Stratégie

Les conflits hybrides pour l'Armée suisse : Vers une défense multi-domaine dans le cadre d'une sécurité globale

Brigadier Hans-Jakob Reichen
Chef du Développement de l'Armée, Etat-major de l'Armée

Avec la publication de l'article « Future Warfare : The Rise of Hybrid Wars »[1] en 2005, le général James N. Mattis et Frank Hoffman déclenchent un débat conceptuel dans le monde occidental concernant le futur de la guerre et la dénomination hybride qui perdure jusqu'à aujourd'hui. Les auteurs décrivent les guerres du futur comme des combinaison d'actions conventionnelles, irrégulières contre des infrastructures critiques, cyber, et de campagnes de désinformation. Les phénomènes décrits ne sont pas nouveaux. L'histoire militaire offre de nombreux exemples de combinaisons d'opérations militaires combinant acteurs réguliers et irréguliers, opérations clandestines et subversion. L'utilisation du terme « hybride » s'est accélérée avec la guerre opposant la Russie et la Géorgie en 2008 et l'annexion de la Crimée en 2014, puis avec l'invasion de l'Ukraine en 2022, s'imposant dans le vocabulaire stratégique des Etats occidentaux. Dans cet article, il s'agit de décrire l'évolution de la compréhension de la menace hybride dans l'armée suisse, les défis pour y faire face et les conséquences pour son développement.

Le développement de la notion de conflits hybrides

Le rapport de politique de sécurité 2000 et la doctrine de l'Armée XXI introduisent l'engagement de sûreté sectorielle pour faire face à la violence de portée stratégique, mais au-dessous du seuil de la guerre, située entre l'appui aux autorités civiles et la défense. Dès son introduction, la mise en œuvre de ce nouveau concept pose le problème de la répartition des responsabilités entre l'armée et les organes civils ainsi que de la conduite au niveau militaire, tous les outils de la défense générale ayant été abandonnés. Les images des guerres en Afghanistan et en Irak renforcent l'impression qu'une situation nécessitant un engagement massif de l'armée en Suisse sans une menace militaire est hautement improbable.

Le rapport de politique de sécurité et le rapport sur l'armée 2010 renoncent au concept de la sûreté sectorielle et séparent clairement les tâches d'appui aux autorités civiles et de défense contre une agression militaire. L'armée s'oriente vers les engagements probables : appuis subsidiaires réels aux autorités civiles et engagements de promotion de la paix. La compétence de défense est à maintenir avec un système global qualitativement bon, quantitativement minimal. En conséquence, l'armée effectue d'une part des tâches de protection au profit des organes civiles dans un contexte de menace réduite et d'autre part maintient un savoir-faire contre une agression militaire peu claire.

En 2010, le brigadier Lätsch et le brigadier Moccand décrivent la menace hybride dans leur article « Moderne Verteidigung »,[2] qui remet en question la conception de l'adversaire pour le développement de la doctrine de la défense. Les auteurs proposent un adversaire ayant recours à des opérations psychologiques, à des mesures économiques, aux actions dans l'espace électromagnétique et cyber et aux forces spéciales, préalablement à un déploiement des forces au sol qui serait composé de troupes régulières et irrégulières, soutenues par des terroristes et des groupes criminels. Les auteurs ne remettent pas en question la séparation entre des engagements d'appui et la défense, notant que ces deux types d'engagement auraient lieu parallèlement et soulignent l'importance de la coopération civile-militaire.

En 2016 le terme de guerre hybride est pour la première fois évoqué dans un rapport de politique de sécurité. Les conflits armés y sont décrits comme une combinaison de moyens militaires, politiques, économiques et aussi criminels. Les forces régulières et irrégulières interagissent fortement, ces dernières agissant au profit d'un état tiers. Le rapport reconnaît qu'avec la guerre hybride, la probabilité que la Suisse soit impliquée dans un conflit armé a augmenté. Selon le rapport, l'armée peut, en cas de menace suffisamment intense et étendue, être engagée pour la défense, même si l'attaque n'est pas perpétrée par l'armée d'un état.

La conduite opérative et la conduite tactique 17 décrivent les acteurs étatiques et non-étatiques d'une menace dite multidimensionnelle et le déroulement possible d'un conflit interétatique. Le conflit hybride y est caractérisé par :

[1] Frank G. Hoffman et James N. Mattis, "Future Warfare: The Rise of Hybrid Wars", Proceedings, 2005.

