



Vers de nouveaux rapports de force des communications stratégiques ?

Le cas de Starlink dans le conflit Russo-
Ukrainien.



MACYB09 / MARSIE 05 :

Remerciements :

Nous tenons à adresser nos sincères remerciements à l'ensemble du corps professoral de l'École de Guerre Économique pour son accompagnement, sa disponibilité et la qualité des enseignements dispensés tout au long de notre parcours. Nous tenons à mentionner plus particulièrement M. Laurent Barrat pour l'appui fourni lors de la rédaction de ce mémoire.

Nous souhaitons également avoir un mot pour nos proches et nos familles, dont la relecture et les encouragements ont été précieux tout au long de la rédaction. Enfin, nous souhaitons souligner la richesse des échanges avec les autres professionnels rencontrés au cours de cette année de formation. Leurs points de vue variés et complémentaires ont contribué à bâtir notre réflexion et à nourrir la construction de ce mémoire.

Aux professionnels qui ont accepté d'échanger avec nous et enrichir ainsi nos propos, nous adressons également nos plus sincères remerciements.

Épigraphe :

*« Le personnel de nombreuses unités militaires de transmission ne sera à la hauteur que si le Commissariat du Peuple aux Postes et Télécommunications met à la disposition du Commissariat à la Guerre, lors de la mobilisation, des employés expérimentés et bien instruits, s'il l'assiste aussi avec ses moyens matériels, par exemple ses téléscrip-teurs, et si, **dans le développement en temps de paix, il tient compte des exigences de la guerre.** »*

- Svetchine Alexandre, Strategiia, 1926.



Table des matières

I.	Etat des lieux.	8
A.	Approche historique des communications stratégiques	8
1.	La communication : condition existentielle de l'État	8
2.	Le triptyque rapidité, confidentialité et intégrité	9
3.	Typologies médiatiques.....	9
4.	De l'ère orale à l'ère mécanique.....	10
5.	Ère électrique : l'instantanéité du commandement.....	12
6.	Ère électronique : l'accélération du commandement.....	13
7.	Ère numérique, communication et architecture informationnelle	15
B.	Une approche de la souveraineté.	16
1.	Origine du mot, multiplicité des sens	16
2.	Les dérivés de la souveraineté.....	17
C.	Origines du conflit.....	19
D.	L'état de l'art en Ukraine avant Starlink	21
1.	L'héritage soviétique et la rupture stratégique de 2014	21
2.	L'émergence d'un écosystème numérique militaire.....	23
3.	La fragilité d'un système numérisé mais non souverain.....	25
4.	Le 24 février 2022 : anatomie d'une attaque.....	28
5.	Lecture : l'attaque comme révélateur.....	31
II.	Starlink, un nouvel acteur et une nouvelle technologie.....	35
A.	« Qui » : M. Musk.....	35
1.	Enfance et arrivée en Amérique	35
2.	Doctrine libertarienne et commande publique	36
3.	SpaceX et Starlink : des instruments au service d'une vision.	38
4.	Cartographie des intérêts au moment du conflit ukrainien	39
B.	« Comment » Starlink est devenu un monopole de fait.....	41
1.	La genèse de SpaceX : capital privé et risque assumé	42
2.	NASA, le tournant de la commande publique	43
3.	Une dépendance gouvernementale assumée et critiquée	45
4.	Starlink, instrument financier de SpaceX	46
5.	Le verrouillage spectro-orbital	50
6.	Grille de lecture intelligence économique.....	53

7. Synthèse.....	54
C. « Quoi - le produit et la technologie »	54
1. Le produit : l'offre standard, composition et fonctionnement	54
2. Architecture du réseau Starlink.	56
3. Analyse des menaces	60
III. Starlink en Ukraine.....	63
A. L'emploi de Starlink par l'Ukraine	64
1. La demande d'aide officielle de l'Ukraine.	64
2. Le volume croissant de terminaux.	66
3. L'utilisation civile et militaire de Starlink.....	67
4. Les attaques sur Starlink	69
5. L'évènement de Sébastopol	75
6. Starlink et la diplomatie américaine	81
B. Qui paye ?.....	83
C. Utilisation de Starlink par les forces russes dans la guerre en Ukraine	85
1. Une logique « judoka »	85
2. La contrebande comme mode d'acquisition	86
3. L'enquête américaine (2024).....	87
4. Le tournant de 2026.....	88
5. Synthèse.....	91
IV. Conclusion	96
V. ANNEXE 1 : Glossaire	101
VI. ANNEXE 2 : La Mer Noire	104
VII. ANNEXE 3 : Entretien avec Olivier BOYER	115
VIII. ANNEXE 4 : Entretien avec un chercheur espace de l'IRSEM.....	118
IX. Sources.....	122

Le 24 février 2022, le président de la Fédération de Russie Vladimir Poutine annonce le lancement d'une « opération militaire spéciale » en Ukraine. Cette décision marque le début d'un conflit de haute intensité, caractérisé par des opérations menées simultanément dans plusieurs milieux : terrestre, aérien, maritime, mais également cybernétique et informationnel. Les premiers jours sont marqués par une forte intensité des combats et une certaine confusion opérationnelle.

Très rapidement, une aide internationale se met en place en soutien à l'Ukraine. Matériels militaires, armements, munitions, mais aussi services et infrastructures numériques sont acheminés vers le théâtre d'opérations. Parmi ces apports figure un équipement en apparence anodin, bien moins spectaculaire que les missiles antichars "Javelin" ou les systèmes de défense "Patriot" : une antenne de communication satellitaire, de dimensions modestes, environ 40 cm sur 60 cm. Pourtant, cet objet va progressivement s'imposer comme un élément central dans la conduite des opérations, et ce dans les deux camps. Un nom : Starlink.

Grâce à sa capacité de déploiement rapide, sa résilience et son accessibilité, ce système devient un outil clef pour les communications tactiques et stratégiques. Installé sur des positions fixes, embarqué sur des véhicules blindés, des drones navals ou terrestres, il se diffuse largement sur le champ de bataille. Cette omniprésence donne à son fournisseur un rôle inédit dans un conflit interétatique.

En effet, l'intégration de cette technologie au cœur des capacités opérationnelles ukrainiennes confère à son opérateur privé un levier d'influence potentiel sur la conduite des opérations. Pour la première fois à une telle échelle, une entreprise technologique semble en mesure d'interagir directement avec la dynamique d'un conflit armé, remettant en question le monopole traditionnel des États sur les fonctions stratégiques critiques.

Alors que la guerre en Ukraine révèle de nouvelles formes d'affrontement, elle met également en lumière l'émergence d'acteurs non étatiques dotés de capacités autrefois réservées aux puissances publiques, notamment dans les domaines des télécommunications, de la donnée et de l'espace. Dès lors, la question suivante s'impose :

« Dans quelle mesure le déploiement de Starlink en Ukraine redéfinit-il les rapports de force entre acteurs étatiques et entreprises technologiques privées ? »

Ce mémoire s'inscrit dans cette réflexion. La première présentera des éléments de contexte sur le cas étudié. La seconde partie s'attachera à SpaceX et Starlink. La troisième partie traitera de la chronologie de Starlink en Ukraine. Nous finirons par conclure d'après les éléments réunis dans ce mémoire.

Compte tenu du caractère évolutif et rapide du sujet, les éléments présentés dans ce mémoire s'appuient sur des données disponibles à la date du 17 août 2026. Il convient donc de considérer que certaines dynamiques analysées sont susceptibles d'évoluer.



I. État des lieux et rappel historique sur les communications stratégiques



I. Etat des lieux.

La problématique choisie impose avant de définir et de contextualiser quatre éléments. D'abord ce qu'est la communication dans le cadre étatique, d'où vient-elle et à quoi sert-elle. Ensuite sera traité la question de la souveraineté, terme aujourd'hui à la mode mais dont la signification a un sens. Cette partie permettra de traiter ensuite la question des origines du conflit. La dernière partie traitera, à la veille du conflit, de l'état de l'art en Ukraine des communications, du matériel à la doctrine.

A. Approche historique des communications stratégiques

1. La communication : condition existentielle de l'État

La communication constitue une condition structurelle de l'existence et du fonctionnement de l'État. Dès les premières formes d'organisation politique territorialisée, gouverner implique de savoir, de décider et de faire appliquer, fonctions indissociables de la capacité à collecter, transmettre et exploiter l'information.ⁱ



Image 1 : Gravure d'une calèche du cursus publicus, un réseau postal mis en place sous l'empire romain.

Les grands empires antiques en fournissent des illustrations précoces. L'Empire achéménideⁱⁱ comme l'Empire romainⁱⁱⁱ mettent en place des réseaux de routes, de relais et de messageries permettant d'assurer la continuité du commandement entre le centre et les périphéries. Dans ces configurations, la communication ne relève pas du soutien logistique, mais de la cohérence politique elle-même.

Sans système de communication maîtrisé, l'État perd sa capacité d'action unifiée et se fragmente en entités locales vulnérables aux ruptures informationnelles. L'effondrement du commandement^{iv} précède souvent celui des forces, soulignant la centralité de la communication dans l'exercice du pouvoir. Cette dépendance apparaît également dans les fonctions régaliennes^v : édicter le droit, garantir la sécurité, rendre la justice, conduire la défense ou la diplomatie reposent toutes sur la circulation organisée de l'information.

Cette infrastructure immatérielle prend corps dans la bureaucratie, entendue comme un système institutionnalisé de traitement de l'information. Cette structure^{vi} rationnelle et hiérarchisée, permet à l'État de gouverner de vastes territoires sans présence permanente du souverain. De la Chine impériale^{vii} à Rome^{viii}, la souveraineté s'exerce moins par la contrainte directe que par la capacité à collecter, traiter et distribuer l'information. La communication apparaît ainsi comme le socle opérationnel du pouvoir étatique et l'un des fondements de son autonomie stratégique.

2. Le triptyque rapidité, confidentialité et intégrité

Si la communication constitue une condition d'existence de l'État, son efficacité stratégique dépend de sa capacité à satisfaire trois exigences permanentes : la rapidité, la confidentialité et l'intégrité du message. Ce triptyque, indépendant des technologies employées, structure l'ensemble des communications stratégiques étatiques et conditionne la capacité de l'État à décider, coordonner et agir. Il ne relève pas d'une construction contemporaine, mais d'un invariant historique : dès qu'un message engage une décision politique, administrative ou militaire, il est soumis à ces contraintes, dont la défaillance transforme la communication en vulnérabilité stratégique.

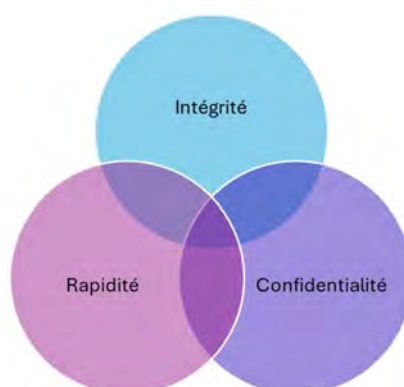


Figure 1 : Les 3 composantes nécessaires à l'organisation des communications.

La rapidité conditionne la conservation de l'initiative : décider ou transmettre trop tard revient à subir le tempo de l'adversaire^{ix}. Toutefois, une communication rapide dépourvue de confidentialité devient immédiatement exploitable par l'ennemi. L'histoire des États est ainsi marquée par des efforts constants de dissimulation des messages, de la cryptographie diplomatique^x aux dispositifs modernes de chiffrement^{xi}. L'intégrité du message constitue la troisième exigence : une information altérée peut produire des effets plus dommageables encore qu'une information interceptée, en conduisant à des décisions erronées au sein de chaînes de commandement complexes.

Ce triptyque ne forme pas un idéal abstrait, mais une contrainte structurelle : toute innovation technique améliorant un paramètre tend à fragiliser les autres et à créer de nouvelles dépendances. L'histoire des communications stratégiques est ainsi traversée par une tension constante entre gains opérationnels et vulnérabilités nouvelles^{xii}, faisant de la maîtrise de l'information un enjeu central de la souveraineté étatique.

3. Typologies médiatiques

L'analyse des communications stratégiques étatiques nécessite un cadre conceptuel permettant d'ordonner les évolutions techniques sans les réduire à une simple chronologie. Les travaux sur les médias de communications^{xiii} offrent un premier point d'appui en distinguant plusieurs ères dominantes de la communication, tout en montrant que chaque support transforme en profondeur l'organisation sociale et politique. Toutefois, ces « ères » ne sont ni étanches ni

strictement bornées : les techniques coexistent et produisent des effets durables, ce qui invite à raisonner en termes de régimes dominants plutôt que de ruptures linéaires.

Si cette typologie est heuristique, c'est-à-dire partiellement étayée, elle demeure insuffisante pour analyser la communication stratégique de l'État, car elle privilégie les effets culturels des médias au détriment des enjeux de commandement, de souveraineté et de sécurité. Il est donc nécessaire de déplacer l'analyse vers les systèmes de communication stratégique étatique, entendus comme des infrastructures organisant la circulation de l'information au sein de l'appareil d'État, dans le respect du triptyque rapidité, confidentialité et intégrité.

Dans cette perspective, il est possible d'identifier six grandes ères de la communication stratégique : orale, écrite, mécanique, électrique, électronique et numérique. Cette classification ne vise ni l'exhaustivité ni une datation rigide, mais met en évidence des ruptures fonctionnelles dans la manière dont les États organisent le commandement et gèrent leurs vulnérabilités informationnelles. Chaque ère constitue à la fois un facteur de puissance et une source de dépendances nouvelles^{xiv}, révélant que l'histoire des communications stratégiques étatiques est moins celle d'un progrès linéaire que celle d'un équilibre instable entre efficacité opérationnelle et exposition accrue aux risques informationnels.^{xv}

4. De l'ère orale à l'ère mécanique

Dans l'ère orale, la communication stratégique repose presque exclusivement sur le porteur humain : le message est mémorisé, incarné et transmis oralement. Cette configuration permet une certaine rapidité, mais expose l'État à une vulnérabilité structurelle majeure, liée à la loyauté, à la fiabilité et à la survie du messager. L'intégrité et la confidentialité du message dépendent entièrement du facteur humain, rendant la manipulation, la trahison ou l'altération informationnelle consubstantielles à ce régime. Les épisodes antiques, d'Hérodote^{xvi} à Thucydide^{xvii}, comme la défaite de Varus^{xviii} à Teutobourg¹, montrent que la perte de maîtrise du canal oral peut produire des effets stratégiques décisifs sans affrontement direct. L'oralité apparaît ainsi comme un régime ambivalent, souple et rapide, mais intrinsèquement instable.

L'apparition de l'écriture constitue une rupture majeure en permettant de dissocier le message de son porteur. Le message écrit fixe la décision, améliore son intégrité et rend possible la délégation, la continuité de l'action publique et l'administration de territoires étendus. Toutefois, cette stabilisation introduit une vulnérabilité nouvelle : l'interception durable de l'intention stratégique. L'écrit transforme l'information en objet appropriable, lisible et exploitable dans le temps, comme l'illustrent la cryptographie antique, les cabinets noirs de l'époque moderne ou l'espionnage diplomatique systématique. L'ère écrite renforce donc la capacité de

¹ En l'an 9 de notre ère, 3 légions complètes mené par Varus, préfet romain, entre dans la forêt de Teutoburg sur les conseils d'Arminius, prince d'origine germane. C'est un piège tendu par ce dernier qui mènera à l'anéantissement complet des 3 légions et à la fin des ambitions romaines en Germanie. C'est sur la base de renseignement erroné que Varus accepte les conseils du traître.

gouvernement, tout en obligeant l'État à penser la confidentialité de manière structurelle.

L'ère mécanique prolonge cette logique en industrialisant la communication écrite par la standardisation, la reproductibilité et la centralisation matérielle. L'imprimerie, les réseaux postaux et le télégraphe optique permettent une diffusion plus rapide et plus cohérente des décisions, renforçant le commandement à distance. Mais cette efficacité repose sur des infrastructures visibles, fixes et capturables, dont la neutralisation, la manipulation ou l'exploitation peuvent produire des effets stratégiques majeurs. L'industrialisation de la communication accroît ainsi simultanément la puissance de l'État et sa dépendance à ses propres systèmes, préparant l'émergence de régimes visant à s'affranchir des contraintes physiques de l'ère mécanique. L'affaire des frères Blancs au XIXe siècle met en avant la faiblesse d'un système dont la sécurité repose avant tout sur les acteurs humains y participant. ^{xix}

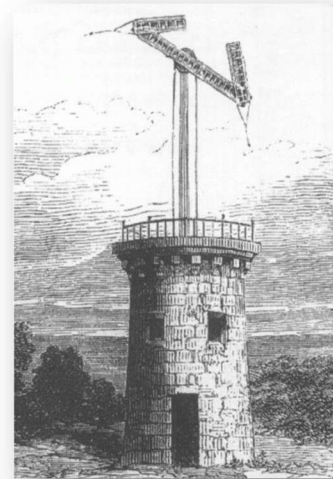


Image 2 : Gravure de télégraphe optique dit "Chappe", dernier système mécanique avant l'avènement du télégraphe électrique.

En 1834, les jumeaux François et Louis Blanc, deux agents de change opérant en Gironde, mettent en place la toute première cyberattaque de l'Histoire en détournant le télégraphe optique Chappe.

Pendant deux ans, ils corrompent des fonctionnaires pour introduire des anomalies codées dans les messages officiels de l'État. Ce stratagème secret leur permet de connaître, avec plusieurs heures d'avance, les fluctuations de la bourse de Paris.

Grâce à ces données confidentielles, ils spéculent à coup sûr sur le marché de Bordeaux avant leurs concurrents. Découverte en 1836, l'affaire débouche sur un procès retentissant en mars 1837 où les deux frères sont finalement acquittés. La loi de l'époque ne prévoyant aucun texte pour punir le vol d'informations, leur acte n'était pas illégal.

Face à ce vide juridique, l'État réagit immédiatement en instaurant le monopole public des télécommunications en mai 1837.

5. Ère électrique : l'instantanéité du commandement

L'ère électrique constitue une rupture décisive dans l'histoire des communications stratégiques étatiques, en dissociant pour la première fois la vitesse de circulation de l'information de toute contrainte mécanique de transport. Avec le télégraphe électrique puis le téléphone, la transmission des ordres et des renseignements devient quasi instantanée à l'échelle nationale, voire continentale. Cette instantanéité transforme la temporalité de l'action étatique : le temps de la décision tend à se confondre avec celui de l'événement, réduisant drastiquement les délais entre le centre politique et les périphéries opérationnelles.

Sur le plan du commandement, cette évolution permet l'émergence d'un pilotage à distance continu. Le télégraphe électrique rend possible une centralisation décisionnelle accrue, dans laquelle l'autorité politique ou militaire peut intervenir presque en temps réel sur des théâtres éloignés. La guerre de Sécession constitue à cet égard un cas fondateur : l'intégration du télégraphe au U.S. Military Telegraph Corps^{xx} permet au président Lincoln de maintenir une unité de commandement sur l'ensemble du territoire de l'Union, en coordonnant simultanément plusieurs armées dispersées. La rapidité de transmission devient alors un avantage stratégique autonome, indépendamment de la supériorité tactique locale.

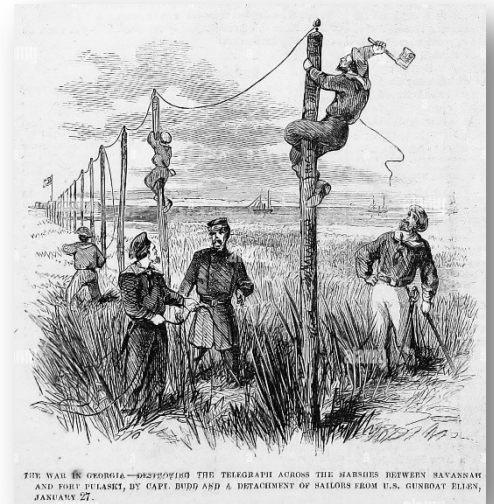


Image 3 : Marins de l'US Navy détruisant un télégraphe en Géorgie durant la guerre de sécession. Cibler la communication devient systématique durant ce conflit.

Toutefois, cette instantanéité repose sur une dépendance critique à des infrastructures filaires continues. Les réseaux télégraphiques et téléphoniques constituent des systèmes sociotechniques complexes, vulnérables à la coupure, au sabotage et à l'interception. Cette fragilité apparaît clairement lors de la Première Guerre mondiale : si le commandement électrique permet une planification centralisée sans précédent, la destruction régulière des lignes par l'artillerie paralyse fréquemment les états-majors, contraints de recourir à des moyens plus lents et moins fiables. L'électricité confère ainsi une puissance de coordination inédite, mais au prix d'une vulnérabilité systémique élevée.

Svetchine² attribue ainsi une partie des défaites russes de la première guerre mondiale à la facilité d'interception et de décodage des messages d'origine électrique. Il est d'autant plus critique sur l'élément humain gérant ces envois, attribuant à des opérateurs "laxistes" l'envoi de messages d'importances vitales sans chiffrement.

² « Mais tous les records ont été battus, bien sûr, par le radiotélégraphe russe pendant la guerre mondiale. [...] Toute médiocrité des Allemands aurait été élevé au rang de génie par notre radiotélégraphe » Strategia, Svetchine, p.566. ed Française.

Par ailleurs, l'accélération des flux d'information engendre une tension nouvelle entre rapidité et capacité de contrôle. La circulation quasi instantanée des données tend à saturer les capacités humaines de traitement, entraînant une complexification bureaucratique et une rigidification des chaînes de décision.^{xxi} Cette ambivalence se manifeste également dans le champ diplomatique, comme l'illustre la dépêche d'Ems³ : la modification volontaire d'un télégramme suffit à déclencher un conflit majeur, démontrant que la perte d'intégrité d'un message électrique peut produire des effets stratégiques immédiats.

L'épisode du télégramme Zimmermann⁴ révèle enfin la dimension critique de cette vulnérabilité : l'interception et le déchiffrement d'un message électrique provoquent un basculement politique décisif avec l'entrée en guerre des États-Unis. Dans l'ère électrique, la maîtrise ou la perte de maîtrise des réseaux filaires devient ainsi un facteur déterminant de la victoire ou de la défaite.

L'ère électrique apparaît donc comme profondément ambivalente. Elle offre à l'État une capacité inédite de commandement instantané et de coordination centralisée, tout en l'exposant à une dépendance critique à des infrastructures vulnérables. Cette tension structurelle prépare logiquement la transition vers l'ère électronique, dans laquelle la radio et les communications hertziennes cherchent à s'affranchir des contraintes physiques visibles du filaire.

6. Ère électronique : l'accélération du commandement

L'ère électronique marque un changement de régime dans l'histoire des communications stratégiques étatiques, en substituant aux réseaux filaires de l'ère électrique une transmission fondée sur les ondes hertziennes. La radio permet une communication rapide, mobile et étendue, indépendante de la continuité matérielle d'un câble et moins vulnérable aux coupures territoriales. Cette rupture répond directement aux limites structurelles des infrastructures filaires, tout en transformant profondément la conduite des opérations militaires et la gouvernance étatique de l'information.^{xxii}

Sur le plan stratégique, les forces terrestres, navales et aériennes peuvent désormais communiquer en mouvement et coordonner leurs actions à longue distance. La radio confère un gain décisif en rapidité et en portée, rendant possible une conduite plus fluide et plus réactive des opérations. Toutefois, cette libération du support matériel ne supprime pas les vulnérabilités : elle les déplace. La communication devient structurellement interceptable, le signal se propageant dans un espace ouvert, exposé à l'écoute, au brouillage et à l'exploitation adverse.

³ La dépêche d'Ems est un imbroglio diplomatique qui a servi de prétexte pour engager la guerre franco-allemande de 1870 : il s'agit principalement d'un télégramme officiel envoyé le 13 juillet 1870 par le chancelier Otto von Bismarck à toutes les ambassades

⁴ Le télégramme Zimmermann est un télégramme diplomatique qui a été envoyé le 16 janvier 1917 par le ministre des Affaires étrangères de l'Empire allemand, Arthur Zimmermann, à l'ambassadeur allemand au Mexique, Heinrich von Eckardt, au plus fort de la Première Guerre mondiale. Il donnait l'instruction à l'ambassadeur de se mettre en contact avec le gouvernement mexicain pour lui proposer une alliance contre les États-Unis. Intercepté et déchiffré par le Royaume-Uni puis rendu public, son contenu a accéléré l'entrée en guerre des États-Unis.

Dans ce contexte, la confidentialité devient une contrainte centrale. La sécurisation des communications ne repose plus sur la maîtrise de l'infrastructure, mais sur des dispositifs de chiffrement intégrés aux équipements. L'essor des systèmes électromécaniques répond à cette exigence, en cherchant à rendre exploitables des communications radio massives et rapides.

L'exemple d'Enigma illustre cette dynamique : au début de la Seconde Guerre mondiale, le chiffrement allemand permet une coordination radio sécurisée entre unités et états-majors, conférant un avantage opérationnel notable, notamment dans la guerre navale.



