir des services et des solutions de cybersécurité aux clients africains…[29]*».*

Les enjeux sont énormes et nul n'est épargné, à ce titre, dans un rapport du *defense science board,* le 28 mai 2013, on apprend que les plans de nombreuses armes américaines avaient été dérobés lors d'une attaque informatique. La Chine est accusée comme étant à l'origine de cette attaque. Ces plans concernaient des dispositifs hautement stratégiques tel que le prototype du futur F35, le F18, les missiles patriot, les radars Aegis, ou l'hélicoptère hybride V-22 Osprey (Nakashima 2013)[30]. D'où une remise en cause accrue de la souveraineté des pays indépendamment de leur puissance militaire ce qui implique le besoin d'une nouvelle conception de notre outil de sécurité. Il est clair qu'internet présente des opportunités remarquables, mais en Afrique la vulnérabilité est telle que des attaques ne sont pas visibles ou ne sont même pas ressenties à défaut d'élaborer des systèmes de protection renforcée. *La porosité entre cyber-crime et terrorisme peut apparaître comme une inquiétude supplémentaire : les états africains développent rapidement leurs infrastructures sans mettre en place les moyens nécessaires à leur protection. Le scénario, souvent joué en Occident, d'une cyberattaque majeure contre des infrastructures vitales doublée d'une attaque terroriste est une hypothèse bien réelle pour ce continent*[31].

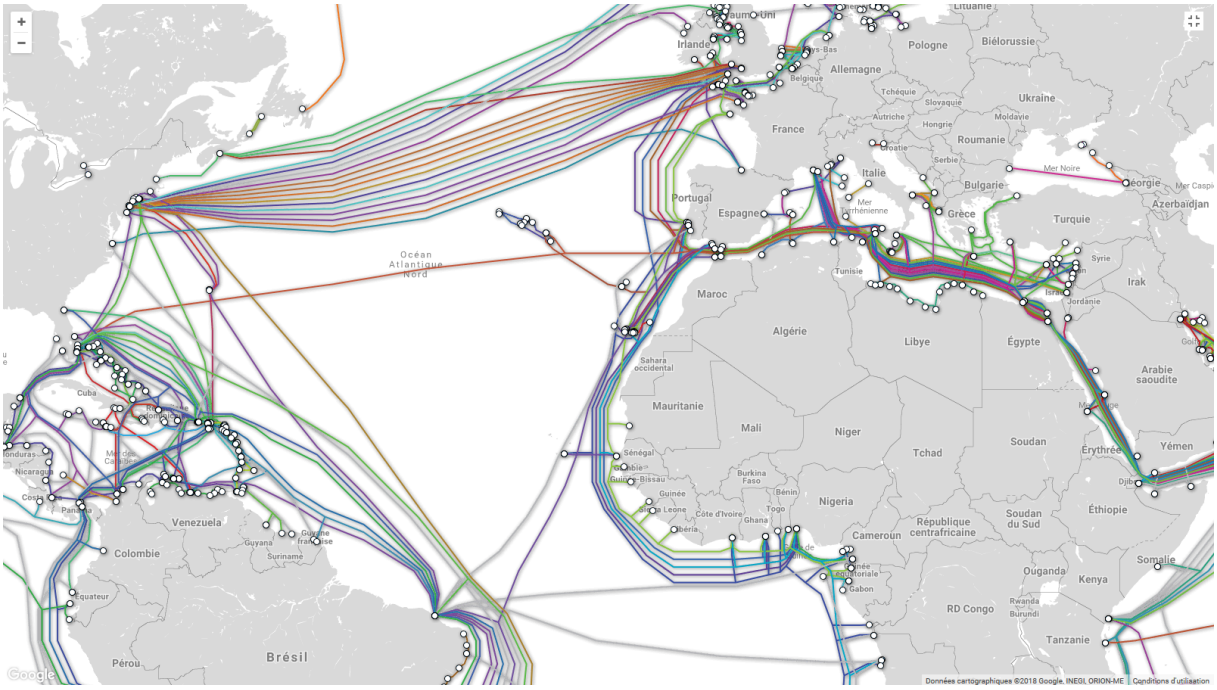
Comme mentionné en introduction, si la force conjointe du G5 Sahel réussit à mettre hors état de nuire les islamistes radicalisés armés (IRA) sur le terrain, ces terroristes pourront à l'avenir utiliser des procédés, peu onéreux en moyens et moins risqués, en alternative aux défaites tactiques sur le terrain. C'est l'une des futures formes d'hybridation de ces groupes si l'on se réfère aux pratiques de Daech qui était aussi audacieux que les Anonymous. L'IRA peut, à défaut d'avoir les aptitudes et connaissances nécessaires pour de telles pratiques, chercher à s'attirer les compétences d'informaticiens, notamment dans la sous-région où les diplômés-chômeurs constituent une cible facile hors de contrôle de l'autorité étatique. Si tel est le cas, les institutions étatiques seront la première cible et l'objectif prioritaire des

[29] https://www.lexpress.mu/article/290412/birger-veut-engranger-75-revenus-lafrique-dici-2020
[30] Didier DANET et Amaêl CATTARUZZA, 2014, « la Cyberdefense quel territoire, quel droit », Paris, Economica § P.60
[31] LA CRIMINALITÉ INFORMATIQUE AVANCÉE EN AFRIQUE, Auteurs : Jean-Jacques Alex, Gilles Chabannes, Pierre-Marie Léoutre, Ronan Mouchoux, Master M2

terroristes mutants, pour faire comprendre à l'opinion nationale et internationale qu'ils existent malgré les idées véhiculées par les Etats qui annoncent la disparition à jamais de ces IRA après une victoire sur le terrain.

a- La connectivité internet en Afrique de l'Ouest et ses conséquences sur les Armées

Les câbles sous-marins : Une petite analyse des côtes atlantiques a permis de constater une hyper connectivité des pays de la sous-région ouest africaine par câbles sous-marins de télécommunication à fibres optiques[32]. C'est un maillage assez dense (parfois redondant pour certains pays) qui relie ces pays de la façade atlantique au reste du monde.



- Un premier câble[33] relie la Cote d'ivoire, le Ghana, le cap vert, le Nigeria, le Togo à l'Europe (Portugal, royaume uni, Espagne),
- Un second câble[34] relie la Cote d'ivoire, le Ghana, la Gambie, la Guinée Bissau, le cap vert, la Guinée Conakry, le Benin, le Sénégal, le Nigéria, le Togo et la Mauritanie à l'Europe (Portugal, royaume uni, Espagne),
- Un troisième câble[35] relie la Cote d'ivoire, le Ghana, le Nigeria, le Sénégal à l'Europe (Portugal, Espagne)

[32] http://www.cablemap.info/
[33] http://en.wikipedia.org/wiki/WACS_(cable_system)
[34] http://www.gloworld.com/glo1.asp; http://en.wikipedia.org/wiki/GLO-1_(cable_system) Widemouth Bay (United Kingdom).

- Un autre câble relie[36] la Cote d'ivoire, le Ghana, la Gambie, la Guinée Conakry, le Benin, le Sénégal, le Nigéria, la Sierra Leone, le Libéria et la Mauritanie à l'Europe (Portugal, Espagne et la France),
- Un autre câble relie[37] le Sénégal et le cap vert à la fois à l'Europe Portugal, Espagne mais aussi l'Amérique du sud Brésil et Argentine.
- A l'avenir, deux câbles sous-marins[38] relieront le Nigéria au Brésil, aux états unis et l'Espagne d'une part et le Nigéria à l'Afrique du sud d'autre part.

En se basant sur les données du State of Broadband Report 2016 de l'UIT, le Club du Sahel et de l'Afrique de l'Ouest (**CSAO**) a dressé la liste des pays les plus connectés à internet dans cette région de l'Afrique (voir page 33).