[2] Daniel Lätsch et Daniel Moccand, „Moderne Verteidigung", Military Power Review, 2010.

- la combinaison de moyens non militaires, politiques, économiques, informels et humanitaires ;
- le recours à la force clandestine, irrégulière et armée par des acteurs étatiques ;
- les acteurs non étatiques sont en mesure d'agir dans tous les espaces et disposent de moyens et de modes d'action leur permettant de défier sérieusement les forces de sécurité étatiques ;
- le recours de manière ouverte aux forces militaires étatiques se produit en dernier recours.

Cependant le déroulement est encore décrit dans une optique linéaire paix – crise – conflit.

Dans le cadre du développement de l'armée (DEVA) en 2018, l'armée est réorganisée, le commandement des opérations est créé, permettant ainsi une cohérence au niveau opératif, les divisions territoriales assurant l'appui aux autorités civiles et les brigades mécanisées maintenant la compétence de défense. Si l'importance de la coopération civil-militaire est mise en évidence, celle-ci est attribuée au service territorial, qui est du ressort des divisions territoriales. Ainsi le fossé doctrinal entre les troupes dédiées à l'appui aux autorités civiles et celles dédiées à la défense se creuse et la problématique du passage entre les deux types d'engagement n'est pas résolue. Les divisions territoriales se concentrent sur les engagements subsidiaires effectifs et les brigades mécanisées s'entraînent sans vraiment intégrer le besoin de coordination du plateau territorial. Au niveau stratégique le cas d'une menace existentielle pour le pays n'est pas étudié en détail. Dans l'instruction, les actions infra-guerrières sont principalement considérées comme un prélude à une attaque au sol par des moyens conventionnels.

Le rapport de politique de sécurité 2021 se penche de façon plus intensive sur les conflits hybrides, sans cependant en donner une définition. Il constate une augmentation des menaces dans l'espace cyber et de l'information et note l'engagement probable et supplémentaire d'armes de longue distance et de forces spéciales en cas de conflit. Le rapport indique que face aux attaques hybrides, la dissuasion militaire doit être complétée par des instruments civils et un renforcement de la résilience. La pandémie qui éclate en 2020 et l'invasion russe de l'Ukraine en 2022 met au grand jour les vulnérabilités de la Suisse face aux dangers et aux menaces de portée stratégique.

La Stratégie de politique de sécurité 2026 consacre l'évolution de la menace hybride et propose la « Sécurité globale » pour y faire face. Trois axes y sont proposés : renforcer la résilience, augmenter la protection et améliorer la capacité de défense. Les conflits hybrides sont définis comme une *« combinaison de moyens déployés par un agresseur étatique dans le but de déstabiliser un autre Etat, de nuire au fonctionnement de ses institutions ou de le soumettre à sa volonté. »*

Avec la publication de ses lignes directrice pour la défense en juin 2026, le Conseil fédéral indique de quelle manière l'Armée suisse doit se renforcer et se réorienter pour rester un élément efficace dans le cadre de la sécurité globale. La priorité est de pouvoir justement parer les actions hybrides et les attaques à distance tout en adaptant et développant les capacités à mener le combat dans le cadre d'une attaque militaire d'envergure. Comprendre les mécanismes d'un conflit hybride et les implications de la stratégie de la sécurité globale constitue dès lors une condition indispensable pour la transformation nécessaire de la doctrine, de la disponibilité, de la capacité à durer et des structures de conduite.

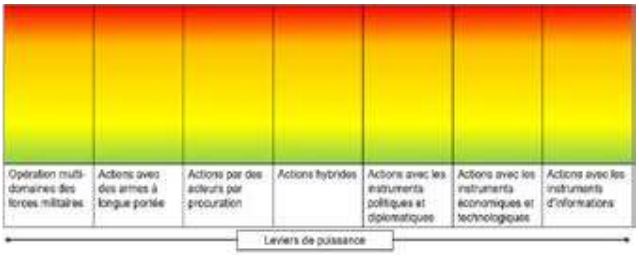
Comprendre le conflit hybride pour l'armée suisse

Si l'armée dispose de bases théoriques au sujet de la menace hybride dans sa doctrine militaire 17, exprimée au travers des règlements de conduite 17, il s'agit dans une première étape d'adapter et de compléter la doctrine concernant les conflits hybrides mais également de comprendre les vulnérabilités de la Suisse face aux actions hybrides.