Image 4 : Heinz Guderian lors de la campagne de France dans son véhicule de commandement. La machine Enigma est visible au premier plan, utilisée par un opérateur.

Cet avantage se retourne toutefois lorsque les Alliés parviennent à exploiter les faiblesses du système. Le déchiffrement progressif des communications Enigma, en particulier à Bletchley Park⁵, permet d'anticiper les mouvements allemands et joue un rôle décisif dans la bataille de l'Atlantique. La confiance excessive accordée par l'Allemagne à un système perçu comme inviolable transforme ainsi un outil de puissance en vulnérabilité stratégique majeure. Une logique similaire s'observe avec le code pourpre japonais : considéré comme sûr par Tokyo, il est néanmoins déchiffré par les services américains, offrant un avantage stratégique décisif dans la compréhension de la politique et des intentions japonaises.

L'ère électronique ne repose cependant pas uniquement sur la technique. L'utilisation des Navajo Code Talkers par les forces américaines montre qu'une hybridation entre oralité et électronique peut répondre efficacement aux contraintes du triptyque rapidité, confidentialité et intégrité, en exploitant des barrières linguistiques et culturelles plutôt que des dispositifs technologiques.^{xxiii}

Enfin, l'ère électronique s'accompagne d'une complexification organisationnelle majeure. Le maintien de communications sécurisées impose la création de services spécialisés, de structures de cryptologie et de renseignement électromagnétique, renforçant les capacités de l'État mais accroissant aussi sa dépendance à des systèmes techniques complexes, souvent mal maîtrisés par le pouvoir politique.

L'ère électronique apparaît ainsi profondément ambivalente. Elle offre à l'État une capacité inédite de communication rapide, mobile et chiffrée, tout en introduisant une vulnérabilité nouvelle : la possibilité d'une exploitation invisible et durable des

⁵ Pendant la Seconde Guerre mondiale, Bletchley Park fut le principal site de décryptage du Royaume-Uni.

communications par un adversaire technologiquement plus avancé. Cette tension entre puissance technologique et dépendance cognitive prépare directement l'entrée dans l'ère numérique, où l'enjeu ne porte plus seulement sur la transmission des messages, mais sur le contrôle des architectures informationnelles elles-mêmes.

La transition de l'ère électronique à l'ère numérique s'opère à la fin de la guerre froide, lorsque la numérisation de l'information, la mise en réseau généralisée des systèmes de communication et l'automatisation logicielle du traitement des données transforment en profondeur la nature même de la communication stratégique. Cette rupture ne repose pas sur une innovation isolée, mais sur la convergence de plusieurs dynamiques : généralisation du signal numérique, interconnexion croissante des réseaux civils et militaires, et délégation du traitement de l'information à des systèmes automatisés. La communication cesse alors d'être un simple flux entre un émetteur et un récepteur pour devenir une architecture informationnelle globale.

7. Ère numérique, communication et architecture informationnelle

Dans l'ère numérique, le centre de gravité stratégique se déplace du support matériel vers les protocoles, les logiciels et les capacités de calcul. Là où l'ère électronique reposait encore sur la maîtrise des fréquences et des dispositifs de chiffrement, l'ère numérique repose sur la capacité à concevoir, exploiter et gouverner des systèmes complexes de circulation et de traitement des données. Comme l'avait anticipé James Beniger^{xxiv}, lorsque les flux d'information excèdent les capacités humaines, le contrôle est nécessairement transféré à des systèmes automatisés, introduisant une rupture majeure dans la relation entre décision politique et information.

Sur le plan stratégique, cette transformation procure un gain de puissance considérable. La fusion de données issues de capteurs multiples, la circulation quasi instantanée de l'information et l'interopérabilité des systèmes permettent une coordination inédite des forces militaires et des administrations. La première guerre du Golfe, en 1991, constitue un moment fondateur : les forces américaines s'appuient sur des réseaux numériques émergents intégrant satellites, systèmes informatiques et bases de données partagées, créant une supériorité décisionnelle écrasante^{xxv}. Le gain stratégique ne provient plus d'un message particulier, mais de la maîtrise de l'architecture informationnelle dans son ensemble.

Toutefois, cette puissance s'accompagne d'une vulnérabilité radicalement nouvelle. Dans l'ère numérique, la perte stratégique ne résulte plus nécessairement de l'interception ou de l'altération d'un message, mais de la dépendance structurelle à des systèmes interconnectés. La cyberattaque contre l'Estonie en 2007 illustre cette logique : sans destruction physique ni interception de communications, des attaques de déni de service suffisent à désorganiser durablement le fonctionnement de l'État, révélant la fragilité d'un système hautement numérisé.

Cette vulnérabilité est accentuée par la convergence civilo-militaire des réseaux numériques, associée à l'innovation duale^{xxvi}. Les infrastructures critiques de communication reposent désormais largement sur des technologies, des standards et des services développés par des acteurs privés transnationaux, échappant en partie au contrôle souverain des États^{xxvii}. Les révélations d'Edward Snowden ont mis en lumière cette dépendance, en montrant que des architectures numériques mondiales pouvaient être exploitées à grande échelle par des acteurs disposant d'un avantage technologique et industriel.

Dans ce contexte, le maintien du triptyque rapidité, confidentialité et intégrité dépend moins de la possession des moyens techniques que de la gouvernance des architectures numériques. L'ère numérique ne se caractérise donc pas seulement par un accroissement des capacités de communication, mais par une remise en cause progressive de l'autonomie stratégique des États. Cette dynamique atteint un seuil critique lorsque des infrastructures privées, comme Starlink, deviennent des composantes centrales de la communication stratégique en situation de conflit armé, posant frontalement la question du contrôle, de la dépendance et de la souveraineté.

Enseignements :

- Les systèmes de communication ont souvent eu pour moteur des besoins d'Etat répondant au triptyque Rapidité, Confidentialité et Intégrité.
- Pour répondre à ce triptyque, les systèmes se sont complexifiés dans une course à la communication entre l'expéditeur et l'intercepteur.
- L'histoire des systèmes montre que l'accroissement de leur technicité exige des ressources humaines et des moyens de soutien toujours plus complexes.
- Ses moyens ont de tout temps été formés, entretenus et pilotés par des structures étatiques.

B. Une approche de la souveraineté.

1. Origine du mot, multiplicité des sens

La souveraineté proviendrait du mot *souverain* lui-même issu du mot latin^{xxviii} populaire **superanus*, « qui est au-dessus ; suprême, excellent », lui-même dérivé de *super*, « au-dessus ».

L'auteur Pierre Bellanger définit le support de la souveraineté comme : « *au sens traditionnel, est d'abord le contrôle, par une population, d'un territoire régi par une loi commune issue de sa volonté collective.* »^{xxix}

La souveraineté est aussi un concept philosophique pour la première fois abordé par Aristote. Il sera ensuite spécifié par Jean Bodin, auteur du début du XVI^e siècle, économiste et juriste. Le concept s'enrichira ensuite au fur et à mesure de la construction des états et prendra des formes multiples en fonction des modes de gouvernance (monarchie absolue, monarchie constitutionnelle, république). Il

introduit la notion d'un élément au-dessus de toute décision et qui ne peut être outrepassé.

Pour finir la souveraineté au sens juridique^{xxx} est défini comme : « *la qualité de l'État de n'être obligé ou déterminé que par sa propre volonté, dans les limites du principe supérieur du droit, et conformément au but collectif qu'il est appelé à réaliser.* »

La souveraineté présente donc en termes d'approche des notions qui peuvent sembler parfois différente mais qui consacrent tous la même fonction : la souveraineté est un principe au-dessus des éléments et qui donne au groupe la capacité de décider sans interférence supérieure.

2. Les dérivés de la souveraineté

La souveraineté comme on a pu le voir précédemment est donc un concept protéiforme intrinsèquement lié à la capacité de décision. Mais depuis le début de la guerre en Ukraine, ce terme politique est devenu de plus en plus présent dans le discours politique. Associé au souverainisme il y a encore dix ans, un mouvement politique mineur en France et dont les plus célèbres représentants seraient M. Dupont-Aignan^{xxxix}, M. De Villiers^{xxxix}, M. Asselineau^{xxxix} ou encore M. Phillipot^{xxxix}, la souveraineté bénéficie aujourd'hui d'une exposition dans les médias et d'une déclinaison en plusieurs « concepts ».

La co-souveraineté est un concept où deux entités ou plus exercent une autorité sur un même territoire ou domaine. On parle de *condominium* en droit international (l'île des Faisans entre la France et l'Espagne)^{xxxv}. Ce principe est apparenté à la souveraineté partagée développé au fil des ans avec l'avènement d'état fédéraux^{xxxvi}

L'in-souveraineté est l'absence de souveraineté. Ce n'est pas la perte de souveraineté mais bien sa totale absence caractérisée par des éléments supérieurs agissant en place de l'objet étudié.

Le suzerain et la suzeraineté ne sont pas directement issu du mot souveraineté, mais partagent la même racine. Le suzerain est celui qui a autorité sur un vassal qui lui prête allégeance. Cela signifie que le vassal a, dans ces décisions et postures, un élément supérieur à prendre en compte. Ce concept ancien est celui de la féodalité.

La souveraineté mise en commun, dont l'exemple le plus abouti est l'Union Européenne, met en avant la décision volontaire de donner tout ou partie de sa souveraineté à une entité juridique supérieure.

La souveraineté partagée évolutive entend un transfert de la souveraineté d'une entité à une autre. ^{xxxvii}

La souveraineté est donc un concept protéiforme dans son application et sa mise en forme, mais il répond toujours à une même idée : la souveraineté est le principe

du contrôle d'un élément permettant une prise de décision sans partage ni interférence possible provenant d'un principe supérieur.

Cette notion d'apparence simple est complexe à appréhender dans un monde multipolaire, mondialisé et surtout basé sur l'interdépendance.



Image 5 : Kim Jong-Un, dirigeant de la République Démocratique de Corée du Nord passant en revue l'équipage du Choe Hyon. Ce navire d'apparence ultra-moderne semble avoir fait l'objet d'une aide importante de la Russie en échange de la participation des troupes nord-coréennes au conflit ukrainien.

Le Juche, souveraineté voulue, dépendance oblige.

Le Juche est une philosophie autarcique développée par Kim Il-Sung, premier et unique président de la République Démocratique de Corée. Basé sur la volonté d'une autarcie extrême afin de rester indépendant de toutes interférences extérieures, celle-ci reste un souhait de façade. La Corée du Nord est très dépendante du commerce avec ces deux voisins directs, la Chine et la Russie. Dépendante aussi de l'aide alimentaire internationale, le souhait de souveraineté s'est donc incarné dans la recherche de *l'ultima ratio regum* : l'arme atomique.

Enseignements :

- La souveraineté se caractérise comme étant le niveau ultime de décision sur un objet, territoire, population ou valeur immatérielle.
- Aucun élément ne peut surpasser et contraindre ce qui est souverain. La souveraineté s'acquière, se perd ou se transmet mais reste un fait. La souveraineté n'est pas déclaratoire.
- La souveraineté est liée aux rapports de force et au contexte dans lesquels ses détenteurs évoluent.
- Le monde moderne définit de nouvelles formes de souveraineté et complexifie l'identification des détenteurs de celle-ci.

C. Origines du conflit.

Pour comprendre les enjeux stratégiques de communication du conflit ukrainien, il nous faut avant tout revenir aux sources de ce conflit. Le 19 août 1991, soit le lendemain d'un coup d'État communiste avorté en Russie, l'Ukraine a déclaré son indépendance à l'unanimité, avec 346 voix sur 362. La déclaration précisait : « Au vu du danger mortel entourant l'Ukraine suite au coup d'État en URSS du 19 août 1991, et en continuation de la tradition millénaire du développement de l'État en Ukraine, en vertu du droit des peuples à disposer d'eux-mêmes, ainsi qu'en accord avec la Charte des Nations unies. ». Dès ce moment, la république d'Ukraine se retrouve confrontée à plusieurs sujets avec son ancienne puissance de tutelle. Parmi les sujets, la question des armes nucléaires, la Crimée, la flotte de la mer Noire et des divisions internes entre l'Ouest et le Sud-Est du pays.^{xxxviii}

A la chute de l'Union des républiques socialistes soviétiques (URSS), l'Ukraine avait en sa possession 1900 ogives et 2500 vecteurs sur son territoire. Bien que les codes soient entre les mains de la République de Russie, leur présence est un objet de négociation à la fois pour l'Ukraine et pour la Russie mais aussi pour les Etats-Unis dont le soutien affiché à l'indépendance de l'Ukraine. L'Ukraine dut renoncer à son statut de puissance nucléaire par défaut afin d'obtenir une reconnaissance de la communauté des États indépendants.^{xxxix}

Autre sujet de discorde, le statut de la Crimée et notamment son port de Sébastopol, siège de la flotte de la mer Noire. La Russie a toujours fait de son accès aux mers chaudes et ce depuis l'époque de Pierre le Grand une des constances de sa politique extérieure. Sur le plan institutionnel, il faut rappeler que la Crimée n'était pas ukrainienne avant 1954 mais constituait un oblast de la République socialiste fédérative soviétique de Russie. La décision de transfert est prise le 19 février 1954 par le Présidium du Soviet suprême de l'URSS. Elle s'inscrit dans un cadre strictement intra-soviétique, où les frontières entre républiques fédérées avaient avant tout une fonction administrative et non géopolitique. Dans l'URSS stalinienne puis post-stalinienne, ces frontières étaient modifiables par décision centrale sans consultation populaire ni enjeu de souveraineté internationale, puisque toutes les républiques appartenaient à un même État unitaire de fait.

Second facteur de crispation, la flotte de la mer Noire. Entre 350 et 370 vaisseaux incluant le croiseur de classe Slava, les destroyers Kashin et Kotlin, les frégates Krivak, les sous-marins diesel des classes Kilo, Foxtrot et Romeo, les navires de débarquement de classes Ropucha et Alligator, ainsi que les bâtiments auxiliaires. Cette flotte fit l'objet d'âpres négociations. Elstine, président de la fédération, signa même en 1992 un décret plaçant la flotte sous son commandement direct. La Fédération considérant que la flotte faisait partie des éléments stratégiques et que l'Ukraine ne pouvait revendiquer ces éléments, le parlement Russe ayant déclaré en janvier 1992 que la transmission de la Crimée à l'Ukraine était illégale. En juillet 1993, le parlement Russe revendique la base de Sébastopol. Eltsine et Kravtchouk, président Ukrainien, ouvrent des négociations qui finissent par arriver à un accord. Environ 80% de la flotte passe sous contrôle russe et un bail de 20 ans est accordé

sur la base de Sébastopol. En 2014, ce sera le point de départ des troupes chargées d'annexer la péninsule.

La révolution orange de 2004 constitue un tournant majeur dans l'histoire politique et géostratégique de l'Ukraine post-soviétique, en cristallisant une orientation pro-occidentale perçue par la Russie comme une remise en cause directe de sa sphère d'influence. Issue de la contestation massive de l'élection présidentielle truquée en faveur de Viktor Ianoukovitch, elle aboutit à l'arrivée au pouvoir de Viktor Iouchtchenko et à une tentative de réorientation stratégique vers l'Union européenne et l'Organisation du traité de l'Atlantique Nord (OTAN), sans toutefois produire de réformes institutionnelles durables ni de stabilisation politique interne. Les divisions structurelles du pays, les rivalités oligarchiques et l'échec à consolider un État de droit affaiblissent progressivement cet élan, permettant le retour de Ianoukovitch en 2010. Pour Moscou, la révolution orange s'inscrit néanmoins durablement dans le registre des « révolutions de couleur », interprétées comme des opérations d'influence occidentales menaçant la sécurité russe. Cette lecture stratégique explique en partie la réaction russe face au soulèvement de Maïdan en 2013-2014, perçu comme la répétition d'un scénario déjà observé en 2004. L'annexion de la Crimée en mars 2014 apparaît ainsi comme l'aboutissement d'un cycle ouvert par la révolution orange : elle marque le passage d'une conflictualité politique et informationnelle à une rupture territoriale assumée, fondée sur la protection des intérêts militaires russes, notamment la base de Sébastopol, et sur la volonté de verrouiller durablement l'Ukraine hors de l'orbite euro-atlantique.

Dès le printemps 2014, des mouvements séparatistes armés émergent dans les oblasts de Donetsk et de Louhansk, avec un soutien politique, logistique et militaire russe progressivement documenté par l'Organisation pour la sécurité et la coopération en Europe (OSCE) et plusieurs centres de recherche occidentaux. Le conflit, qui oppose l'armée ukrainienne à des forces séparatistes appuyées par Moscou, devient une guerre hybride combinant opérations militaires conventionnelles limitées, actions clandestines, désinformation et pression économique. Les accords de Minsk I (2014) et Minsk II (2015), négociés sous l'égide de la France et de l'Allemagne, instaurent des cessez-le-feu fragiles sans régler les causes politiques du conflit, installant une situation de « ni guerre ni paix » durable à l'est de l'Ukraine.

Dans ce contexte, l'Ukraine engage une transformation profonde de son appareil de sécurité et de défense. L'annexion de la Crimée, perçue comme la preuve de l'effondrement des garanties de sécurité héritées du mémorandum de Budapest de 1994, pousse Kiev à rompre avec une posture de neutralité de facto. Les forces armées ukrainiennes sont progressivement réorganisées, professionnalisées et partiellement modernisées avec l'aide occidentale, notamment américaine, britannique et canadienne. Parallèlement, l'Ukraine renforce sa coopération avec l'OTAN sans adhésion formelle, tandis que la Russie accroît sa présence militaire en Crimée, transformant la péninsule en bastion stratégique en mer Noire, doté de capacités anti-accès et de projection de puissance.

Au-delà du champ militaire, l'après Crimée marque une intensification de la guerre informationnelle et cybernétique. L'Ukraine devient un laboratoire de la conflictualité numérique : cyberattaques contre les infrastructures énergétiques, campagnes de désinformation visant les institutions ukrainiennes et occidentales, instrumentalisation des médias et des réseaux sociaux. Ces dynamiques, étudiées notamment par l'Institut de relations internationales et stratégiques (IRIS) révèle l'importance croissante des communications stratégiques dans la résilience étatique. Les faiblesses structurelles des réseaux ukrainiens, hérités de l'époque soviétique et insuffisamment modernisés, apparaissent alors comme un facteur de vulnérabilité majeur, préparant le terrain aux enjeux qui émergeront de manière décisive à partir de 2022 avec le recours massif à des solutions de communication privées comme Starlink.

D. L'état de l'art en Ukraine avant Starlink

Analyser le dossier Starlink suppose d'examiner d'abord la posture ukrainienne en matière de communications stratégiques à la veille de l'invasion russe à grande échelle. Sans cette mise en perspective, le déploiement de la constellation SpaceX à partir du 26 février 2022 apparaît comme un acte de générosité spontané, comblant un vide capacitair. Replacé dans cette perspective, il apparaît comme la substitution d'une dépendance à une autre. Le fournisseur change, la nature du problème souverain demeure.

Cette section suit l'ordre chronologique. Elle décrit l'héritage soviétique et post-soviétique, puis la première inflexion de 2014 et l'adoption de Tooway. Elle examine ensuite l'émergence d'un écosystème numérique militaire fondé sur l'agilité et la fragilité structurelle qui en résulte. Elle analyse enfin la cyberattaque du 24 février 2022 dans ses dimensions chronologique, technique et institutionnelle, avant d'en tirer les enseignements qui serviront de grille de lecture au reste du mémoire.

1. L'héritage soviétique et la rupture stratégique de 2014

À la veille de l'invasion russe à grande échelle de 2022, les forces armées ukrainiennes (FAU) présentent un profil de communication hétérogène. Trois facteurs l'expliquent : trois décennies de sous-investissement, une modernisation tardive et une dépendance à des infrastructures sur lesquelles Kiev n'a aucun levier de contrôle.

Le rapport de la RAND Corporation^{xl} rappelle le poids de cet héritage. Après 1991, l'Ukraine indépendante conserve la doctrine, l'organisation et le matériel de l'armée soviétique. Les transmissions des forces terrestres continuent de reposer sur des lignes au sol héritées de cette période.

Ce dispositif combine un réseau filaire fixe et des moyens tactiques mobiles, dont le vieillissement diverge. L'infrastructure fixe continue de fonctionner sans être remplacée : elle est durable en exploitation, mais elle expose les réseaux militaires, y compris les échelons de commandement supérieurs, aux ruptures d'alimentation

électrique. Le parc de postes radio, soumis à l'usure, aux pertes et à l'obsolescence, s'érode sans être remplacé, faute d'investissement.

Le facteur humain aggrave ce retard. Les cadres des FAU, formés à l'époque soviétique ou dans les premières années de l'indépendance, privilégient les systèmes qui leur sont familiers. Les équipements plus récents demeurent largement non testés en conditions opérationnelles.^{xli}

Il faudra attendre 2014 et la fin de l'invasion de la Crimée par la Russie pour que de nouveaux moyens de communication soient introduits au sein des FAU. C'est d'abord la société civile, et non l'État ukrainien, qui comble le vide capacitaire en matière de communications directement sur la ligne de contact. En effet, des réseaux de volontaires identifient, financent et acheminent vers les unités combattantes de l'est du pays des équipements de communication commerciaux étrangers face au manque cruel de liaisons entre les troupes.

Le contrôle du satellite KA-SAT est passé progressivement d'un contrôle d'Eutelsat à Viasat, par la création d'une coentreprise en 2016 (Euro Broadband Infrastructure) dont Viasat a racheté la participation restante à Eutelsat en 2021.⁶

L'Ukraine, dont les unités de contact dépendaient de ce réseau depuis sept ans (Crimée), n'est associée ni à la décision ni à la négociation. Dix mois avant l'invasion russe, la couche satellitaire de ses communications tactiques passe ainsi sous propriété américaine par le seul effet d'une opération capitaliste privée.

L'exploitation du segment sol est réalisé par la société Skylogic, filiale d'Eutelsat, opère la partition grand public du réseau KA-SAT, satellite en bande Ka mis en orbite en 2010 par l'opérateur français Eutelsat. Conçus à l'origine pour des usages civils dans des zones rurales mal desservies, ces terminaux se révèlent d'une utilité opérationnelle immédiate. Ils permettent aux unités déployées de maintenir une connectivité internet stable sur la ligne de contact, là où les réseaux mobiles terrestres ont été détruits, brouillés ou simplement saturés.



Image 6 : Antenne Tooway de la société Viasat.

La simplicité de mise en œuvre, la stabilité d'accès à Internet et son utilisation à grande échelle correspondent aux attentes des FAU, qui vont alors en faire un de leurs principaux moyens de communication. Une étude de terrain conduite en 2017 par l'Army Cyber Institute de West Point s'appuie sur des entretiens menés en Ukraine auprès de l'état-major, du ministère de la Défense et de personnels revenus du Donbass. Elle rapporte que le manque de moyens contraignait de nombreux militaires à employer pour le commandement des équipements acquis à titre personnel : téléphones

⁶ KA-SAT est exploité depuis avril 2021 par Viasat (entreprise américaine) suite à un rachat des parts d'Eutelsat

mobiles, postes radio commerciaux et ordinateurs portables. Les personnels interrogés évaluaient la dotation en postes radio à environ un pour trois cent cinquante hommes^{xlii}. Faute de communications militaires durcies et d'infrastructures satellitaires souveraines, les FAU se sont adaptées dans l'urgence en employant des moyens civils pour un usage militaire.

L'adoption du modèle satellitaire n'est pas uniquement dû au manque de matériel au niveau tactique. Le terminal commercial est certes acquérable immédiatement, par des volontaires et hors marché public, quand le renouvellement d'un parc radio suppose un investissement d'Etat. Mais il est aussi jugé plus sûr. L'étude de l'Army Cyber Institute relève que les personnels ukrainiens tenaient les communications par satellite pour moins exposées que la téléphonie mobile et que le réseau filaire. Ce dernier intégrait en effet le dispositif d'interception SORM, hérité de la période soviétique, dont les responsables ukrainiens reconnaissaient qu'il demeurerait vraisemblablement accessible à une manipulation russe^{xliii}.

L'année 2014 révèle ainsi la faiblesse globale des moyens de communications militaires des FAU. Les infrastructures héritées de l'ère soviétique ne suffisent plus à elles seules à mener une guerre et doivent être complétées à marche forcée. Des solutions d'achat sur étagère⁷ comme les terminaux Tooway comblent ce manque. Un produit commercial étranger entre ainsi dans la chaîne de communication militaire ukrainienne

Comme indiqué dans la partie précédente, le maintien du triptyque rapidité, confidentialité et intégrité entraîne un changement de la gouvernance des architectures numériques militaires ukrainiennes. Face à une situation d'urgence, l'Ukraine intègre dans sa chaîne de commandement un service privé (et non militaire) dont elle ne maîtrise ni la propriété, ni les conditions de continuité, ni le régime juridique.