De façon générale, sur le plan de l'accès et l'utilisation d'internet au niveau individuel, le Nigeria est classé premier avec un taux de 47,4 %. Ainsi, près d'un Nigérian sur deux a accès à internet, ce qui explique le développant des pratiques de spamming et de social engineering pour mener des «arnaques à la Nigériane». C'est un phénomène très répandu et qui continue de causer d'énormes pertes. (Dite aussi fraude 419, du nom de l'article du code pénal nigérian la réprimant), le «419 scam» (fraude 419) est un procédé qui consiste à envoyer à une victime potentielle un spam, mail non sollicité. Le contenu du spam sera alléchant et reproduira à peu près ceci : «*Je vous demande de l'aide pour sortir illégalement une très grosse somme d'argent du Nigeria. En échange, vous toucherez une commission sur cette somme. Il vous suffit de donner votre numéro de compte en banque afin que l'argent y soit versé*».

Derrière le Nigeria, on trouve le CAP vert avec un taux de 43 %, suivi du Ghana avec 23,5 %, le Sénégal avec 21,7 % et la Côte d'Ivoire avec 21 %. La Mauritanie vient en 6ème position devant le Burkina Faso. Le Tchad avec 2,7 % et le Niger avec 2,2 % ferment la marche.

En ce qui concerne l'internet mobile, le CAP Vert prend la première place avec un taux de connexion de 73 %, suivi par le Ghana avec 66,8 %. Loin derrière ces deux pays, on trouve la Côte d'Ivoire avec 40,4 %, le Sénégal avec 26,4 % et le Nigeria avec 21 %. Le Liberia avec 20,5 % de taux de connexion est placé 6ème dans ce

[35] http://www.mainonecable.com/; http://en.wikipedia.org/wiki/Main_One_(cable_system)
[36] http://en.wikipedia.org/wiki/ACE_(cable_system)
[37] http://www1.alcatel-lucent.com/submarine/refs/cibles/atls/atlantis2.htm, http://en.wikipedia.org/wiki/ATLANTIS-2
[38] http://www.wasace.com; http://en.wikipedia.org/wiki/WASACE_(cable_system)

classement. Le Niger et le Tchad occupent les deux dernières places avec respectivement 1,8 % et 1,4% de taux de connexion[39.]

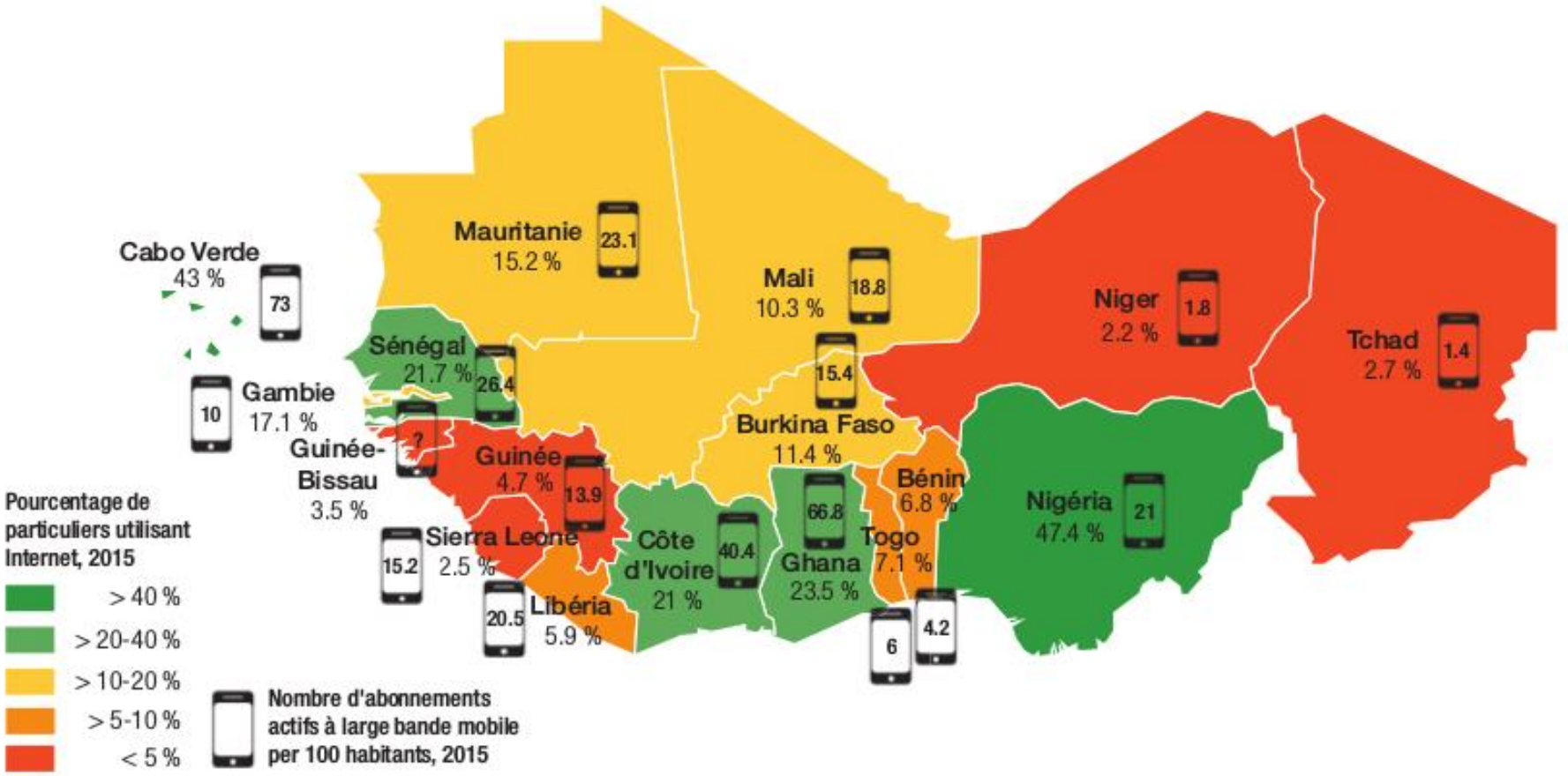
Comme on peut le constater, de nombreux pays d'Afrique de l'ouest, notamment parmi les plus pauvres, se retrouvent dans un contexte de déficit technologique, d'un manque d'accès aux connaissances qui risque de les empêcher de profiter adéquatement de la globalisation des marchés et de la mondialisation, la fracture numérique reste béante malgré la forte augmentation de la connectivité et la mise en œuvre dans certains pays de plan en matière de technologie large bande ou d'une stratégie NTC. Ce qui explique un avenir prometteur selon une étude de la GSM Association, une organisation basée à Londres qui représente près de 800 opérateurs de téléphonie mobile à travers 220 pays du monde, « au cours des quatre prochaines années, l'Afrique de l'Ouest devrait enregistrer une croissance moyenne de 6 % par an du nombre d'abonnés, une des plus fortes croissances mondiales, se traduisant par 45 millions d'abonnés supplémentaires d'ici 2020»[40.] Croissance motivée essentiellement par l'accessibilité des smartphones et le développement du haut débit. Actuellement, 23 réseaux 4G fonctionnent dans sept pays de la région, dont 14 lancés depuis début 2016, et tous les pays de la sous-région dispose de réseaux 3G.

