Laboratoire Africain de
Recherches en Cyberstratégie

La stratégie militaire appliquée au cyberespace africain

Entretien avec le Colonel Roger KUITCHE

Le ®Colonel Roger KUITCHE retraité des Forces Armées est reconnu pour son expertise en stratégie militaire, mais aussi pour son exposition internationale significative, notamment en lien avec les mécanismes des Nations Unies et d'autres organisations internationales. Il est également le CEO de la société Best Practice, où il se concentre sur le coaching et le conseil stratégique aux décideurs, notamment dans le domaine de la sécurité et de la paix. En plus de son rôle dans le secteur privé, il est impliqué dans des initiatives visant à démystifier la stratégie militaire appliquée aux entreprises et aux administrations, ce qui montre son engagement à partager ses connaissances et son expertise.

Explorons ensemble ce projet bien ficelé de notre expert stratège.

COLONEL KUITCHE

Notes sur Best Practice

La rédaction : Comment s'est façonnée votre vision stratégique ? Parlez-nous de votre expérience militaire.

RTD Colonel : La participation active à la guerre de Bakassi a été la pierre angulaire de ma formation dans ce domaine. Plus tard, en tant que commandant de la 41ème Brigade d'infanterie motorisée, (2014-2016) je crois avoir joué un rôle crucial dans les opérations contre Boko Haram. Cette expérience m'a appris l'importance de la résilience, de la coordination et de la stratégie à long terme.

Comme membre de la Mission de l'Union Africaine au Soudan (MUAS) de 2005 à 2007 avec la fonction d'Officier Mouvement au sein du Darfur Integrated Task Force, et plus tard commandant du détachement camerounais à la MICOPAX en RCA (2010-2012), notre vision de la diplomatie militaire et des opérations internationales a été renforcée. De 2016 à 2019, attaché défense du Cameroun auprès du Haut- Commissariat du Cameroun au Nigeria et accrédité dans 10 pays de l'Afrique de l'Ouest, élargissant ma focale, j'ai acquis une compréhension approfondie de la coopération internationale et de la diplomatie militaire. Ces deux missions m'ont permis de développer des compétences en négociation et en gestion des relations complexes.

Pendant la pandémie de Covid-19, j'ai suggéré d'appliquer des principes militaires pour proposer des solutions économiques et stratégiques, en comparant la lutte contre le virus à une guerre, nécessitant une stratégie rigoureuse et une adaptation rapide aux nouvelles menaces, permettant de tirer profit de la crise qui est à la fois risque et opportunité pour relancer nos économies.

Par ailleurs, à la prise de ma retraite, je fonde le cabinet de consultance stratégique "Best Practice", où j'applique les enseignements de la stratégie militaire aux entreprises et aux administrations. Je m'inspire notamment des enseignements de Sun Tzu ente autres stratèges, pour aider les organisations à contourner les difficultés et à transformer les défis en opportunités. En somme, Ma stratégie allie résilience, adaptabilité et coopération, qualités essentielles tant dans le domaine militaire que dans le monde des affaires.

La rédaction : Quels sont selon vous les principaux défis auxquels le cyberespace africain est confronté, et comment une approche stratégique peut-elle aider à les surmonter.

RTD Colonel : Le cyberespace africain fait face à plusieurs défis majeurs qui nécessitent une approche stratégique pour être surmontés. Entre les cyberattaques grandissantes, les

infrastructures très peu fournies voire inexistantes, et la cybergouvernance peu accrue, nous aurions tout à gagner en favorisant une approche cyber orientée stratégie dans le cyberespace africain. Approche capable de limiter les risques et appréhender les enjeux.

Bon nombre de citoyens, d'entreprises et même de gouvernements ne sont pas suffisamment informés des risques liés à la cybersécurité. Une voie de sortie serait la formation continue des experts et la sensibilisation des acteurs sur les bonnes pratiques en matière de cybersécurité. Aussi, l'Afrique est de plus en plus ciblée par des cybercriminels en raison de la faiblesse des mesures de sécurité. La création de centres de réponse aux incidents de cybersécurité et la coopération internationale pour lutter contre la cybercriminalité constitueraient une approche intéressante.

Les infrastructures technologiques en Afrique sont souvent obsolètes ou insuffisantes pour faire face aux cybermenaces modernes. Par conséquent, les réseaux gouvernementaux et les systèmes militaires, sont vulnérables aux cyberattaques. Une stratégie de cybersécurité avec des mesures de protection renforcées pour ces infrastructures, ainsi que des plans de réponse aux incidents doit être mise sur pied. Investir dans des infrastructures robustes et sécurisées est essentiel. Il serait intéressant d'inclure des partenariats public-privé pour financer et développer ces infrastructures.