L'opérateur privé est-il alors tenu de garantir la disponibilité du service en cas de crise ? Quelles sont ses obligations envers un client devenu belligérant ? La gouvernance du numérique change de nature dans la guerre de 2014 et prépare la séquence de 2022. Elle installe un précédent selon lequel une couche critique des communications ukrainiennes peut relever d'un fournisseur privé étranger sans que la question de la propriété du moyen ne soit posée.

2. L'émergence d'un écosystème numérique militaire

Face à ce changement de gouvernance, les Ukrainiens ne restent pourtant pas inactifs. Privés des moyens d'une autonomie satellitaire, ils s'appuient sur les terminaux disponibles et sur la connectivité qu'ils procurent pour numériser rapidement la conduite des opérations. Deux applications développées lors du conflit en Crimée illustrent ce propos : Kropyva et Delta.

⁷ C'est-à-dire acheter un produit directement prêt à l'emploi sans passer par des phases de conception et intégration. Le prêt à porter du matériel.

Kropyva, dont le nom signifie ortie en ukrainien, est une application de cartographie permettant de marquer une position ennemie. L'application identifie les pièces d'artillerie à portée et coordonne leurs tirs. Ainsi apparentée à un logiciel d'artillerie, Kropyva améliore la précision du ciblage et réduit jusqu'à dix fois le délai entre la réception des ordres et la frappe des cibles. Les artilleurs y accèdent depuis une tablette ou un téléphone mobile et saisissent les coordonnées de l'ennemi. Celles-ci sont transmises automatiquement à la batterie disponible la plus proche, accompagnées des trajectoires de tir pré-calculées.



Image 7 : Soldat ukrainien marquant une position ennemie via l'application Kropyva.

C'est l'organisation de bénévoles nommée Army SOS qui a développé Kropyva en 2014, et 90 à 95 % des unités d'artillerie ukrainiennes l'ont par la suite adoptée comme système principal de conduite de tir^{xliv}. L'innovation, couplée aux terminaux satellitaires avec accès à Internet, est ici poussée par des civils plutôt que structurée par l'état ukrainien.

De façon similaire, l'application Delta, qui agrège des informations de sources hétérogènes pour fournir une image opérationnelle commune, servira rapidement de situation tactique de référence pour les centres de commandement des FAU. Delta agrège les flux de drones, les données issues des médias sociaux et l'imagerie satellitaire en un système d'infovalorisation poussé. Le commandement ukrainien y gagne en capacité de planification et de ciblage^{xlv}.

Delta a là encore été développée par *Aerorozvidka*, un groupe de volontaires d'abord civils puis intégrés aux forces armées. Le projet a débuté en 2016 puis a été transféré au ministère de la défense ukrainienne en 2023 et intègre désormais certains standards de l'OTAN. Là encore, l'innovation est issue du monde civil et apporté au milieu militaire, avec un succès certain.

Entre 2014 et 2022, l'Ukraine a ainsi développé pas moins de onze nouveaux systèmes d'info-valorisation au combat grâce à des innovations issues de personnels de la société civile, en lien direct avec les armées. L'approche ukrainienne s'inscrit en rupture avec les doctrines occidentales contemporaines, où

de tels systèmes sont traditionnellement pensés, testés et mis en place par des politiques publiques.

C'est le cas notamment du programme américain du Joint All-Domain Command and Control (JADC2) dont la stratégie est rendue publique par le Département de la Défense en mars 2022 et qui ambitionne de connecter en temps réel l'ensemble des capteurs, décideurs et acteurs de tous les domaines opérationnels, toutes armées comprises. Cette stratégie américaine assume explicitement l'objectif de fournir un avantage informationnel à travers une coordination intégrée et globale entre tous les capteurs militaires, américains et alliés. L'urgence d'une telle architecture se justifie alors par les capacités croissantes des compétiteurs stratégiques des États-Unis que sont la Chine et la Russie^{xlvi}. C'est ici la politique publique et des programmes d'investissement colossaux qui sont à l'oeuvre.

L'écosystème militaire numérique ukrainien fait un réel bond technologique en profitant de l'agilité et de la frugalité des moyens employés. Les produits grand public détournés de leurs usages initiaux comme les terminaux satellitaires Tooway, conçus rappelons-le pour la desserte de zones rurales mal couvertes, ou les applications d'info-valorisation couplées à l'IA⁸ élèvent le numérique au centre de la guerre.

Cette politique ukrainienne répond aux impératifs économiques du moment. Mais elle a aussi le défaut structurel de transférer dans la sphère privée la maîtrise des fondamentaux de la guerre numérique. Kropyva et Delta, pour ne citer qu'elles, partagent en effet une faiblesse commune : leur fonctionnement est entièrement conditionné à la disponibilité d'une connexion internet stable. Cette dernière repose sur des infrastructures satellitaires dont l'Ukraine ne maîtrise ni la propriété, ni l'exploitation, ni la sécurisation comme nous le verrons par la suite.

Une rupture de la couche de transport, qu'elle soit du fait d'une attaque cinétique, d'une cyberattaque ou simplement de nature contractuelle, neutralise instantanément l'ensemble de la couche applicative. La modernisation ukrainienne est donc jusqu'en 2022 une numérisation sans souveraineté. Ce recours à un produit non souverain est justifié par l'urgence, mais jamais assorti d'un cadre contractuel clair alors que la technologie gagne en importance sur le terrain. C'est cette absence de cadre, et non le recours initial au produit Tooway, qui produit la vulnérabilité.

3. La fragilité d'un système numérisé mais non souverain

Parallèlement à cette modernisation militaire, la société ukrainienne engage une numérisation accélérée à la suite de la révolution de Maïdan et des réformes de gouvernance électronique du gouvernement Zelensky et de son ministre Fedorov.

En 2023, 63 % des Ukrainiens déclarent ainsi utiliser régulièrement les services en ligne de l'état, un chiffre en hausse pour la troisième année consécutive selon le

⁸ Intelligence Artificielle

Programme des Nations Unies pour le Développement^{xlvii}. Cette numérisation civile intense crée une dépendance structurelle à la connectivité Internet pour l'ensemble des fonctions régaliennes, qu'il s'agisse de l'administration, des services d'urgence, du transport ou de la communication gouvernementale. Elle redouble ainsi la vulnérabilité militaire et brouille la frontière entre infrastructure civile et infrastructure de défense, devenues parfois indissociables dans la guerre à venir.

À l'automne 2021, alors que la Russie masse ses troupes aux frontières, le gouvernement ukrainien et ses services de sécurité s'interrogent sur une tentative russe de couper les communications ukrainiennes dès les premières heures d'une offensive. Cette prise de conscience ne débouche cependant sur aucune diversification de la couche satellitaire. Au matin du 24 février 2022, la couche satellitaire du dispositif ukrainien repose en quasi-totalité sur une seule infrastructure commerciale étrangère, et avec elle l'ensemble des systèmes numériques civils et militaires qui en dépendent.

Cette dépendance changera uniquement de main en 2022 avec l'apparition de Starlink. Mykhailo Fedorov formalisera publiquement en 2023 cette même dépendance en déclarant au New York Times^{xlviii} : « *Starlink is indeed the blood of our entire communication infrastructure now. This is one of the fundamental components of our success.* »⁹. Le produit Starlink est ici comparé au « sang » de toute l'infrastructure de communication ukrainienne. La formule illustre à elle seule la nature vitale et donc la vulnérabilité du lien établi.



Image 8 : Installation d'un terminal Starlink par un soldat ukrainien en 2022, L'arrivée des équipements permet de rétablir rapidement la connectivité des unités de contact, privées de liaison satellitaire depuis le 24 février. Crédits : « Le Monde »

⁹ Bien sûr que Starlink est le sang de notre système entier de communication, maintenant. C'est une des principales composantes de notre succès.



Focus : Mykhaïlo Fedorov



Né en 1991, il est l'homme central dans la gestion du numérique en Ukraine, ayant notamment occupé les postes suivants :

- En charge de la stratégie de la campagne numérique de Zelensky lors des élections en Ukraine en 2019 ;
- Vice-premier ministre, ministre de la transformation numérique dans le gouvernement Hontcharouk du 29/08/2019 au 04/03/2020 ;
- Vice-premier ministre, ministre de la transformation numérique dans le gouvernement Chmyhal du 04/03/2020 au 17/07/2025 ;
- Premier vice-premier ministre dans le gouvernement Svrydenko, du 17/07/2025 au 14/01/2026 ;
- Ministre de la Défense du 14/01/2026 au 15/07/2026, puis démission.

Il lancera en 2020 l'application gouvernementale Diia, l'application officielle de services publics numériques de l'Ukraine. Elle fonctionne comme une sorte de portefeuille numérique et joue le rôle d'un portail administratif sur smartphone. L'Ukraine s'étant fixée pour ambition de rendre tous les services publics disponibles en ligne, Diia est devenue l'interface principale de cette politique.

Lancée en avril 2023, Brave1 est une initiative publique ukrainienne consacrée aux technologies de défense. Il s'agit d'un écosystème qui fait le lien entre l'armée, l'État, les startups, les ingénieurs et les investisseurs pour faire passer rapidement une technologie du prototype au champ de bataille. Elle a été à l'initiative du ministère ukrainien de la transformation numérique, alors dirigé par Mykhailo Fedorov, avec plusieurs autres institutions de défense et de sécurité.

Drone Line est un programme militaire ukrainien lancé au printemps 2025 à l'initiative du président Volodymyr Zelensky et mis en place par Fedorov, alors ministre de la Défense. Il est devenu l'un des éléments importants de la stratégie de guerre technologique de l'Ukraine. Son objectif est de transformer l'utilisation des drones en un système permanent et structuré de défense le long du front, plutôt que de les utiliser de manière dispersée. C'est une doctrine d'emploi coordonné des drones.

Son rôle central dans la mise en place des politiques liées au numérique en fera l'interlocuteur privilégié de Musk à partir de 2022 et sa nomination au poste de ministre de la Défense - alors qu'il n'a pas de parcours militaire - témoigne du poids du numérique dans le conflit.

4. Le 24 février 2022 : anatomie d'une attaque

a. La chronologie de l'incident dans le cadre de l'offensive

Le 24 février 2022, à l'heure précise où les premières colonnes blindées russes franchissent la frontière ukrainienne, une cyberattaque paralyse le réseau KA-SAT de Viasat. Pour comprendre l'importance de cet incident, il faut le replacer dans la séquence générale de l'opération russe initiale, dont le Royal United Services Institute britannique (RUSI) a livré une reconstitution détaillée dès avril 2022^{xlix}.

Dans les premières heures du 24 février, les radars de défense aérienne ukrainiens commencent à subir un brouillage sévère sur l'ensemble des bandes de fréquence. Plus à l'intérieur du territoire, des radars subissent eux aussi une saturation provoquée par des drones leurres simulant des avions russes¹⁰.

Lorsque les défenses aériennes ukrainiennes s'allument pour engager ces cibles fictives, elles sont attaquées à leur tour. Un spécialiste ukrainien de guerre électronique cité par RUSI résume la perception du moment en déclarant que les forces ukrainiennes pensaient se voir privées de l'ensemble du spectre électromagnétique autour de Kiev. L'attaque initiale, mêlant frappes de missiles balistiques et de croisière, attaques électroniques et raid aéroporté sur Hostomel vise à dégrader simultanément les radars, les communications et les défenses aériennes ukrainiennesⁱ. Rien de nouveau donc : les forces armées de la Fédération de Russie (FAFR) cherchent d'abord à rendre inopérants les systèmes ukrainiens de transmission de l'information, en vue de l'action quasi simultanée des troupes aéroportées et terrestres.

C'est dans ce paysage électromagnétique saturé que la cyberattaque contre Viasat prend toute sa portée. La perte de la couche satellitaire de Tooway prive alors instantanément les unités de contact d'une connectivité Internet qui les rattachait à la chaîne de commandement, dans un moment où l'environnement radio est par ailleurs fortement perturbé. Le ministre Fedorov déclarera au New York Times que des dizaines de milliers d'utilisateurs ukrainiens, dont de nombreuses unités militaires, sont alors brutalement déconnectés de l'accès à Internetⁱⁱ.

L'attaque ne se limite pas à l'Ukraine. Elle rend les modems Viasat KA-SAT inopérants en Ukraine et provoque la perte de communication, pour la surveillance et le contrôle à distance de 5 800 éoliennes Enercon en Allemagneⁱⁱⁱ. Cette contamination européenne involontaire constitue un événement majeur en soi. Elle révèle l'imbrication des infrastructures civiles européennes avec les infrastructures cibles d'un conflit qui se voulait localisé. Elle ouvre, juridiquement et stratégiquement, la question de l'extension du conflit hybride au-delà du théâtre ukrainien et pose, pour les opérateurs européens d'énergies renouvelables mais

¹⁰ Il s'agit des drones E95M. Fabriqué par la société russe ENIKS, ce type de drone est à l'origine un drone-cible aérien : il sert à entraîner les équipages de défense antiaérienne et à tester des radars et des missiles sol-air. Il est utilisé au début du conflit pour faire révéler les défenses anti-aériennes des FAU.

comme plus largement pour les clients de firmes satellitaires, la question de leur vulnérabilité collatérale aux opérations cyber d'un belligérant qui ne les cible pourtant pas spécifiquement.

b. La séquence technique selon Viasat

Selon le communiqué de Viasat du 30 mars 2022, l'attaque se déploie en deux phases. Une première phase consiste en une attaque par déni de service provenant de plusieurs modems¹¹ et d'autres équipements situés physiquement en Ukraine. Cette attaque met temporairement hors ligne les modems KA-SAT. La seconde phase voit la disparition progressive des modems du service Viasat^{liii}.

Une analyse plus poussée révélera ensuite que les attaquants ont en réalité procédé en trois temps. Ils ont d'abord exploité un équipement de connexion à distance mal configuré pour pénétrer le réseau interne de KA-SAT. Ils ont ensuite progressé à l'intérieur de ce réseau jusqu'à atteindre le segment d'administration, celui depuis lequel l'opérateur pilote à distance les modems de ses abonnés. Ils ont enfin utilisé cet accès pour adresser simultanément à un très grand nombre de modems des ordres d'administration en apparence légitimes, mais dont le contenu était destructeur. L'attaque n'a donc reposé sur aucune faille des modems eux-mêmes : elle a détourné contre eux le canal de commande prévu pour leur maintenance. Ces ordres ont écrasé des données essentielles au fonctionnement des modems. Ceux-ci se sont trouvés incapables de se reconnecter au réseau, sans devenir pour autant physiquement inutilisables. Cette distinction explique que la remise en service ait été possible par la suite, au prix d'une intervention sur chaque équipement.

c. AcidRain : l'identification d'une arme

L'enquête technique conduite par les chercheurs Juan Andrés Guerrero-Saade et Max van Amerongen, du laboratoire Sentinellabs, permet d'identifier l'arme employée. Le 15 mars 2022, un fichier suspect est téléversé vers VirusTotal¹² depuis l'Italie sous le nom « ukrop ». Les chercheurs le nomment AcidRain et le caractérisent comme un effaceur de données, programme dont l'unique fonction est de rendre inutilisables les modems et routeurs qu'il infecte.

Conçu pour opérer sans adaptation au matériel visé, il constituait une capacité réutilisable contre d'autres infrastructures de télécommunications. Cette conception générique justifie l'alerte transversale émise ensuite par l'agence américaine de cybersécurité. Les chercheurs relèvent des similitudes de développement avec VPNFilter, campagne d'infection de routeurs attribuée en 2018 par le FBI au gouvernement russe, filiation qui rapproche AcidRain du groupe d'attaquants désigné sous le nom de Sandworm sans que le lien puisse être établi avec certitude. Viasat a confirmé l'emploi d'AcidRain dans l'attaque du 24 février^{liv}.

¹¹ SurfBeam2 et SurfBeam2+ sont des systèmes terrestres ou modem qui permettent la communication avec le réseau satellite.

¹² VirusTotal est un service en ligne qui permet d'analyser des fichiers, des liens (URLs), des domaines et des adresses IP pour détecter des éléments potentiellement malveillants.

La généricité ou la capacité de ce vecteur à fonctionner dans différentes situations pose une question de maîtrise. Un programme conçu pour fonctionner sans adaptation au matériel visé produit des effets au-delà de la cible désignée, comme l'atteste la mise hors service de 5 800 éoliennes en Allemagne. Ces effets se sont produits sur le territoire d'un état membre de l'OTAN sans entraîner de réaction collective.

d. L'attribution officielle américaine via la CISA

L'attribution institutionnelle américaine intervient en deux temps. L'agence américaine de cybersécurité et de sécurité des infrastructures (CISA) et le Bureau fédéral d'investigation (FBI) publient conjointement, le 17 mars 2022, une alerte consacrée au renforcement de la cybersécurité des fournisseurs et des clients de communications par satellite (SATCOM). Cette alerte¹³, émise dans le cadre de la campagne Shields Up, vise à relever le niveau de vigilance des organisations américaines sur la sécurité de leurs réseaux.

Le 10 mai 2022, la mise à jour de l'alerte attribue formellement l'attaque contre le réseau KA-SAT à des acteurs cyber malveillants soutenus par l'État russe¹⁴.

Cette attribution est précieuse à double titre. Premièrement, elle clôt techniquement le débat sur l'origine de l'attaque, là où certaines analyses privées comme celle de SentinelLabs¹⁴ ne pouvaient fournir qu'un faisceau d'indices. Deuxièmement, elle inscrit l'incident dans une qualification d'état à état, donc dans la revendication diplomatique. L'attaque cyber contre Viasat n'est pas, selon la doctrine américaine, l'œuvre d'acteurs non gouvernementaux ou de criminels opportunistes. Elle est une opération étatique russe.

L'alerte de la CISA ne se limite également pas à l'attribution. Elle fournit aux opérateurs et à leurs clients une liste détaillée de mesures de durcissement, parmi lesquelles l'authentification à plusieurs facteurs pour les comptes d'administration, le chiffrement des liaisons satellitaires, l'intégration du trafic satellitaire dans les outils de supervision de sécurité des opérateurs et le déploiement de solutions de détection sur les équipements raccordés en aval des terminaux.

L'attaque sur Viasat fait (tardivement) prendre conscience aux autorités des enjeux liés à la cybersécurité des communications par satellite (SATCOM), y compris dans la gamme non militaire et de la faiblesse de certaines structures. Cette hybridation des ressources et des usages, soit une utilisation de satellites civils au profit d'usagers militaires, se répétera avec Starlink par la suite, amplifiant les enjeux déjà évoqués.

¹³ Il s'agit de l'alerte AA22-076A.

¹⁴ SentinelLabs est la division de recherche en cybersécurité de Sentinelone, entreprise qui commercialise des solutions de cybersécurité.

5. Lecture : l'attaque comme révélateur.

Si Viasat affirme avoir « largement stabilisé » son réseau en quelques heures, la stabilisation complète prend plusieurs jours, pendant lesquels les forces russes progressent significativement en territoire ukrainien. Si l'expert en cybersécurité ukrainien Victor Zhora qualifie initialement l'attaque de perte colossale de communications au tout début de la guerre, il nuance ensuite son propos en soulignant que la coordination entre les forces et entre les dirigeants de l'État et les forces n'avait pas été compromise. Le rapport RAND attribue ce maintien à la dépendance persistante de l'armée ukrainienne aux lignes terrestres plutôt qu'aux satellites pour une part importante de ses communications^{lvi}. Cette nuance impose de distinguer deux couches que l'analyse confond souvent. La couche de commandement stratégique, qui relie les échelons supérieurs entre eux et à l'autorité politique, repose sur les lignes terrestres héritées. Elle survit. La couche tactique de contact, qui relie les bataillons, les compagnies et les points d'appui de pelotons, repose sur Tooway. Elle disparaît.

Cette asymétrie était établie avant la guerre : l'étude de l'Army Cyber Institute relevait en 2017 que les échelons bataillon et supérieurs disposaient d'équipements sécurisés, tandis que les difficultés de communication en dessous de ce niveau demeuraient non résolues^{lvii}. Ce qui s'effondre le 24 février 2022 n'est donc pas la chaîne de commandement ukrainienne, c'est la connectivité de la ligne de contact. Le maintien de la couche stratégique ne constitue pas pour autant une solution de substitution durable. Le réseau terrestre hérité présente trois vulnérabilités que la suite du conflit met successivement en évidence. Il est fixe, donc exposé à la capture à mesure que le territoire est occupé. Il dépend de l'alimentation électrique dont le rapport RAND relevait déjà la criticité pour les échelons de commandement supérieurs^{lviii} et que les frappes russes sur les infrastructures énergétiques prendront pour cible à partir de l'automne 2022. Il est également interceptable par construction.

L'épisode du 24 février 2022 doit être lu comme la matrice opérationnelle du basculement ukrainien vers Starlink. Il révèle, sur le mode négatif, quatre caractéristiques structurelles qui définissent le nouveau régime de communication stratégique en zone de conflit. Ces quatre caractéristiques fournissent la grille d'analyse qui sera utilisée tout au long de la suite du mémoire.

Premièrement, l'asymétrie entre architectures. Le réseau KA-SAT repose sur un satellite unique et sur un segment sol centralisé, dont la compromission d'un seul point suffit à interrompre le service pour l'ensemble des abonnés. Une constellation distribuée en orbite basse ne présente pas ce point de rupture unique. Cette différence explique l'attractivité immédiate de Starlink pour l'Ukraine après le 24 février. Elle ne dit rien, en revanche, de la vulnérabilité des deux systèmes à une décision de leur propriétaire, qui est le sujet des parties suivantes.

Deuxièmement, l'absence de souveraineté de l'utilisateur sur la couche de transport. L'Ukraine, en tant qu'utilisatrice de Tooway, n'avait aucun levier juridique, opérationnel ou contractuel pour empêcher l'attaque ou en accélérer la

résolution. La rapidité de la stabilisation dépendait entièrement de Viasat et des équipes techniques de Skylogic. Cette dépendance, qui transforme tout incident technique en crise diplomatique de fait, est la signature des architectures de communication étrangères opérées en zone de conflit. La bascule de Tooway à Starlink, comme nous le verrons plus tard, ne corrige pas ce défaut. Elle en aggrave la dimension en concentrant la décision opérationnelle dans les mains d'un opérateur unique non ukrainien et non régulé par les mécanismes nationaux.

Troisièmement, la perméabilité juridique et politique entre infrastructure civile et infrastructure militaire. L'attaque contre Viasat vise une infrastructure commerciale civile dont l'usage militaire ukrainien est sans cadre contractuel formalisé. Les 5 800 éoliennes Enercon allemandes affectées ne sont, elles, l'objet d'aucune intention militaire de l'attaquant. La qualification du fait belliqueux devient problématique. S'agit-il d'une attaque contre une infrastructure civile ? D'une attaque contre une infrastructure militaire alliée de fait ? D'un dommage collatéral assumé par l'attaquant ? Cette indétermination est, en soi, un instrument de la guerre hybride russe, dont l'effet est de paralyser la réponse juridique et politique.

Quatrièmement, l'effet de cascade européen. L'incident allemand, par sa portée énergétique et sa dimension transfrontière, ouvre la question de la responsabilité internationale de l'attaquant pour les dommages infligés hors théâtre. Cette dimension, sous-traitée dans le débat public francophone, mérite une attention particulière. Elle indique que la guerre d'origine cyber, par ses effets de cascade, est par nature désinscrite des frontières où elle s'origine. Toute architecture européenne de communication qui n'a pas explicitement intégré cette dimension de cascade dans sa conception est, par construction, vulnérable.

Le service Starlink est activé en Ukraine deux jours après l'invasion, à la suite d'une demande publique adressée de M. Fedorov à Elon Musk^{lix}. Cette substitution ne comble pas un vide absolu, puisque la couche de commandement stratégique a tenu. Elle restaure une couche précise, celle de la connectivité tactique de contact, et elle la restaure selon les mêmes modalités que celles qui prévalaient depuis 2014 : par recours à un opérateur commercial étranger, hors cadre contractuel souverain. La rapidité de cette substitution, présentée publiquement comme un acte de générosité, doit donc être lue non comme la résolution d'une dépendance mais comme sa reconduction, sur une infrastructure dont le degré de concentration décisionnelle est cette fois sans précédent.