Cela engendrera de nouvelles croissances des menaces auxquelles nous seront confrontés en cyberespace. Ces menaces à la sécurité nationale et économique des États augmentent chaque année en fréquence de portée et de gravité de l'impact. Les cybercriminels, les pirates et les adversaires étrangers ou locaux sont de plus en plus sophistiqués et capables d'utiliser Internet à des fins néfastes. Les statistiques démontrent que parmi les dix pays les plus attaqués par des hackers, quatre sont en Afrique, nommément le Kenya, le Nigeria, l'Afrique du Sud et l'Égypte. *«L'un des principaux défis technologiques auxquels sont confrontées les entreprises en Afrique est la cybersécurité, explique le* Chief Executive Officer *(CEO) de* BIRGER*., Jacques Harel. D'où le lancement d'un centre de cyberdéfense, en partenariat avec Symantec, pour fournir des services et des solutions de cybersécurité aux clients africains mais aussi à ceux de Maurice et des îles de la région[41].»*

[39] Source: CSAO

[40] https://afrique.latribune.fr/africa-tech/telecoms/2017-07-20/telephonie-mobile-l-afrique-de-l-ouest-connaitra-une-des-plus-fortes-croissances-mondiales-d-ici-2020-etude-744398.html

[41] http://fr.allafrica.com/stories/201609271175.html



Sources : The State of Broadband Report 2016, Union internationale des télécommunications (UIT): Indicateurs des télécommunications/TIC.

Consultable au Site : http://www.ticeduforum.ci/internet-voici-les-pays-dafrique-de-louest-les-plus-connectes/

Quel Impact sur les armées ouest africaines (G5 Sahel) ? Selon la NSA, protéger dans le cadre numérique consiste à connaître la menace, sécuriser les réseaux et les données, soutenir les armées et être à la pointe de la recherche[42]. Le réseau étant par essence ouvert, multiforme, il s'avère fréquemment que les attaques utilisent de nombreuses techniques reposant à la fois sur le ciblage humain et technique. La première chose à effectuer est d'identifier les faiblesses possibles de son système d'information et de son environnement technique et humain. Si l'on a une idée assez claire des menaces et types d'attaques potentiels, tel n'est pas le cas pour les contre-mesures à savoir la sécurisation des réseaux des données numériques organiques des armées. A mon sens nos armées sont à l'image des différentes institutions des états (voir pire pour certains pays) et à défaut d'avoir une idée des systèmes d'informations en place ou les typologies des réseaux et infrastructures existantes, on peut faire une extrapolation à ce qui existe dans les institutions étatiques. A ce titre on peut constater le manque de gouvernance en matière de systèmes d'information à l'image de la direction interministérielle des SIC (DISIC) en France chargée d'élaborer les politiques de définition et de gestion des SI de l'Etat et l'existence de systèmes d'information très simple qui sont logiquement isolées d'internet.

L'Agence Privée d'Investigations et d'Analyses Stratégiques (APIAS), l'un des rares cabinets en Afrique qui s'occupe de la cybersécurité, de la cyberdéfense, de la prévention et de l'élaboration de la stratégie en matière de maintien de l'ordre, a essayé de cartographier les cibles de certaines attaques. Elle cite entre autres l'attaque de 2013 du groupe Anonymous Côte d'Ivoire qui a attaqué les fournisseurs d'accès à internet pour leur réclamer la baisse des tarifs afin de démocratiser l'accès à internet à l'ensemble des ivoiriens. En avril 2014, le serveur de l'Agence de l'Informatique de l'Etat sénégalais a été attaqué par le collectif Anonymous Sénégal, 47 sites gouvernementaux (primature, ministère des finances, de l'éducation nationale, de l'agriculture…) ont été effacés. En janvier 2015, le serveur de l'Agence de l'Informatique de l'Etat du Sénégal a de nouveau été attaqué suite aux évènements de Charlie Hebdo en France. La « Nigerian Cyber Army » attaque régulièrement les sites gouvernementaux, comme celui de l'Assemblée nationale du Nigeria. En mars 2015, le groupe a attaqué le site internet de la Commission

[42] https://www.nsa.gov/

Electorale Nationale Indépendante du Nigeria. Il existe également un groupe nommé « Anonymous Africa » qui milite contre la corruption et pour la démocratie.

C'est aussi le cas de cyberattaques de sites web du gouvernement burkinabè, des institutions comme la douane, le ministère des Mines, et le ministère de l'Agriculture.

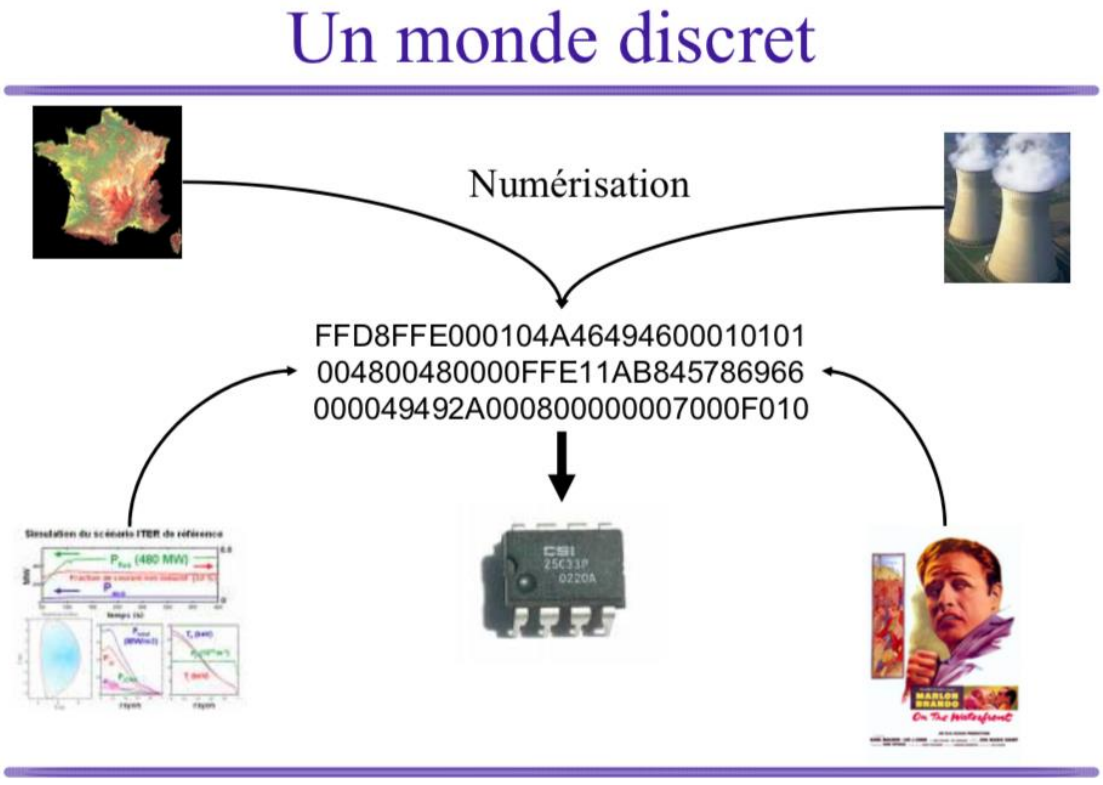
Dans ces conditions, il est possible de présumer que les serveurs des armées sont attaqués et des sites bloqués à l'image de ces institutions.

Les armées doivent commencer des efforts sérieux et systématiques pour faire les meilleurs choix en matière de risque. La réflexion vitale sur ces enjeux ne peut donc plus être ignorée et doit être dès à présent prise en compte car la plus grande valeur d'une armée dans le domaine du numérique est certainement la sécurité de ses systèmes d'informations.

Au regard de l'intérêt des nouvelles technologies de l'information et de la communication, il est opportun, voire primordial que la réflexion et l'action soient enclenchées afin que la sécurité des réseaux, des systèmes de données et le partage d'expériences soient mis en place, tout ceci de concert avec les professionnels privés du domaine dans nos pays et avec nos partenaires internationaux.

b- Sécurisation des infrastructures et Systèmes d'Informations existants

Un système d'information (SI) est un ensemble de machines connectées entre elles de façon permanente ou temporaire permettant à une communauté de personnes physiques ou morales d'échanger des données (sons, images, textes, etc.). Selon cette définition, des systèmes aussi variés que le réseau d'un opérateur de téléphonie, le site Internet d'un ministère, l'ordinateur individuel du particulier ou le réseau de commandement des forces armées sont des systèmes d'information[43]. La sécurisation des infrastructures et Systèmes d'Informations ou tout simplement la sécurité des systèmes d'information (SSI) est donc le fait d'assurer en toute circonstance le partage de ces ressources entre utilisateurs. Ces ressources qui font désormais partie intégrante du fonctionnement des administrations, de l'activité des entreprises et du mode de vie des citoyens.