De nombreux pays africains n'ont pas encore mis en place des cadres réglementaires solides pour la cybersécurité. Une stratégie nationale de cybersécurité, comprenant des lois et des régulations claires, est cruciale pour protéger les données et les systèmes critiques. La coopération internationale et l'innovation technologique devant être au cœur de la stratégie.

La rédaction : Pouvez-vous donner un ou deux exemples concrets où une approche stratégique intégrée a conduit à des résultats positifs

RTD Colonel : L'opération contre Boko Haram est un excellent cas de figure. Lors de ces opérations, j'étais commandant de la 41^{e} BRIM et commandant d'armes de la place de Kousséri entre 2004 et 2016. Mon approche alliait coordination Inter-Forces et Engagement communautaire.

Toutes les Forces de Défense et de Sécurité camerounaises confondues présentes dans le Logone et Chari (armées, police, gendarmerie, gardiens de prisons) ont été mobilisées dans une synergie face à Boko Haram. Plus tard, Les forces armées camerounaises ont travaillé en étroite collaboration avec les forces de sécurité nigérianes et tchadiennes, ainsi qu'au sein de la Force

Multinationale Mixte avec le Niger et le Bénin. Cette coordination a permis de partager des renseignements, de planifier des opérations conjointes et de maximiser l'efficacité des attaques contre les positions de Boko Haram. En impliquant les communautés locales à travers les comités de vigilance et en gagnant leur confiance par des Actions Civilo-Militaires (ACM), les forces armées ont pu obtenir des informations cruciales sur les activités de Boko Haram, ce qui a conduit à des opérations plus ciblées et efficaces. Cette approche intégrée a permis de réduire significativement l'influence de Boko Haram dans la région et d'améliorer la sécurité des populations locales.

La rédaction : Quelles sont les missions et les objectifs de votre structure Best Practice ?

RTD Colonel : Le cabinet **Best Practice**, que j'ai fondé après ma retraite, a pour mission primaire d'appliquer là où c'est possible, les principes et les stratégies militaires au monde des affaires et des organisations. Entre autres missions secondaires, nous visons :

- La consultance Stratégique (fournir des conseils stratégiques aux entreprises et aux organisations pour les aider à naviguer dans des environnements complexes et incertains. (VUCA) ; élaboration de plans stratégiques, la gestion de crise et l'optimisation des opérations.)

- La formation (Offrir des programmes de formation inspires des principes militaires pour développer les compétences en leadership, en gestion de crise et en stratégie.)

- La gestion du changement (Aider les organisations à gérer les transitions et les changements, en nous basant sur « la courbe et l'équation du changement » qui permet de vaincre les résistances.)

- La sécurité et la résilience (Conseiller sur les meilleures pratiques en matière de sécurité, y compris la cybersécurité, et aider les organisations à renforcer leur résilience face aux menaces et aux crises.)

Best Practice vise à transformer les défis en opportunités. C'est notre objectif principal. En appliquant des stratégies militaires éprouvées au monde des affaires, nous développons des leaders capables de naviguer dans le monde VUCA. Nos objectifs secondaires incluent amélioration de l'efficacité opérationnelle, le renforcement du leadership, la promotion d l'innovation ; ainsi que l'assurance d'une durabilité

La rédaction : Quelle est la plus-value que Best practice apporte aux organisations et gouvernements en matière de stratégie et de sécurité

RTD Colonel : Best Practice apporte une valeur ajoutée significative aux organisations et aux gouvernements en matière de stratégie et de sécurité grâce à cinq approches clés.

1. Approche Stratégique Militaire

Best Practice utilise des principes et des techniques militaires éprouvés pour aider les organisations à élaborer des stratégies robustes et adaptables. Cela inclut l'analyse de la situation (Évaluation approfondie des environnements internes et externes pour identifier les opportunités et les menaces) ; la planification stratégique (Développement de plans stratégiques détaillés qui tiennent compte des objectifs à long terme et des ressources disponibles.) ; et enfin la gestion des risques (Identification et atténuation des risques potentiels grâce à des stratégies proactives.)

2. Renforcement de la Sécurité

En matière de sécurité, Best Practice offre des solutions complètes pour protéger les actifs et les informations sensibles :

Cybersécurité : En collaboration avec LARC, mise en place de mesures de protection contre les cybermenaces, y compris la formation du personnel et l'implémentation de technologies de pointe ;

Sécurité Physique : Évaluation et amélioration des mesures de sécurité physique pour protéger les infrastructures critiques ;

Réponse aux Incidents : Développement de plans de réponse aux incidents pour minimiser les impacts des crises et assurer une reprise rapide des opérations.

