Intelligence College in Europe
Collège du Renseignement en Europe

Webinaire : défis pour la sécurité européenne

Résumé de conclusions – Mars 2021

En raison de la situation sanitaire en cours depuis mars 2020, le Collège de renseignement en Europe a dû remettre en question les méthodes traditionnelles d'échange et de réflexion et trouver de nouvelles modalités de dialogue.

Avec le soutien du Comité de pilotage, trois pays membres (Italie, Roumanie et Finlande) ont proposé un séminaire sous le format d'un webinaire interactif dédié aux nouveaux défis de la sécurité européenne pour les services de renseignement.

Ce webinaire a abordé trois sujets, identifiés comme des défis communs pour tous les membres :

- **L'impact des technologies numériques sur la sécurité nationale, sur la base des travaux menés par le Dr Donatella Sciuto et le Dr Stefano Zanero du *Dipartimento di Elettronica, Informazione e Bioingegneria* du *Politecnico* de Milan, en Italie. Les évolutions dans ce domaine exigent que nos pays s'adaptent rapidement afin de rester dans cette « course à l'innovation ».**
- **Propagande, désinformation, opérations secrètes d'information, en référence aux travaux du Dr Cristina Ivan de l'Académie nationale de renseignement *Mihai Viteazul*. Ces concepts, loin d'être purement théoriques, posent des questions sur le rôle des services de renseignement, leur perception au sein de nos sociétés, de même que leur dialogue avec nos décideurs nationaux et européens, ainsi qu'avec la société civile.**
- **La guerre hybride, basée sur un rapport universitaire finlandais. Bien que ce phénomène ne soit pas nouveau, son utilisation se développe rapidement dans un monde marqué par la réduction des conflits « conventionnels », grâce aux développements technologiques.**

Plusieurs pays membres du Collège ont contribué à ce webinaire en partageant leurs points de vue nationaux et leur analyse stratégique des sujets abordés avec les membres. Leur participation a nourri la discussion, apportant des points de vue marqués par les prismes spécifiques d'analyse de la menace inhérents à chaque pays. En ce sens, ce webinaire a été l'occasion de s'interroger collectivement sur les lectures parfois divergentes des menaces, afin que chaque membre puisse mieux comprendre ses homologues européens. Cette publication est une synthèse de ces échanges.

Il convient de remercier tous ceux qui ont participé activement à la réussite de ce premier webinaire. Ce succès et les discussions fructueuses autour de ces trois sujets ouvrent la voie à de nouveaux échanges au sein du Collège. Ces thématiques, qui s'inscrivent dans le thème de la présidence britannique en 2021 (*Fusing intelligence and policy to build resilience in the 21st century*), seront très probablement abordés à nouveau, et complétés par d'autres, sur lesquels les membres pourront à nouveau confronter leurs points de vue et renforcer leur compréhension stratégique mutuelle.

L'impact des technologies numériques sur la sécurité nationale

Les technologies numériques, déclinées à différents niveaux (espace, informatique quantique, intelligence artificielle (IA), *machine learning*[1] (ML)) redéfinissent le paysage de la sécurité nationale et créent de nouveaux angles d'attaque potentiels. Elles ont un impact profond sur les équilibres économiques et sociaux et posent des questions en termes de droit. Elles ont donné naissance à une société hyperconnectée qui va s'intensifier avec le déploiement de la 5G et des nouvelles constellations de satellites.

L'évolution de leur impact se caractérise par les aspects suivants:

- Les progrès technologiques permettront à un plus grand nombre d'acteurs d'acquérir des capacités sophistiquées qui n'étaient auparavant accessibles qu'aux États disposant de ressources importantes. Le secteur civil, suivant les logiques de marché, est devenu le moteur en matière de technologie et peut aujourd'hui disposer de plus de ressources.
- Les technologies numériques peuvent remodeler la relation entre le capital et le travail dans les économies mondiales, ainsi que les relations entre ces économies.
- Si elles fournissent de nouveaux outils aux services de renseignement, elles créent également de nouvelles menaces. L'IA et le ML peuvent être utilisés par la communauté du renseignement pour aider à établir des faits, mais ils fournissent également aux adversaires les moyens de créer et de diffuser de fausses informations convaincantes. Le ML est également susceptible de faire l'objet d'attaques adverses. Dans de nombreux organes de renseignement et de défense, un adversaire compétent pourrait avoir la volonté et la capacité d'attaquer les systèmes, soit en infectant les données, soit en les modifiant soigneusement pour biaiser l'analyse.
- Même si les individus exposent certaines informations relevant de leur vie privée sur Internet, la société devient paradoxalement de plus en plus sensible à la question du partage des données personnelles. Par conséquent, le concept de *privacy par design* selon lequel chaque information traitée doit proposer un haut niveau de protection des données personnelles est devenu prépondérant. Ainsi, la question principale émerge : l'accès à des données claires. En effet, la donnée, en tant que source pour les services de renseignement, va se développer à grande vitesse mais il sera de plus en plus difficile d'y déceler la donnée pertinente déchiffrée.

Ce changement de donne peut-il générer une redistribution du pouvoir militaire au niveau international ? Il convient de noter que si la sphère militaire a été un moteur essentiel au niveau technologique sur le plan pratique, les innovations profondes résultent toujours du domaine civil sur le plan plus stratégique. En outre, si l'IA est effectivement aujourd'hui utilisée dans la lutte informatique offensive (LIO) comme défensive (LID), les technologies en œuvre sont encore très modestes et ne répondront pas avant longtemps à une telle prévision.

En conclusion, de l'avis de tous, ce changement de paradigme qui diminue le contrôle des Etats sur la technologie, son développement, son exportation et son exploitation, exige de la communauté du renseignement qu'elle devienne plus agile et innovante pour faire face à un monde de plus en plus volatile. Mais comme le souligne un chercheur : qu'y a-t-il de nouveau dans le fait que la communauté du renseignement doive s'adapter aux nouvelles technologies? Cela implique notamment la nécessité d'une souveraineté européenne en matière de technologies numériques mais aussi d'une légitimation, par la loi, de l'action des services de renseignement, en particulier en matière d'accès aux données.

[1] Ou apprentissage automatique

Propagande, désinformation, opérations informationnelles secrètes

La propagande, la désinformation et les opérations informationnelles « secrètes » ont fait l'objet d'une attention accrue ces dernières années en Occident, tant de la part des institutions chargées de la sécurité que de la société en général. Dans le domaine de l'ingérence informationnelle, on peut distinguer trois niveaux de manipulation de l'information. Ils vont de l'offensive classique de propagande politique et diplomatique, souvent approuvée au plus haut niveau de l'État, aux opérations secrètes d'information et à la guerre hybride. Entre les deux, il existe un large éventail de techniques de désinformation. Il peut s'agir aussi bien de relayer et amplifier des faits d'actualité afin de donner plus d'écho au narratif étatique préalablement défini, contribuant ainsi à renforcer sa crédibilité, que d'actions et de messages concertés visant à perturber, à instiller la méfiance et à retourner la population d'un État ennemi contre ses propres autorités gouvernementales.

La propagande est une manipulation intensive de l'information pour influencer les perceptions et la capacité du public cible à prendre des décisions objectives. Elle n'exclut pas les faits, mais elle les présente de manière arrangeante et parfois déformée afin de pouvoir persuader à tout prix. L'objectif est d'obtenir des avantages stratégiques, du capital politique, voire des gains financiers, ou simplement de redorer l'image d'un dirigeant. Elle doit être perçue comme un appel à la rationalité ou comme une information qui offre une nouvelle perspective sur un problème donné. Elle fait souvent appel à un lourd bagage émotionnel qui écarte la compréhension rationnelle des faits.