Le durcissement de la sécurité pour assurer cette fonctionnalité est d'autant plus vital, car les services qu'ils nous assurent sont tout aussi indispensables que l'approvisionnement en eau ou en électricité. Cette sécurisation est assez difficile à

[43] http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/064000048.pdf

en croire la définition de la sécurité par Buzan qui pense qu'il n'est pas facile de se soustraire à la menace de manière absolue et qu'en général chaque solution à une menace est le point de départ d'une autre[44] ce qui est vrai en partie dans le domaine du numérique. A ce titre et pour mieux réussir ce chalenge, les armées doivent avoir des compétences ou expertises dans les équipements ou moyens destinés à protéger les systèmes d'information (**sécurité de l'information**), avoir la capacité d'apporter son concours aux contrôles et mesures que peuvent nécessiter ces systèmes d'information (**sécurité des systèmes**) et enfin assurer une veille technologique sur l'évolution (l'innovation) et la connaissance des menaces pour mieux gérer les crises éventuelles (gestion des crises et risques)[45]. En bref il s'agit de la constitution d'une capacité cyber qui prendra en compte la doctrine, l'organisation, les ressources humaines, l'entraînement, le soutien et les équipements (DORESE).

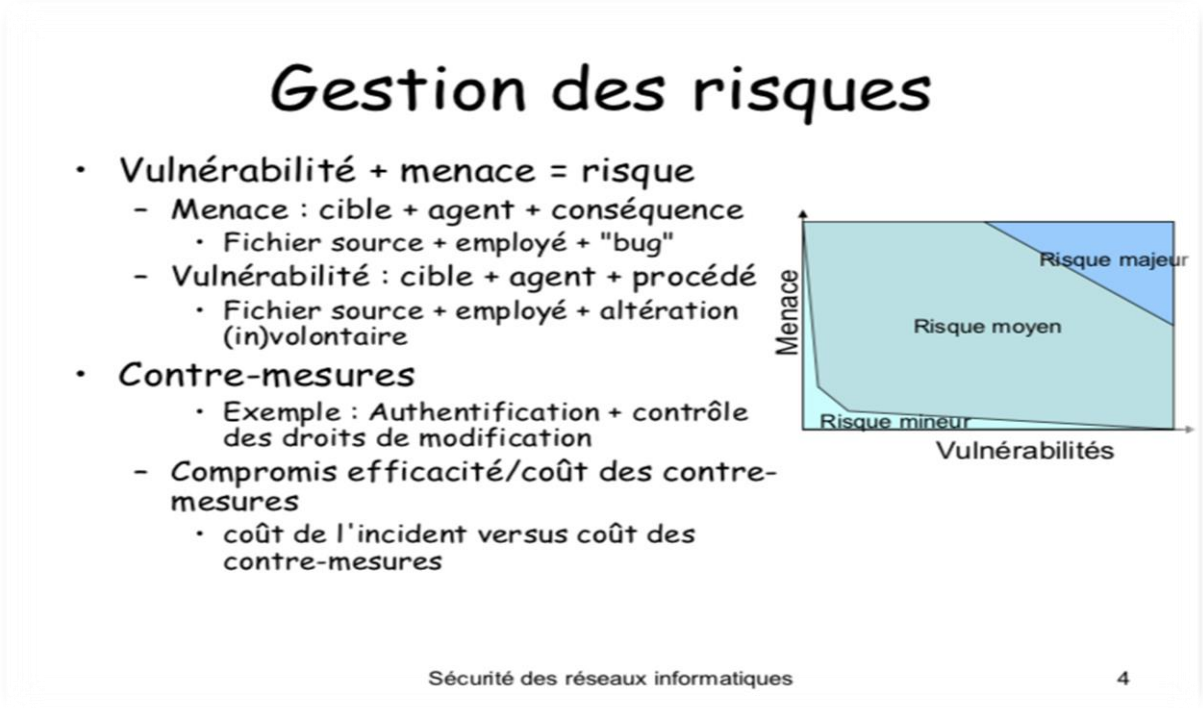
De la sécurité de l'information : la sécurité de l'information passe par la confidentialité à savoir la protection des données sensibles contre l'intrusion et le vol via le cryptage et les protocoles, la préservation de l'intégrité de ces données contre toute altération, usurpation d'identité ou fausses informations par la superposition de plusieurs niveaux de sécurité : sensibilisation humaine, contrôle d'accès, firewalls, mot de passe et enfin garantir la disponibilité de ces services quelques soit le dysfonctionnement (Déni de Service).

De la sécurité des systèmes : aujourd'hui les réseaux interconnectent tout le monde, entreprise, administration, militaire et facilitent par conséquent la propagation de toute menace via les matérielles : ordinateurs, sites web, imprimantes, clés usb... ; et les logicielles : suites Office, emails, pdf, video, ... La sécurité des systèmes d'information requiert de mobiliser des ressources financières et humaines dont le retour sur investissement est souvent difficile à justifié. A ce titre, les armées doivent fournir un soutien spécifique aux Etats pour fournir des services de support efficaces et accessibles, résoudre les problèmes de SSI et préconiser des produits de sécurité surtout en matière de transactions dans ce domaine très sensible, car la

[44] Dictionnaire de la guerre et de la paix, sous la direction de Benoit Durieux, Jean-Baptiste jeangène Vilmer, Frédéric Ramel, § P. 1274
[45] Sécurité des systèmes d'information, Jean-Yves Marion, Université de Nancy Loria

sécurité des systèmes d'information est un enjeu national à caractère stratégique, politique et économique. Ce qui explique à mon avis l'implication forte des forces armées et de sécurité dans la gestion de la SSI. Mais nos forces armées et de sécurité ont-elles les moyens et les compétences nécessaires pour assurer de manière autonome la protection de nos infrastructures et de nos systèmes ? Question logique à laquelle la réponse est non, quand bien même nos moyens seraient mutualisés ce qui n'est pas le cas. C'est cette mutualisation des compétences et des moyens qui nous permettra de prendre le lead dans nos pays dans ce domaine et nous procurer d'avantage la crédibilité et l'efficacité pour définir et mettre en œuvre une politique globale de SSI.

De la gestion des crises et risques : La planche suivante résume de manière succincte la gestion des risques[46].



Une erreur est de penser que la SSI ne concerne que le seul technicien de la boite. Elle est la responsabilité de tous car les conséquences d'un incident vont au-delà du système d'information et l'ensemble de l'entreprise en dépend[47]. La SSI est l'affaire de tous ; d'un point de vue organisationnel, du personnel, au juridique en passant par la gestion des relations extérieures pour assurer la cohérence durant la crise.

[46] https://www.irisa.fr/prive/bcousin/Cours/1-Securite-des-reseaux.2P.pdf
[47] https://www.journaldunet.com/solutions/expert/63147/les-5-grands-principes-de-la-gestion-du-risque-informatique.shtml

Techniquement, la surveillance du système d'information et l'inventaire continu des outils informatiques et des données qu'il traite font partie des bonnes pratiques à adopter.

D'après une étude du *Ponemon Institute pour Arbor Networks*, les délais d'identification des menaces frappant le système d'information atteignent souvent les cent jours : de 98 jours dans le secteur financier à 197 jours pour le e-commerce. il est donc impératif d'assurer une surveillance continue des systèmes d'information et de veiller à ce que toutes les anomalies soient remontées rapidement vers un spécialiste pour être analysées.

Selon la complexité du système il est difficile d'identifier rapidement la panne ; une organisation doit inventorier chaque composant de son système d'information et les données qu'il gère afin de répondre efficacement à n'importe quel incident et assurer la résilience.

