Dr Papa GUEYE, Commissaire de Police
Directeur général de l'Ecole nationale de
Cybersécurité à Vocation régionale
.....

CYBERSECURITE, CYBERGUERRE ET CYBERDEFENSE :

Réponses pour un Etat souverain ?

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

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

1. INTRODUCTION

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

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

La cyberstratégie commande l'adoption de nouvelles règles de sécurité et de défense qui n'annihilent pas celles antérieures, lesquelles demeurent importantes. En termes clairs, ces

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

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

nouvelles règles ne remettent pas en cause les fondamentaux classiques de la conduite de la guerre, de la gestion de la sécurité publique (maintien et rétablissement de l'ordre) et ceux liés à la défense de l'intégrité du territoire dans lesquels le nouvel élan trouve son inspiration.

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

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

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

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

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

En ce qui concerne la criminalité[5], qui se manifeste à travers l'intrusion illicite dans les systèmes, le vol, la destruction de données ou même tout acte criminel perpétré via les réseaux, l'enjeu est l'établissement de la preuve, devenue très difficile à cause de sa volatilité et de la nature transfrontalière des infractions. Ainsi, se pose la lancinante question de la coopération qui doit également s'adapter pour éviter les lenteurs préjudiciables à l'action de la justice.

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

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

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

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

2. LE CYBERESPACE, UN DOMAINE STRATEGIQUE[7].

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

Le cyber a connu des évolutions avec son application dans divers domaines qui favorise l'usage de termes comme « e-réputation », « e-commerce », « e-gouv », « e-administration ». Cette nouvelle matrice conceptuelle s'est installée comme un centre d'intérêt majeur dans le champ de la sécurité défense et de la stratégie. Un bref rappel historique des cas d'agression cyber permet d'illustrer cette réalité.

En novembre 1988, le « ver Morris » a déclenché la première cyberattaque reconnue et signalée, qui a infecté des machines ciblées, provoquant leur ralentissement et leur plantage pour favoriser la perpétration d'attaques par déni de service et/ou de subtilisation de données. Certains logiciels d'attaques sont conçus pour cibler des vulnérabilités non encore identifiées dans les systèmes informatiques[8].

Depuis le début de la guerre dans le Donbass en 2014, l'Ukraine est devenue la cible privilégiée des hackers russes, leur terrain d'entraînement favori. Récemment, dans la nuit de l'invasion de l'Ukraine par la Russie, le 24 février 2022, des structures étatiques ont fait l'objet d'attaques par un virus informatique[9]. Pour faire face à l'intrusion numérique de l'information, l'Ukraine a créé une IT ARMY[10]. Ces illustrations montrent que le cyber est un

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

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

[8] Vulnérabilité non encore identifié ou vulnérabilité *zero-day* également orthographiée 0-day ou vulnérabilité du jour zéro[1] est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu.

[9] France info du 8 mars 2022, Guerre en Ukraine : quand les combats armés se doublent d'affrontements dans le cyberespace https://www.francetvinfo.fr/replay-radio/le-choix-franceinfo/guerre-en-ukraine-quand-les-combats-armes-se-doublent-d-affrontements-dans-le-cyberespace_4974759.html

[10] Cette IT Army ou Armée numérique est constituée d'unités offensives et défensives. L'unité offensive mènerait des opérations d'espionnage numérique contre les envahisseurs russes. Quant à l'unité défensive, elle défendrait les infrastructures telles que des centrales électriques et des systèmes d'approvisionnement en eau.

facteur stratégique qui entre dans l'échelle des menaces et sa prise en compte ne relève pas seulement d'un simple débat d'experts ; c'est aussi un devoir de sécurité nationale.

3. LE CYBER, UN ESPACE D'EXPRESSION DES RIVALITES ET D'EXTENSION DES CONFLITS.

Terrain d'expression des rivalités, le cyber est au cœur des actions hostiles et des conflits. Il constitue le domaine de prédilection, par excellence, de l'exploitation des fragilités inhérentes aux systèmes gouvernementaux, des vulnérabilités liées au carence technologique et au manque d'organisation de certains Etats. A titre d'exemple, nous pouvons citer le virus Stuxnet, qui à la suite d'un travail de renseignement d'ingénierie, de coordination et de planification extrêmement pointues, a permis de ralentir les capacités de riposte d'un pays[11]. Cela montre que tout rapport de force doit dorénavant intégrer la notion de cybersécurité et de cyber action.