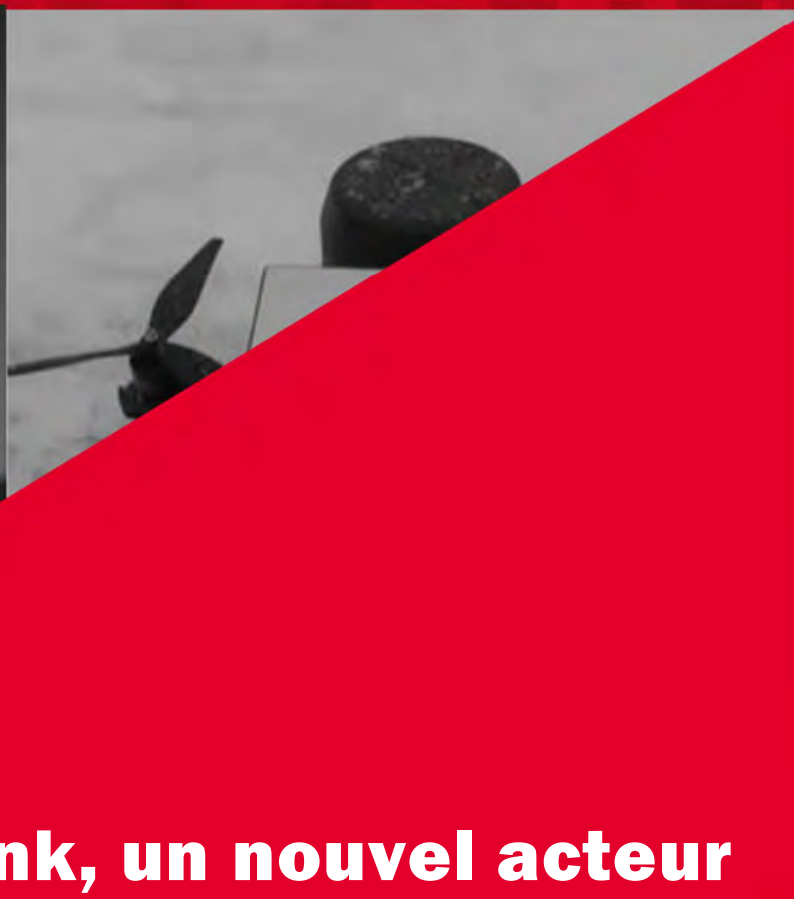
Il permet de comprendre comment Starlink a pu, par structure, par appui, par cout et par simplicité de déploiement, supplanter les infrastructures déjà existantes.

Enseignements :

- Le réseau KA-SAT était vulnérable par son architecture centralisée. La constellation Starlink supprime ce point de rupture unique, mais déplace la vulnérabilité de l'architecture vers la décision de l'opérateur.
- L'État ukrainien confie la couche de transport à un opérateur privé étranger, déléguant ainsi une part de la mise en œuvre de son système de communication.
- L'utilisation de cette technologie duale et transnationale expose les utilisateurs extérieurs au conflit. Une attaque sur un objectif jugé militaire de l'Etat A peut ainsi toucher une infrastructure civile de l'état B.
- Cette attaque peut avoir des répercussions par l'entraînement dans le conflit d'une partie ayant fait l'objet de dommages collatéraux.



Image 9 : Quartier général lors d'un exercice OTAN incluant l'utilisation de DELTA, système ukrainien. Une unité ukrainienne participant à l'exercice NATO REPMUS 2025 a pu montrer les capacités d'un système éprouvé sur le terrain.



II. Starlink, un nouvel acteur et une nouvelle technologie



II. Starlink, un nouvel acteur et une nouvelle technologie

A. « Qui » : M. Musk.

L'objet de cette section est de fournir le portrait d'Elon M. Musk au moment du conflit ukrainien. Il ne s'agit pas d'écrire une biographie pour elle-même, ni de retracer la trajectoire entrepreneuriale d'un homme d'affaires américain parmi d'autres. Il s'agit de comprendre comment un individu privé à la tête d'un conglomérat technologique sans précédent dans l'histoire industrielle contemporaine est devenu dans les faits sinon en droit un acteur puissant. Cette qualification, qui peut paraître excessive à première lecture, sera étayée par les sources disponibles.

La section procède en quatre temps. Elle examine d'abord les origines personnelles de M. Musk dans l'Afrique du Sud de l'apartheid et le contexte familial dans lequel il se construit. Elle reconstitue ensuite la formation de sa doctrine implicite, où le libéralisme technophile cohabite avec une dépendance assumée à la commande publique. Elle expose la fonction de SpaceX et de Starlink dans le projet civilisationnel martien qu'il déclare poursuivre. Elle cartographie ses intérêts économiques et géopolitiques au moment du conflit ukrainien, intérêts dont la nature interdit de le traiter comme un acteur neutre.

Une précaution s'impose sur les sources. Le matériau biographique et psychologique de cette section provient pour l'essentiel de la biographie qu'Isaacson consacre à M. Musk en 2023, ouvrage fondé sur deux années d'accès direct à ce dernier et à son entourage. Cet accès en fait la source la plus documentée disponible et en constitue la limite. Les éléments factuels, dates, montants et opérations capitalistiques sont vérifiables par ailleurs et traités comme établis. Les déclarations rapportées sont fiables quant à leur énonciation, non quant à leur contenu. Les interprétations qui en sont tirées ici relèvent de la lecture et sont signalées comme telles.

1. Enfance et arrivée en Amérique

Elon Reeve Musk naît le 28 juin 1971 à Pretoria, Afrique du Sud, dans une famille marquée par des tensions profondes et dans un pays alors structuré par l'apartheid. Sa mère, Maye Haldeman, est mannequin et diététicienne d'origine canadienne. Son père, Errol Musk, est ingénieur et homme d'affaires, élu au conseil municipal de Pretoria sur une liste anti-apartheid en 1972. M. Musk grandit, avec son frère cadet Kimbal et sa sœur cadette Tosca, sous le régime d'apartheid.^{ix}

La famille maternelle est elle-même marquée par une trajectoire d'aventure et de migration qui structurera durablement l'imaginaire familial de M. Musk. Le grand-père maternel, Joshua Haldeman, ostéopathe de profession, émigre du Canada vers l'Afrique du Sud en 1950, en partie par hostilité aux institutions internationales et au libéralisme nord-américain. Cette généalogie est utile à signaler. Elle situe le

contexte idéologique dans lequel M. Musk grandit, mélange d'anti-étatisme et de fascination pour la frontière, qui sera redéployé plus tard dans la rhétorique martienne. Son père et sa mère divorcent quand Elon est jeune et les enfants restent initialement avec la mère^{lxi}.

L'environnement familial donne des éléments de contexte sur la façon dont M. Musk se construit. Sa mère a déclaré que le père faisait régulièrement preuve de violence physique envers elle, parfois en présence de ses enfants. À l'âge de dix ans, Elon prend la décision de quitter sa mère pour aller vivre chez son père à Pretoria. Il qualifiera plus tard cette décision de très mauvaise idée, déclarant que son père l'avait torturé psychologiquement. Ce dernier a réfuté l'ensemble des accusations^{lxii}.

Deux traits personnels complémentaires semblent ressortir des éléments biographiques qui l'entourent. Le premier est le syndrome d'Asperger, forme de trouble du spectre autistique caractérisée par des difficultés d'interaction sociale, que M. Musk a indiqué présenter, sans toutefois la moindre preuve médicale présentée. Le second est un intérêt pour la science-fiction et les jeux vidéo, qu'il désignera plus tard comme la raison principale de son orientation vers la technologie.^{lxiii}

Ces éléments biographiques ne suffisent pas à expliquer les décisions prises plus tard. Ils situent en revanche une posture dont la constance est, elle, documentée : l'arbitrage personnel semble primer sur le conformisme institutionnel.

L'émigration constitue le second moment fondateur. À dix-sept ans, il quitte seul l'Afrique du Sud pour le Canada, après avoir refusé le service militaire dans l'armée du régime d'apartheid. Il rejoint ensuite l'Université de Pennsylvanie, où il obtient deux licences, en économie et en physique. Il commence un doctorat à Stanford qu'il abandonne deux jours après son arrivée, et fonde avec son frère Kimbal l'entreprise Zip2 en 1995. Celle-ci est revendue à Compaq Computer en 1999 pour 307 millions de dollars, dont 22 millions lui reviennent personnellement. La même année, il fonde X.com, société de paiement en ligne, qui fusionne avec Confinity, cofondée par Peter Thiel, pour devenir PayPal. Cette dernière est rachetée par eBay en juillet 2002 pour 1,5 milliard de dollars, dont environ 250 millions reviennent à Elon en tant que principal actionnaire.^{lxiv}

Ces deux opérations le dotent d'un capital initial qui constituera le fonds d'amorçage de SpaceX, dont la généalogie financière est traitée ultérieurement. Le réinvestissement quasi intégral de cette fortune dans un projet à haut risque, plutôt que sa sécurisation par diversification, indique dès cette période qu'il fait passer le projet industriel avant la sécurité patrimoniale.

2. Doctrine libertarienne et commande publique

La période californienne, entre 1995 et 2002, aurait façonné sa façon de penser, mélange de libertarisme antibureaucratique et de dépendance pragmatique à la commande publique. La séquence X.com et PayPal en constitue un élément important.

Il fonde X.com en 1999, mais l'investisseur principal lui retire la direction générale la même année au profit d'un dirigeant expérimenté. Après la fusion avec Confinity en mars 2000, il reprend ce poste en écartant celui qui l'occupait. En septembre 2000, alors qu'il se trouve à l'étranger, le conseil d'administration le démet à son tour au profit de Peter Thiel. M. Musk aura donc, en moins de deux ans, perdu deux fois la direction d'une entreprise qu'il avait fondée, par décision d'un conseil et sans y avoir pris part^{lxv}.

L'idéologie associée à Elon Musk éclaire l'évolution du rapport de force entre États et entreprises technologiques. Selon l'IRIS, il est rattaché à un courant qualifié de libertarianisme autoritaire, aux côtés d'acteurs majeurs de la Silicon Valley comme Peter Thiel ou David Sacks, tous deux issus de l'épisode PayPal. Sans s'en revendiquer explicitement, Musk a évolué dans cet environnement et en partage plusieurs conceptions^{lxvi}.



Image 10: Peter Thiel en 2014. Homme d'affaires d'origine allemande et libertarien déclaré.

Ce courant se caractérise par une conception restrictive du rôle de l'État aux fonctions régaliennes essentielles, telles que la sécurité et la protection de la propriété privée, au profit d'un élargissement du rôle des acteurs privés. Il s'accompagne d'une confiance marquée dans la capacité de la technologie à résoudre des problématiques complexes, approche souvent qualifiée de techno-solutionnisme, concept développé notamment par Alvin M. Weinberg. Cette vision est également défendue par plusieurs figures de la Silicon Valley, comme Marc Andreessen ou David Sacks^{lxvii}.

Sur le plan doctrinal, ces orientations s'inscrivent dans une filiation avec les théories de Milton Friedman¹⁵ qui promeut un libre marché étendu et une intervention minimale de l'État. Certaines prises de position publiques d'Elon Musk, notamment sa référence à M. Friedman^{lxviii} lors de débats sur les politiques commerciales américaines, illustrent cette proximité intellectuelle.

Sans constituer une adhésion formelle à un corpus structuré, ces positions s'inscrivent dans une dynamique de redéfinition du rôle de l'État, où les infrastructures privées occupent une place croissante. Cette évolution est particulièrement visible dans le cas de Starlink, dont l'usage dans des contextes stratégiques interroge directement la souveraineté des États.

Cette position prend chez Elon une dimension téléologique¹⁶ qui la distingue du libertarianisme classique de la Silicon Valley. L'État n'y est pas seulement inefficace : il est un obstacle à ce qu'il présente comme la mission de l'humanité, à savoir sa propre préservation par son établissement sur plusieurs planètes. Il déclare que la survie de la conscience humaine dépend de sa capacité à quitter une planète unique, exposée à un impact d'astéroïde ou à sa propre destruction, et désigne la sortie de

¹⁵ Et dans une version plus radicale, de Murray Rothbard.

¹⁶ Qui relève de la téléologie, c'est-à-dire l'étude des fins, du but ou de la finalité

l'orbite terrestre comme la prochaine étape évolutive majeure. Quelle que soit la sincérité de cette finalité, elle structure les arbitrages de l'entreprise ^{lxx}.

Cette téléologie est présentée comme l'opérateur central de la cohérence des décisions de M. Musk. Reid Hoffman, qui s'interrogeait sur la viabilité économique du projet martien décrit le mécanisme à l'œuvre : M. Musk part d'une mission, puis cherche le moyen de la financer pour qu'elle tienne économiquement. Là où une entreprise classique sélectionne ses missions selon leur rentabilité espérée, M. Musk sélectionnerait les rentabilités selon leur compatibilité avec ce qu'il estime être sa mission. ^{lxx}

Les implications pour les États clients ne sont pas neutres. Lorsqu'un État souscrit au service Starlink, il finance une entreprise dont la finalité déclarée n'est pas la fourniture du service, mais le financement d'un projet spatial privé.

Le rapport de Musk à la commande publique américaine est contradictoire dans les énoncés, cohérent dans les pratiques. Il dénonce publiquement les inefficacités de l'État fédéral, en particulier sous l'administration Biden, tout en captant les contrats les plus rémunérateurs de la NASA, de la Space Force et du Département de la Défense. Sam Altman¹⁷, concurrent, résume la posture : Musk veut que le monde soit sauvé, mais à condition d'en être le sauveur. Ce dernier accepte le financement public sans en accepter la tutelle, ce qui se vérifiera dans le dossier ukrainien par une certaine réticence à se coordonner avec le Pentagone. ^{lxxi}

3. SpaceX et Starlink : des instruments au service d'une vision.

Avec le produit de la vente de PayPal, Musk fonde Space Exploration Technologies, SpaceX, en mai 2002. Il en est président-directeur général et ingénieur en chef. Le projet déclaré est de rendre l'humanité multiplanétaire en colonisant Mars, en réduisant le coût d'accès à l'espace grâce à des lanceurs réutilisables. ^{lxxii}

Le formulaire ¹⁸ déposé en mai 2026 auprès de la Securities and Exchange Commission, le régulateur boursier américain, énonce comme objectif ultime l'établissement d'une présence humaine autonome sur d'autres planètes, et décrit Starship comme le véhicule destiné à acheminer vers Mars les personnes, les équipements et les fournitures nécessaires à des implantations permanentes. ^{lxxiii}

Starlink est conçu comme l'instrument de financement de Starship, lui-même conçu comme l'instrument du voyage vers Mars. La constellation n'est donc pas une fin en soi : elle doit générer les revenus nécessaires aux ambitions d'Elon Musk. SpaceX met en orbite les charges utiles de ses clients, ce qui dégage des profits. Ces profits financent les lancements dédiés à Starlink. Les abonnements Starlink génèrent enfin des revenus récurrents, que SpaceX déclare vouloir affecter au développement de ses lanceurs et à ses objectifs d'exploration spatiale. ^{lxxiv}

¹⁷ Fondateur d'OpenAI.

¹⁸ Le formulaire S-1 est un document officiel expliquant l'objectif de l'entreprise déposé auprès du régulateur boursier.

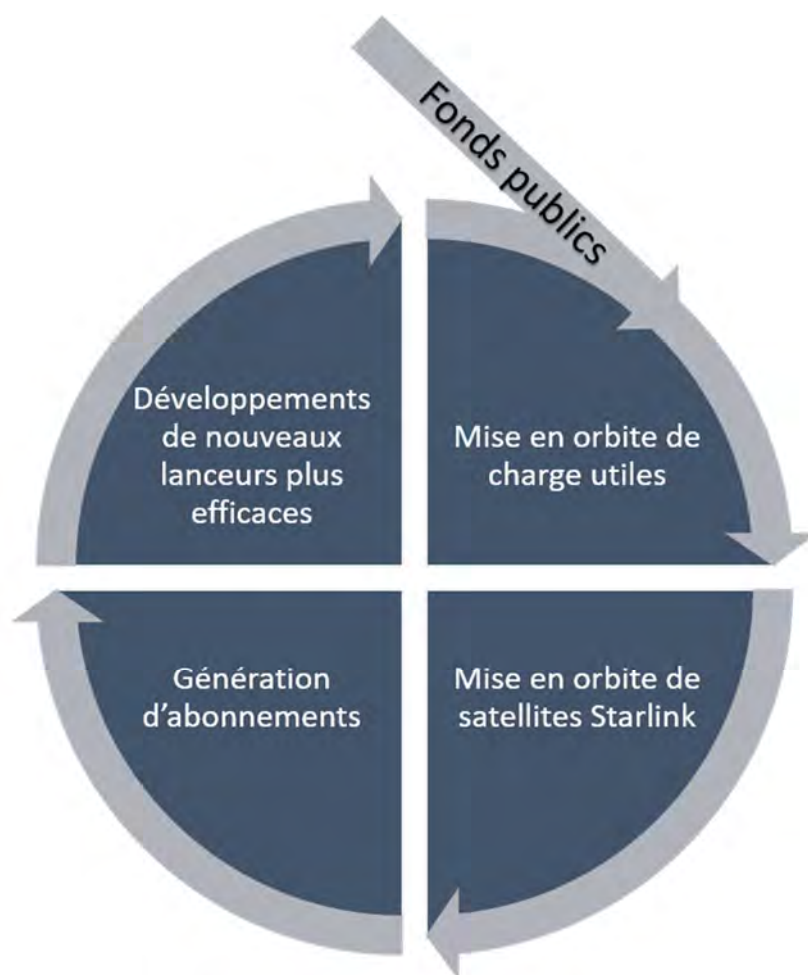


Figure 2 : Schéma de financement SpaceX et Starlink

Ce schéma éclaire la nature de l'engagement de SpaceX en Ukraine. Lorsque Starlink y est déployé en février 2022, l'opération n'est pas seulement un soutien à un État allié. C'est aussi une vitrine pour un produit dont la rentabilité doit financer une mission spatiale plus large.

4. Cartographie des intérêts au moment du conflit ukrainien

Elon Musk évolue, au moment du conflit ukrainien, dans un ensemble d'intérêts économiques et politiques distincts de ceux des États qui dépendent de son service. En dresser la carte permet de comprendre pourquoi aucun belligérant ni aucun allié ne peut le traiter comme un acteur neutre. Deux de ces intérêts sont contemporains du déploiement de février 2022 : l'exposition industrielle chinoise et les contacts avec la diplomatie russe. Deux autres lui sont postérieurs et relèvent d'une accumulation de leviers : le rachat de Twitter¹⁹ en octobre 2022 et la nomination au DOGE²⁰ fin 2024.

¹⁹ Renommé X en 2023

²⁰ Département de l'Efficacité gouvernementale (DOGE)



Figure 3 : Un résumé visuel des intérêts d'Elon Musk.

Le premier intérêt auquel il est exposé est chinois. Une usine de Shanghai produit en effet la moitié des véhicules Tesla^{lxxv} qui dépend de la bienveillance des autorités chinoises pour la production. La Chine soutenant par ailleurs la Russie dans le conflit, cela aura un impact concret lors de l'épisode de Sébastopol décliné par la suite. M. Musk^{lxxvi} a également reconnu publiquement que Pékin désapprouve sa décision de fournir un service Internet à l'Ukraine et lui a demandé l'assurance qu'il ne déploierait pas une technologie comparable en Chine. La couverture géographique de Starlink ne relève donc pas de la seule technique, mais aussi de contrainte géopolitique.

Le second intérêt est russe. Lors d'un appel téléphonique d'octobre 2022 entre M. Musk et le sous-secrétaire à la Défense américain, ce dernier indique avoir eu des échanges réguliers avec l'ambassadeur russe, qui l'aurait averti que l'attaque de la Crimée constituerait une ligne rouge susceptible d'entraîner une réponse nucléaire.^{lxxvii}

Cette diplomatie privée appelle plusieurs observations stratégiques. Premièrement, elle est conduite hors de tout mandat institutionnel. M. Musk n'est ni diplomate, ni représentant d'un État, ni mandaté par une instance internationale. Il agit en sa qualité d'acteur économique privé exerçant une diplomatie de fait. Deuxièmement, le canal russe est unidirectionnel. M. Musk reçoit des messages de l'ambassade russe et les transmet, sans contrôle de leur authenticité ni de leur portée, à des décideurs américains. Il devient ainsi, fonctionnellement, un canal de communication entre Moscou et Washington, en dehors des voies diplomatiques officielles. Troisièmement, l'asymétrie de traitement est manifeste : M. Musk parle aux Russes au plus haut niveau, mais s'adresse aux Ukrainiens à travers son personnel technique ou des messages directs au vice-Premier ministre.

Le troisième intérêt est la concentration médiatique avec X. La prise de contrôle de la plateforme en octobre 2022, pour 44 milliards de dollars, place sous le contrôle

d'un même acteur privé l'infrastructure de communication militaire d'un État en guerre et l'une des principales plateformes d'information de l'espace occidental.

La nomination à la tête du DOGE en 2024. Nommé à la tête du Department of Government Efficiency par Donald Trump fin 2024, Musk se trouve en position d'arbitre de l'efficacité budgétaire des agences fédérales, dont plusieurs sont clientes de SpaceX. Le principal fournisseur d'infrastructure spatiale du gouvernement américain devient ainsi arbitre du budget de ses propres clients.

Les deux premières positions pèsent sur les arbitrages de 2022. Les deux suivantes documentent une accumulation de leviers dont la partie III examinera les effets.

Enseignements :

- Au moment du conflit SpaceX est une société non cotée dont le fondateur conserve le contrôle. Aucun contre-pouvoir actionnarial, aucune obligation de publication ne vient encadrer une décision de déploiement, de restriction ou de désactivation du service.
- Starlink n'est pas une fin mais un étage de financement du programme Starship. Sa viabilité commerciale prime donc sur les besoins opérationnels du client.
- Les intérêts de Musk ne sont pas alignés sur ceux de son client. Son exposition industrielle chinoise et ses contacts directs avec la diplomatie russe interdisent de le traiter comme un acteur neutre.

B. « Comment » Starlink est devenu un monopole de fait

L'objet de cette section est d'éclairer la question centrale du dossier Starlink, qui n'est pas d'abord celle de son déploiement en Ukraine, mais celle de son existence même. Comment une entreprise privée a-t-elle pu accumuler, en moins de deux décennies, une infrastructure spatiale dont la capacité opérationnelle excède celle de plusieurs États souverains réunis, sans clientèle commerciale préexistante de taille comparable et sans cadre réglementaire spécifique ? La réponse à cette question, qui détermine la nature du pouvoir détenu par M. Musk au moment du conflit ukrainien, exige de remonter à la généalogie financière de SpaceX et de Starlink, puis d'examiner les mécanismes d'occupation orbitale et de capture institutionnelle qui ont permis la constitution d'un monopole de fait.

La section procède en six temps. Elle examine d'abord les capitaux initiaux personnels qui ont permis l'amorçage de SpaceX entre 2002 et 2008. Elle reconstitue ensuite le tournant de 2008, où la conjonction d'un sauvetage privé par le Founders Fund²¹ et d'un contrat NASA²² de 1,6 milliard de dollars transforme une start-up au bord de la faillite en partenaire stratégique du gouvernement américain. Elle documente la consolidation, à partir de 2014, de la dépendance gouvernementale assumée et publiquement critiquée par les responsables eux-mêmes. Elle expose la structure financière de Starlink comme instrument de financement de la mission martienne. Elle examine les mécanismes d'occupation orbitale et spectrale qui transforment l'avance de SpaceX en barrière à l'entrée

²¹ Société d'investissement en capital risque fondé par Peter Thiel.

²² L'administration nationale de l'aéronautique et de l'espace (USA)

durable, à travers la décision de la Commission fédérale des communications (Fédéral Communications Commission), l'ordre FCC 22-91 de décembre 2022 et de l'enquête Foust de 2023. Elle conclut par une grille de lecture en intelligence économique qui qualifie précisément les trois mécanismes de capture à l'œuvre.

1. La genèse de SpaceX : capital privé et risque assumé

La fondation de SpaceX en mai 2002 est financée sur les capitaux personnels de M. Musk, qui anticipe la cession imminente de PayPal à eBay, annoncée en juillet 2002 et finalisée en octobre 2002 pour un montant total de 1,5 milliard de dollars dont environ 250 millions lui reviennent personnellement ^{lxxviii}. Sur cette dotation, M. Musk investit approximativement 100 millions de dollars dans le développement de la fusée Falcon 1, le reste étant alloué à Tesla ^{lxxix}.

Cette concentration de risque personnel sur deux entreprises à capital intensif et à risque technologique extrême, SpaceX et Tesla, est, en soi, une anomalie dans l'écosystème entrepreneurial. M. Musk a engagé l'essentiel de sa fortune dans deux paris industriels, plutôt que de la sécuriser par diversification. Ce modèle financier se définira par l'absence de levier institutionnel précoce et par un haut degré d'engagement personnel du fondateur.

Lors des différentes campagnes de financement, il était attendu que Space X, alors en difficulté financière, soit en faillite. Une anomalie de valorisation entre deux cycles de financement laisse entendre une intervention extérieure à Space X ^{lxxx}. Le sauvetage vient d'abord d'un investissement privé. Le Founders Fund, créé par Peter Thiel, Ken Howery et Luke Nosek, anciens cofondateurs de PayPal, accepte d'investir 20 millions de dollars en juillet 2008, juste après l'échec du troisième lancement de sa fusée réutilisable ^{lxxxi}. Cette opération fait office de bouée de sauvetage qui permet à M. Musk d'envisager un quatrième lancement couronné de succès.

La première hypothèse est celle de la réparation personnelle entre anciens de PayPal. Peter Thiel a reconnu publiquement, dans plusieurs entretiens ultérieurs, qu'une partie de son raisonnement consistait à corriger l'éviction de M. Musk de la direction de PayPal en 2000 ^{lxxxii}. La seconde hypothèse est celle d'une confiance maintenue dans le projet industriel malgré les trois échecs. Le choix d'investir aux conditions de 2007 indique que Founders Fund croyait à la viabilité technique du projet et anticipait sa rentabilité (Les négociations avec la NASA pour un contrat *Commercial Resupply Services*²³ étaient en cours depuis 2006).