Pour contenir une attaque on suit le protocole suivant : bloquer les accès non autorisés, bloquer les sources de malwares (adresses email ou site web), fermer les serveurs mails et les ports, changer les mots de passe compromis ou suspects, filtrer le pare-feu, délocaliser les pages d'accueil, et enfin isoler le système. Après avoir neutralisé le danger, il faut rétablir le réseau, l'accessibilité aux données et la connectivité. Ensuite, restaurer le système, confirmer qu'il fonctionne normalement et résoudre les vulnérabilités afin d'éviter un incident identique, ce qui implique de rebâtir les parties infectées du réseau. Enfin, remplacer les fichiers compromis, réinitialiser les comptes touchés, installer les dernières mises à jour, changer les mots de passe et renforcer la sécurité du réseau, avec une attention particulière au pare-feu. Il convient finalement de tester les systèmes et de confirmer l'intégrité des systèmes opérationnels et de contrôle. On suppose bien sûr que la sécurité physique des réseaux et leur disponibilité sont assurées.

c- Partage et retour d'expériences Cyber

Logiquement chacune des armées du G5 Sahel réagit de façon individuelle et se protège avec les moyens dont elle dispose. Quand bien même l'ampleur de la menace et des enjeux plaide cependant pour une approche plus large et plus collaborative. L'échange d'informations sur les incidents, le partage de bonnes pratiques et la mise en place de formules de collaboration doivent être une composante essentielle de la riposte mais aussi constitue la clé du succès.

Il est important que puisse émerger un réseau structuré d'échanges et de coopération, ce que le chercheur Guy-Philippe Goldstein appelle un « WhiteNet », qui est, d'une certaine façon, un pendant au « DarkNet ». Ce WhiteNet devrait intégrer l'ensemble des acteurs impliqués (entreprises, institutions publiques, centres de recherche universitaires, start-up et groupes de cybersécurité privés, etc.), tout en bénéficiant de la protection d'un tiers, d'un partenaire de confiance.

En Australie, une initiative de ce type a vu le jour en 2017. PwC Australie a lancé une organisation de partage de cyber intelligence dénommée JCSC (Joint Cyber Security Center). Il s'agit d'un centre permettant de partager des informations en lien avec les menaces cyber (caractéristiques des attaquants surveillés, nouveaux scénarios d'attaques, vulnérabilités, etc.) entre les grandes entreprises australiennes issues de différents secteurs d'activité. Ce dispositif a plusieurs objectifs [48]:

- Partage rapide d'informations sur les nouvelles menaces et les modes opératoires des attaquants,
- Développement de manière collaborative et sans orientation commerciale de solutions de cybersécurité,
- Mise en place d'une compréhension commune des risques,
- Accès par l'ensemble des participants à certains outils et ressources pour améliorer leur cybersécurité,
- Elaboration et promotion d'une vision cohérente sur les besoins de sensibilisation.

[48] https://www.hbrfrance.fr/chroniques-experts/2017/12/18178-nouveaux-outils-mieux-maitriser-risque-cyber/

Les Américains ont également crée un fichier d'analyse des cyber-incidents, le Cyber Incident Data and Analysis Repository (ou CIDAR). Ce fichier permettrait de disposer d'une nouvelle capacité de partage de l'information entre le gouvernement fédéral, les responsables de la sécurité des entreprises et les assureurs. Il permettrait d'améliorer la sensibilisation aux risques liés à la cybercriminalité et d'aider à identifier les tendances à plus long terme.

Face aux menaces informatiques, les différentes institutions - publiques et privées - doivent savoir collaborer et échanger les informations, affirme dans un rapport l'Agence européenne chargée de la Sécurité des réseaux informatiques (ENISA). Les analystes identifient dans cette étude les freins et les incitations en matière de partage de données, notamment dans le secteur privé, pour assurer la sécurité informatique à l'échelle européenne[49].

Par extension, il s'agit également pour nos pays et nos armées de relever les défis avec plus d'efficacité et plus d'imagination en prenant appui sur les expertises existant notamment en France (ANSSI) et/ou ailleurs. Des opportunités sans précédent s'offrent à tous, aussi bien individuellement que collectivement à travers la mise en valeur des structures du G5 Sahel. Nous avons l'obligation de préparer l'avenir en intensifiant l'effort de coordination via une instance ayant en charge l'élaboration d'une vision d'ensemble cohérente, d'une compréhension commune des risques, la collecte et le partage rapide des informations et solutions concernant les activités cyber de tout genre dans la sous-région et permettre à tous les pays membre l'accès aux outils et ressources nécessaires pour améliorer leurs procédures de cyberdéfense. Cette structure fera partie d'une approche de solution globale inclusive.

[49] https://atelier.bnpparibas/smart-city/article/cybersecurite-passe-partage-information

Chapitre 3 : Solutions : Une Approche globale inclusive

« *Pour faire face aux risques et aux menaces qui pèsent sur des systèmes d'information devenus indispensables au fonctionnement de la Défense et aux missions conduites par les armées, le ministère s'est doté d'une organisation Cyberdéfense. Plusieurs acteurs complémentaires travaillent ensemble, en collaboration avec différents partenaires, pour une Cyberdéfense efficace et performante*[50] ». Ce paragraphe introductif de l'organisation de la Cyberdéfense au sein du Ministère des armées françaises montre si besoin il y a la nécessité de mutualiser les efforts des différents acteurs étatiques ou non (nationaux ou partenaires) pour la protection et la défense des systèmes d'information dans l'espace numérique. En d'autres termes, unir les forces, aider, se protéger, identifier, informer, former, dénoncer, voilà les efforts à conjuguer pour se mettre au niveau des attentes et des défis. Les récents retours d'expérience ont montré toute l'importance pour les armées de maîtriser les outils numériques en opérations mais aussi dans l'administration courante. Il ne s'agit pas seulement d'adapter les moyens de transmission des données en fonction de la sensibilité des informations à transmettre, mais surtout pouvoir détecter très tôt les événements aussi bien par une détection par signatures que par comportement. Il faut comprendre la volonté et l'idée de manœuvre de l'attaquant et rechercher à déterminer son identité. Peu de nations sont capables de le faire seules faute de moyens technologiques importants et d'un savoir-faire hors du commun nécessaires. A ce titre la création **d'un Pôle Militaire d'Excellence Cyber** sous-régional chargé d'accompagner et de sécuriser le développement du numérique et qui apporterait son expertise et son assistance technique aux armées et aux administrations des différents états serait un choix opportun. Une fois mise sur pied, cette structure serait un acteur majeur de la cyber sécurité à l'image de l'ANSSI en France et aurait pour mission de renforcer et d'assurer le service de veille, de détection, d'alerte et de réaction aux attaques des systèmes d'informations tout en développant la recherche et les capacités en matière de cybersécurité afin d'anticiper les menaces et d'accompagner les évolutions technologiques. Cette structure pourra également prendre en compte la nécessaire coopération en matière juridique dans le domaine.