Une simple pénétration dans le système de défense et sécurité d'un Etat peut avoir des impacts néfastes, allant de l'entrave de la manœuvre en cas de guerre, à la perturbation du fonctionnement des systèmes des armes et des communications, en passant par le blocage des centrales d'énergie ainsi que des sources d'approvisionnement. De plus, l'accès dans un système tiers permet de récupérer des données stratégiques, de les manipuler dans le but de se positionner, de modifier la perception de l'opinion en vue de l'influencer et éventuellement de l'orienter.

Ces exemples illustrent que le conflit ne se déroule plus exclusivement sur le terrain des opérations classiques, il se matérialise à travers le numérique par les procédés ci-après :

- **Le cyber espionnage** qui constitue la première brique de la cyber conflictualité. Toutes les actions offensives cyber débutent par une phase d'observation et de reconnaissance de la cible[12] dans tous les aspects de sa configuration et de sa mutation.
- **Le hacking ou sabotage informatique** qui se traduit par des attaques ou agressions par l'utilisation de virus qui détruisent les systèmes informatiques.
- **La subversion cyber** [13] vise à modifier des décisions, des informations par la décontextualisation ou par d'autres procédés.

[11] Pour plus de détails sur le processus et les différents étapes mis en œuvre par les Cyberpirates, voir GUEYE (P), Criminalité organisée, Terrorisme, Cybercriminalité : Réponses de Politiques criminelles éd : Harmattan 2018

[12] L'opinion du 2 avril 2022, Espionnage, sabotage, influence… le cyber, nouveau terrain d'affrontement entre Etat https://www.lopinion.fr/international/espionnage-sabotage-influence-le-cyber-nouveau-terrain-daffrontement-entre-etats,

L'opinion du 2 avril 2022, Espionnage, sabotage, influence… le cyber, nouveau terrain d'affrontement entre Etat https://www.lopinion.fr/international/espionnage-sabotage-influence-le-cyber-nouveau-terrain-daffrontement-entre-etats,
russe/

- **La cyberguerre économique** qui a modifié la concurrence classique qui régissaient le monde économique en introduisant de profond changement dans la façon d'espionner, de saboter et de subvertir.

4. REPONSES STRATEGIQUES POUR UNE SOUVERAINETE NUMERIQUE

L'action stratégique doit désormais s'orienter vers l'opérationnel du fait que le cyber est un nouveau théâtre d'engagement, permettant d'influencer et de modifier la perception et la volonté de l'adversaire. On note à ce niveau une récurrence des actions offensives recouvrant aussi bien la lutte informatique offensive que l'influence numérique. Il s'agit d'un véritable champ de bataille de l'information, pour l'information, par l'information et contre l'information.

Dès lors, les Etats sont tenus de renforcer leurs connaissances et leurs capacités d'anticipation surtout dans le domaine du renseignement opérationnel. La propagande djihadiste sur les réseaux sociaux a rendu urgente la priorisation de la problématique cyber à tous les échelons à partir d'une approche systémique.

Sous ce rapport, il est impératif pour les Etats de mettre en place et/ou de consolider des mécanismes pratiques et très opérationnels notamment :

1. La prospective stratégique qui permettra aux acteurs d'anticiper et d'être capable d'agir en fonction de l'évolution permanente et variante des menaces mais en plus d'identifier les contours, actuels et futurs. Il s'agit de former des ressources humaines ayant des capacités d'anticipation afin de protéger les systèmes d'information vitaux dans le territoire national.
2. La cyber protection active qui permettra non seulement d'organiser la sécurité d'un système mais aussi être sans cesse aux aguets, à travers des actions de mise à jour du système et de mobilisation permanent à l'attention des décideurs.
3. Le contrôle et la surveillance de l'information par la mise en place de structures de veille active et de centres d'opération ou de réaction rapide 24/7, en cas d'incident[14].
4. L'adaptation du renseignement opérationnel[15] pour renforcer la défense et pour préparer les actions offensives et de riposte.

