Cyberdéfense : enjeux et défis des Armées

***« L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique »* Albert Einstein.**

Par le commandant Aly MIME

Les récentes polémiques sur l'origine de la gigantesque panne d'électricité au Venezuela qui, pour le gouvernement, était causée par une cyberattaque commanditée par un pays étranger, laissent entrevoir à quel point le cyberespace est maintenant considéré dans les conflits.

En 2007, la première cyberattaque visant des structures étatiques eut lieu en Estonie et a été attribuée dès les premiers jours à la Russie par les autorités estoniennes[1]. Après l'attaque des centrifugeuses iraniennes en 2010 avec la cyberarme «Stuxnet», développée par les Etats unis et Israël[2], le potentiel de destruction de ces programmes malveillants est avéré. Les derniers développements technologiques ont permis aux grandes puissances numériques d'intégrer dans leur arsenal des cyberarmes capables de déstabiliser des pays, en les espionnant ou même en sabotant leurs infrastructures vitales. L'extension du cyberespace à l'ensemble des activités humaines rend possible en permanence et de façon imprévisible pour un adversaire de détruire une infrastructure vitale, en bénéficiant d'un anonymat. Il est important de se rendre à l'évidence que « ce qui pouvait relever hier encore de la science-fiction ou, du moins, de scénarios catastrophes dont on peinait à envisager le caractère réalisable à un horizon prévisible apparaît dorénavant comme une possibilité sérieuse, comme une menace tangible et comme une éventualité stratégique à prendre en considération en termes de doctrine militaire, de conduite des opérations et, plus globalement, d'organisation de la protection et de la résilience de l'ensemble de la société. »[3] Conscient de ce défi, beaucoup de pays ont adopté des stratégies et ont mis en place des structures dédiées, chargées d'organiser, de coordonner et de gérer la réponse face aux cybermenaces. Parallèlement, les armées ont également pris la mesure des enjeux de ce nouveau milieu de confrontation, en réorganisant leur outil de défense. En effet, à l'ère de l'information, la défense ne se limite plus à la seule défense physique des frontières. La récurrence de ces attaques dans le cyberespace, impliquant justement des grandes puissances, appelle à s'interroger sur la manière d'organiser la défense pour faire face aux défis inhérents de ce milieu complexe.

Face à ces menaces diffuses, polymorphes et évolutives issues de cet espace, il convient pour les Etats de faire de la cyberdéfense une priorité nationale, de définir des orientations stratégiques pour protéger leurs intérêts vitaux dans le cyberespace. Pour les Armées, il s'agira de développer des capacités en matière de cyberdéfense permettant tout en garantissant la protection de leurs réseaux, d'être en mesure de mener des opérations dans ce nouvel espace et de contribuer à la cyber-résilience des infrastructures critiques de l'Etat. Pour remplir efficacement cette mission, certaines armées ont mis en place un commandement cyberdéfense avec les mêmes prérogatives que les commandements des états-majors d'armée (terre, air et mer).

Cet article se propose d'évaluer le cyberespace et les principales menaces cyber pouvant affecter la défense et la sécurité nationale d'un pays, puis d'analyser le rôle de l'Etat dans la cyberdéfense d'une nation, avant d'étudier la manière de réorganiser l'outil de défense pour faire face à ces menaces.

---

[1] Philippe Crouzillacq, « L'Estonie dénonce les cyber-attaques terroristes russes », 01net.com, le 11 juin 2007.

[2] David E. SANGER, « Obama Order Sped Up Wave of Cyberattacks Against Iran », nytimes.com, le 01 juin 2012.

[3] BASTIEN LACHAUD et ALEXANDRA VALETTA-ARDISSON « commission de de la Défense nationale et des forces armées françaises en conclusion des travaux d'une mission d'information sur la cyberdéfense », le 4 juillet 2018.

I- Le cyberespace et les principales menaces cyber

11- Le cyberespace, milieu de confrontation à part entière.