La désinformation désigne toute une série de tactiques et de stratégies utilisées pour propager des informations fausses, inexactes ou hors contexte qui ont été détournées de leur réelle signification. Son intention est de provoquer des dommages et des profits et elle peut affecter gravement les processus démocratiques, la sécurité nationale et la cohésion sociale. Si la propagande est accomplie par l'intermédiaire d'institutions étatiques dont les liens sont théoriquement facilement traçables, les opérations de désinformation demandent beaucoup d'efforts pour en découvrir les sources initiales. La désinformation représente une forme de propagande dont l'objectif principal reste illégal et clandestin.

Une opération informationnelle secrète peut être définie comme l'ensemble des actions secrètes ou semi-secrètes qui rendent la désinformation possible et renforcent son efficacité. Elles comprennent une utilisation systématique et concertée de techniques telles que la contrefaçon de documents, la falsification de preuves, la manipulation de faits et la comptabilisation erronée d'événements. Les mécanismes de type *bots* ou *trolls* génèrent et reproduisent des théories du complot qui sapent la crédibilité et la légitimité de la cible.

Les opérations de désinformation dans le contexte de la pandémie COVID-19

De nos jours, les menaces générées par la propagande et la désinformation sont rendues efficaces en exploitant les vulnérabilités systémiques de nos écosystèmes numériques, le volume massif d'informations et la possibilité d'utiliser des algorithmes pour en assurer la diffusion. La pandémie de COVID-19 est un exemple de ce phénomène.

L'Organisation Mondiale de la Santé a attiré l'attention, dès le mois de mars, sur le fait que les fausses informations relatives à la COVID-19 « se propagent plus vite que le virus lui-même » et a qualifié ce phénomène « d'infodémie de niveau planétaire ». Ainsi, entre le 22 janvier et le 25 mars, la base de données EU vs. Disinfo a comptabilisé pas moins de 39 cas de *fake news* qui attribuaient l'origine du coronavirus aux États-Unis, et 24 autres qui soutenaient la théorie du complot selon laquelle la COVID-19 aurait été utilisée comme arme biologique contre la Chine et son économie. Autre fait marquant, entre le 22 janvier et le 1er avril 2020, la base de données publique Eu vs Disinfo a collecté pas moins de 150 exemples de *fake news* pro-Kremlin axées sur la pandémie de Covid-19. L'une des théories les plus diffusées est celle de l'inexistence réelle de la pandémie qui serait un canular visant à faire avancer un

agenda occulte pour contrôler la population mondiale. De prétendus entretiens de « scientifiques et experts réputés » sont utilisés pour désinformer sur la gravité de la maladie, en faisant circuler de fausses données sur l'impact de la pandémie et en offrant des « conseils médicaux » qui sont en contradiction directe avec l'expertise médicale. Cela démontre le caractère mondial de l'*infodémie*, les récits étant diffusés et adaptés en fonction du public cible local.

Depuis lors, le public a été sensibilisé et les gouvernements, les institutions de santé et de sécurité, ainsi que les organisations internationales ont activement contribué à fournir des sources d'information fiables et à dénoncer la nature factice des récits de désinformation.

Comment faire face à ces phénomènes ?
Les mesures sécuritaires ont toujours été placées au premier plan. Cependant, les institutions publiques doivent également devenir proactives en renforçant la résistance des communautés à la propagande, en consolidant la confiance et l'implication dans le débat démocratique, ainsi que l'éducation à long terme à la pensée critique, à la culture numérique et au débat rationnel. Cela nécessite une approche transverse, en direction de l'ensemble de la société.
Pour contrer la désinformation, il faut agir sur deux niveaux :

- celui du message : exposer l'erreur de logique, vérifier les faits, les chiffres, etc ;
- celui de la source : exposer la véritable source, sensibiliser le public au modus operandi de la désinformation.

