diploweb.com La revue géopolitique
ISSN : 2111-4307

Podcast et synthèse rédigée

# Planisphère. La géopolitique résiste-t-elle au cyber ? Avec F. Manet

jeudi 6 mars 2025,par Emilie BOURGOIN, Florian MANET, Pierre VERLUISE

**Citer cet article / To cite this version :**
Emilie BOURGOIN, Florian MANET, Pierre VERLUISE, **Planisphère. La géopolitique résiste-t-elle au cyber ? Avec F. Manet**, *Diploweb.com : la revue géopolitique, 6 mars 2025.*

**La géopolitique résiste-t-elle au cyber ? Le cyber, est-ce virtuel, immatériel ou matériel ? De quelles façons la couche matérielle du cyber est-elle un champ d'affrontement géopolitique entre acteurs étatiques mais aussi non étatiques ? Pourquoi la couche logicielle du cyber est-elle l'enjeu de l'expression des rivalités de puissance étatique comme non étatique ? Comment pouvons-nous comprendre la géopolitique des infrastructures numériques ? Dans le cyber, l'État est-il un acteur disqualifié ? Pour répondre, nous avons l'honneur de recevoir Florian Manet.**

**Cette émission, Planisphère, La géopolitique résiste-t-elle au cyber ? Avec F. Manet, sur RND**

La page pour récupérer les codes afin d'intégrer cette émission sur votre site académique ou institutionnel.

**Cette émission, Planisphère, La géopolitique résiste-t-elle au cyber ? Avec F. Manet, sur RCF**

Lien direct vers cette émission sur RCF, avec possibilité de récupérer l'iframe

**Planisphère, sur Spotify**

**Synthèse de cette émission, Planisphère, La géopolitique résiste-t-elle au cyber ? Avec F. Manet, rédigée par Émilie Bourgoin pour *Diploweb.com*. Revue et validée par F. Manet**

Dans un monde de plus en plus connecté, la dimension géopolitique du cyberespace soulève de nombreuses interrogations [1]. Le cyber, souvent essentiellement perçu comme un domaine immatériel, prend de plus en plus d'importance dans les enjeux de pouvoir entre États et entre acteurs privés. Le colonel Florian Manet met en lumière les aspects matériels et les confrontations géopolitiques qui se jouent dans cet espace numérique. La question centrale est alors de savoir si l'organisation géopolitique traditionnelle peut encore résister à la montée en puissance des menaces cyber, ou si elle est irrémédiablement transformée par cette nouvelle dimension.

**Florian Manet**

Florian Manet publie « *Thalassopolitique du narcotrafic international, la face cachée de la mondialisation ?* » aux éditions EMS. Il s'exprime à titre personnel. Crédit photographique : Pierre Verluise
*Verluise/Diploweb.com*

## La dimension matérielle du cyber

Contrairement à une idée répandue, le cyber n'est pas un espace purement immatériel. Il repose sur une infrastructure physique complexe, composée de câbles sous-marins, de *data centers* et d'une multitude d'objets connectés. Avec environ 1,2 million de kilomètres de fibres optiques sillonnant les océans, ces installations matérielles constituent la colonne vertébrale des échanges de données mondiaux. Florian Manet souligne l'importance de ces infrastructures, qui sont devenues des cibles potentielles d'actes malveillants. Le cyber, bien que virtuel dans ses effets, repose sur une base matérielle concrète, indispensable au bon fonctionnement des sociétés modernes.

## Les attaques sous-marines : Nord Stream 2 en 2022 brisent un accord tacite

L'exemple le plus frappant de l'importance stratégique des infrastructures sous-marines est l'attaque sur le gazoduc Nord Stream 2 en septembre 2022 [2]. Cet incident a mis en lumière la vulnérabilité des installations *offshore*, qu'il s'agisse de gazoducs ou de câbles de communication. Le milieu marin comme l'éloignement des côtes n'est plus guère une protection. **L'attaque a brisé un accord tacite selon lequel ces infrastructures restaient à l'abri des agressions**. Le précédent créé par cet acte impose une révision des stratégies de protection des infrastructures critiques sous-marines, qui sont devenues des enjeux géopolitiques de premier plan. La protection de ces installations est désormais une priorité pour les États et les alliances comme l'OTAN.