Les modalités de la concurrence entre Etats a changé. La distinction entre paix, crise et guerre s'est estompée au profit d'un continuum allant de la compétition économique et politique au conflit armé. La force armée conventionnelle ou irrégulière n'est pas l'unique instrument de la puissance pouvant influencer le comportement d'un autre Etat. Un état dispose d'une palette de leviers possibles :

- avec les instruments d'informations ;
- avec les instruments économiques et technologiques ;
- avec les instruments politiques et diplomatiques ;
- au moyen d'actions hybrides ;
- par des acteurs par procuration ;
- avec des armes à longue portée ;
- au moyen d'opérations multi-domaines avec les forces militaires ;
- au moyen d'armes nucléaires.

L'élément central réside moins dans l'utilisation individuelle des leviers que dans leur coordination et leurs effets qui se renforcent mutuellement. Chaque lévier profite des développements technologiques exponentiels de ces dernières années. Le développement technologique dans le domaine numérique a cependant augmenté la dépendance des forces armées envers des fournisseurs globaux. Les actions d'information et surtout de désinformation sont l'accélérateur dans cette palette de leviers, utilisant toutes les possibilités technologiques existantes (connectivité mondiale, réseaux sociaux, intelligence artificielle). Cela permet d'agir à grande vitesse, à large échelle et avec une attribution souvent difficile.



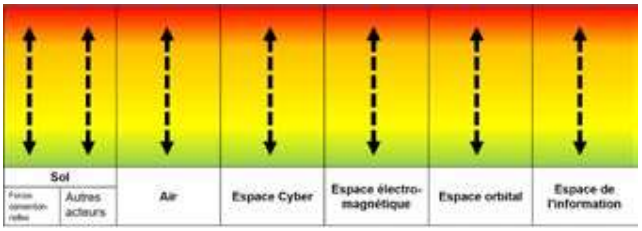
Leviers de puissance.

L'adversaire peut envenimer la concurrence horizontalement en utilisant plus de leviers ou verticalement en élevant le niveau de pression, voire de violence d'un ou plusieurs leviers, tout en maintenant un niveau d'ambiguïté suffisant pour empêcher une attribution claire et compliquer ainsi notre réponse. C'est dans cette zone grise que les adversaires des démocraties développent leur champ d'action aujourd'hui. La concurrence n'est pas linéaire dans le temps, elle ne se dirige pas nécessairement vers une opération militaire. Le temps est utilisé pour user les démocraties et leurs dirigeants habitués aux actions de courte durée. Les actions dans la zone grise peuvent se prolonger pendant des années, car l'objectif n'est pas de vaincre rapidement dans une opération multi-domaine, mais de réduire progressivement notre capacité d'action

en affaiblissant la capacité de décision, la confiance dans nos institutions, la cohésion sociale et en créant un climat d'incertitude favorable aux intérêts de l'agresseur. La concurrence entre états est une continuité où s'entremêlent pressions diplomatiques, coercition économique, cyberattaques, campagnes de désinformation, espionnage, démonstrations de puissance militaire et de menaces implicites de l'utilisation de la force militaire.

Les actions hybrides sont les actions qui utilisent la violence dans les différents espaces ou environnements (air, sol, mer, espace, cyber, électro-magnétique, information), mais dont l'auteur ne peut pas être clairement défini. Les auteurs sont donc des acteurs aussi bien étatiques, que non-étatiques, qui agissent de manière clandestine, irrégulière ou non-conventionnelle. L'éventail d'acteurs va des services de renseignement, aux forces spéciales, aux groupes potentiellement violents ou armés, aux organisations criminelles en passant par les entreprises privées militaires et de sécurité, voire des groupes qui sont instrumentalisés. Les groupes non-étatiques peuvent disposer de matériel ou utiliser des modes d'action auparavant réservées aux forces militaires.

Le spectre d'acteurs et leurs capacités font que le degré de menace ou de violence, n'est pas nécessairement équivalent dans les différents espaces. Il est possible que l'état de conflit soit déjà atteint dans l'espace cyber, alors sans l'être dans les airs. Cette situation, couplée avec l'utilisation des leviers diplomatiques / politiques et économique / technologique rend encore plus difficile la décision de se référer à un cas de défense selon le droit international.