[50] https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation

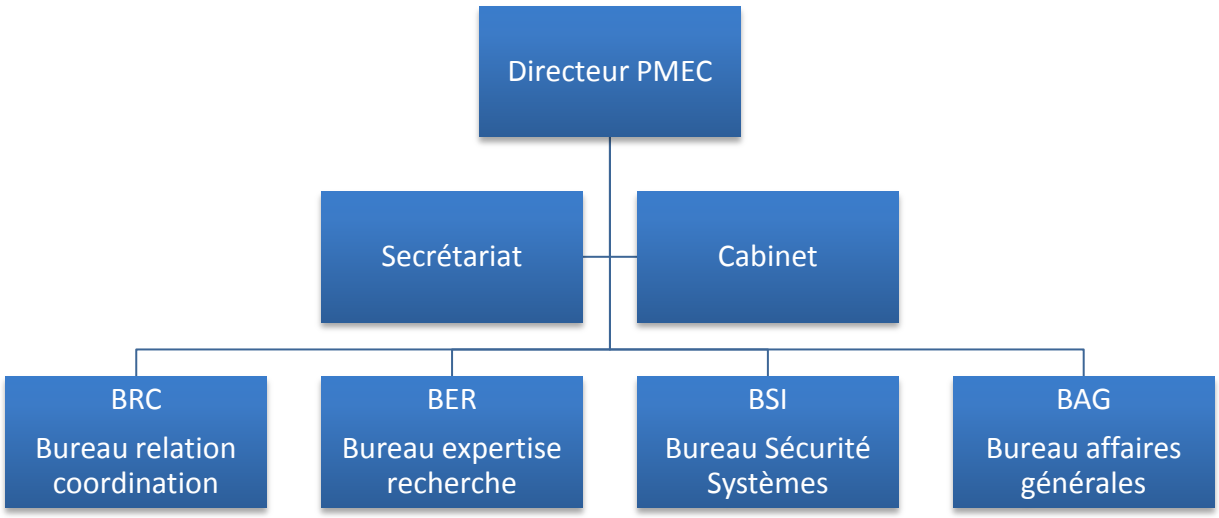
a. Mise en place d'un Pôle Militaire d'Excellence Cyber (de Recherche et de développement des capacités sur la Sécurité numérique)

Durant la quatrième édition du Forum sur la paix et la sécurité en Afrique (Dakar) qui s'est achevée mardi 14 novembre 2017, également présent, Jean-Yves Le Drian a annoncé la création par la France, à Dakar, d'une école africaine de cybersécurité. Dakar donc, qui accueillera, dans quelques semaines ou quelques mois, une nouvelle école à vocation régionale (ENVR) dédiée à la cyberdéfense, se positionne ainsi comme le partenaire «périphérique» le plus fiable de la bande sahélo-saharienne[51]. Cette action vient à point nommé pour justifier notre vision par rapport à l'opportunité et l'impératif de la mise en place d'un pôle militaire d'excellence cyber (**PMEC)** G5 Sahel qui sans être l'opposé ou le conquérant de cette école sera son partenaire logique et pourra s'en ressourcer. Le pôle cyber doit permettre de faire rayonner au niveau régional, les compétences et savoir-faire dans le domaine cyber. Cet organe à l'image d'une CyberTaskForce aurait la double et lourde tâche d'acculturer les milieux militaires et politique en vue d'une mutualisation des efforts des pays concernés, faciliter le recrutement des spécialistes dans le domaine dans les différents états, de réagir et anticiper les attaques dans le domaine cyber. Ce pôle spécialisé, s'appropriera l'expertise technique et opérationnelle et se renforcera dans le domaine du numérique.

Pour faire simple et sans nier la réalité disparate et discordante du terrain, nous devrons procéder par étape. Dans nos armées l'outil informatique (numérique) est pour la plupart sous tutelle des transmissions (traditionnelles) des armées à défaut d'un organe de système d'information et de communication avec parfois des mécontentements de certains ingénieurs au détriment de l'efficacité générale. Aussi il me paraît opportun d'accompagner la montée en puissance des structures du G5 Sahel pour mettre en œuvre ce pôle cyber au niveau des armées et ensuite l'extrapoler après maturité à la sous-région ouest-africaine. Il sera sous la tutelle d'un commandement unifié et centralisé à la fois dépendant des différents CEMA/CEMGA ou à défaut placée sous l'autorité du secrétariat permanant G5 Sahel. Les modalités

[51] https://www.ttu.fr/g5-sahel-menu-discussions-alger-dakar/

de la chaine commandement pourront être revues ultérieurement mais une première approche me parait comme suit :



Actuellement, c'est la tendance des différents pays ou organisation régionales qui à défaut de moyens individuels, s'organisent pour créer un outil cyberdéfense capable de confronter ces nouvelles menaces (la stratégie européenne de cybersécurité, etc…).

Les Etats-Unis ont consacré en 2016, 19 milliards de dollars de leur budget fédéral à la cybersécurité. En Europe, ce montant, calculé en cumulant les investissements de chacun des pays membres, est estimé à environ 1 milliard d'euros. Autrement dit, le manque d'investissements est réel, ce qui pèse sur l'autonomie stratégique de l'UE et représente une menace pour ses entreprises[52].

En ce qui concerne la sous-région subsaharienne, cet organe (PMEC), doit avoir les ressources nécessaires pour l'acquisition des compétences fondamentales pour mieux prévenir les cyberattaques par des exercices de cybersécurité à l'échelle sous régional.

[52] https://www.latribune.fr/technos-medias/cyberattaques-que-contient-le-paquet-cyber-que-l-europe-veut-voter-en-2018-751009.html

b- Création et Renforcement du cadre juridique Cyber

Il est nécessaire de fixer les grandes orientations d'une stratégie innovante de prévention et de répression de la cybercriminalité en Afrique de l'ouest combinant les réponses étatiques, sociétales et techniques et qui tiennent compte des capacités et des ressources des Etats concernés tout en s'inspirant des bonnes pratiques recensées à l'échelle internationale et des lignes directrices de l'Union Internationale des Télécommunications sur la cybersécurité pour les pays en développement[53].
Selon le Global Center for Information and Communication Technologies de l'ONU, seuls 5 pays disposent d'une législation traitant du cybercrime :

- **Afrique du Sud** : Electronic Communications and Transactions Act (2002)
- **Mauritanie** : Computer Misuse and Cybercrime Act (2003)
- **Zambie** : Computer Misuses and Crimes Act (2004)
- **Kenya :** Keny Communication (Amendment) Act (2009)
- **Cameroun** : Cybersécurité et la Cybercriminalité au Cameroun (2010)

Seule la Zambie a ratifié la convention sur le Cybercrime du conseil de l'Europe. Des évolutions notables sont cependant à noter, comme la ratification par la Tanzanie fin 2015 du 'Cyber Crimes Act of 2015', avec des peines de prison pouvant aller jusqu'à dix ans. La plupart des pays africains présentent des faiblesses structurales de leur appareil d'État, voire une instabilité politique majeure. Cet état de fait conduit la lutte contre le cybercrime à ne pas être, pour les dirigeants, une menace majeure. Les forces de l'ordre assignées à cette mission, quand elles existent, sont largement sous-qualifiées et sous dotées. L'Union Africaine a tenté de mettre en place une convention sur la cybersécurité et la protection des données personnelles mais elle n'a pour l'heure été ratifiée par aucun pays africain[54].
Donc le vide juridique est largement béant, ce qui montre le besoin à apporter des conseils et soutenir la constitution de capacités locales afin de promouvoir les conditions réglementaires et techniques nécessaires à un environnement juridique et un cadre d'action souples et ouverts à tous. Dans ce cadre précis la Mauritanie pourra partager son expertise dans le domaine et faciliter l'échange d'expériences avec les pays concernés en étroite collaboration avec d'autres partenaires.