Avec l'introduction massive des drones dans les conflits, notamment en Ukraine, la guerre prend une nouvelle forme, où les barrières géographiques sont facilement contournées. Les drones terrestres, aériens et marins peuvent être utilisés pour saturer les réseaux et cibler des infrastructures critiques comme les câbles sous-marins et les *data centers*.

## Le *dark web* : un espace d'activités illicites

Le *dark web,* une partie obscure de l'Internet accessible uniquement via des navigateurs spécifiques comme Tor, est un espace où les activités illicites prolifèrent. Initialement développé par des agences de renseignement américaines, Tor permet d'accéder à des marchés non indexés où s'épanouissent des activités illicites à l'échelle mondiale. Ainsi, circulent des données volées obtenues notamment lors de cyberattaques comme des rançongiciels et où sont proposés à la vente des produits ou substances illicites comme des armes, des produits stupéfiants ou des contenus pédopornographiques. Ainsi, le cyberespace décloisonne des espaces géographiques, culturels, dessinant de fait une nouvelle géopolitique. À titre d'illustration, des solutions logicielles contribuent à opacifier des échanges par voie numérique en rendant incertaine la localisation géographique des acteurs. Des outils comme les VPN ( ou *Virtual Private Network*) permettent aux utilisateurs de masquer leur localisation

géographique précise, ce qui présente l'avantage de protéger les internautes dans des zones soumises à forte censure ou pour éviter d'être repérés.

En plus des VPN, il convient d'évoquer d'autres typologies de cyberattaques qui illustrent à dessein les enjeux géopolitiques du cyberespace dans leurs capacités à fragiliser toutes tentatives d'attribution d'un acte malveillant. Il s'agit des attaques par DDOS, autrement dit des attaques par déni de service distribué. Des machines zombies c'est-à-dire des ordinateurs indûment contrôlés à distance par des hackers sont mobilisées, simultanément, pour saturer par des requêtes envoyés en grand nombre sur des services en ligne par exemple. L'effet est immédiat : le service ne peut répondre et se trouve de fait inopérant dans ses fonctionnalités ou « service ». Ces attaques, déclenchées à l'insu des propriétaires des machines, saturent les serveurs visés, rendant difficile l'identification des attaquants. Ainsi, la géographie physique n'est plus un obstacle, transformant la cybercriminalité en un défi majeur pour la sécurité internationale.

## Les *data centers* : installations physiques névralgiques au cœur de la guerre cyber ?

Les *data centers*, véritables centres névralgiques du cyberespace, jouent un rôle clé dans la sécurisation des données et des communications à l'échelle mondiale. Ces infrastructures, souvent gérées par des entreprises privées, hébergent de nombreux serveurs contenant des données comme des boites mail, des fichiers d'entreprise ou des données techniques (logs de connexion, journaux d'événements etc.…). Ces centres sont devenus des points clés pour les cyberattaques. Pour les attaquants comme pour les services étatiques. Ils focalisent l'attention de toutes les parties. Ils constituent **des portes d'entrée vers le « point d'eau » que constitue la «  *data*  »**, cet or du XXI -ème siècle. Il s'agit alors d'accéder à la donnée, de la rendre intelligible en passant outre les obstacles du chiffrement et des architectures informatiques souvent complexes. Ou d'exploiter les traces laissées sur les réseaux numériques par les acteurs malveillants afin de les identifier et, de fait, d'attribuer l'attaque à un groupe cybercriminel ou para-étatique. Dans ce cadre, une géopolitique des *data centers* émergent, distinguant les acteurs publics comme privés sur le critère de la compliance et de la coopération sollicitée par les autorités publiques.