Différenciation du degré de menace/ puissance dans les différents espaces.

La Suisse présente plusieurs vulnérabilités face aux actions hybrides. Notre société est ouverte, libérale et interconnectée. Nos services financiers et notre industrie constituent des objectifs privilégiés pour l'espionnage et dépendent d'un accès à l'énergie et aux chaînes logistiques mondiales. Le fonctionnement de notre pays est, lui, dépendant des infrastructures critiques, qui elles-mêmes reposent sur des systèmes numériques. Une partie de nos infrastructures critiques contribuent également au fonctionnement des nations européennes, devenant ainsi potentiellement des cibles pour un agresseur. Finalement, la présence de nombreuses organisations internationales, de sièges d'entreprises multinationales et d'institutions financières fait du territoire suisse un espace stratégique où s'exercent la concurrence entre Etats.

Les conséquences pour le développement de l'armée

Depuis plus de vingt ans, l'interprétation de l'évolution des conflits et les conséquences pour le développement de l'armée ont maintenu une séparation organisationnelle et doctrinale entre les appuis aux autorités civiles et le cas de défense. Qu'un engagement de l'armée soit subsidiaire ou primaire est uniquement une question politique et juridique. Les cyberattaques, les actes de sabotage, l'espionnage, les violations de l'espace aérien et les activités d'influence originaires de Russie s'intensifient en Europe et touchent déjà la Suisse. La menace représentent les actions hybrides et à distance n'est pas seulement probable, mais aussi extrêmement dangereuse pour notre population, notre société et pour notre pôle économique. Pour la Suisse, l'enjeu ne consiste donc plus seulement à disposer d'une Armée sachant défendre le territoire en cas d'agression militaire conventionnelle, mais de développer cette sécurité globale, dans laquelle l'armée contribue à protéger le pays, sa population et les infrastructures critiques face aux menaces hybrides et à distance. Pour l'Armée suisse, cette approche implique une évolution doctrinale importante, axée sur l'unité de la conduite, une conduite des opérations multi-domaines, un renforcement de sa capacité à agir avec l'ensemble des acteurs et une augmentation de sa résilience propre. L'armée doit pouvoir faire face de manière flexible à cette continuité de la menace et rompre avec la distinction marquée entre les engagements d'appui et les engagements de défense. La création des divisions d'engagement, assurant l'ensemble des engagements dans son secteur, est un pas décisif dans cette direction.

L'armée doit augmenter sa propre résilience, le meilleur antidote face aux actions hybrides, dont elle sera également la cible. Cela passe par militaires informés, des infrastructures et des réseaux robustes, une conduite capable d'assurer la continuité de l'action et une troupe entraînée, capable d'agir de manière autonome dans le cadre de l'intention. La résilience est un facteur de dissuasion : un adversaire est moins enclin à mener des actions hybrides contre une organisation capable d'en absorber les effets.

Dans le cadre des opérations multi-domaines, il s'agit d'orchestrer les activités militaires dans tous les domaines opérationnelles et l'ensemble des environnements, de les synchroniser avec les activités civiles pour créer des effets convergents, aussi rapidement que la situation l'exige. En effet il ne s'agit plus seulement de gérer la coopération avec les acteurs civils, mais de penser l'engagement dès sa conception dans un contexte civil-militaire. Cette coopération doit être particulièrement étroite dans l'espace cyber et de l'information, car il y est impossible de tracer des limites de secteurs. La coopération civile-militaire n'inclut plus seulement la coopération avec les polices cantonales ou l'office fédéral de la douane et de la sécurité des frontières, mais avec l'ensemble des acteurs pertinents.

Il est également nécessaire de repenser les modalités de la coopération internationale afin de protéger la Suisse et sa population car les actions cybernétiques, les campagnes informationnelles ou les réseaux d'espionnage ne s'arrêtent pas aux frontières nationales.

La révision de la doctrine, les changements structurels et les investissements dans les nouveaux systèmes sont indispensables, mais ils ne suffiront pas. Le véritable défi est d'abord d'ordre culturel. Il consiste à dépasser une vision sectorielle d'appui ou de défense de l'engagement de l'armée pour adopter une approche globale où la dimension militaire est intégrée dans un ensemble cohérent.

H.-J. R.