[53] https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/47118/133493.pdf?sequence=1
[54] LA CRIMINALITÉ INFORMATIQUE AVANCÉE EN AFRIQUE, Auteurs : Jean-Jacques Alex, Gilles Chabannes, Pierre-Marie Léoutre, Ronan Mouchoux, Master M2

c- Coordination des efforts des différentes armées (G5 Sahel) et des partenaires

Les programmes militaires nationaux relèvent du passé, c'est ensemble que nous devons confronter le futur pour une réussite sûre. Comme les européens l'ont compris et réussi en aéronautique (A400M et Euro-fighteur TAIFON), et comme la dit un jour un président en exercice du G5 Sahel : «*Ensemble, conjuguons nos efforts pour faire des pays du G5 Sahel, un espace de paix, de prospérité et de concorde* ». Nous sommes condamnés à conjuguer nos efforts pour faire face à la montée de la menace terroriste et à la pression des technologies de l'information pour avoir une place dans ce monde au mieux, ou se protéger des aléas de ces menaces au pire. Aujourd'hui, ce manque de coordination entrave l'existence effective et l'efficacité d'un traitement approprié du terrorisme et de la cybercriminalité dans la bande sahélo-sahélienne et empêche la mise en place des bases d'une harmonisation de la politique de lutte contre ces fléaux qui menace l'humanité toute entière. Cela engendre forcement, une certaine disparité entre l'ampleur que prennent ces phénomènes et la faiblesse des réponses en termes de capacités juridiques et techniques d'appréhension, de prévention, de poursuite et de répression. Ensemble nous devrons définir la réaction face à ces menaces (nature des attaques, des acteurs, des cibles, ripostes) tout en définissant la réponse concertée pour mieux cadrer la contre-mesure et isoler le mal. Avec les avantages multiples de l'opérationnalisation de la force conjointe G5 Sahel, l'espoir est permis si cette dernière arrive à combler les lacunes des dispositifs militaires nationaux et internationaux impuissant pour l'heure à enrayer les groupes djihadistes dans la région. Cet espoir sera réalisé si un jour cette force de coopération entre armées sahéliennes parvient à sécuriser nos espaces frontaliers et remplacer l'opération Barkhane dans la traque et la destruction des groupes armés terroristes, dans l'ensemble de la bande sahélo-saharienne. L'intégration d'un outil cyberdéfense au sein du secrétariat permanent G5 Sahel complètera le processus sécuritaire tel que stipulé dans la stratégie pour le développement et la sécurité : « *Les pays membres du G5 Sahel ont besoin d'une utilisation renforcée et coopérative des moyens de lutte contre l'insécurité, notamment dans le domaine de la défense nationale, de la surveillance du territoire, de la police judiciaire, de* ***la cybercriminalité****, du contrôle des flux migratoires, de la lutte contre la criminalité organisée transnationale et du terrorisme ».*

Conclusion

D'une superficie de plus de 6 millions de kilomètres carrés et riche de plus de 320 millions d'habitants, l'Afrique de l'ouest dispose d'atouts indiscutables au regard de sa position géostratégique entre l'Europe, l'Amérique et la Chine et de son potentiel de développement. Largement irrigué en câbles sous-marins grâce à sa façade maritime, la sous-région profite d'un maillage dense pour l'accès à Internet et aux télécommunications. L'interconnexion des zones reculée ou enclavée par fibres optiques se heurte au manque de réseaux nationaux et par conséquent elle est souvent laissée à la diligence des opérateurs de télécommunication. C'est un aspect de souveraineté nationale qui dépasse normalement le cadre des opérateurs - qui mettent en avant l'intérêt des marchés - vu le nombre d'abonnés et la dépendance accrue et exponentielle au numérique. Les Etats doivent prendre leurs responsabilités et investir dans le domaine pour mettre en marche la locomotive du progrès avant qu'il ne soit tard.

Un proverbe français dit : « Le monde appartient à ceux qui se lèvent tôt.» Pour réaliser ses ambitions, il faut se mettre à l'œuvre sans attendre. « Paris appartient à ceux qui se lèvent tôt.[55]» Les proverbes anciens font en effet souvent référence à la nécessité d'être matinal pour mener à bien les travaux de la terre notamment.

A défaut d'avoir la maitrise des outils de sécurité des données numériques et les moyens de se les approprier, les armées subsahariennes préfèrent soit de ne pas mettre un contenu d'importance stratégique en ligne ou tout simplement isoler les réseaux à contenu sensible (données circulant sur intranet).

Cette fuite en avant avec les désavantages qu'elle procure n'est plus possible aujourd'hui car autour de nous tout est connecté (les objets connectés) et fait partie de notre quotidien. Il faut alors développer des outils permettant de mieux gérer l'accès à nos données informatiques, en passant par le cryptage de celles-ci et enfin pouvoir identifier les failles de sécurité pour anticiper les cyber-attaques et administrer les crises et enfin profiter pleinement des atouts des nouvelles technologies.

Pour réussir une approche globale de cyberdéfense dans la sous-région ouest africaine et mettre en place un organe pour une action cyber concertée – dans la zone subsaharienne ou plus précisément la bande sahélo-saharienne- qui est un

[55] http://www.linternaute.com/proverbe/330/le-monde-appartient-a-ceux-qui-se-levent-tot/

objectif légitime et nécessaire mais dont la réalisation semble à priori encore lointaine malgré les perspectives françaises encourageantes (Ecole de Cyberdéfense à Dakar). Dans le contexte purement militaire, des évolutions sont nécessaires. Certaines sont en cours (montée en puissance G5 Sahel, Ecole Supérieure Polytechnique en Mauritanie). Mais beaucoup reste à faire dans les deux axes majeurs : d'une part l'impératif de maitrise de la technologie du numérique et d'autre part l'impératif de la mise en place du cadre juridique et institutionnel. La création d'un pôle militaire d'excellence cyber au niveau des pays du G5 Sahel pourra être le cadre adéquat de l'expérimentation d'une structure sous régionale plus complète et plus aguerrie. Pour qu'ensemble nous bâtissions une vision commune : « *Faire des pays du G5 Sahel un espace économiquement intégré, socialement prospère, culturellement riche, où la sécurité et la paix règnent durablement, en se fondant sur l'état de droit, la bonne gouvernance et la démocratie, par la création d'une communauté moderne,* ***ouverte à l'innovation et à la technologie****, unie, solidaire et tolérante, contribuant efficacement à l'amélioration constante de la qualité de vie de toutes ses populations et à tous les niveaux.* [56]»

[56] http://www.g5sahel.org/images/Docs/SDS_G5S_VF.pdf

REFERENCES BIBLIOGRAPHIQUES

REVUE STRATEGIQUE DE LA DEFENSE ET DE SECURITE NATIONALE FRANÇAISES DU 17 OCTOBRE 2017.

HTTP://WWW.DEFENSE.GOUV.FR/PORTAIL/ENJEUX2/LA-CYBERDEFENSE/LA-CYBERDEFENSE/PRESENTATION

HTTP://DATA-SCIENTIX.COM/CYBERDEFENSE-MENACES-ET-DIMENSIONS-DE-SECURITE-SUJET-DETUDE-POUR-LE-DATA-SCIENTIST/

HTTP://WWW.DEFENSE.GOUV.FR/PORTAIL/ENJEUX2/LA-CYBERDEFENSE/LA-CYBERDEFENSE/PRESENTATION

HTTP://WWW.JEUNEAFRIQUE.COM/398696/ECONOMIE/ACCES-A-INTERNET-CONTINENT-AFRICAIN-ENTRE-PROGRES-INEGALITES/

HTTP://WWW.LEMONDE.FR/EUROPE/ARTICLE/2007/06/27/L-ESTONIE-TIRE-LES-LECONS-DES-CYBERATTAQUES-MASSIVES-LANCEES-CONTRE-ELLE-PENDANT-LA-CRISE-AVEC-LA-RUSSIE_928568_3214.HTML#JGS4T1GOYVIJRKF1.99

HTTP://WWW.01NET.COM/ACTUALITES/LESTONIE-DENONCE-LES-CYBER-ATTAQUES-TERRORISTES-RUSSES-350759.HTML

DANIEL VENTRE, CYBERATTAQUE ET CYBERDEFENSE, HERMES SCIENCE LAVOISIER § P. 96

HTTPS://WWW.SSTIC.ORG/MEDIA/SSTIC2010/SSTIC-ACTES/CYBERDEFENSE/SSTIC2010-ARTICLE-CYBERDEFENSE-LAGADEC.PDF

MICHEL LALLEMENT, L'ÂGE DU FAIRE. HACKING, TRAVAIL, ANARCHIE, EDITIONS DU SEUIL, JANVIER 2015 §P02

HTTPS://WWW.CRIMECNAM.NET/K2-USER-GROUPS/M-2/CRM-210.HTML

ANSSI, VULNERABILITIES 0`DAY, PREVENTION ET BONNES PRATIQUES,

HTTP://WWW.SSI.GOUV.FR/IMG/PDF/GUIDE_VULNERABILITES_0DAY.PDF

DIDIER DANET ET AMAEL CATTARUZZA, 2014, « LA CYBERDEFENSE QUEL TERRITOIRE, QUEL DROIT », PARIS, ECONOMICA § P.43

HTTPS://AFRIQUE.LATRIBUNE.FR/AFRICA-TECH/2017-05-18/CYBER-SECURITE-L-AFRIQUE-UNE-PROIE-FACILE-715875.HTML

WWW.DEFENSE.GOUV.FR

DICTIONNAIRE DE LA GUERRE ET DE LA PAIX, SOUS LA DIRECTION DE BENOIT DURIEUX, JEAN-BAPTISTE JEANGENE VILMER, FREDERIC RAMEL, § P. 337