Ces deux hypothèses ne s'excluent pas mutuellement. Elles ont vraisemblablement pesé toutes les deux dans des proportions que les sources publiques ne permettent pas d'établir. Ce qui peut être affirmé sans réserve, en revanche, est la portée de l'opération. Le tour de table de juillet 2008 installe au capital de SpaceX un noyau d'investisseurs idéologiquement alignés sur la vision libertarienne de M. Musk. Ce noyau recoupe l'écosystème politique qui portera Donald Trump à partir de 2016

²³ Services commerciaux de ravitaillement

puis J. D. Vance à partir de 2024, par l'intermédiaire de l'engagement personnel de Peter Thiel.

À cet investissement institutionnel s'ajoutent, dans la même séquence, plusieurs contributions personnelles documentées par M. Isaacson. Bill Lee, un ami de M. Musk, investit 2 millions de dollars. Sergey Brin, cofondateur de Google, investit 500 000 dollars en chèque personnel. Antonio Gracias, ami et associé de M. Musk, prête un million de dollars. Jeff Skoll, premier président d'eBay, apporte également un soutien financier. Des employés de Tesla signent eux aussi des chèques de soutien^{lxxxiii}. Cette mobilisation du réseau personnel, combinée aux apports du Founders Fund, finance le quatrième lancement de Falcon 1, qui réussira le 28 septembre 2008.

Ce succès opérationnel conditionne toute la séquence ultérieure. Il ouvre l'accès au contrat NASA de décembre 2008, qui transforme la trajectoire de l'entreprise et constitue la seconde source du sauvetage. Ce contrat rend possible le financement de la constellation Starlink, à laquelle l'Ukraine aura recours en 2022. La trajectoire qui conduit un opérateur privé au cœur des communications militaires ukrainiennes tient donc, à son point d'origine, à un sauvetage in extremis par un cercle restreint d'investisseurs.

2. NASA, le tournant de la commande publique

Le 22 décembre 2008, trois mois après le quatrième lancement réussi de Falcon 1,



Image 11 : Lori Garver, fonctionnaire américaine et responsable de la National Aeronautics and Space Administration de 2009 à 2017.

Bill Gerstenmaier, chef du vol spatial de la NASA et qui rejoindra plus tard SpaceX, annonce à M. Musk par téléphone que SpaceX va recevoir un contrat de 1,6 milliard de dollars pour effectuer douze allers-retours vers la Station spatiale internationale^{lxxxiv}. Le contrat lui-même, attribué le 23 décembre 2008 dans le cadre du programme Commercial Resupply Services, constitue le pivot de la trajectoire financière de SpaceX. Il transforme une start-up au bord de la faillite en partenaire essentiel de l'agence spatiale américaine, avec une visibilité budgétaire pluriannuelle.

Le contexte politique de cette décision mérite une attention particulière. Lori Garver²⁴, qui sera nommée administratrice adjointe de la NASA en juillet 2009 et qui était alors membre de l'équipe de transition d'Obama

²⁴ Avec 2744 jours de mandat, elle détient à ce jour la plus longue occupation du poste de responsable-adjoint de la National Aeronautics and Space Administration.

sur les questions spatiales, tentait depuis 2008 de convaincre le candidat démocrate que l'approche américaine de la construction de fusées devait changer. La NASA prévoyait de mettre fin au programme Space Shuttle et espérait le remplacer par un nouveau programme appelé Constellation, géré de manière traditionnelle par attribution de contrats à l'United Launch Alliance Lockheed-Boeing. Mais le coût projeté avait plus que doublé et le programme était loin d'être achevé. Garver recommanda à Obama d'abandonner Constellation et de permettre plutôt à des entreprises privées, telles que SpaceX, de développer des fusées pouvant emmener des astronautes dans l'espace ^{lxxxv}.

Le choix politique de l'administration Obama, en supprimant Constellation fin 2009, opère un transfert massif de capacité industrielle du secteur public et de ses partenaires historiques vers une entreprise privée encore non éprouvée. La raison en est un échec de programme public, dont les surcoûts et les retards créent une fenêtre politique d'opportunité. Cette fenêtre est accompagnée d'un plaidoyer interne par une figure légitime de l'agence, Lori Garver, et d'un climat d'innovation technologique favorable qui valorise la rupture comme méthode. Cette combinaison crée les conditions d'un transfert de capacité que des circonstances normales n'auraient pas permis.

Le résultat opérationnel est sans précédent. En 2020, SpaceX effectue sa première mission habitée vers la Station spatiale internationale, mettant fin à près d'une décennie de dépendance américaine vis-à-vis des engins russes pour cette tâche. SpaceX lance désormais plus de satellites que toute autre entreprise privée, avec 4 519 en orbite en juillet 2023, occupant un grand nombre des routes orbitales terrestres ^{lxxxvi}.

La substitution de SpaceX à Roscosmos pour le transport des astronautes américains, dans un contexte de tensions géopolitiques croissantes avec Moscou, constitue une opération de réduction de dépendance interétatique au prix d'une augmentation de la dépendance public-privé. L'État américain s'est libéré d'une dépendance à un État adversaire au prix d'une dépendance à un acteur privé qui, contrairement à un sous-traitant traditionnel structurellement aligné sur la commande publique, conserve une marge d'autonomie significative dans ses arbitrages opérationnels. Cette marge sera précisément ce qui pose problème en Ukraine quatorze ans plus tard.

La séquence de contrats publics ne s'arrête pas en 2008. À partir de 2014, SpaceX remporte des contrats successifs avec l'US Air Force puis la Space Force. Le programme Starshield, dévoilé en 2022, formalise la dualité civile et militaire de la constellation. Il s'agit de la déclinaison gouvernementale de Starlink : les mêmes satellites de série, dotés d'un chiffrement renforcé et capables d'embarquer des équipements fournis par les agences clientes. En septembre 2023, SpaceX signe son premier contrat avec la Space Force au titre de Starshield, pour 70 millions de dollars ^{lxxxvii}. La consolidation du modèle dual a, depuis 2008, transformé un opérateur privé en pilier de l'architecture spatiale du gouvernement américain.

3. Une dépendance gouvernementale assumée et critiquée

L'examen de l'écosystème institutionnel autour de SpaceX révèle, en 2022 et a fortiori en 2023, une dépendance gouvernementale assumée et qui est publiquement critiquée par les responsables gouvernementaux. Cette critique publique mérite d'être documentée, car elle constitue la démonstration, par les institutions américaines elles-mêmes, du problème posé par SpaceX.

Jim Bridenstone, administrateur de la NASA sous la première administration Trump entre 2018 et 2021, résume l'inquiétude des décideurs publics. Plusieurs responsables sont alarmés par la dépendance de la NASA vis-à-vis de SpaceX pour des services essentiels. Il déclare qu'il n'y a qu'une seule chose pire qu'un monopole gouvernemental, et c'est un monopole privé dont le gouvernement est dépendant. Il craint que tous les œufs aient été mis dans le même panier, et que ce soit le panier SpaceX ^{lxxxviii}.

Cette formulation, qui vient d'un ancien administrateur d'agence civile et d'un Républicain, est doublée par le constat de Colin Kahl, ancien sous-secrétaire au Pentagone. Celui-ci observe que le gouvernement américain est massivement à la traîne pour construire une architecture spatiale plus résiliente, et que cette architecture ne fonctionnera que si l'on peut tirer parti de l'explosion du secteur spatial commercial ^{lxxxix}.

Cette double déclaration trace les contours d'un consensus bipartisan : la dépendance est connue, jugée problématique mais assumée comme une nécessité d'urgence. Il n'y a pas, à l'intérieur de l'État américain, de désaccord sur le diagnostic. Il y a seulement un désaccord sur les remèdes, certains plaidant pour une diversification accélérée vers Blue Origin et Rocket Lab, d'autres pour une régulation plus stricte de SpaceX, d'autres encore pour une acceptation pragmatique de la position acquise.

Cette dépendance concerne également le renseignement, sous une forme moins visible. Le formulaire S-1, document d'enregistrement déposé par SpaceX auprès du régulateur boursier américain le 20 mai 2026, assigne à Starshield trois missions : l'observation de la Terre, les communications gouvernementales sécurisées et l'hébergement de charges utiles. Cette dernière expression désigne un service précis : une agence conçoit un capteur, par exemple un instrument d'imagerie ou d'écoute, et le fait embarquer sur un satellite Starlink existant au lieu de construire et de lancer un satellite qui lui serait propre. Le même document identifie le National Reconnaissance Office, l'agence qui exploite les satellites espions américains, parmi les clients de lancement de SpaceX ^{xc}. L'agence de renseignement met donc ses capteurs en orbite en se greffant sur la chaîne industrielle de Starlink, sans posséder ni satellite ni lanceur. Elle se trouve, de ce fait, dans la même position de dépendance que la NASA et le Pentagone.

Cette absence de contrôle produit un second effet, sur un tout autre terrain que celui de la commande publique : l'usage des terminaux par l'adversaire. La sénatrice démocrate Elizabeth Warren formalise la critique parlementaire au secrétaire à la Défense. Elle écrit qu'elle est très préoccupée par les révélations selon lesquelles

l'armée russe utilise les services Starlink de SpaceX pour des opérations militaires offensives contre les forces ukrainiennes. Elle ajoute que le rapport du Wall Street Journal sur l'usage russe des terminaux Starlink est profondément préoccupant et révèle une menace sérieuse pour la sécurité nationale des États-Unis et de leurs alliés ^{xci}.

Cette lettre documente ensuite, sur sept questions précises, l'incapacité opérationnelle du Département de la Défense à imposer à SpaceX un comportement aligné sur les intérêts américains. La sénatrice cite la déclaration publique de l'assistant secrétaire au Pentagone²⁵ pour la politique spatiale, qui a dit lors d'une audition que le Département de la Défense n'est pas en position de forcer SpaceX à agir et que c'est quelque chose qu'on doit accepter et intégrer ^{xcii}. Prononcée publiquement par le responsable de la politique spatiale du Pentagone, cette déclaration équivaut à une reconnaissance officielle de la perte de contrôle. SpaceX semble détenir un pouvoir de monopole sur l'accès à internet par satellite, ce qui constitue un problème préoccupant pour la sécurité nationale^{xciii}.

L'apport de la lettre est de transformer un diagnostic d'analystes en question parlementaire formelle. La question Starlink est alors inscrite à l'agenda législatif américain, ce qui ouvre la possibilité d'auditions, de rapports d'enquête et, éventuellement, de législations spécifiques visant à reprendre le contrôle. Cette dynamique parlementaire est l'une des principales sources d'incertitude pour SpaceX, dont les négociations avec le Pentagone à partir de 2025 doivent intégrer le risque d'un encadrement législatif renforcé.

4. Starlink, instrument financier de SpaceX

La création de Starlink, annoncée en janvier 2015 et opérée commercialement à partir de 2019, doit être lue dans la continuité directe de cette logique d'occupation. L'objectif de la constellation, du point de vue de M. Musk, est triple. Premièrement, fournir un service de connectivité internet à haut débit et basse latence à l'échelle mondiale, en particulier dans les zones rurales mal desservies. Deuxièmement, générer un flux de revenus récurrents susceptible de financer le développement du programme Starship. Troisièmement, démontrer la maîtrise par SpaceX de l'intégration verticale entre lanceurs, satellites et terminaux utilisateurs, ce qui consolide son monopole structurel.

a. Origine des fonds et dynamique des valorisations

Contrairement aux contrats NASA et DoD ²⁶, Starlink n'est pas un produit directement subventionné par une agence publique. La déclaration à la commission permet, pour la première fois, de chiffrer l'effort de financement consenti depuis l'origine. De façon schématique, une entreprise dispose de deux moyens principaux pour financer sa croissance : vendre des parts de son capital à des investisseurs, ou réinvestir l'argent que dégagent ses propres activités. Depuis sa fondation en 2002

²⁵ John Plumb

²⁶ Department of Defense (Département de la défense).

jusqu'en 2025, SpaceX indique n'avoir vendu qu'un peu plus de 9 milliards de dollars de parts pour financer le développement conjoint de ses segments Space et Connectivity²⁷ ^{xciv}. L'essentiel de la construction de Starlink n'a donc pas été payé par des investisseurs extérieurs.

Le segment Space devient positif en EBITDA²⁸ ajusté de manière durable à partir de 2018, soit dix ans après le contrat NASA de 2008. C'est cette trésorerie d'exploitation, engendrée par une activité de lancement dont le premier client est le gouvernement américain, complétée par des levées externes ponctuelles, qui finance la construction de la constellation. Le segment Connectivity ne devient à son tour positif en EBITDA ajusté qu'à partir de 2023 ^{xcv}. Autrement dit, Starlink a été bâti pendant huit ans sur les revenus de l'activité de lancement, elle-même adossée à la commande publique. La question posée en ouverture de section trouve ici sa réponse : la constellation n'a pas eu besoin d'un marché commercial préexistant, car son coût de construction a été financé par une activité en amont dont l'État américain était le client principal.

La séquence se prolonge à la veille de l'ouverture du capital, dans une direction inattendue. En février 2026, SpaceX absorbe xAI et reprend à cette occasion les dettes de xAI et de X Corp, l'ancien Twitter. En mars, SpaceX emprunte 20 milliards de dollars auprès d'un groupe de banques pour rembourser ces dettes en une seule fois. Cet emprunt ne finance donc ni Starlink ni Starship : il solde le passif des autres entreprises de M. Musk. En contrepartie, les banques ont exigé que les actifs Starlink ne puissent être cédés hors du périmètre du groupe. La constellation devient ainsi la garantie de l'équilibre financier de l'ensemble du portefeuille industriel de M. Musk.

b. La concomitance avec le conflit ukrainien

La levée de mai 2022, contemporaine du début du déploiement en Ukraine, illustre l'imbrication des temporalités. Le Belfer Center²⁹ note que SpaceX a annoncé en mai 2022 une valorisation de 127 milliards de dollars et une levée de 2 milliards supplémentaires ^{xcvi}. Entre la veille de l'invasion russe en février 2022 et la fin 2025, la valorisation de SpaceX a été multipliée par environ six, passant de 127 milliards à 800 milliards de dollars ^{xcvii}. La concomitance entre la vitrine ukrainienne et cette progression valorielle pourrait établir un lien matériel entre l'usage opérationnel du produit et sa valeur financière.

La guerre a fourni à SpaceX une démonstration grandeur nature de la robustesse et de l'utilité militaire de sa technologie, dans des conditions opérationnelles extrêmes qu'aucune campagne commerciale n'aurait pu reproduire. Starlink a offert à M. Musk une scène pour démontrer la puissance de sa technologie, à un moment idéalement synchronisé avec ses besoins de financement ^{xcviii}.

²⁷ Starlink appartient au segment Connectivity

²⁸ L'EBITDA (bénéfice avant intérêts, impôts, dépréciation et amortissement) est un indicateur financier qui mesure la performance opérationnelle brute d'une entreprise sans tenir compte des choix de financement, de la fiscalité ou de l'usure des actifs.

²⁹ Centre de recherches en affaire de la Kennedy School.

Cette observation invalide le récit selon lequel l'engagement de SpaceX en Ukraine aurait été financièrement désintéressé. Si l'on rapporte le coût net assumé par SpaceX du déploiement initial, de l'ordre de 100 millions de dollars sur la première année ^{xcix}, à la hausse de valorisation de plusieurs centaines de milliards sur la même période, le déploiement ukrainien apparaît rétrospectivement comme un investissement de visibilité au rendement remarquable. Il serait cependant excessif d'attribuer à la seule Ukraine la multiplication de la valorisation, qui tient aussi à la croissance de Starlink, aux contrats publics et aux progrès de Starship. Mais la vitrine ukrainienne y a indéniablement contribué, pour un coût marginal au regard de la valeur créée.

c. *Structure et verrouillage du contrôle actionnarial.*

La structure actionnariale de SpaceX présente trois caractéristiques d'intérêt :

- Premièrement, la présence du Founders Fund, dont Peter Thiel est l'un des principaux soutiens de l'écosystème conservateur américain, installe une ligne d'influence directe entre l'actionnariat de SpaceX et l'exécutif américain à partir de janvier 2025, sans équivalent direct chez les concurrents comme Boeing, Lockheed Martin, Blue Origin ou Rocket Lab ^c.
- Deuxièmement, la nature non cotée a longtemps protégé SpaceX de la transparence exigible d'une société publique. Cette opacité explique que la sénatrice Warren, en avril 2024, ait été contrainte de fonder ses questions sur des sources journalistiques et des déclarations publiques, faute d'accès à des documents internes. Cette asymétrie d'information entre l'État régulateur et l'opérateur régulé est l'un des facteurs qui rendent la reprise de contrôle difficile en pratique.
- Troisièmement, aucun investisseur souverain européen ne figure au capital de SpaceX. Les États européens, qui s'apprêtent à devenir clients de Starlink, ne disposent donc d'aucun levier actionnarial sur les décisions de l'opérateur.

L'introduction en bourse ne lève pas cette asymétrie, elle la consolide. Le prospectus prévoit deux catégories de titres : les actions de catégorie A, offertes au public, confèrent une voix par action, tandis que les actions de catégorie B en confèrent dix. Les porteurs de catégorie B élisent 51 % des sièges du conseil d'administration. M. Musk conservant après l'opération la majorité des droits de vote, SpaceX relève de la qualification de *controlled company*³⁰ au sens des règles de cotation du Nasdaq et déclare son intention de se prévaloir des exemptions correspondantes, notamment celles qui imposent un comité des rémunérations et un comité des nominations composés exclusivement d'administrateurs indépendants^{ci}. L'ouverture du capital transfère donc le risque financier à des actionnaires publics sans transférer le pouvoir de décision. Le contrôle de

³⁰ Désigne une entreprise cotée en bourse dont la majorité des droits de vote est détenue par un seul actionnaire.

l'infrastructure reste juridiquement entre les mains d'une personne physique enregistrée auprès du régulateur boursier américain.

d. Prééminence de Starlink dans les revenus de SpaceX

Avant d'examiner les montants, il faut identifier à qui Starlink vend. Le service compte environ 10,3 millions d'abonnés répartis sur 164 pays au 31 mars 2026. Cet indicateur agrège les formules souscrites en ligne, qu'elles soient résidentielles, itinérantes ou professionnelles, mais il exclut les clients entreprises et gouvernementaux liés par un contrat négocié dans l'aviation, le maritime, la mobilité terrestre, les sites fixes et les administrations ^{cii}. Or ce sont précisément ces derniers qui portent les enjeux. Parmi les clients-entreprises, des opérateurs tels que United Airlines, Carnival, Maersk ou John Deere, avec des déploiements couvrant des flottes entières. Il mentionne également des administrations civiles, de l'agence américaine de gestion des catastrophes aux gouvernements philippin, jamaïcain et équatorien. Le volet militaire relève, lui, de Starshield.

La structure des revenus confirme que Starlink est devenu, en quelques années, la principale source de revenus de SpaceX. Le chiffre d'affaires passe de 10,4 milliards de dollars en 2023 à 18,7 milliards en 2025 ^{ciii}. Pour le seul exercice 2025, le segment Connectivity, qui regroupe Starlink, génère 11,4 milliards de revenus, soit 61 % du total. Cette base repose sur une clientèle passée de 2,3 millions d'abonnés fin 2023 puis 10,3 millions au premier trimestre 2026, dans un modèle d'abonnement récurrent. Le service de connectivité satellitaire est devenu, en moins de cinq ans après son lancement commercial, le cœur économique du groupe.

Tableau 1 : Récapitulatif du chiffre d'affaires de SpaceX sur la période 2023-2025

Chiffre d'affaires en milliards de dollars	SpaceX	Connectivity	Poids de Connectivité dans SpaceX
2023	10,4	3,9	38 %
2024	14	7,6	54 %
2025	18,7	11,4	61 %

Jusqu'en 2023, le financement allait dans un sens : l'entreprise investissait dans Connectivity à mesure que le segment Space dégageait de l'excédent, complété par des levées de capitaux externes ^{civ}. Le rapport s'est depuis inversé. En 2025, le segment Connectivity dégage un résultat opérationnel de 4,4 milliards de dollars, tandis que le segment Space enregistre une perte de 0,7 milliards ³¹. L'excédent tiré des abonnements couvre désormais le déficit du groupe. Ces deux segments ne forment pas la totalité du groupe : le segment AI, issu de l'absorption de xAI, enregistre pour le même exercice une perte opérationnelle de 6,4 milliards, qui explique l'essentiel de la perte consolidée de 2,5 milliards. La constellation ne finance donc pas seulement le groupe, elle est devenue le seul centre de profit d'un

³¹ Après avoir absorbé 3 milliards de recherche et développement consacrés au seul programme Starship

ensemble dont les deux autres segments consomment de la trésorerie. La vocation de Starlink est désormais une réalité comptable lisible dans des états financiers audités. La dépendance interne de SpaceX à Starlink, doublée de la dépendance externe de l'État américain et de l'Ukraine à Starlink, constitue un triple verrouillage dont aucune sortie n'est aisée à court terme.

5. Le verrouillage spectro-orbital

Trois documents permettent de décrire ce verrouillage. Une étude de l'IRSEM publiée en 2025 expose les règles d'attribution de la ressource spectre-orbite. L'ordonnance³² de la Commission fédérale des communications³³ du 1er décembre 2022 en montre l'application au cas de SpaceX³⁴. Une enquête de Jeff Foust pour parue en octobre 2023 sous le titre « Le monopole accidentel » en documente les effets sur les concurrents.

a. L'attribution de la ressource spectro-orbitale

Un satellite ne fonctionne qu'en disposant d'une bande de fréquences associée à une position orbitale, ce que l'on nomme un couple spectre-orbite. L'attribution relève de l'Union internationale des télécommunications (l'UIT). Deux règles en gouvernent l'accès. Les opérateurs privés ne peuvent pas déposer en leur nom propre et doivent passer par une administration nationale, sans être tenus de s'adresser à celle de leur pays d'origine. La priorité se règle ensuite à l'antériorité du dépôt, l'opérateur disposant de sept ans pour mettre en orbite son premier satellite, puis de sept années supplémentaires pour déployer la constellation complète.

Ce régime n'attribue pas de fréquences en exclusivité. Contrairement à la téléphonie mobile terrestre par exemple, où chaque opérateur détient une licence sur des tranches réservées, les bandes satellitaires sont partagées entre plusieurs systèmes qui doivent se coordonner pour ne pas se brouiller. La séparation repose sur la géométrie des émissions plutôt que sur le découpage du spectre. Elle suppose donc un nombre limité d'émetteurs simultanés dans le champ d'une même antenne.

La ressource est par ailleurs physiquement limitée. L'étude de l'IRSEM^{CV} rappelle que les spécialistes estiment qu'il n'y a de place, d'un point de vue physique, spectral et économique, que pour deux constellations en orbite basse en bande Ku, deux en bande Ka et deux en bandes basses. La date de dépôt devient dès lors un actif, dont la valeur augmente à mesure que les concurrents antérieurs échouent à déployer dans les délais.

b. L'ordonnance du 1er décembre 2022

³² Order FCC 22-91

³³ Federal Communications Commission, FCC

³⁴ Gen2

La FCC, par son ordonnance 22-91 publiée le 1er décembre 2022, autorise SpaceX à déployer une partie de sa constellation Gen2 Starlink. La FCC fait la part belle à SpaceX pour le marché américain et la favorise auprès de l'UIT en lui accordant le déploiement d'une constellation d'envergure. L'autorisation porte sur 7 500 satellites aux altitudes de 525, 530 et 535 kilomètres, sur les 29 988 satellites initialement demandés par SpaceX ^{cvi}.

Cette autorisation constitue un acte fondateur du verrouillage orbital. Elle intervient dix mois après le déploiement ukrainien, dans une période où la visibilité opérationnelle de la constellation est à son maximum, et elle accorde à SpaceX le droit de multiplier par sept la taille de sa constellation. Le rapprochement des deux séquences ne permet pas d'établir que la démonstration ukrainienne a pesé sur la décision réglementaire. Il situe en revanche l'autorisation dans le moment où l'utilité de Starlink est publiquement reconnue.

L'ordonnance documente, au paragraphe 10, les objections formelles des concurrents. Viasat, l'opérateur dont le réseau KA-SAT avait été visé par AcidRain en février 2022, soutient que la taille de la constellation Gen2 préempterait 86 % des altitudes entre 360 et 700 kilomètres et que les autres opérateurs ne pourraient accéder à l'orbite basse sans la permission de SpaceX ^{cvi}. Sur la question du partage spectral, Viasat documente que le système SpaceX causera des interférences aux systèmes plus petits 100 % du temps, déclenchant un partage forcé de bande passante qui pénalisera structurellement les concurrents alors que SpaceX en sera lui-même indemne du fait du nombre de ses satellites. Cette mécanique d'éviction par densité orbitale et spectrale est documentée par la procédure réglementaire elle-même.