3. Développement du Leadership

Best Practice forme les leaders à prendre des décisions stratégiques et à gérer des équipes dans des environnements complexes. Nous offrons notamment une formation en leadership ainsi que des coachings et mentorats.

4. Innovation et Adaptabilité

L'innovation est au cœur de l'approche de Best Practice, permettant aux organisations de rester compétitives et résilientes ; car comme le dit si bien Fokam Kamga Kammogne, « dans le métier de capitaine d'industrie, la recherche et l'innovation restent les seules forces du progrès et de l'existence » nous promouvons la pensée créative pour la résolution efficace des

problèmes. Nous développons également des stratégies flexibles qui permettent aux organisations de s'adapter rapidement aux changements de l'environnement.

5. Coopération et Partenariats

Best Practice favorise les partenariats et l'engagement communautaire entre les secteurs public et privé pour renforcer la sécurité et la résilience. Notre cabinet apporte modestement une approche intégrée et multidimensionnelle qui combine stratégie, sécurité, leadership, innovation et coopération pour aider les organisations et les gouvernements à atteindre leurs objectifs et à surmonter les défis complexes.

La rédaction : Comment envisagez-vous la collaboration entre les secteurs public et privé pour renforcer la sécurité dans le cyberespace.

RTD Colonel : La collaboration entre les secteurs public et privé est fondamentale pour renforcer la sécurité dans le cyberespace. Comment y parvenir ?

Par des partenariats Public-Privé (PPP)...

Les partenariats public-privé permettent de combiner les ressources et les expertises des deux secteurs pour développer des solutions de cybersécurité robustes. C'est dans ce cadre que l'Union européenne a mis en place le Partenariat Public-Privé européen pour la cybersécurité (cPPP), qui réunit des acteurs publics et privés pour travailler sur des projets de recherche et d'innovation en cybersécurité.

Via le partage d'Informations...

Le partage d'informations sur les menaces et les incidents de cybersécurité est crucial. Les gouvernements peuvent fournir des renseignements sur les cybermenaces émergentes, tandis que les entreprises peuvent partager des informations sur les attaques qu'elles subissent. Cela permet une réponse plus rapide et plus efficace aux cyberattaques.

Au moyen de la formation et de la sensibilisation...

Les deux secteurs peuvent collaborer pour développer des programmes de formation et de sensibilisation à la cybersécurité. Cela inclut la formation des employés, la sensibilisation du public et le développement de compétences en cybersécurité. Des initiatives conjointes peuvent être mises en place pour former les petites et moyennes entreprises (PME) aux meilleures pratiques en matière de cybersécurité.

Développement de Normes et de Régulations

Les gouvernements peuvent travailler avec le secteur privé pour élaborer des normes et des régulations en matière de cybersécurité. Cela implique la création de cadres réglementaires qui encouragent les entreprises à adopter des mesures de sécurité robustes et à se conformer aux meilleures pratiques.

Innovation et Recherche

Les partenariats public-privé peuvent également stimuler l'innovation en cybersécurité. En collaborant sur des projets de recherche et développement, les deux secteurs peuvent créer de nouvelles technologies et solutions pour protéger le cyberespace. Ainsi, des fonds publics peuvent être alloués à des projets de recherche menés par des entreprises privées.

Réponse aux Incidents

En cas de cyberattaque, une réponse coordonnée entre les secteurs public et privé est essentielle. Les gouvernements peuvent fournir un soutien logistique et des ressources, tandis que les entreprises peuvent apporter leur expertise technique pour contenir et résoudre l'incident.

Une collaboration étroite entre les secteurs public et privé permet de renforcer la résilience du cyberespace en combinant les forces et les ressources des deux secteurs. Cela conduit à une meilleure protection contre les cybermenaces et à une réponse plus efficace aux incidents de cybersécurité.

La rédaction : Comment voyez-vous l'évolution de la stratégie militaire face aux nouvelles menaces dans le cyberespace

RTD Colonel : Les forces armées intègrent de plus en plus le cyberespace dans leurs doctrines et stratégies globales. C'est pour cela que l'OTAN considère désormais le cyberespace comme le **cinquième domaine de guerre** aux côtés de la terre, de la mer, de l'air et de l'espace. Cela signifie que les opérations cybernétiques sont planifiées et exécutées en coordination avec les opérations traditionnelles.

Tout d'abord, les nations investissent dans le développement de capacités cybernétiques offensives et défensives. Les capacités offensives incluant des cyberattaques visant à perturber les réseaux ennemis, tandis que les capacités défensives impliquent la protection des

infrastructures critiques et la résilience face aux attaques. A cet effet, les États-Unis ont créé le Cyber-Command pour centraliser et renforcer leurs opérations cybernétiques.