DICTIONNAIRE DE LA GUERRE ET DE LA PAIX, § P. 338/339

RAPPORT_FINAL_JUILLET_2015, MASTER DE CYBERSECURITE, SOUS L'EGIDE DU CSFRS

ANSSI, «MENACE SUR LES SYSTEMES INFORMATIQUES, GUIDE N°650, HTTP://WWW.SSI.GOUV.FR/IMG/PDF/GUIDE650-2006-09-12.PDF

BERTRAND BOYER, CYBERSTRATEGIE L'ART DE LA GUERRE NUMERIQUE NUVIS,§P 166

DAVID A. FULGHUM, CYBER-WARFIGHTING RULES BIGINNING TO EMERGE. TRADUCTION DE L'AUTEUR.

LA CRIMINALITÉ INFORMATIQUE AVANCÉE EN AFRIQUE, AUTEURS : JEAN-JACQUES ALEX, GILLES CHABANNES, PIERRE-MARIE LEOUTRE, RONAN MOUCHOUX, MASTER M2

DOC CNAM/CRM210 INTRODUCTION GENERALE AU CYBER

HTTPS://WWW.SSI.GOUV.FR/ENTREPRISE/PRINCIPALES-MENACES/SABOTAGE/

RAPPORT_FINAL_JUILLET_2015, MASTER DE CYBERSECURITE, SOUS L'EGIDE DU CSFRS, ANNEXE 7

SESSION NUMBER C22 INTRODUCTION TO ADVANCED SECURITY THREATS, BRYAN KISSINGER,PHD, ISACA SF FALL CONFERENCE NOVEMBER 8TH, 2011

DOCUMENTATION CNAM ; INTRODUCTION GENERALE, CYBERCRIMINALITE, CYBERSECURITE, CYBERDEFENSE, AUTEUR : PHILIPPE BAUMARD PROFESSEUR DES UNIVERSITES, AGREGE DES FACULTES CONSERVATOIRE NATIONAL DES ARTS ET METIERS,

HTTPS://WWW.LEXPRESS.MU/ARTICLE/290412/BIRGER-VEUT-ENGRANGER-75-REVENUS-LAFRIQUE-DICI-2020

DIDIER DANET ET AMAEL CATTARUZZA, 2014, « LA CYBERDEFENSE QUEL TERRITOIRE, QUEL DROIT », PARIS, ECONOMICA § P.60

LA CRIMINALITÉ INFORMATIQUE AVANCÉE EN AFRIQUE, AUTEURS : JEAN-JACQUES ALEX, GILLES CHABANNES, PIERRE-MARIE LEOUTRE, RONAN MOUCHOUX, MASTER M2

HTTP://WWW.CABLEMAP.INFO/

HTTP://EN.WIKIPEDIA.ORG/WIKI/WACS_(CABLE_SYSTEM)

HTTP://WWW.GLOWORLD.COM/GLO1.ASP; HTTP://EN.WIKIPEDIA.ORG/WIKI/GLO-1_(CABLE_SYSTEM)

WIDEMOUTH BAY (UNITED KINGDOM).

HTTP://WWW.MAINONECABLE.COM/; HTTP://EN.WIKIPEDIA.ORG/WIKI/MAIN_ONE_(CABLE_SYSTEM)

HTTP://EN.WIKIPEDIA.ORG/WIKI/ACE_(CABLE_SYSTEM)

HTTP://WWW1.ALCATEL-LUCENT.COM/SUBMARINE/REFS/CIBLES/ATLS/ATLANTIS2.HTM,

HTTP://EN.WIKIPEDIA.ORG/WIKI/ATLANTIS-2

HTTP://WWW.WASACE.COM; HTTP://EN.WIKIPEDIA.ORG/WIKI/WASACE_(CABLE_SYSTEM)

SOURCE: CSAO

HTTPS://AFRIQUE.LATRIBUNE.FR/AFRICA-TECH/TELECOMS/2017-07-20/TELEPHONIE-MOBILE-L-AFRIQUE-DE-L-OUEST-CONNAITRA-UNE-DES-PLUS-FORTES-CROISSANCES-MONDIALES-D-ICI-2020-ETUDE-744398.HTML
HTTP://FR.ALLAFRICA.COM/STORIES/201609271175.HTML
HTTP://WWW.TICEDUFORUM.CI/INTERNET-VOICI-LES-PAYS-DAFRIQUE-DE-LOUEST-LES-PLUS-CONNECTES/
HTTPS://WWW.NSA.GOV/
HTTP://WWW.LADOCUMENTATIONFRANCAISE.FR/VAR/STORAGE/RAPPORTS-PUBLICS/064000048.PDF
DICTIONNAIRE DE LA GUERRE ET DE LA PAIX, SOUS LA DIRECTION DE BENOIT DURIEUX, JEAN-BAPTISTE JEANGENE VILMER, FREDERIC RAMEL, § P. 1274
SECURITE DES SYSTEMES D'INFORMATION, JEAN-YVES MARION, UNIVERSITE DE NANCY LORIA
HTTPS://WWW.IRISA.FR/PRIVE/BCOUSIN/COURS/1-SECURITE-DES-RESEAUX.2P.PDFHTTPS://WWW.JOURNALDUNET.COM/SOLUTIONS/EXPERT/63147/LES-5-GRANDS-PRINCIPES-DE-LA-GESTION-DU-RISQUE-INFORMATIQUE.SHTML
HTTPS://WWW.HBRFRANCE.FR/CHRONIQUES-EXPERTS/2017/12/18178-NOUVEAUX-OUTILS-MIEUX-MAITRISER-RISQUE-CYBER/
HTTPS://ATELIER.BNPPARIBAS/SMART-CITY/ARTICLE/CYBERSECURITE-PASSE-PARTAGE-INFORMATION
HTTPS://WWW.DEFENSE.GOUV.FR/PORTAIL/ENJEUX2/LA-CYBERDEFENSE/LA-CYBERDEFENSE/PRESENTATION
HTTPS://WWW.TTU.FR/G5-SAHEL-MENU-DISCUSSIONS-ALGER-DAKAR/
HTTPS://WWW.LATRIBUNE.FR/TECHNOS-MEDIAS/CYBERATTAQUES-QUE-CONTIENT-LE-PAQUET-CYBER-QUE-L-EUROPE-VEUT-VOTER-EN-2018-751009.HTML
HTTPS://IDL-BNC-IDRC.DSPACEDIRECT.ORG/BITSTREAM/HANDLE/10625/47118/133493.PDF?SEQUENCE=1
LA CRIMINALITÉ INFORMATIQUE AVANCÉE EN AFRIQUE, AUTEURS : JEAN-JACQUES ALEX, GILLES CHABANNES, PIERRE-MARIE LEOUTRE, RONAN MOUCHOUX, MASTER M2
HTTP://WWW.LINTERNAUTE.COM/PROVERBE/330/LE-MONDE-APPARTIENT-A-CEUX-QUI-SE-LEVENT-TOT/
HTTP://WWW.G5SAHEL.ORG/IMAGES/DOCS/SDS_G5S_VF.PDF