La FCC a connaissance détaillée des effets d'éviction que la constellation Gen2 produira. Elle l'autorise tout de même, certes partiellement (7 500 satellites sur 29 988), en se réservant la possibilité d'examiner ultérieurement les phases suivantes. Le caractère graduel de l'autorisation, loin d'être un instrument de modération, fonctionne en réalité comme un instrument d'accélération. En autorisant SpaceX à déployer 7 500 satellites, la FCC rend les autorisations suivantes plus difficiles à refuser. Chaque satellite déjà en orbite devient un argument pour autoriser le suivant.

c. *Le rapport Foust : The Accidental Monopoly*

Jeff Foust, journaliste senior de SpaceNews, publie en octobre 2023 une enquête intitulée *The Accidental Monopoly: How SpaceX became (just about) the only game in town* ³⁵. L'apport principal est la citation directe d'acteurs concurrents de la pratique de prix prédateurs imputée à SpaceX. Vice-président de la business unit Vega chez Arianespace ³⁶, est cité en exposant que SpaceX vend ses missions

³⁵ Le monopole accidentel : comment SpaceX est devenu (presque) le seul acteur incontournable du secteur,

³⁶ Marino Fragnito

Transporter à un cinquième du prix Vega équivalent³⁷. Il conclut, sans ambages, que SpaceX est prêt à perdre de l'argent sur les missions Transporter pour évincer la concurrence^{cviii}.

Le rapport documente également le choix initial d'Amazon d'écarter SpaceX comme prestataire de lancement de sa constellation Kuiper, malgré des conditions tarifaires et techniques plus favorables que celles des concurrents retenus. Ce choix d'exclusion est révélateur : Amazon a préféré payer plus cher plutôt que de financer le développement d'un écosystème dont sa propre constellation deviendrait dépendante. Il n'a toutefois pas pu être tenu intégralement. Contraint par un calendrier réglementaire et par le retard des lanceurs qu'il avait retenus, Amazon a contracté trois lancements Falcon 9 en décembre 2023, sur plus de quatre-vingts commandés au total.

Foust documente enfin la situation de Telesat, opérateur canadien de constellation LEO, et de Globalstar, opérateur télécom américain, contraints d'externaliser leurs lancements vers SpaceX faute d'alternatives crédibles. Cela transforme les concurrents en clients. C'est une caractéristique des monopoles : quand même les rivaux dépendent de l'opérateur dominant pour exister. Space X montre ici un exemple de contrôle vertical complet sur sa propre chaîne, mais aussi sa capacité à s'imposer comme seul acteur indépendant dans ce domaine. Il impose ainsi un « péage » à ses concurrents sur l'accès aux orbites basses.

d. Synthèse du verrouillage orbital et spectral

Trois leviers convergent :

- Le premier est l'occupation orbitale : les plans orbitaux utiles sont en nombre limité, et la priorité acquise par l'antériorité du dépôt auprès de l'IUT³⁸ oblige les entrants suivants à s'adapter à la constellation en place. L'avance de SpaceX devient ainsi une barrière à l'entrée.
- Le second est l'occupation spectrale : les bandes ne font pas l'objet d'attributions exclusives mais d'un partage coordonné, qui suppose un nombre limité d'émetteurs. La densité de la constellation Starlink dégrade cette coexistence pour l'ensemble des usagers de la bande, sans qu'aucune règle d'attribution ne soit enfreinte.
- Le troisième est la pratique des prix prédateurs : des prix de lancement que les concurrents jugent inférieurs aux coûts, et qui les évincent tout en finançant, par les revenus capturés, la poursuite de l'occupation orbitale.

Ces trois leviers ne s'ajoutent pas, ils se catalysent entre eux. Grâce à son intégration verticale, SpaceX peut les combiner. Réserver une place dans l'espace ne coûte presque rien, mais sans capacité de lancement, ça ne sert à rien. SpaceX, elle, peut lancer : ça transforme une réservation en occupation réelle, donc en droit valable. Les lancements rapportent de l'argent, qui permet d'occuper plus de places.

³⁷ Soit 5 000 dollars par kilo contre 25 000 dollars pour Vega

³⁸ Union Internationale des Télécommunications

Les concurrents, eux, perdent leurs réservations s'ils ne lancent pas à temps. Et ces positions renforcent le service, qui finance de nouveaux lancements.

La combinaison des trois leviers constitue une configuration de monopole dont aucune des trois dimensions ne peut être traitée isolément. La régulation antitrust américaine, fondée sur le test du *consumer welfare*³⁹ qui privilégie le prix bas comme indicateur d'absence d'abus, est mal outillée pour identifier ce type de monopole où le prix bas est précisément le levier de l'éviction. La régulation européenne, plus attentive aux effets d'éviction, ne dispose pas de juridiction directe sur SpaceX en tant qu'opérateur de droit américain.

6. Grille de lecture intelligence économique

L'application des grilles de l'intelligence économique à l'écosystème Starlink permet de qualifier précisément la position stratégique acquise par SpaceX. Deux méritent d'être nommés, qui font écho aux trois niveaux d'analyse précédents (financier, gouvernemental, orbital).

a. L'intégration verticale

SpaceX a opéré, en moins de deux décennies, une intégration verticale qui couvre la production des lanceurs, la production des satellites, l'exploitation orbitale, la production des terminaux utilisateurs et l'opération du service. Aucun concurrent occidental ne dispose, en 2022, d'une intégration équivalente. Arianespace produit des lanceurs mais n'a ni constellation propre, ni terminaux, ni opération de service. Eutelsat opère des satellites mais ne produit ni lanceurs ni terminaux. OneWeb, racheté par Eutelsat en 2023, a une constellation embryonnaire mais dépend de lanceurs tiers, ce qui inclut SpaceX. Amazon Kuiper construit une constellation mais dépend de lanceurs tiers, dont ceux de SpaceX pour une part marginale de son déploiement.

La conséquence est qu'aucun acteur ne peut concurrencer SpaceX sur l'ensemble du cycle. La maîtrise par un seul opérateur de toute la chaîne de valeur permet une optimisation des coûts dont les concurrents peuvent difficilement s'approcher, ce qui en retour empêche l'émergence d'alternatives crédibles à court terme. L'intégration verticale apparaît comme un facteur de monopole.

b. La dépendance opérationnelle

Au moins neuf pays, d'Europe et au Moyen-Orient, ont interrogé les autorités américaines, dans les dix-huit mois suivant le déploiement, sur les garanties dont disposaient les États clients face à un opérateur privé dont ils dépendaient pour des communications de sécurité^{cix}. Cette mobilisation diplomatique inhabituelle dont la confidentialité est elle-même symptomatique dit la prise de conscience tardive du caractère systémique de la dépendance. Peu de pays ont accepté de

³⁹ Bien-être du consommateur.

s'exprimer publiquement ce qui constitue, en soi, le marqueur d'un rapport de force déséquilibré entre États souverains et un opérateur privé.

7. Synthèse

Le projet Starlink n'est pas devenu industriel sans client. Il est devenu industriel parce qu'il a su répondre aux besoins de l'État américain, à travers la NASA, la Space Force, le Département de la Défense et plusieurs agences de renseignement, en client structurel, sans que cette relation ne soit construite sur un cadre contractuel symétrique. La générosité fondatrice envers l'Ukraine en février 2022, présentée comme un geste philanthropique, est en réalité la démonstration d'un produit dont la NASA, le DoD et les armées étaient les destinataires implicites.

La conjonction entre actionnariat libertarien⁴⁰, ancien réseau PayPal devenu influence politique sous Trump, contrats publics américains massifs⁴¹, statut longtemps non coté qui protégeait de la transparence et intégration verticale unique constitue, pour un opérateur d'infrastructure, une combinaison rare dans l'histoire industrielle contemporaine⁴². L'épisode Starlink peut être lu comme un cas de capture d'un État souverain par un acteur privé non régulé, opérée par substitution graduelle, à l'invitation même des États clients, dans des circonstances d'urgence où la vitesse de réponse l'a emporté sur la prudence.

Enseignements :

- Starlink n'a pas eu besoin d'un marché commercial préexistant. Sa construction a été financée par la commande publique avec une absence de contrôle public.
- La position acquise ne repose pas sur un avantage commercial mais sur trois verrous cumulés : occupation des plans orbitaux, saturation des bandes de fréquence, et prix de lancement que les concurrents ne peuvent égaler.
- La dépendance est reconnue par les responsables américains eux-mêmes, de la NASA au Pentagone, sans qu'aucun levier de correction n'ait été identifié.
- Aucun État européen ne dispose de levier actionnarial, réglementaire ou industriel sur SpaceX. Les futurs clients européens de Starlink entreront dans la même relation que l'Ukraine en 2022, sans plus de garanties.

C. « Quoi - le produit et la technologie »

1. Le produit : l'offre standard, composition et fonctionnement

Lorsque vous voulez acheter un kit Starlink en France, trois offres vous sont proposées.⁴³

La première, dite « Résidentiel 100 Mbit/s »⁴⁴ offre une connectivité fiable et économique, idéale pour les usages basiques tels que la navigation Internet et la

⁴⁰ Founders Fund, lien avec l'écosystème politique Thiel-Vance

⁴¹ NASA, DoD, NRO, Space Force

⁴² Des similitudes avec la Standard Oil de la famille Rockefeller sont à étudier.

⁴³ Chiffres de mai 2026.

⁴⁴ 29€ /mois

consultation de courriels. La deuxième formule, « Résidentiel 200 Mbit/s » ⁴⁵, s'adresse aux utilisateurs recherchant une performance accrue pour le streaming vidéo et le télétravail occasionnel. Enfin, l'offre « premium Résidentiel Max » ⁴⁶ constitue la solution la plus performante, dotée des débits maximaux disponibles et enrichie d'un kit Mini gratuit pour les déplacements. Toutes ces offres partagent des avantages communs : données illimitées, configuration Plug & Play, disponibilité supérieure à 99,9 %, résistance aux intempéries et période d'essai de 30 jours.

Le kit Starlink, illustré par la photo ci-dessous, est très simple à prendre en main et composé de quelques pièces seulement :

- Un routeur de troisième génération assurant la distribution du signal Wi-Fi dans l'habitation ;
- Deux câbles : alimentation électrique et raccord antenne et routeur ;
- Une base ou béquille de support permettant une installation flexible ;
- Une antenne sous forme de parabole, capable de capter les signaux émis par les satellites en orbite basse. L'antenne établit une communication bidirectionnelle avec les satellites qui survolent la terre, créant ainsi un pont numérique entre l'utilisateur et le réseau Internet mondial. Pour garantir une connexion stable, l'antenne exige une vue dégagée du ciel, sans obstruction majeure, ce qui explique l'importance capitale du choix de son emplacement d'installation.
- Le prix du kit Starlink en France varie entre 300 et 500 euros, selon le modèle



Image 12 : Kit Starlink au complet.

choisi.

C'est la partie « immergée de l'iceberg », où le client final voit la technologie dans son état le plus réduit, ignorant des autres éléments qui constituent le cycle du produit et que nous allons décrire maintenant.

⁴⁵ 39 € /mois

⁴⁶ 59€ /mois

2. Architecture du réseau Starlink.

L'architecture comprend trois segments principaux : spatial, sol et utilisateur, comme illustré dans le schéma ci-dessous et chacun jouant un rôle crucial dans la fourniture d'un accès Internet global, à haut débit et à faible latence.

a. L'architecture classique de Starlink : La constellation en orbite basse.

Le segment spatial est constitué d'une constellation de satellites en orbite basse (LEO) ⁴⁷ en architecture maillée, avec plus de 10000 satellites en 2026, et une autorisation pour en déployer encore environ 30000. Les satellites, situés entre 300 et 600 km d'altitude, sont équipés d'antennes à réseau phasé et de liaisons laser inter-satellites (ISL) pour les communications spatiales, ce qui réduit la dépendance aux stations au sol. Cependant, cette approche introduit une complexité accrue et des délais de propagation supplémentaires.

La constellation en LEO conjugue trois atouts : une couverture étendue aux latitudes intermédiaires (et donc à certaines zones difficiles d'accès), une très bonne latence (autour de 20 à 50 ms) et une bande passante de 1 Gbps⁴⁸ résidentiel en conditions nominales. Cette performance repose sur une architecture maillée où les satellites communiquent via des liaisons laser inter-satellites (ISL), optimisant le routage.

L'intégration du réseau satellites avec les réseaux terrestres s'effectue via des stations sol (gateway) stratégiquement placés près des nœuds Internet majeurs. Les défis techniques, tels que la latence variable et la bande passante fluctuante, sont relevés grâce à des adaptations des protocoles de transport ⁴⁹ et des mécanismes de contrôle avancés.

Les satellites de nouvelle génération, Starlink Gen3, dont les premiers lancements sont prévus à partir du deuxième semestre 2026, visent une latence inférieure à 20 ms (donc de meilleures performances), ainsi qu'une intégration avec les réseaux 5G terrestres.

⁴⁷ Low Earth Orbit : Orbite Terrestre basse

⁴⁸ 1 Gbit/s ou 1 Gbps signifie que la connexion peut théoriquement transférer jusqu'à 1 milliard de bits par seconde.

⁴⁹ TCP, SCTP, QUIC : protocole de communication internet.

Le segment sol comprend les stations au sol (gateway) et les centres de contrôle. Les stations au sol sont placées près des nœuds internet majeurs, et servent de points d'entrée et de sortie pour le trafic entre le réseau spatial en LEO et l'internet traditionnel. Les centres de contrôle gèrent le réseau, assurant une coordination efficace des satellites et une optimisation des ressources. Les centres référencés sur le site de Starlink et les plus proches de l'Ukraine se situent en Pologne (Varsovie), en Bulgarie (Sofia) et en Allemagne (Francfort). Bien que les données des centres de contrôles utilisés par Starlink dans le cadre du conflit en Ukraine ne soient pas connues, ces infrastructures physiques au sol constituent de véritables infrastructures critiques à protéger.

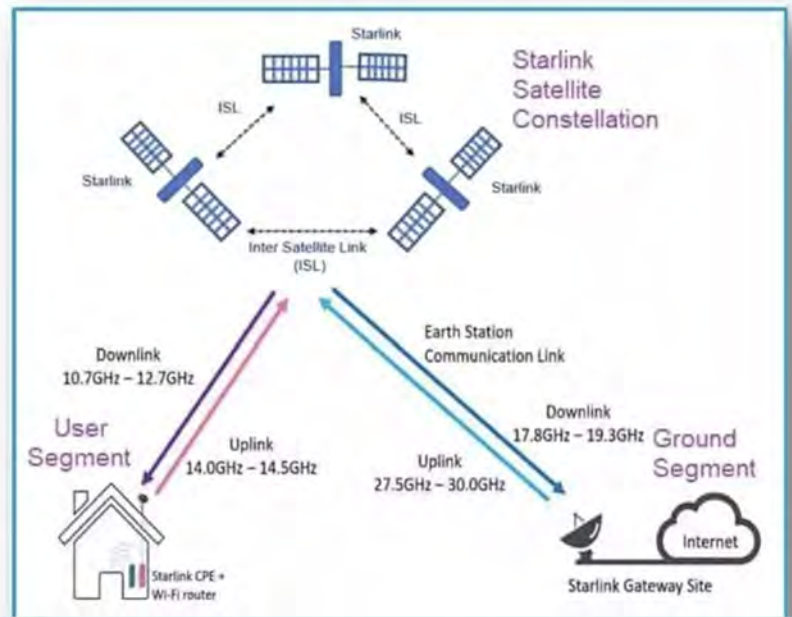


Figure 4: Schéma explicatif du fonctionnement de Starlink et des 3 composantes majeures le constituant.

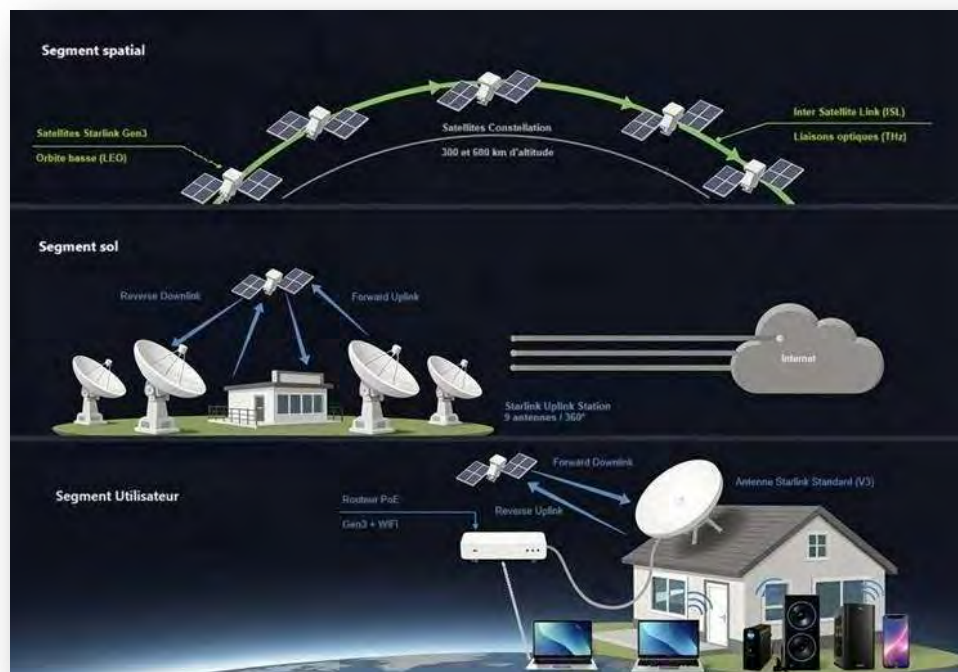


Figure 5 : Détails des différents composants de fonctionnement du système Starlink

Les terminaux utilisateurs sont quant à eux les antennes paraboliques motorisées présentées ci-dessus et capables de suivre automatiquement les satellites et basculer d'un satellite à l'autre, sans interruption de service. Le segment utilisateur

comprend donc ces terminaux, tant grand public que professionnels, qui assurent l'interface utilisateur. Leur compacité et leur portabilité les rendent adaptés aux déploiements mobiles et aux zones reculées.

b. Une autre utilisation possible pour le LEO : le Direct to Cell

La technologie Direct to Cell⁵⁰, développée en partenariat avec des acteurs comme Apple, vise à élargir la couverture des communications mobiles dans les zones non desservies par les réseaux terrestres. Cette innovation, basée sur le standard NR-NTN⁵¹, marque une étape cruciale vers une connectivité hybride, combinant réseaux terrestres et satellites pour une résilience accrue. Dans ce cas, plus besoin de stations au sol et de centre de contrôle.

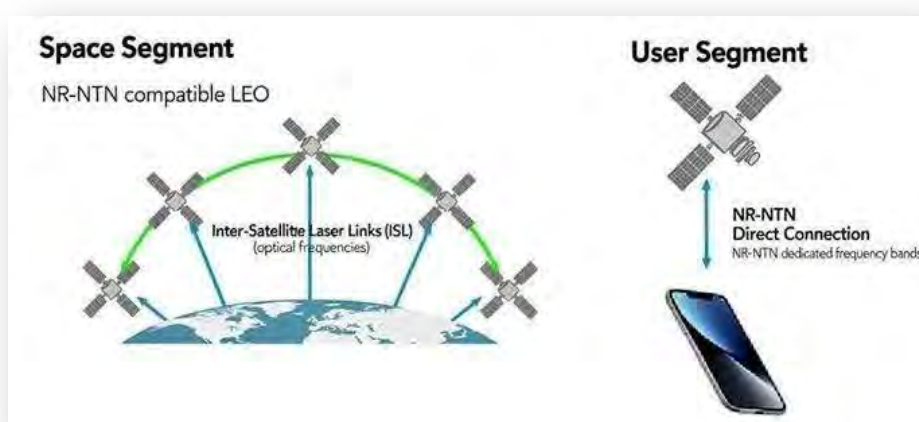


Figure 6 : Schéma d'explication de la différence entre le segment espace et utilisateurs.

c. Comparaison avec les systèmes traditionnels.

La fibre optique est une technologie de communication terrestre qui utilise des câbles en fibre de verre ou en plastique pour transmettre des données sous forme de lumière. Cette technologie offre des débits très élevés, pouvant atteindre plusieurs téraoctets par seconde sur de longues distances. Pour les utilisateurs finaux, les débits peuvent aller jusqu'à 10 gigabits par seconde, voire plus, en fonction des infrastructures et des technologies utilisées. La latence de la fibre optique est très faible, généralement inférieure à 10 ms, ce qui la rend idéale pour les applications en temps réel comme la visioconférence, le gaming et les services cloud. Parmi les avantages de la fibre optique, on peut citer son haut débit, sa faible latence et sa fiabilité, car elle est moins sensible aux interférences électromagnétiques et aux conditions météorologiques. Cependant, le déploiement de la fibre optique est

⁵⁰ D2C : Directement vers le téléphone

⁵¹ New Radio Non-Terrestrial Networks : Nouveaux réseaux radio non terrestres

coûteux, en particulier dans les zones rurales ou isolées, et elle nécessite une infrastructure physique, ce qui peut limiter sa disponibilité dans certaines zones.

La 5G est la cinquième génération de technologie de communication mobile, conçue pour offrir des débits plus élevés, une latence plus faible et une meilleure fiabilité que les générations précédentes. La 5G offre des débits théoriques allant jusqu'à 20 Gbps, bien que les débits réels varient en fonction des conditions du réseau et de l'équipement utilisé. En pratique, les débits peuvent atteindre plusieurs centaines de mégabits par seconde (Mbps). La latence de la 5G est très faible, généralement inférieure à 10 ms, ce qui la rend adaptée aux applications en temps réel comme les véhicules autonomes, la réalité augmentée et les services cloud. Parmi les avantages de la 5G, on peut citer son haut débit, sa faible latence et sa flexibilité, car elle peut être déployée dans diverses bandes de fréquences, offrant une flexibilité accrue pour répondre aux besoins spécifiques des utilisateurs. Cependant, la couverture de la 5G est encore limitée dans certaines zones, en particulier dans les zones rurales ou isolées, et elle peut être sujette aux interférences dans les bandes de fréquences plus élevées.

Comme décrit plus haut, la constellation LEO offre des débits allant jusqu'à 1 Gbps pour les utilisateurs résidentiels dans les zones peu congestionnées. Les débits réels varient en fonction des conditions du réseau et de l'équipement utilisé. La latence est généralement inférieure à 50 ms, et donc comparable aux performances de la 5G et de la fibre optique, avec une latence encore meilleur pour les satellites de nouvelle génération (Gen3, 20 ms visés). Parmi les avantages de la constellation LEO, on peut citer une couverture étendue aux zones peu densément peuplées où les infrastructures terrestres sont limitées, une résilience aux défaillances d'infrastructures terrestres, un déploiement rapide des terminaux grâce à leur portabilité. Cependant, l'accessibilité reste limitée en raison des coûts.

La fibre optique demeure la meilleure solution pour les applications stationnaires exigeant un débit maximal. La 5G offre une flexibilité accrue dans les zones densément peuplées. L'offre satellitaire, quant à elle, offre une couverture étendue et une certaine indépendance vis-à-vis des infrastructures terrestres. Le choix technologique ne relève donc pas d'une hiérarchie absolue, mais d'une adéquation aux environnements opérationnels. .

Tableau 2: Comparatif des offres sur différents aspects opérationnels

Comparaison des Technologies					
Technologie	Débit	Latence	Couverture	Résistance aux Interférences	Coût
Fibre Optique	Jusqu'à 10 Gbps	< 10 ms	Limitée par l'infrastructure	Très élevée	Élevé
5G	Jusqu'à 20 Gbps	< 10 ms	Limitée par la couverture	Moyenne	Moyen
Starlink	Jusqu'à 1 Gbps	< 50 ms (Gen2), < 20 ms (Gen3)	Mondiale	Élevée	Élevé

3. Analyse des menaces

Les conflits contemporains ont révélé l'importance stratégique des communications par satellite LEO et la vulnérabilité critique de ces systèmes face aux techniques de brouillage et d'interférence sophistiquées.

Selon les analyses académiques récentes, les forces russes ont déployé des systèmes de brouillage GPS et des perturbateurs de fréquences pour neutraliser les communications ukrainiennes reposant sur les constellations Starlink et autres réseaux LEO civils, comme l'a documenté le rapport de l'Académie des Sciences française sur les grandes constellations de satellites.⁵²

Les constellations LEO, malgré leur résilience inhérente due à la multiplicité des satellites, demeurent vulnérables aux attaques ciblées exploitant les fréquences de liaison montante. L'Agence de l'Union européenne pour la cybersécurité (ENISA) et Satconsult ont mené une évaluation complète de la cybersécurité des communications LEO en février 2024⁵³, révélant que ces systèmes font face à des menaces multiples incluant le brouillage (jamming), le leurre (spoofing), le piratage des réseaux de communication, ainsi que des attaques par ransomware et dénis de service distribués (DDoS). Nous y reviendrons plus tard.