## L'État, concurrencé par les géants du numérique

L'un des changements majeurs apportés par le cyber concerne la remise en cause de la souveraineté des États sur les infrastructures de communication. Autrefois maîtres de leurs réseaux de communication, les gouvernements voient aujourd'hui leur autorité défiée par des entreprises privées de taille mondiale, comme les GAFAM (Google, Apple, Meta, Amazon, Microsoft) et les BATX (Baidu, Alibaba, Tencent, Xiaomi). Ces géants du numérique, qui contrôlent des infrastructures critiques, ont acquis une influence géopolitique transnationale. Les États se retrouvent en position de dépendance vis-à-vis de ces entreprises pour l'accès à des services essentiels. Cette situation complexifie encore plus les relations internationales, car les entreprises privées, au même titre que les États, deviennent des acteurs géopolitiques de premier plan.

## Les cryptoactifs : une nouvelle forme de monnaie indépendante des États ?

Un autre exemple du défi lancé aux États dans l'espace cyber est la montée en puissance des cryptoactifs. Ces devises numériques, basées sur la blockchain ou chaine de blocks constituant un registre numérique de transactions décentralisées, échappent au contrôle des gouvernements et des banques centrales. Elles contribuent à l'émergence d'une Finance Décentralisée qui unifie le marché des transactions financières à l'échelle internationale sur le principe d'une dérégulation absolue. Contrairement aux monnaies traditionnelles, **ces cryptoactifs ne sont adossés à aucune autorité étatique, ce qui en fait une alternative autonome et transnationale**. Ces nouvelles formes de monnaie sont l'expression même de la décentralisation du cyberespace, où **les États perdent peu à peu leur emprise sur des secteurs stratégiques, comme la finance**. C'est donc un marqueur caractéristique de l'identité d'une puissance publique qui s'en trouve contesté.

## La manipulation de l'information : une arme cyber au service de guerre hybride ?

L'une des armes les plus redoutables du cyberespace est **la manipulation de l'information**. Elle agisse sur le champ de la connaissance et des perceptions, affectant, de fait, l'ordre public socio-économique. Elle contribue à remettre en cause la valeur de la parole publique et de la vérité de faits établis. Ainsi, à titre d'illustration, les technologies d'intelligence artificielle permettent aujourd'hui de produire des contenus falsifiés extrêmement réalistes, que ce soient des images, des vidéos ou des enregistrements audios. Dans ce nouvel écosystème numérique, la vérité devient mouvante et manipulable à volonté. Les « *deepfakes* », ces montages numériques qui prêtent des propos ou des actions fictives à des personnalités publiques, posent des questions éthiques et philosophiques sur la liberté de communication et sur la responsabilité de l'État dans la régulation de l'information. La manipulation de l'information via le cyber n'est plus uniquement l'apanage des États ; elle est désormais à la portée de groupes criminels et para-étatiques ou, bien encore, d'acteurs privés, ce qui modifie les rapports de force géopolitiques.

## Ressources recommandées

Pour approfondir ces sujets complexes, le Colonel Florian Manet recommande le **Rapport annuel sur la cybercriminalité 2024**, publié par le ministère de l'Intérieur et le Commandement du cyberespace. Ce document constitue une référence essentielle pour comprendre les évolutions récentes de la cybercriminalité et les stratégies mises en place pour y faire face.

Les victimes de cybermalveillance peuvent aussi recourir au site dédié cybermalveillance.gouv.fr

## P.-S.

Florian Manet, Colonel de la gendarmerie nationale. Il commande le volet opérationnel du Commandement du Cyberespace du Ministère de l'Intérieur.

Interview organisée et conduite par Pierre Verluise, docteur en Géopolitique, fondateur du *Diploweb*, il produit Planisphère sur Radio Notre Dame et RCF depuis septembre 2024. Cette émission a été diffusée en direct le 4 mars 2025.
Synthèse par Émilie Bourgoin, étudiante en quatrième année au BBA de l'EDHEC et alternante au sein de la cellule sûreté d'un grand groupe. Elle a la charge du suivi hebdomadaire de l'actualité des livres, revues et conférences géopolitiques comme de la rédaction des synthèses des épisodes de l'émission Planisphère pour *Diploweb*.

---

## Notes

[1] NDLR : Cette émission a été enregistrée le 23 septembre 2024. La synthèse a été revue et validée le 6 mars 2025.

[2] NDLR : Les gazoducs Nord Stream 1 et 2, situés en mer Baltique, ont subi quatre explosions dont trois le 26 septembre 2022 et une le 29 septembre 2022.