Par ailleurs, la résilience est devenue un élément central des stratégies de cybersécurité. Les militaires travaillent à renforcer la résilience de leurs réseaux et systèmes pour assurer la continuité des opérations en cas d'attaque. Des mesures telles que la redondance des systèmes, la segmentation des réseaux et des exercices réguliers de simulation d'attaques sont prises.

De plus, la coopération internationale est essentielle pour faire face aux menaces cybernétiques qui ne respectent pas les frontières nationales. Les alliances, comme l'OTAN, et les partenariats bilatéraux jouent un rôle crucial dans le partage d'informations, la coordination des réponses aux incidents et le développement de normes communes.

Les stratégies militaires incluent également des efforts pour établir des normes internationales de comportement dans le cyberespace et pour dissuader les adversaires potentiels. La dissuasion peut inclure des menaces de représailles cybernétiques ou conventionnelles en réponse à des cyberattaques. L'innovation technologique enfin, est au cœur de l'évolution des stratégies militaires dans le cyberespace. Les avancées en intelligence artificielle, en apprentissage automatique et en cryptographie jouent un rôle crucial dans le développement de nouvelles capacités cybernétiques. Ces éléments sont des aux forces armées de mieux se préparer et de répondre aux menaces cybernétiques de manière efficace et coordonnée. Reste que l'Afrique n'est pas encore pleinement consciente de ces enjeux.

La rédaction : Quels conseils donneriez-vous aux jeunes professionnels qui souhaitent se lancer dans le domaine de la stratégie, en particulier en contexte africain ?

RTD Colonel : Aux jeunes professionnels souhaitant se lancer dans le domaine de la stratégie, en particulier dans le contexte africain, je leur prodigue ci-dessous quelques conseils clés :

Mettez l'accent sur votre formation !

L'éducation reste la base. Je vous conseillerais de suivre des études en gestion, économie, sciences politiques ou des domaines connexes. Les programmes de formation technique et professionnelle peuvent également offrir des compétences pratiques précieuses. Obtenir des certifications en gestion de projet, en analyse stratégique ou en cybersécurité peut renforcer votre profil.

Développez des compétences pratiques !

L'expérience pratique est inestimable. Faites des stages ou des emplois dans des entreprises ou des organisations où vous pouvez appliquer des concepts stratégiques. Le bénévolat et le volontariat sont des pistes que très peu de jeunes exploitent. Misez aussi sur des projets personnels ou communautaires pour développer vos compétences en gestion et en stratégie quelle qu'en soit la taille.

Élargissez votre réseau professionnel !

Participer à des conférences, ateliers et événements professionnels permet de rencontrer les experts du domaine. Le réseautage offre des opportunités de collaboration. Si possible, trouvez aussi un mentor expérimenté dans le domaine de la stratégie. Un mentor peut offrir des conseils précieux et vous aider à naviguer dans votre carrière.

Adaptez-vous au contexte Africain !

Il est nécessaire pour vous de comprendre les spécificités du marché africain, y compris ses défis et opportunités. Cela inclut bien-sur la connaissance des secteurs clés (agriculture, les technologies de l'information et de la communication (TIC), et les énergies renouvelables.) Vous devez par ailleurs vous familiariser avec les régulations locales pouvant affecter les stratégies d'entreprise. Tâchez d'être réceptif aux changements, le contexte africain peut être dynamique et imprévisible, et l'adaptabilité est une compétence clé.

Innovez, apprenez !

Soyez ouverts, l'Afrique est un terrain fertile pour les solutions innovantes, notamment dans les domaines de la fintech et des technologies mobiles. Gardez a l'esprit que la formation est une continuité. Lire des livres, des articles et des études de cas sur la stratégie et la gestion enrichira vos connaissances. Participer à des formations continues et à des programmes de développement professionnel vous maintient à jour des dernières tendances et pratiques en matière de stratégie.

Soignez votre image et votre social !

Bonne renommée vaut mieux que ceinture dorée nous dit l'adage. La réputation est l'arme fatale qui vous ouvrira toutes les portes. Travaillez sur des projets qui ont un impact social positif. Les stratégies qui prennent en compte le développement durable et l'inclusion sociale sont particulièrement pertinentes en Afrique. Collaborez avec les communautés locales pour comprendre leurs besoins et pourquoi pas proposer des solutions.

En gros il faut faire preuve d'audace, de beaucoup d'audace, ne plus valoriser tant la stabilité, mais avoir le goût de l'incertitude, de l'inconnu. C'est la voie royale pour s'en sortir.