Les recherches menées par des exploitants aériens, notamment Transavia, documentent depuis janvier 2024 plus de 600 détections de spoofing en vol, avec des erreurs de position atteignant jusqu'à 100 nautiques. Ces observations empiriques soulignent que le brouillage et le leurre de communications LEO requiert une sophistication technique moins élevée que préalablement anticipé, rendant cette menace accessible à des acteurs étatiques de second rang. Les zones de détection de spoofing se rapprochent progressivement de l'Union européenne, avec des cas identifiés en Finlande et en Mer Noire.

Les incidents documentés révèlent des conséquences opérationnelles graves : fausses alarmes du système d'avertissement de proximité du terrain (EGPWS), inhibition des résolutions TCAS⁵⁴, et dégradation des barrières de sécurité aérienne. Ces vulnérabilités démontrent l'interdépendance croissante des infrastructures terrestres critiques comme l'énergie, les transports, etc... avec les services fournis par les satellites de positionnement et de communication, dont les LEO.

⁵² Académie des sciences, Grandes Constellations de Satellites : Enjeux et Impacts, avril 2024.

⁵³ LEO Satcom cybersecurity assessment, ENISA, février 2024.

⁵⁴ Correspond à la désactivation automatique de certaines alertes de manœuvre d'évitement pour éviter des corrections de trajectoire dangereuses ou inadaptées près du sol.

Enseignements :

- Le kit Starlink, simple à utiliser, repose sur une architecture complexe comprenant une constellation de satellites en orbite basse, des stations au sol et des terminaux utilisateur, garantissant une connectivité fiable même dans les zones reculées.
- La technologie LEO offre une couverture étendue, une faible latence et une résilience accrue face aux infrastructures terrestres, mais reste vulnérable aux attaques de brouillage et de spoofing sophistiquées.
- La convergence des réseaux satellitaires et terrestres, notamment avec la 5G et la fibre optique, souligne l'importance stratégique de la cybersécurité pour protéger ces infrastructures critiques face aux menaces contemporaines.



Image 13 : Lancement d'un Starship. Crédits : SpaceX



III. Starlink en Ukraine.



III. Starlink en Ukraine.

À la suite d'une longue période de tensions entre les deux pays que sont l'Ukraine et la fédération de Russie, le président russe Vladimir Poutine signe unilatéralement le 21 février 2022 l'acte de reconnaissance des deux territoires séparatistes du Donbass en Ukraine : la République populaire de Donetsk et la République populaire de Louhansk.

Dans la nuit du 21 au 22 février, des véhicules blindés et des troupes russes pénètrent ainsi dans l'est de l'Ukraine sous couvert de maintien de la paix. Le 24 février, une étape est franchie, le chef du Kremlin annonce en effet une opération militaire d'envergure sur le territoire ukrainien dans l'objectif, « de défendre les séparatistes du Donbass ». Cette fois-ci, Moscou ne s'arrête pas à l'est de l'Ukraine puisque de puissantes explosions frappent plusieurs grandes villes, dont la capitale Kiev.

Le but de guerre initial de l'armée russe était bel et bien la prise de Kiev, la capitale ukrainienne, afin de faire chuter le gouvernement de Volodymyr Zelensky et le remplacer par un régime plus favorable aux intérêts russes sur le long terme.

Cinq manœuvres militaires principales sont alors menées simultanément^{CX}:

- La principale depuis la Biélorussie pour s'emparer de Kiev,
- Les secondaires depuis le nord-est ukrainien pour s'emparer de Kharkiv,
- Depuis l'est pour s'emparer de Marioupol
- De la Crimée pour s'emparer de Kherson.
- Une tête de pont devait être réalisée via l'aéroport d'Holstomel

Cette dernière manœuvre (situé à 35 kilomètres au nord-ouest de Kiev) pour pouvoir ensuite acheminer par air les forces russes depuis la Russie, encercler puis prendre Kiev dans le but de faire tomber le régime en place. L'offensive échoue dans les premiers jours du conflit, transformant ce qui devait être une opération de courte durée en une guerre d'usure.

Ce qui marque aussitôt la nature du conflit, ce sont les elongations

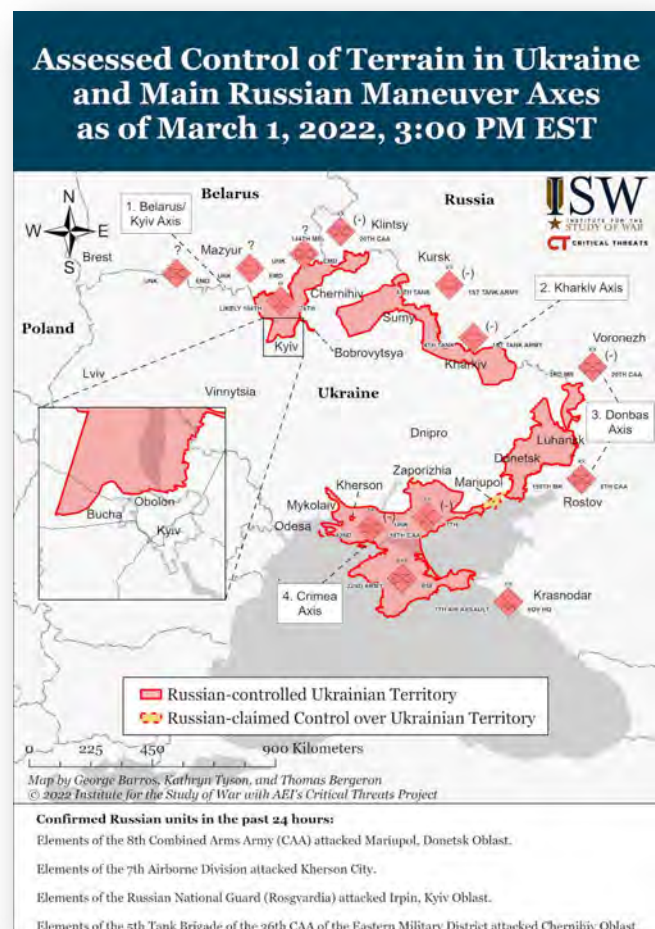


Image 14 : Carte de l'invasion russe au 1er mars 2022.

géographiques qui entraînent des défis immenses en termes de communications, tant civiles que militaires. L'Ukraine s'étend sur environ 1 000 kilomètres d'ouest en est et sur 600 kilomètres du nord au sud, la majeure partie de son territoire étant fait de plaines. Sur des fronts tactiques très importants, l'utilisation d'internet, l'accès aux satellites et la transmission en temps réel des données sont des enjeux majeurs.

Une étude de l'Institut français des relations internationales (IFRI) en février 2022 évoque également de façon très claire les caractéristiques de cette « nouvelle » forme de guerre⁵⁵ : *« one of the central findings of this report is that few of the technologies observed in Ukraine are truly new in isolation. Drones, satellite communications, electronic warfare, precision strikes, and data fusion all predate the war. What is new and consequential is the way these technologies have been combined, scaled, integrated and employed through a fundamentally digital-native mindset. »*⁵⁵

Dans ce conflit où le digital est donc omniprésent, le produit Starlink va alors apparaître comme un outil irremplaçable pour la coordination des actions militaires, et un produit de première nécessité pour l'accès à internet au profit des populations et infrastructures civiles.

A. L'emploi de Starlink par l'Ukraine

1. La demande d'aide officielle de l'Ukraine.

Face à cette situation d'urgence extrême et la perte du réseau satellitaire KA-SAT, le vice-premier ministre et ministre de la transformation numérique ukrainien, Mykhailo Fedorov, demande alors de l'aide le 26 février 2022, via Twitter, aux différents patrons de la tech américaine. Il sollicite notamment Elon Musk pour l'envoi de système Starlink et retrouver ainsi un accès rapide à internet.⁵⁶

⁵⁵ « L'une des principales conclusions de ce rapport est que peu des technologies observées en Ukraine sont véritablement nouvelles si l'on les considère isolément. Les drones, les communications par satellite, la guerre électronique, les frappes de précision et la fusion de données existaient tous avant le conflit. Ce qui est nouveau et déterminant, c'est la manière dont ces technologies ont été combinées, déployées à grande échelle, intégrées et mises en œuvre dans une optique fondamentalement axée sur le numérique. »

⁵⁶ « Pendant que vous essayez de coloniser Mars, les Russes essayent de coloniser l'Ukraine. Pendant que vos fusées volent et atterrissent avec succès, les russes utilisent les leurs pour attaquer les civils. Nous vous demandons de donner à l'Ukraine des terminaux Starlink et de demander aux Russes sains d'esprits de tenir aux côtés de l'Ukraine. »



Image 15 : Tweets postés par M.Fedorodov interpellant M.Musk sur la situation ukrainienne.

Ce dernier répond dans la foulée et les premiers systèmes arrivent très vite sur le sol ukrainien, à priori dès le 28 février 2022, soit quatre jours seulement après le début du conflit.

En réalité, les démarches entre l'Ukraine et l'entreprise de M. Musk avaient débuté bien avant cette demande officielle sur les réseaux sociaux. Ainsi, le 07 mars 2022, au sein du California Institute of Technology, Gwynne Shotwell, présidente et COO de SpaceX⁵⁷, a publiquement annoncé que les échanges sur le produit Starlink étaient en cours depuis au moins un mois et demi. Mykhailo Fedorov énoncera lui en juin 2022 que les discussions existaient depuis déjà un an.

Si pour l'Ukraine l'arrivée de Starlink est une nécessité pour la conduite de la guerre, cette demande inattendue constitue également une opportunité majeure pour M. Musk. En effet, la situation financière de Starlink avant 2023 n'est pas à la hauteur des promesses initiales : le chiffre d'affaires de Starlink en 2022 est alors de 1,4 milliards de dollars contre 12 espérés initialement pour 7 milliards de bénéfices.

Les satellites volent mais n'ont pas encore la clientèle et les revenus attendus. Venir s'implanter en Ukraine avec son produit permet à Musk plusieurs coups :

- Trouver un marché demandeur d'accès à internet (environ 40 millions d'habitants en Ukraine en 2022) dans un environnement dégradé ;
- Continuer à donner une image de bienfaiteur de l'humanité, en cohérence avec son *storytelling*⁵⁸ ;
- Valoriser son produit comme système dual, même s'il défendra, dans un premier temps, seulement un usage civil ;

⁵⁸ Construction du récit

- Continuer ainsi à être alimenté par des contrats conséquents du gouvernement américain en démontrant sa capacité à évoluer dans un environnement militaire de son produit comme démontré précédemment.

2. Le volume croissant de terminaux.



Image 16 : Publié par M. FEDOROV le 28 février 2022 avec la mention « Starlink --- ici. Merci Elon », les 500 premiers terminaux acheminés avec le soutien de DAI et USAID.

Il reste assez difficile de suivre précisément le volume de terminaux Starlink livrés à l'Ukraine depuis février 2022. Dans les premiers jours du conflit, ce sont 500 terminaux Starlink qui arrivent en Ukraine, mis en valeur par un post sur X de Mykhailo Fedorov présentant une photo de terminaux dans un camion militaire.

Un rapport de l'USAID^{cxii} de 2025 indique que les premières livraisons qui ont lieu via l'USAID à partir de 2022 totalisent par la suite plus de cinq mille terminaux livrés progressivement à l'Ukraine, grâce au financement de l'USAID et de SpaceX.

Le chiffre exact est de 5175 terminaux répartis entre 1508 financés par l'USAID et 3667 donnés par SpaceX. Les terminaux offraient une connexion gratuite et illimitée à internet pendant trois mois (de

début mars à début juin 2022).

En ce qui concerne les terminaux de l'USAID et SpaceX, ceux-ci transitaient via l'entreprise DAI Global LLC qui les fournissaient ensuite au State Service of Special Communications and Information Protection (SSSCIP) ukrainien, en charge de sécuriser les communications gouvernementales ukrainiennes et de défendre l'état contre les cyberattaques.

Selon le rapport de l'USAID, d'autres livraisons ont eu lieu, sans que les volumes de terminaux soient connus. Ces terminaux ont été financés par le département de la défense américain, des gouvernements (masqués dans le rapport) ainsi que des donateurs privés (non précisés dans le rapport). On peut toutefois citer la Pologne et l'Allemagne qui ont toutes deux affirmées leur soutien à Kiev par l'envoi et le financement de terminaux Starlink :

- La Pologne, en mai 2024, via son ministre de la numérisation Krzysztof Gawkowski, a indiqué qu'entre 2022 et 2024, près de 323 millions de zlotys (77 millions d'euros) ont été dépensés pour le système Starlink, pour environ 25000 terminaux financés intégralement (fourniture du matériel et abonnement) et 5000 abonnements de terminaux. Selon le ministre, la Pologne devient ainsi « le plus grand fournisseur mondial d'accès à internet

en Ukraine ». D'autres chiffres énoncent un financement à hauteur de 20 millions de dollars pour l'année 2025. Un mémorandum de coopération a été signé en mai 2024 entre Mykhaïlo Fedorov et Krzysztof Gawkowski dans le domaine de la cybersécurité. Pour la Pologne, celle-ci est engagée dans une « cyberguerre froide avec la Russie ».^{cxiii}

- L'Allemagne^{cxiv} déclare en janvier 2023, lors d'une visite de sa ministre fédérale des affaires étrangères Annalena Baerbock en Ukraine, qu'elle financera pour 20 millions d'euros de système Starlink, soit l'équivalent de 10000 terminaux, dont un tiers est destiné aux forces armées ukrainiennes.
- La France et le Royaume-Uni ont également participé, sans plus de précisions sur la hauteur de leur engagement.

Concernant les acteurs privés, on peut noter que des personnalités comme Niall Ferguson et Marc Benioff ont participé à des levées de fonds privées pour l'achat de terminaux Starlink, environ 5000^{cxv}.

Dans l'année 2022, soit en un an environ, le nombre de terminaux aurait augmenté jusqu'à 22000, avec des demandes répétées du gouvernement ou des forces armées ukrainiennes vers Musk. Ce chiffre serait situé entre 40000 et 50000 en 2026, difficilement vérifiable. L'augmentation exponentielle de ces chiffres démontre toutefois que le système se démarque par son succès et garantit un accès rapide et stable à internet au profit de ses usagers.

3. L'utilisation civile et militaire de Starlink

Initialement, le produit Starlink ne devait pas - en tous cas officiellement - servir à un quelconque usage militaire mais uniquement pour des usages civils. Un jeu subtil de responsabilité entre l'USAID, DAI Global LLC et le SSSCIP a permis de contourner cette règle. L'USAID, en qualité d'agence d'aide internationale du gouvernement des États-Unis ne voulait pas, ou ne pouvait pas pour des raisons diplomatiques, fournir directement à l'Ukraine un système de communication dont ses forces armées auraient pu se servir. Cela aurait constitué un soutien armé direct au profit de l'Ukraine, contraire à la vocation première plus « humanitaire » de l'agence. En passant par un tiers⁵⁹, l'USAID se dédouane habilement de sa responsabilité sur la traçabilité du produit.

Starlink est ainsi dès le début du conflit mis à profit de la population ukrainienne, des communications et l'accès à internet au profit des chemins de fer, des écoles, des hôpitaux du pays, des abris d'urgence, etc... en cas de coupure de courant à la suite d'une attaque russe ou bien pour répondre aux destructions des moyens de communications.

⁵⁹ DAI Global LLC, une entreprise spécialisée dans les missions de soutien à l'USAID.

En l'absence de données publiques sur les régions les plus consommatrices de Starlink, on peut raisonnablement supposer que les zones prioritaires sont les régions touchées par le conflit (Kherson, Zaporijjia, Donetsk, Louhansk, Kharkiv) ou encore les grands nœuds urbains ou énergétiques touchés par des attaques aériennes régulières (Kiev, Lviv...). Les populations peuvent alors bénéficier d'un système type Wi-Fi en libre accès, comme le montrent les photos ci-dessous :



Image 17 : Terminaux Starlink mis en place pour fournir une connexion aux civils sur la place de l'Indépendance, après le retrait de l'armée russe de Kherson, le 13 novembre 2022.

Les terminaux sont particulièrement mobiles, très simples en termes d'installation et de prise en main, ce qui est parfaitement adapté aux politiques de sécurité civiles en cas de crise, comme l'exemple de Chido⁶⁰ en 2024 en France le rappellera. Mais ce produit dépasse le simple rôle de fournisseur d'accès à internet au profit des populations et devient très rapidement un outil parfaitement adapté aux attentes de l'armée ukrainienne.

Par ses qualités évoquées ci-dessus, il permet en effet de maintenir les communications entre unités, de soutenir la transmission d'ordres, d'alimenter les systèmes de drones et de conserver une capacité de commandement même lorsque les infrastructures terrestres sont détruites ou perturbées. Avoir l'avantage du numérique face aux forces armées russes, qui n'ont pas un tel système, permet aux forces armées ukrainiennes (FAU) de compenser leur infériorité matérielle ou humaine par une infovalorisation en temps quasi-réel, et reprendre ainsi l'avantage au combat. Les FAU l'adoptent alors quasi-instantanément et de manière massive, créant évidemment une forte dépendance.

M. Musk écrira même en mars 2025 dans un Tweet que son système est devenu « la colonne vertébrale de l'armée ukrainienne et que la ligne de combat s'effondrerait s'il coupait le système ». Il reconnaît publiquement ici que son produit possède un usage militaire, ce qu'il contestait initialement.

⁶⁰ Le 14/12/2024, le cyclone Chido frappe l'île de Mayotte, rendant les réseaux de communication inutilisables. L'État français achète alors des kits satellitaires Starlink pour répondre au plus vite à ses besoins en communication.

Starlink et Kyivstar :

Un projet commun voit même le jour entre Kyivstar, le plus grand opérateur de téléphonie mobile d'Ukraine, et Starlink pour permettre un accès internet direct entre les téléphones portables équipés de réseaux 4G ou LTE et les satellites Starlink en orbite afin de pouvoir envoyer et recevoir des messages texte. Le réseau, dont le lancement est prévu pour la mi-2026, devrait permettre aux ukrainiens d'accéder aux services cellulaires dans les régions montagneuses et rurales du pays.

Après la phase de guerre de mouvement qui dure jusqu'en décembre 2022, l'Ukraine lance en juin 2023 une opération de reconquête, ou contre-offensive, destinée à reprendre les territoires occupés par la Russie, à savoir les oblasts de Zaporijjia et de Donetsk.

Les FAU, qui ont adopté la doctrine militaire occidentale fondée sur la supériorité informationnelle, la précision et la décentralisation du commandement sont conscientes que cette opération est complexe à de nombreux égards. Elle s'étend en effet sur des distances géographiques conséquentes (environ 1600 kilomètres de front), mobilise de très nombreuses ressources, tant humaines que matérielles et nécessite des capacités technologiques particulièrement fournies, notamment dans le domaine des communications, de l'imagerie et du renseignement satellitaire.

Les FAU s'appuieront alors majoritairement sur l'aide américaine et sur Starlink pour répondre à ces besoins, qu'elles ne peuvent à elles seules fournir, ni leurs partenaires européens. Dans ce cadre, Starlink permet de transmettre des ordres entre les niveaux stratégiques, opérationnels et tactiques, de communiquer sur le champ de bataille, de piloter et de recevoir les images des caméras des drones et de bénéficier d'une connectivité lorsque les dispositifs terrestres sont hors service.

Pour permettre des actions militaires sur une telle échelle et avec un tel volume d'échange d'information, il apparaît essentiel que le produit résiste à minima aux différentes attaques des forces armées russes.

4. Les attaques sur Starlink

Nous l'avons vu précédemment, dès le début du conflit en Ukraine, Starlink a été activé pour fournir une connectivité essentielle à la population, à l'armée et au gouvernement ukrainien. Cette forte dépendance et l'utilisation d'une telle technologie a évidemment attiré l'attention des forces russes, notamment à travers des groupes cyber, les acteurs du renseignement et les forces armées en vue d'entraver, bloquer, paralyser ou détruire ce système de communication.

a. Les cyberattaques

Sans prétendre connaître et développer ici toutes les cyberattaques ayant eu lieu sur le produit Starlink, nous nous efforcerons d'en aborder deux, relativement documentées, issues d'un rapport du Center for Security Studies. Ce rapport illustre notamment les cyberattaques sur Starlink au début du conflit, en décrivant les attaquants cyber, leurs modes opératoires et l'organisation de leur « *kill chain* »⁶¹.

Une des premières cyberattaques^{cxvi} connues, qui ne concernait pas directement les satellites Starlink, a été dénoncée par le SBU⁶² en août 2023. Cette cyberattaque est attribuée officiellement à une unité réputée liée au service russe de renseignement militaire GRU⁶³ du nom de Sandworm⁶⁴.

Le mode opératoire de Sandworm :

Il repose sur une démarche progressive. Le groupe commence par identifier ses cibles et leurs vulnérabilités en collectant des informations et en exploitant des failles de sécurité, notamment au moyen de courriels frauduleux. Il prépare ensuite ses opérations en développant ou en adaptant des outils informatiques capables de s'introduire dans les systèmes visés, d'y rester discrets et, si nécessaire, de détruire des données.

Une fois l'accès obtenu, Sandworm conserve une présence durable sur les réseaux compromis afin de contrôler les systèmes à distance. Cette position lui permet de mener des actions variées, telles que l'espionnage, le vol d'informations sensibles, le sabotage ou la destruction d'infrastructures numériques. Certains logiciels, comme *AcidRain*, illustrent cette polyvalence en combinant des fonctions d'intrusion, de surveillance et de destruction.

Enfin, le groupe maintient son accès afin de préparer de futures opérations ou de poursuivre la collecte de renseignements. Ces actions s'inscrivent dans une logique stratégique visant à affaiblir les capacités de l'adversaire, perturber le fonctionnement de ses infrastructures critiques et soutenir les objectifs géopolitiques de la Russie.

Sandworm est associé à des attaques à des fins d'espionnage et de sabotage graves contre plusieurs entités de secteurs critiques dans le monde, notamment en Ukraine et les pays qui la soutiennent dans le cadre de la guerre déclenchée par la Russie en 2022. Reconnu pour ses capacités avancées en cyber-guerre, ses opérations furtives et ses techniques de sabotage de grande envergure, il a été notamment responsable de plusieurs attaques majeures, telles que le déploiement de logiciel malveillant destructeur et l'infiltration de réseaux militaires et civils (connu notamment pour NotPetya en 2017).

⁶¹ Modèle utilisé pour identifier et décrire les étapes d'une cyberattaque.

⁶² Le SBU (Service de sécurité d'Ukraine) est le principal service de sécurité intérieure de l'Ukraine. Il est notamment chargé de la contre-ingérence, du contre-espionnage, de la lutte contre le terrorisme et de la protection de la sécurité nationale.

⁶³ Security Service of Ukraine.

⁶⁴ Ou encore FROZENBARENTS, UAC-0082, Voodoo Bear, APT44, Unit 74455.

En 2023 donc, ce virus a déployé des logiciels malveillants sophistiqués dans le but d'infiltrer des appareils Android utilisés par les soldats ukrainiens et recueillir ainsi des informations sur la configuration des terminaux Starlink et leur connexion aux satellites. Sans pour autant cibler directement les satellites, ces opérations montrent une volonté de recueillir des renseignements sur le produit. L'effet de l'attaque de Sandworm sur la prise d'information du système reste, en ce qui est des sources ouvertes, inconnu à ce jour.^{cxvii}

Killnet quant à lui, est un groupe d'hacktivistes pro-russes, considéré comme un acteur de cyber-mobilisation, souvent impliqué dans des attaques par déni de service (DDoS) contre des cibles occidentales, notamment dans le contexte du conflit en Ukraine. Le mode opératoire ou « kill chain » de Killnet illustre une méthodologie structurée et efficace pour mener des cyberattaques, principalement par DDoS.

Le mode opératoire de Killnet :

Il repose principalement sur des attaques visant à perturber le fonctionnement des services en ligne. Le groupe commence par identifier ses cibles en recueillant des informations accessibles publiquement, notamment sur les sites internet et les réseaux sociaux, afin de repérer leurs points faibles.

Il prépare ensuite ses opérations en coordonnant ses membres et en mobilisant des réseaux d'ordinateurs compromis pour générer un important volume de trafic vers les systèmes visés. Cette surcharge provoque des ralentissements, voire l'interruption temporaire des services en ligne.

Au-delà de l'attaque elle-même, Killnet cherche à lui donner un fort retentissement médiatique. Le groupe revendique régulièrement ses actions sur les réseaux sociaux, en particulier sur Telegram, où il diffuse des messages à caractère politique ou idéologique. Cette stratégie vise autant à perturber les infrastructures ciblées qu'à exercer une pression psychologique, influencer l'opinion publique et démontrer sa capacité de nuisance.

C'est ce qu'il s'est passé les 18 et 19 novembre 2022, lorsque Killnet a revendiqué sur Telegram qu'il avait mené des attaques DDoS successives sur Starlink, qui empêchait alors de nombreux usagers de se connecter à Starlink. Cette attaque ne visait là encore pas le système satellitaire mais bien l'interface utilisateur, à la différence de l'attaque sur Viasat.