A cette fin, plusieurs actions peuvent être menées par les Etats :

- Exposer les opérations d'information et leur modus operandi par le biais des médias, des organisations de la société civile chargées de la veille de la pratique démocratique, de la recherche universitaire, etc. ;
- Promouvoir l'utilisation d'organisations fiables de vérification des faits ;
- Encourager l'utilisation de plugins qui rendent la vérification des faits disponible à l'échelle mondiale ;
- Impliquer les plateformes de médias sociaux et les entreprises de la Tech pour qu'elles prennent des mesures cohérentes afin d'identifier et d'interdire en temps utile les comptes qui diffusent de la désinformation[2] ;
- Donner aux citoyens les moyens de comprendre, de vérifier et de contribuer au mouvement populaire de lutte contre la propagande et la désinformation.

Les communautés du renseignement, en particulier, doivent reconsidérer leur rôle, consolider le dialogue et l'engagement avec les décideurs et le grand public, promouvoir activement un ensemble de valeurs partagées et une culture de sécurité commune et, enfin et surtout, être toujours prêtes à s'impliquer dans un débat fondé sur des faits, rationnel et cohérent.

Il faut garder à l'esprit qu'il n'est pas illégal de dire ou de publier des absurdités. C'est un droit constitutionnel pour chaque citoyen. Cela ne devient dangereux que si cela fait partie d'une opération d'information. Cela pose le problème de la distinction entre la liberté d'expression et une attaque d'information malveillante. Outre les actions mentionnées, les communautés du renseignement peuvent essayer d'utiliser la technologie pour attribuer un message à sa source (de manière anonyme).

[2] Le Code européen de bonnes pratiques contre la désinformation a été adopté, en octobre 2018, suite à une communication de la Commission européenne intitulée « *Lutter contre la désinformation en ligne »: une approche européenne »* (avril 2018). Différentes sociétés et associations ont adhéré au Code en reconnaissant ainsi leur rôle dans la lutte contre la désinformation. Il en va particulièrement ainsi pour Google, Facebook, Twitter, Microsoft, Mozilla et, depuis juin 2020, TikTok.

La Guerre Hybride – une très courte introduction

La guerre hybride, menée contre des pays européens, poserait un défi de taille à l'Europe. Le terme « menaces hybrides » a lui-même suscité scepticisme et réticence chez certains acteurs de la défense et de la sécurité nationale. Son utilisation massive dans les débats de l'UE et de l'OTAN en a fait un concept vague, fourre-tout et sans substance.

Dans ce contexte, il est nécessaire de bien définir cette notion. Les critères permettant de parler de guerre hybride peuvent être résumés ainsi :

- Une menace hybride se caractérise par le recours par un acteur hostile étranger, étatique ou non, à une combinaison intégrée de modes opératoires volontairement ambigus et asymétriques à des fins offensives de perturbation, d'intimidation ou de déstabilisation pouvant entraîner dans la durée une fragilisation des Etats et des sociétés.
- Cette notion fait référence à une stratégie globale d'engagement de la part d'acteurs hostiles ayant atteint un haut niveau d'intégration, aux échelons politique et stratégique, de leurs appareils civils, militaires et de renseignement. Cette stratégie globale se compose d'un ensemble d'actions de niveau tactique et/ou stratégique combinant des moyens variés (militaires ou non, conventionnels ou non, etc.), éventuellement en concomitance avec le recours ou la menace de recours à la force. Ces actions, tout en restant en deçà du seuil d'agression armée ou du seuil de déclenchement de l'article 5 du traité de l'Atlantique Nord ainsi que de l'article 42.7 du TUE, visent à intimider ou déstabiliser l'adversaire en réduisant ses capacités d'attribution et de riposte, pouvant aller jusqu'à les paralyser.
- De la terreur, du sabotage et de la subversion à la guérilla, à la guerre conventionnelle et même au domaine nucléaire, tous les niveaux d'escalade possibles peuvent être inclus ou même combinés.
- Bien que la guerre hybride ait des implications au niveau opérationnel et tactique, elle est principalement de nature stratégique, utilisant des centres de gravité multiples et changeant de manière flexible et dynamique.
- La guerre hybride peut commencer bien avant le début du conflit ouvert, et dans un cas extrême, elle offre même la possibilité de gagner une guerre malgré la défaite militaire. Il peut être perçu comme « l'art de créer du pouvoir ».
- Elle empêche une réponse rapide et unifiée de la part de l'adversaire ou de la communauté internationale, créant une ambiguïté dans les interfaces suivantes :
    - Entre guerre et paix : opérer dans une « zone grise », afin de brouiller les lignes traditionnelles d'ordre et de responsabilités et de contribuer à leur dissolution ultérieure.
    - Entre ami et ennemi : les actions ne peuvent leur être clairement attribuées en temps voulu.
    - Entre conflits intra-étatiques et interétatiques et donc entre sécurité intérieure et sécurité extérieure, impliquant des acteurs étatiques, non étatiques et pseudo-étatiques.