Le cyberespace est définit par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) française comme un « espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques»[4]. C'est grâce au développement très rapide des Technologies de l'Information et de la Communication (TIC), et en particulier de l'Internet que le cyberespace tient aujourd'hui une place considérable dans nos sociétés. Les systèmes d'information sont partout présents, dans les pays développés comme dans ceux en voie de développement, et dans toutes les formes d'activités, jusqu'aux plus sensibles. Ils sont devenus les centres nerveux de nos sociétés. Néanmoins, l'interconnexion croissante de ces systèmes d'information et de communication rend plus vulnérable la sécurité des infrastructures et des données. Elle constitue une faille amplement exploitée par des individus, des groupes d'individus ou des États mal intentionnés, d'autant plus que le cyberespace est un espace anonyme et sans frontières dans lequel il est difficile d'identifier les auteurs lors d'une cyberattaque. De plus, tout investissement humain et financier conséquent n'est plus nécessaire pour engager une cyberattaque. En effet, quelques ordinateurs connectés et des malware ou spyware (virus malveillants ou espions) performants, téléchargeables en ligne, permettent à une poignée de hackers, délocalisés et sans lien direct avec le service commanditaire, d'engager une attaque. Qui plus est, ce domaine virtuel, en perpétuelle évolution, est fragile car il subit le rythme effréné des avancées technologiques dans le domaine dont la sécurité n'est pas toujours garantie. Toutes ces facilités offertes par cet espace ont favorisé sa transformation en un milieu de conflictualité. La guerre dans le cyberespace est une réalité. C'est ainsi que le Sommet de l'Organisation du Traité de l'Atlantique Nord (OTAN) de juillet 2016 à Varsovie[5] a d'ailleurs réaffirmé que le cyberespace est désormais considéré comme le cinquième champ de bataille et qu'à ce titre il est un terrain d'opérations militaires au même titre que la terre, l'air, l'espace ou la mer. Dès lors, la compréhension des menaces qui affectent la défense et la sécurité nationale dans ce milieu demeure indispensable pour conceptualiser un dispositif national de protection et de défense informatique efficace.

12- Les cybermenaces : menaces en constante évolution.

La menace cyber ne cesse de croitre dans ses formes et son intensité. Les auteurs des cyberattaques poursuivent quatre types d'objectifs non exclusifs entre eux : l'espionnage, les trafics illicites, la déstabilisation et le sabotage. Ces cybermenaces visent les citoyens, les entreprises, les infrastructures vitales y compris le gouvernement et les Armées.

Le cyberespionnage n'est qu'une transposition dans le monde numérique d'activités traditionnelles de renseignement. Son objectif est d'abord à la portée des services de renseignement des pays techniquement avancés qui, depuis longtemps, ont développé des systèmes d'interception des communications à des fins d'espionnage économique, technologique ou politique. Les révélations d'Edward Snowden, l'article du journal "Le Monde Afrique"[6] sur l'espionnage informatique de la Chine au siège de l'Union africaine et les allégations contre la Russie par beaucoup de pays[7] montrent l'ampleur de cette forme d'espionnage des grandes puissances. Le recours à cette pratique n'est cependant plus l'apanage quasi exclusif des services spécialisés des Etats du fait de la prolifération de programmes malveillants et sophistiqués dans les marchés noirs (le dark web) de la cybercriminalité.

[4] https://www.ssi.gouv.fr/entreprise/glossaire/c/

[5] https://www.nato.int/cps/fr/natohq/official_texts_133169.htm

[6] https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html

[7] https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/les-etats-unis-les-pays-bas-le-canada-et-le-royaume-uni-accusent-la-russie-d-avoir-mene-plusieurs-cyberattaques-a-leur-encontre_2970247.html