[14] La résilience consiste en l'ensemble des mesures prises pour faire fonctionner un réseau attaqué pendant la crise, puis revenir à un état normal de fonctionnement après la crise (y compris avec des opérations de reconstruction, dans les cas les plus graves)

[15] Certains spécialistes distinguent le renseignement d'origine cyberespace (ROC), qui est celui qui vient *du* cyberespace mais contribue à nourrir la situation globale du renseignement militaire et qui intéresse plus le décideur ; et le renseignement d'intérêt cyberdéfense (RIC) qui vise à construire une situation particulière de l'espace cyber, aussi bien ami et neutre que surtout ennemi. A titre d'exemple, les mots de passe des comptes des réseaux sociaux de TV5 Monde, visibles dans un reportage de France 2, constituent du RIC, tandis que les cartes dynamiques de course de l'application Strava, permettant par l'observation de l'activité de soldats, de repérer des sites militaires, sont du ROC.

5. Le renforcement des partenariats nationaux et internationaux dans les domaines d'intérêts stratégiques.
6. L'innovation et la créativité : la recherche et la création d'un patrimoine technique national indexé aux identités locales et aux attentes spécifiques des comités et des acteurs.
7. La domestication de la technologie importée.

En conclusion, le cyber est désormais au centre de toutes les stratégies conflictuelles, qu'elles soient militaires ou non. L'action dans le cyberespace impose ainsi, la prise de conscience de cette dimension générale, qui au fond ne peut plus se réduire à un simple environnement technologique.

Le cyber fusionne les champs traditionnels des hostilités, des oppositions géopolitiques et des concurrences économiques. Il s'agit d'une globalisation du cyber dans les conflits et la criminalité, ce qui nécessite pour tout Etat souverain la maitrise des risques dans un but de sécurité et de défense nationale.

Pour ce faire, une approche holistique stratégique et opérationnelle et très pragmatique est nécessaire, fixant ainsi d'une manière concrète la doctrine et les plans d'action.

BIBLIOGRAPHIE

- *GUEYE (P) Criminalité organisée, terrorisme et cybercriminalité : réponses de politiques criminelles, éd. Harmattan 2018*
- *Le cyberespace, nouveau domaine de la pensée stratégique, collection Cyber stratégie dirigée par O. KEMPF, éd. Economica 2013,175 pages.*
- *« L'intégration des citoyens dans une stratégie nationale de cyberdéfense », par Vincent Joubert et Gergana Petkova, Note de la FRS, n°02/2014*
- *Enquête sur la sécurité numérique des entreprises par Bruno Gruselle, Note de la FRS, n°01/2013*
- *Cyber dissuasion par Bruno Gruselle, Bruno Tertrais, Alain Esterle, Recherches & Documents, FRS, n°03/2012*
- *« Espionnage entre alliés: On a vraiment changé d'échelle » par François Heisbourg (interview),* L'Express, *01 juillet 2013*
- *« Espionnage : Personne n'a intérêt à briser les relations » par Alain Esterle (interview),* Public Sénat, *01 juillet 2013*
- *« La dissuasion au défi du cyberespace » par Vincent Joubert, in « La dissuasion »,* Les Champs de Mars, *n°25, La Documentation française, 18 juin 2013*
- Stocktaking Study of Military Cyber Defence Capabilities in the European Union (milCyberCAP): Unclassified Summary *Alain Esterle (parmi les auteurs), RAND, 10 juin 2013*
- *Le cyberespace : Nouveau domaine de la pensée stratégique, sous la direction de S. Dossé, O. Kempf, C. Malis, avec Alain Esterle (parmi les auteurs), Économica, juin 2013*
- *« Le Défi des nouveaux usages numériques : la sécurité des entreprises à la peine » par Bruno Gruselle,* Sécurité & Stratégie, *n°11, hiver 2012-2013*