Cela dit, la guerre hybride n'est pas un phénomène nouveau. Elle a existé tout au long de l'histoire de la guerre et ne représente donc pas fondamentalement un « défi nouveau ». Le concept a été largement abordé par exemple par Sun Tzu, les stratèges byzantins, Clausewitz ou plus récemment par le général A. Beaufre ou le théoricien militaire D. Galula. Pour prendre des exemples récents, la confrontation « sous le seuil » avec l'Iran dans les années 1980 et l'intervention en Côte d'Ivoire en 2004 face à des *proxies* constituent des exemples de guerre hybride Le recours à la ruse et au subterfuge est une constante de la stratégie militaire même si un chercheur note que « la guerre est rarement déclarée de nos jours comme au bon vieux temps ».

La surprise stratégique de l'annexion de la Crimée, ainsi que l'éclatement du conflit dans le Donbass, ont donné à la guerre hybride une apparence de nouveauté, tout en se concentrant presque exclusivement sur la menace russe, cependant, d'autres pays, notamment l'Iran, et des acteurs non-étatiques (Hezbollah, Daech) peuvent également utiliser de telles stratégies. Le véritable changement de donne réside dans les nouvelles vulnérabilités auxquelles nous sommes confrontés :

- La mondialisation, l'étroite interaction internationale, les vulnérabilités internes des sociétés démocratiques et leurs clivages socio-économiques et culturels et les sociétés interconnectées ont le potentiel d'ouvrir des champs supplémentaires pour des méthodes de guerre hybride.
- L'évolution de notre environnement stratégique favorise une augmentation des confrontations en deçà du seuil de conflit ouvert. Les clivages au sein des sociétés européennes, par exemple, grandissent et s'approfondissent.
- La désintégration des instruments multilatéraux et le retour à des politiques de pouvoir décomplexées et désinhibées encouragent cette tendance.
- D'un point de vue militaire, et en particulier en ce qui concerne la question des cyberattaques, l'hybridité en tant que nouveau paradigme pour comprendre la réalité plurielle de la cyber-conflictualité est cohérente avec la réalité du « cyber-champ ».

Comment relever ce défi ? La prise de conscience est la première condition préalable. Il est important de reconnaître les conflits hybrides à un stade précoce et d'empêcher la transition vers une phase agressive à grande échelle.

Lutter efficacement et à long terme contre la guerre hybride nécessite beaucoup plus de forces, de ressources et d'efforts que les opérations hybrides offensives. Outre les mesures à long terme pour renforcer la résilience, la capacité à effectuer en permanence des analyses approfondies de situations de guerre / conflit spécifiques, d'acteurs et de stratégies connexes deviendra une compétence clé pour contrer et répondre aux méthodes de guerre hybride.
Cela comprend une approche transverse pouvant se déployer sur l'ensemble du spectre d'action de l'Etat et de la société, ainsi qu'une coopération et une coordination internationales, en particulier entre l'UE et l'OTAN.

C'est la raison pour laquelle des stratégies sont développées au niveau national (Revue stratégique de défense et de sécurité nationale de 2017 ou loi estonienne sur la défense nationale).

En outre, l'identification des menaces hybrides est une priorité stratégique pour la coopération UE-OTAN, comme indiqué dans les déclarations conjointes de Varsovie et de Bruxelles (2016, 2018).