Au début, la cybercriminalité se réduisait à des actions ponctuelles conduites par des hackers isolés, pour lesquels la prouesse technique elle-même, au-delà de toute motivation politique ou financière, constituait souvent une finalité en tant que telle. Les effets de leurs cyberattaques étaient souvent limités à des campagnes de « defacement » de sites Internet. Aujourd'hui, les réseaux cybercriminels se sont beaucoup développés et professionnalisés. L'émergence des monnaies virtuelles telles que la monnaie bitcoin associée à l'utilisation des réseaux d'anonymisation comme Tor, a favorisé l'explosion de la cybercriminalité. En 2017, le groupe de hackers Shadow Brokers aurait subtilisé un arsenal de cyberarmes à la National Security Agency (NSA) des Etats-Unis. Ces outils, livrés sur internet, auraient suscité une vague de cyberattaques.[8] Les cybercriminels parviennent dorénavant à capter des sommes très importantes d'argent. D'après une étude réalisée conjointement par INTERPOL et Trend Micro sur les activités cybercriminelles en Afrique de l'Ouest, les montants dérobés chaque année sont estimés en moyenne à 2,7 millions de dollars entre les années 2013 et 2017.[9] Depuis un certain temps, on assiste à un effacement progressif de la frontière entre lutte contre la cybercriminalité et les objectifs de cyberdéfense, en raison soit de la nature ambiguë de certaines cyberattaques, soit de l'ampleur de leurs effets. En effet, l'apparition d'attaques informatiques conduites à des fins de cybercriminalité mais qui, par leur spécificité, sont susceptibles de paralyser des activités critiques, constituent donc une menace en matière de sécurité nationale.

Le troisième type d'objectif poursuivi par ces acteurs malveillants est la déstabilisation. Observé, notamment dans les élections présidentielles de plusieurs pays, ce type d'opération est lié au développement d'Internet et des réseaux sociaux. Ces nouveaux moyens de communication ont longtemps été considérés comme des facteurs favorisant la liberté d'expression ainsi que la diffusion du savoir et de l'information parce qu'ils jouissent de la spécificité d'échapper à priori au contrôle des Etats et s'affranchissent des frontières. Ces moyens ont contribué à la chute de certains régimes pendant le « printemps arabe ». Ce nouvel espace d'expression est cependant exploité dans une logique de propagande politique et propagation d'idéologies aux contenus contestables. Les groupes extrémistes, terroristes se sont ainsi appropriés l'espace des réseaux sociaux. Les fake news se diffusent beaucoup plus vite que les faits réels. Les opinions peuvent être aisément manipulées. En 2016, à l'occasion de la campagne présidentielle américaine, la compromission des messageries électroniques et la divulgation massive d'informations confidentielles concernant la candidate démocrate ont fini par perturber le processus électoral. Ainsi, la menace cyber peut atteindre le processus démocratique. Cette menace, exécutée par des groupes terroristes ou des puissances étrangères dans l'objectif de provoquer des actions violentes ou déstabilisatrices pour la société, est très sérieuse.

Enfin, les cyberattaques peuvent causer des dégâts dans le monde physique. Dans la poursuite de leurs efforts de modernisation et d'efficacité, les infrastructures essentielles (énergie, eau, réseaux de transport etc.) continuent de bénéficier d'une automatisation et de la connexion à Internet leurs dispositifs. Bien que l'accès à Internet des dispositifs de télésurveillance et d'acquisition de données (SCADA pour Supervisory Control and Data Acquisition) comporte plusieurs avantages, notamment, la gestion à distance, elle peut également exposer ces infrastructures au risque cyber. Une cyberattaque est susceptible de paralyser l'activité d'une entité non seulement en neutralisant ses réseaux, mais aussi en détruisant ses équipements les plus critiques. En mai 2017, le rançongiciel WannaCry a infecté plusieurs ordinateurs vulnérables dans au moins 100 pays. Il s'est notamment propagé dans plusieurs structures sanitaires offrant des services d'urgence. L'incident a occasionné l'annulation de plusieurs rendez-vous, dont des chirurgies.[10] Les cybercriminels seraient de la Corée du Nord.

Au Sénégal, après les attentats de Charlie Hebdo en 2015, le groupe de Hackers Anonymous avaient attaqué le site de l'Agence de l'informatique de l'Etat (ADIE). En fin janvier de cette année, une cyberattaque avait visé la compagnie nationale Air Sénégal pour tenter en vain de retarder le démarrage de ses services qui devaient démarrer en début février. Les cybercriminels auraient tenté de faire tomber en vain la plateforme de réservation de la compagnie par l'attaque très connue

[8] https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

[9] https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2017/Selon-une-etude-realisee-par-INTERPOL-et-Trend-Micro-une-economie-souterraine-de-la-cybercriminalite-se-developpe-en-Afrique-de-l-Ouest

[10] https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

par déni de service distribuée (DDOS pour Distributed Denial of Service). Il y'a deux semaines, le journal Libération révélait que la Banque de Dakar (BDK) avait été victime d'une attaque informatique qui auraient permis aux cybercriminels de subtiliser des sommes importantes d'argent.

L'ampleur des cybermenaces, en particulier celles qui portent sur les services essentiels au fonctionnement du pays, a conduit les Etats à prendre en compte la cyberdéfense au plus haut niveau.

II- Le rôle de l'État dans la prise en compte de ces menaces

Définit par l'ANSSI comme étant l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels, la cyberdéfense doit constituer une priorité nationale pour tout Etat. Le rôle de l'État est fondamental dans la prise en compte des menaces cybernétiques. C'est à travers des orientations stratégiques claires, un modèle d'organisation et de gouvernance approprié et une coopération internationale que les Etats pourront faire face aux cyberattaques qui violent leur souveraineté nationale.

21- La nécessité d'une stratégie adaptée

L'une des premières étapes pour la cyberdéfense est de disposer d'une stratégie. C'est ainsi que dès novembre 2017, le Sénégal a élaboré sa stratégie nationale de Cybersécurité à l'horizon 2022 (SNC2022)[11] dans laquelle il est stipulé :
« En 2022 au Sénégal, un cyberespace de confiance, sécurisé et résilient pour tous ». Afin de réaliser cette vision, le Gouvernement s'est fixé cinq objectifs stratégiques à atteindre. Il s'agit de:

1: renforcer le cadre juridique et institutionnel de la cybersécurité au Sénégal ;
2: protéger les infrastructures d'information critiques et les systèmes d'information de l'Etat;
3: promouvoir une culture de la cybersécurité;
4: renforcer les capacités et les connaissances techniques en cybersécurité ;
5: participer aux efforts régionaux et internationaux de cybersécurité.

L'atteinte des deux premiers objectifs stratégiques serait suffisante pour le Sénégal pour mettre en place un système de cyberdéfense permettant de mieux répondre aux attaques cyber, voire de les prévenir. Le renforcement du cadre juridique et institutionnel permettra de corriger les manquements constatés dans notre arsenal juridique cyber et de mettre en place des structures dédiées pour la gouvernance. En effet, pour la protection des infrastructures jugées critiques de l'Etat qui constitue le deuxième objectif stratégique, en plus de leur recensement et de leur classification, une loi, qui définit les responsabilités et les obligations de ces infrastructures en termes de protection de leurs systèmes d'information critiques, devrait être adoptée. Elle devrait les contraindre à déclarer de façon immédiate des incidents cybers affectant de manière significative leurs systèmes d'information critiques. Egalement, une stratégie de cyberdéfense, qui décrira l'approche nationale face à ces menaces qui visent notre défense et notre sécurité, complètera ces orientations. Les structures de gouvernance qui seront créées reflèteront le modèle d'organisation et de gouvernance que le Sénégal mettra en place pour faire face à aux défis cyber.

22- Un modèle d'organisation et de gouvernance approprié pour faire face à ces menaces

L'étude des modèles d'organisation et de gouvernance de cyberdéfense fait ressortir deux modèles principaux : le modèle français qui sépare les missions et capacités offensives et des missions et capacités défensives et celui des pays anglo-saxons dont les capacités de cyberdéfense sont concentrées au sein de la communauté du renseignement.[12] Dans la stratégie nationale de cybersécurité du Sénégal, il est prévu de mettre en place les structures suivantes:

- une autorité nationale de cybersécurité, instance de coordination nationale ;
- un CERT (*Computer emergency response team*) national, chargé de la veille et de la réponse des incidents ;
- un centre de commandement et de contrôle pour la cyberdéfense.

En outre, l'Ecole nationale de Cybersécurité à vocation régionale nouvellement créée se chargera de la formation des policiers, des militaires et des civils dans le cadre de la prévention et de la répression de la cybercriminalité.

[11] http://www.numerique.gouv.sn/sites/default/files/SNC2022-vf.pdf

[12] La NSA aux Etats-Unis et le Government Communication Headquaters (GCHQ) au Royaume-Unis.

Le Sénégal pourrait s'inspirer d'un des modèles d'organisation et de gouvernance qui s'adapte le mieux à son contexte. Les menaces qui composent le cyberespace représentent des dangers qui s'affranchissent des frontières, la réponse sécuritaire ne devrait pas se limiter au volet national et pourrait par conséquent prendre en compte de la coopération internationale.

23- La coopération internationale

Les cyberattaques traversent les frontières et peuvent être dirigées simultanément contre plusieurs Etats. La surveillance des réseaux et la mise au point des réactions en cas d'incident justifient dans le cadre de la cybersécurité et de la cybercriminalité une coopération et une assistance internationales. De même les organismes internationaux devraient prendre en compte les cyberattaques dans le cadre de la juridiction pénale internationale. De manière plus générale, la cyberdéfense constitue aujourd'hui une préoccupation commune à de nombreux Etats. Plusieurs organisations multilatérales ont mis la cybersécurité à l'ordre du jour de leurs travaux. L'Organisation des Nations Unies (ONU) a adopté plusieurs documents concernant les technologies de l'information et de la communication et leurs aspects relatifs à la sécurité. Le Sénégal a déjà ratifié la convention de Budapest sur la cybercriminalité et la convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Au niveau régional, l'Union Africaine a adopté en 2014 à Malabo, une convention sur la Cybersécurité et la Protection des données personnelles. Un simple constat permet de révéler que toutes ces conventions tournent autour de la lutte contre la cybercriminalité et la protection des données à caractère personnel. D'où la nécessité pour les Etats, d'une part, d'harmoniser la sémantique dans le monde cyber, d'autre part, de se mettre d'accord sur un cadre juridique applicable en cas de cyberguerre : un droit international du cyberespace. En effet, le chantier est vaste dans ce domaine et les Etats devraient, à l'instar des pays de l'OTAN qui ont élaboré les Manuels de Tallinn (1.0 et 2.0) et le droit international applicable aux opérations cyber[13], travailler en coopération sur ces sujets. De plus, une coopération opérationnelle des structures d'alerte et d'assistance (CERT) est nécessaire.
Etant donné que la cyberguerre est devenue une réalité, une réorganisation de notre outil de défense est indispensable.

III- La cyberdéfense, une priorité pour les Armées

Dans la stratégie nationale de cybersécurité, il est stipulé : « les forces nationales de défense (les armées) sont chargées de défendre le Sénégal contre les cybermenaces dirigées vers la souveraineté et à la sécurité nationales et enquêteront sur toutes les menaces relevant du domaine de la défense (cyberterrorisme, guerre cybernétique, etc.) Les forces nationales de défense, à travers le centre national de commande et de contrôle de la cyberdéfense, sont responsables des systèmes de sécurisation des informations et des infrastructures utilisées pour la défense nationale et travailleront en collaboration avec la structure nationale de cybersécurité pour soutenir la protection et la prévention contre les cyber incidents au niveau national, ainsi que l'atténuation de leurs effets et les retours d'incidents ». Dès lors, les Armées sont appelées à développer des capacités de cyberdéfense pour pouvoir préserver la souveraineté dans le cyberespace. Comme toute capacité militaire, celle de la cyberdéfense doit s'appuyer sur les six éléments constitutifs d'une capacité à savoir: une doctrine, une organisation, des ressources humaines, de l'entraînement, du soutien et des équipements.

31- Une doctrine, une réorganisation et des ressources humaines de qualité, piliers fondamentaux pour construire un système de cyberdéfense appropriée.

Chaque Etat a son approche du contrôle du cyberespace. La doctrine cyber, en cours d'élaboration dans les Armées sénégalaises, fixera le cadre d'emploi précis de l'utilisation du cyber en temps de paix, de crise ou de conflit. Elle précise les règles et les procédures permettant de conduire l'action cyber. Son intention sera donc de donner aux militaires, en particulier au commandement, « une même manière de voir, de penser et d'agir ». Une réorganisation sera aussi nécessaire pour intégrer les nouvelles structures dédiées à la cyberdéfense. A ce propos, la stratégie nationale de

[13] http://revel.unice.fr/psei/index.html?id=1852#tocfrom1n3

cybersécurité prévoit l'érection d'un centre de commandement cyber à l'horizon 2022 au sein des Armées sénégalaises.
A la création du commandement des opérations cyber en 2017, le ministre français de la Défense disait : « En l'espace de quelques années, la guerre s'est métamorphosée : il est donc nécessaire de créer une nouvelle composante au sein des armées pour asseoir notre souveraineté et notre indépendance nationales, et rester ainsi maîtres de notre destin ...». Avant cette date, beaucoup de pays disposaient déjà de commandement de cyberdéfense. Ainsi, l'Armée américaine a créé depuis 2009 son commandement cyber, United States Cyber Command (USCYBERCOM).
En ce qui concerne les ressources humaines, les transformations numériques actuelles et à venir suscitent de fortes attentes de profils hautement qualifiés et feront émerger de nouvelles compétences et de nouveaux métiers. Alors, Il serait indispensable de bien appréhender ces transformations en termes de RH pour se doter et mettre en œuvre des outils adéquats : modes de recrutement et rémunérations adaptés, parcours professionnels attractifs et favorables à la fidélisation du personnel.

32- L'entrainement, le soutien et les équipements

Les Armées sénégalaises pourraient contribuer à la cyber-résilience de ses propres infrastructures et de celles jugées vitales pour l'Etat, à travers l'entrainement. La Direction des Transmissions et de l'Informatique des Armées (DIRTRANS) dispose déjà d'un centre d'alerte et de réaction aux attaques informatiques (CERT), qui assure la protection de ses réseaux contre les attaques. L'organisation d'exercices cyber intégrant des infrastructures critiques de l'Etat aura l'avantage de permettre aux structures de travailler ensemble de connaitre les procédures à suivre en cas de crise cyber majeur et de développer des réflexes permettant de gérer les impacts y découlant et reprendre leurs activités. Ces exercices et les simulations d'incidents cybers majeurs sont des moyens permettant aux personnels civils de ces structures d'améliorer leurs capacités de prise de décision en cas de surprise. C'est ainsi que le Directeur des Transmissions et de l'Informatique des Armées a prévu d'organiser en 2020, un exercice cyber en y intégrant certaines infrastructures critiques de l'Etat.
En ce qui concerne les équipements, force est de constater qu'ils coûtent chers et le fonctionnement des structures créées nécessite un budget pour renouveler les licences et prendre en compte les formations. Un simple simulateur d'incident cyber coûte environ 4 milliards de franc CFA. La technologie et la maitrise technologique sont fondamentales pour mettre en place une structure de cyberdéfense.

En définitive, les TIC regorgent beaucoup d'opportunités. Elles ont réussi à transformer notre façon de vivre. Les services qu'elles offrent ont fini de créer de nouvelles dépendances. Les facilités qu'offre le cyberespace ont encouragé des acteurs malveillants à initialement mener des activités qui visaient des individus. Aujourd'hui, les cyberattaques sont passées du statut d'instrument de nuisance à celui d'outil de combat à part entière. La liste des Etats qui ont dû faire face à ces opérations hostiles ne cesse de s'allonger. Le cyberespace systématise l'asymétrie des conflits. Avec peu de moyens, un groupe d'individus, bien informé et doté d'une agilité technologique efficace, éventuellement mandaté par un Etat, peut déstabiliser le fonctionnement d'une infrastructure sensible, d'un territoire donné ou même d'un pays tout entier. Les défis en termes de sécurité nationale sont donc particulièrement importants. Conscient de ces défis, les Etats ont mis en place des stratégies, ont érigé des structures dédiées pour la gouvernance et l'organisation de cyberdéfense. Ces menaces aussi ont poussé les Armées à réorganiser leur outil de défense pour assurer la souveraineté des Etats dans le cyberespace.
Par ailleurs, avec les TIC en constante évolution (Big Data, Intelligence Artificielle) la guerre du futur pourrait être gagnée par celui qui bénéficiera de l'initiative de l'espace cyber.