La réaction rapide de SpaceX, notamment par des mises à jour logicielles à distance, a permis de limiter l'impact de ces opérations. Bien que le service ait été interrompu plusieurs heures dans le cadre de Killnet, il semble toutefois assez réaliste d'énoncer que l'impact de telle cyberattaque reste minime sur le déroulement d'une guerre de plusieurs années, même si ponctuellement et temporairement un avantage peut être créé.

b. La guerre électronique.

En plus des cyberattaques, il existe aussi d'autres stratégies pour perturber les communications adverses. Sans développer toutes les techniques, nous en retiendrons deux, les plus évocatrices. C'est donc l'exemple du brouillage ou « jamming » et de la tromperie avec de faux signaux ou « spoofing ».

Le brouillage ou « jamming », consiste à perturber ou bloquer les signaux de communication par des émissions radioélectriques. Dans le conflit en Ukraine, la Russie a utilisé cette technique pour désorganiser les communications satellitaires, notamment celles de Starlink afin de limiter l'efficacité des opérations militaires ukrainiennes. Par exemple, des unités russes ont déployé des équipements de guerre électronique tels que les matériels « Volna Kupol Garant »⁶⁵ ou « Kalinka », actifs à compter de 2024 et qui émettent un brouillage dirigé spécifiquement vers les liaisons satellites Starlink.

Ces matériels de brouillage spécifiques sont en revanche coûteux, facilement repérables et énergivores, ce qui pour le moment ne permet leur utilisation que pour un format plutôt défensif (sur le territoire russe pour empêcher les attaques de drone de sites sensibles par exemple) ou ponctuel sur des phases d'effort militaire.



Image 18 : Photographie supposée du système de brouillage russe Volna Kupol Garant

Le « spoofing » consiste lui à envoyer de faux signaux pour tromper les récepteurs, notamment ceux de GPS ou GNSS, en leur faisant croire qu'ils reçoivent des données légitimes. Lors du conflit en Ukraine, des acteurs russes ont utilisé cette technique pour manipuler les systèmes de navigation, en particulier pour désorienter ou faire

⁶⁵ Système motorisé (camion avec ou sans remorque) avec alimentation électrique (autonome ou non), avec un rayon d'action de 20 km² environ pour brouiller les liaisons satellitaires Starlink.

dévier les véhicules ou drones ukrainiens. Ces attaques de spoofing peuvent durer plusieurs heures, provoquant des erreurs de positionnement et compromettant la sécurité des opérations militaires ou civiles.

Starlink en Iran en 2026 :

Il est intéressant de noter que le gouvernement iranien a réussi à brouiller de manière massive les communications via Starlink en janvier 2026. Présents avec plusieurs milliers d'exemplaires dans le pays, les terminaux servaient notamment à la population iranienne à se coordonner pour des actions de contestation du pouvoir alors en place.

Des moyens de guerre électronique, très probablement venus de Russie et de Chine, ont réussi à brouiller les communications via Starlink. Ainsi, le 9 janvier 2026, 80% du trafic Starlink en Iran est perturbé, réduisant à peau de chagrin les communications entre citoyens iraniens.

Une des raisons du succès du brouillage de Starlink en Iran et à la différence de l'Ukraine, est que les terminaux étaient relativement concentrés (dans les villes) et peu mobiles, donc plus facilement susceptibles d'être impactés durablement par le brouillage.

Une seconde raison de la durabilité du brouillage est que les moyens de guerre électronique n'avaient pas la possibilité d'être détruits par la population iranienne, au contraire de l'Ukraine où les forces armées ont des moyens de frapper ces systèmes dans la profondeur.

Si ces opérations n'affectent pas les terminaux ou les satellites de Starlink, ils peuvent rendre leur utilisation inutile voire dangereuse car faussée par les données d'entrée.

Pour renforcer la résilience contre les attaques de jamming et de spoofing, plusieurs solutions existent, dont les techniques d'étalement de spectre⁶⁶ qui permettraient de rendre la détection et le brouillage du signal beaucoup plus difficiles pour un attaquant. Une autre approche consiste à utiliser des techniques de dissimulation, où le signal est camouflé, rendant sa détection par un agent extérieur quasi impossible⁶⁷.

⁶⁶ Techniques de communications furtives et de dissimulation du signal : FHSS (Frequency-Hopping Spread Spectrum) ou DSSS (Direct Sequence Spread Spectrum). En changeant périodiquement la fréquence ou en dispersant le signal sur une large bande, ces méthodes empêchent un brouilleur de suivre ou de bloquer efficacement la transmission, car il lui faudrait une capacité de suivi en temps réel et une puissance de brouillage très élevée.

⁶⁷ Un entretien avec Monsieur Olivier BOYER sur les communications furtives est en annexe 3.

Un produit "*secure by design*" intégrant ces techniques permettrait de prévenir efficacement les attaques de jamming et de spoofing. Ces techniques pourraient permettre à des produits comme Starlink de maintenir leur disponibilité et la confidentialité de ses communications même en présence d'attaques sophistiquées, en respectant les principes fondamentaux de la communication furtive : faible probabilité de détection, faible probabilité d'interception, et faible probabilité d'exploitation. Comme dans le cas de la guerre des drones, les mesures de défense et les contre-mesures d'attaques se succèdent, reste à voir qui garde le plus longtemps l'avantage.

c. La destruction physique

Enfin, une façon assez simple et radicale d'empêcher le fonctionnement de Starlink reste la destruction physique de la chaîne de produit Starlink. Comme cela a été développé dans la partie technique, il suffit donc de détruire soit le terminal physique au sol, soit la grappe de satellites en orbite basse.

Le terminal physique au sol reste évidemment une cible nettement plus simple et accessible. Les terminaux ukrainiens sont ainsi régulièrement la cible de tirs de destruction de la part des forces armées russes. Cependant, le volume de terminaux fabriqués par SpaceX est de 15 000 unités par jour en 2024 et plus de 20 000 depuis 2025. Même si cette production n'a pas pour seule clientèle l'Ukraine, le stock ne semble donc pas manquer pour le moment.

En ce qui concerne la destruction de satellite en orbite basse, la Russie maîtrise le savoir-faire technique de destruction de satellite en orbite basse. Elle a à ce titre testé et réussi le tir d'un missile antisatellite qui a détruit un de ces vieux satellites en novembre 2021. Cependant la destruction d'un satellite dans l'espace n'est pas neutre. Ce test a en effet généré plus de 1500 débris orbitaux ainsi que de nombreux fragments plus petits, suscitant de vives critiques internationales en raison du risque pour les autres satellites et pour la station spatiale internationale (ISS).

L'intérêt pour la Russie de détruire physiquement un ou des satellites de Starlink se révélerait très coûteux pour elle :

- Financièrement d'abord : tirer un missile antisatellite pour détruire quelques satellites remplaçables rapidement n'est pas forcément rentable ;
- Techniquement ensuite : elle utilise aussi des satellites en LEO, qui pourraient être atteints par les débris ;
- Diplomatiquement enfin : son principal soutien dans le conflit, la Chine, a une forte politique de développement de satellites LEO dans l'espace et souhaite pouvoir l'exploiter. Détruire des satellites en LEO au risque de polluer de manière massive l'espace et gêner son principal soutien au conflit n'est pas dans l'intérêt russe.
- La lutte anti-satellite reste donc pour le moment une arme de non emploi dans le cadre ukrainien.

La résilience de Starlink (volume élevé de terminaux répartis dans l'espace géographique, faible latence satellitaire, transmission de données entre satellites...) a permis à l'Ukraine de pouvoir continuer à communiquer malgré les attaques subies. Ces dernières ont souvent été liées à des opérations de renseignement ou de sabotage, qui visaient les maillons les plus faibles de la chaîne de communication, comme les appareils Android des utilisateurs. Si le produit est résilient sur la partie satellite et terminal, il n'est en revanche, par sa nature, pas protégé comme peut l'être un produit militaire et reste accessible au plus grand nombre.

Cette faille majeure liée à la nature du produit conduira l'armée russe à utiliser jusqu'en février 2026 des terminaux Starlink sur certains de ses drones pour augmenter leur portée et contourner les brouillages, malgré les interdictions officielles et les sanctions. Ce point fera l'objet par la suite d'un développement plus approfondi.

5. L'évènement de Sébastopol

Avant d'évoquer ces événements ayant débuté en 2024, revenons à un épisode plus ancien, qui concerne une attaque ukrainienne avortée contre la flotte russe en mer Noire^{cxviii}. Dans sa biographie publiée en septembre 2023, Elon Musk affirme en effet avoir « ordonné secrètement à ses ingénieurs de désactiver la couverture satellitaire de Starlink dans un rayon de 100 kilomètres de la côte de Crimée », empêchant ainsi toute attaque de la flotte russe par des drones sous-marins ukrainiens via Starlink. La flotte de guerre russe, alors stationnée à Sébastopol en septembre 2022, aurait donc échappé à une attaque des FAU, sur décision unilatérale de M. Musk.



Image 19 : Base maritime de Sébastopol de la fédération de Russie.

Cette assertion, non démentie par les FAU ou par le gouvernement ukrainien par la suite, a été reprise par de nombreux articles de presse venant des médias du monde

entier⁶⁸ et a nourri le débat sur la place qu'un acteur privé pouvait occuper dans la conduite d'un conflit armé.

Les versions sur la nature du blocage divergent : s'agit-il d'un blocage par anticipation, et donc exclure la zone proche de la Crimée du signal satellitaire ? Ou s'agit-il plutôt d'une coupure satellitaire en pleine action, alors que les drones sous-marins ukrainiens étaient déjà envoyés et ont été interrompus avant d'atteindre leur objectif ? Les versions et contre-versions des uns et des autres ne permettent pas, en l'absence d'autres données, de trancher cette question. N'en demeure pas moins une question de fond : un acteur privé intervient et décide d'interdire l'usage de son produit à un État, alors même que ce dernier poursuivait un but de guerre précis, et non des moindres à savoir couler une partie de la flotte adverse.

Pour essayer de comprendre la nature d'un tel événement, nous allons tenter de décrire les mécanismes qui peuvent l'expliquer et en faire ensuite la synthèse.

Revenons tout d'abord au narratif de M. Musk, dont voici les principaux éléments de communication sur X (ex-Twitter), concernant la Crimée et les coupures de Starlink avant 2023 :

- 17/09/2022 : « *Starlink is meant for peaceful use only* »⁶⁹
- 03/10/2022: « *Crimea is formally part of Russia as it has been since 1783. (Until Khrushchev's mistake)* »⁷⁰
- 04/10/2022: « *Trying to retake Crimea will cause massive death, probably fail and risk nuclear war. This would be terrible for Ukraine and Earth* »⁷¹
- 08/02/2023: « *We were really pleased to be able to provide Ukraine connectivity and help them in their fight for freedom. It was never intended to be weaponized. However, the Ukrainians have leveraged it in ways that were unintentional and not part of any agreement.* »⁷² Gwynne Shotwell, présidente de SpaceX.

⁶⁸ Le Monde, CNN, The Washington Post...

⁶⁹ Starlink est destiné à un usage uniquement pacifique

⁷⁰ La Crimée fait officiellement partie de la Russie depuis 1783. (Jusqu'à l'erreur de Khrouchtchev)

⁷¹ Tenter de reprendre la Crimée entraînerait de nombreuses morts, échouerait probablement et risquerait une guerre nucléaire. Ce serait terrible pour l'Ukraine et la Terre

⁷² Nous étions vraiment heureux de pouvoir fournir à l'Ukraine une connectivité et de l'aider dans leur lutte pour la liberté. Cela n'a jamais été destiné à être militarisé. Cependant, les Ukrainiens l'ont utilisé de manière non intentionnelle et en dehors de tout accord.

- Finalement M. Musk en date du 07/09/2023 pour justifier son action, « Il y a eu des demandes urgentes des autorités pour activer Starlink au-dessus de Sébastopol. L'intention évidente était de couler la flotte russe à l'ancre. Si j'avais accepté leurs demandes, alors SpaceX aurait été explicitement complice d'un acte de guerre majeure et de l'escalade du conflit. »

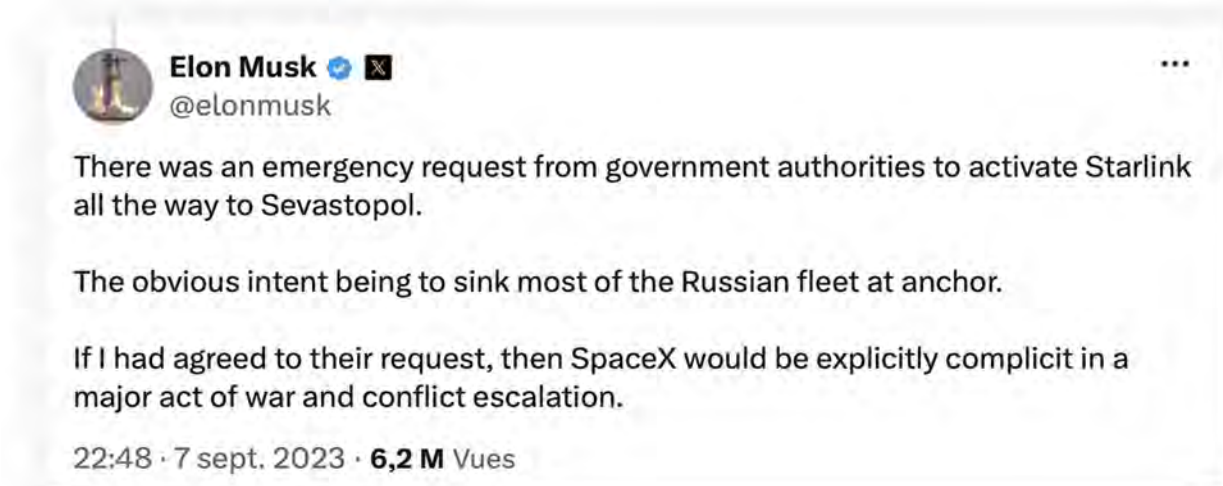


Image 20 : Tweet d'Elon Musk en date 7 septembre 2023. « »

Dans une rhétorique déjà utilisée de bon samaritain, ce dernier justifie donc cette interdiction d'emploi par la possibilité qu'une attaque ukrainienne réussie contre la flotte russe puisse conduire à une escalade du conflit avec une potentielle riposte nucléaire où la responsabilité de Starlink serait engagée. Ce premier niveau d'analyse colle au narratif de M. Musk mais n'est pas satisfaisant pour comprendre en profondeur les enjeux d'un tel blocage.

Les FAU, conscients du rôle stratégique de la marine russe en mer Noire et du blocus initié par cette dernière, persistent à attaquer la flotte russe stationnée dans le port de Sébastopol en Crimée. Une attaque, elle bien effective, a lieu le 29 octobre 2022, touchant plusieurs navires russes, à l'aide de drones maritimes et aériens. Si l'énoncé du *Battle Damage Assessment* varie en fonction de la source (guerre cognitive), la Russie annonce ensuite se retirer, temporairement dans les faits, de l'initiative céréalière de la mer Noire⁷³. Mais pas de déployer le feu nucléaire.

⁷³ En juillet 2022, inquiets de la pression mondiale sur les prix alimentaires comme du manque de marchandise, l'ONU et la Turquie réunissent les belligérants pour négocier l'initiative céréalière de la mer Noire (*Black Sea Grain Initiative*), qui autorise l'Ukraine à écouler ses produits via la mer moyennant des inspections russes dans le Bosphore. L'accord conclu entre l'ONU, la Turquie, la Russie et l'Ukraine établit ainsi un corridor humanitaire maritime sûr en mer Noire. Plus de mille navires chargés de céréales et d'autres denrées alimentaires ont quitté les trois ports ukrainiens de Tchornomorske, d'Odessa et de Ioujny/Pivdenny durant la période de mise en œuvre de l'initiative. Le 17 juillet 2023, la Russie a annoncé sa décision de mettre fin à l'initiative céréalière de la mer Noire, officiellement suite au bombardement du pont de Crimée. Cette solution aura permis à 32.9 millions de tonnes de marchandises d'être exportées pendant ce laps de temps.

Les arguments de Gwynne Shotwell, comme quoi Starlink n'a jamais eu pour vocation de devenir une arme dans la guerre en Ukraine, sont eux aussi peu crédibles, étant donné les combats documentés menés depuis déjà une année avec cette technologie et la volonté du gouvernement américain de mettre en place le Commercial Augmentation Space Reserve⁷⁴, où SpaceX est un candidat de premier plan.

Le problème de fond qui se pose en revanche, où M. Musk peut avoir de réelles craintes, est celui de « voir son projet engagé dans une situation guerrière qui lui échapperait » et où ses intérêts commerciaux pourraient être engagés. SpaceX fait ainsi signe à son principal client, en l'occurrence le gouvernement américain, qu'il ne doit pas être considéré comme un acteur militaire et donc ne doit pas être une cible pour un gouvernement. Son produit, sur le terrain, est quant à lui bien assimilé à un système d'arme. Il est donc dans une forme de zone grise juridique.

La réponse du gouvernement américain est rapide et prend bien en compte que cette zone grise doit être clarifiée, sans que cela semble effectif pour le moment, comme en témoignent les mots du général B. Chance Saltzman, chef des opérations de l'espace au sein de la *United States Space Force* : « *Going forward, all space users will be in the combat zone during a conflict. You cannot separate civilian and military assets in this domain. So, we all share the risk if a war comes to space.* »⁷⁵ M. Musk craint d'être associé à une arme, donc être une cible. Une cible d'autant plus fragile que ses intérêts le pousse à ménager la Russie et son principal soutien dans la guerre en Ukraine qu'est la Chine.

La Russie a en effet clairement indiqué par le biais des Nations Unies en octobre 2022^{cxix} qu'elle pouvait envisager les faits suivants : « *Nous souhaitons également souligner une tendance extrêmement dangereuse qui s'est clairement manifestée au cours des événements en Ukraine. Il s'agit de l'utilisation par les États-Unis et leurs alliés de composants d'infrastructures spatiales civiles, y compris commerciales, à des fins militaires. Apparemment, ces États ne réalisent pas pleinement que de telles activités constituent essentiellement une implication indirecte dans des conflits armés. Les infrastructures quasi-civiles peuvent devenir des cibles légitimes pour des frappes de représailles.* »

Comme évoqué plus haut, la Russie a la capacité de destruction de satellite, même si elle ne l'a pas utilisé dans un conflit. La menace est cependant bien comprise par SpaceX, qui donne ainsi, en empêchant une opération militaire d'envergure des FAU, une sorte de gage de bonne conduite. Ce que M. Musk redoute probablement n'est pas tant une attaque cinétique visant à détruire l'un de ses satellites par la Russie, mais plutôt une contrainte économique et financière sur ses intérêts.

⁷⁴ Le Commercial Augmentation Space Reserve (CASR) ou Commercial Space Reserve Program est un programme du département américain de la Défense et de l'U.S. Space Force visant à garantir l'accès prioritaire aux capacités spatiales commerciales en cas de crise ou de conflit.

⁷⁵ À l'avenir, tous les utilisateurs de l'espace seront en zone de combat pendant un conflit. Il est impossible de distinguer les actifs civils et militaires dans ce domaine. Nous partageons donc tous le risque si une guerre s'étend dans l'espace.

Nous l'avons dit plus haut, la destruction de satellite reste pour le moment une arme de non-emploi, la Russie ayant trop de contraintes pour l'utiliser librement. La Chine a toutefois le même discours officiel que la Russie sur l'emploi de Starlink comme une arme dans le conflit en Ukraine, et ces deux pays agissent de concert pour la mise en place du « *prevention of the placement of weapons in outer space and of the threat or use of force against outer space objects (PPWT)*⁷⁶ ». En considérant Starlink comme une arme, ces deux États légitiment sa destruction ou son obstruction dans l'espace comme sur terre.

Or, comme cela a été développé dans la seconde partie, M. Musk a de forts enjeux économiques avec la Chine, via Tesla notamment. Il se doit donc de maintenir de bonnes relations avec le gouvernement chinois, sous peine de sanctions ou d'actions de contraintes économiques. Et quand la Chine soutient la Russie pour dire que son produit est considéré comme une arme, le message est clair.

M. Musk est donc tiraillé entre plusieurs forces. D'un côté, il reçoit des messages directs de Mykhailo Fedorov⁷⁷ qui lui décrit la finalité stratégique de l'opération et la portée du système d'armes. De l'autre, il discute de la situation avec Jake Sullivan, conseiller à la sécurité nationale de Joe Biden, et enfin il appelle l'ambassadeur russe pour lui assurer que Starlink n'est utilisé qu'à des fins défensives. Rarement un chef d'entreprise n'a discuté à si haut niveau avec des décideurs politiques, des diplomates et des militaires.

Il devient un interlocuteur dont on ne peut se passer pour débloquer certains traits du conflit. Le fait de pouvoir à distance, sans en référer au gouvernement ukrainien, bloquer cette technologie, permet un réel "*kill switch*" (bouton d'arrêt) unilatéralement défini. L'Ukraine planifiait en effet certaines de ses opérations en ignorant que le service serait inopérant dans une zone géographique critique.

Les différents coups de fils émis ou reçus par M. Musk démontrent une façon totalement inédite de faire de la diplomatie, où les voies institutionnelles sont court-circuitées, du fait de la nature même de la dépendance technique. Même s'il n'est techniquement ni un diplomate ni un homme d'État (en tous cas en 2022), reste qu'il est traité comme un acteur souverain. Il est l'aveu d'un déplacement de l'autorité, qui passe de l'État vers un acteur privé qui détient la capacité opérationnelle critique. Ce déplacement n'a pas dû convenir aux diplomates et membres du gouvernement américain à l'époque.

⁷⁶ Le PPWT (Traité sur la prévention du placement d'armes dans l'espace extra-atmosphérique et de la menace ou de l'emploi de la force contre des objets spatiaux) est un projet de traité international parrainé par la Russie et la Chine. Présenté initialement en 2008 auprès de la Conférence du désarmement à Genève, il vise à « interdire le déploiement ou la menace de déployer des armes dans l'espace extra-atmosphérique ».

⁷⁷ Alors vice-Premier ministre ukrainien chargé du numérique.



*Image 21 : Le navire de débarquement russe *Caesar Kunikov*, détruit, filmé par le drone naval ukrainien MAGURA V5. 14 février 2024. Mer Noire. Image extraite de la vidéo de la Direction du renseignement du ministère de la Défense de l'Ukraine.*

D'aucun attribue ce déplacement d'autorité à la seule personnalité de M. Musk. C'est le cas de Dimitri Alperovitch⁷⁸ qui formule que "l'on est complètement à la merci de ses caprices et de ses désirs". Cette formule, qui peut paraître expressive, dit en termes précis la nature de la dépendance. Ce n'est pas une dépendance à une institution, à un État ou à un mécanisme contractuel. C'est une dépendance à une personne physique, dont les décisions sont par construction soumises à ses propres dynamiques psychologiques, idéologiques et économiques.

Il n'en reste pas moins vrai que l'épisode de Sébastopol soulève des questions inédites en termes juridiques. Le contrat entre l'Ukraine et SpaceX, dans la mesure où il existe formellement, est de nature commerciale et ne prévoit vraisemblablement pas de clauses opérationnelles permettant à l'opérateur d'en bloquer l'usage. Le fait que ce dirigeant d'entreprise ait pu, sans préavis et sans contestation effective, désactiver la couverture sur la Crimée, indique que le rapport contractuel entre l'Ukraine et SpaceX est, en pratique, déséquilibré au profit de l'opérateur.

De la même façon, cet événement démontre que la maîtrise d'une infrastructure de communication militaire alliée par un acteur privé tiers constitue, par construction, un facteur d'incertitude opérationnelle pour l'État client. Toute planification militaire ukrainienne ultérieure devrait, en théorie, intégrer le paramètre de la disponibilité conditionnelle du service Starlink, paramètre dont la valeur dépend des arbitrages d'un acteur privé étranger. Cette indétermination opérationnelle est un facteur de dégradation des capacités militaires ukrainiennes.

Surtout cet épisode créé un précédent. La coupure existe bel et bien, ce n'est plus une possibilité. Et ce déclenchement a un impact sur la crédibilité de M. Musk à

⁷⁸ Cofondateur du Silverado Policy Accelerator et figure reconnue de la cybersécurité américaine.

long terme. Illustrons nos propos avec l'incident de mars 2025. En février 2025, l'administration américaine Trump II exerce une pression croissante sur Kiev pour signer un accord concernant l'exploitation des ressources minérales ukrainiennes. Selon Reuters, cette pression inclut la menace de couper l'accès à Starlink afin d'inciter l'Ukraine à accepter des conditions économiques jugées très favorables à Washington. La menace a été évoquée après que M. Zelensky a rejeté une proposition initiale du secrétaire au Trésor américain, lors de rencontres à Kiev et Munich.

M. Musk avait alors déclaré, encore une fois sur X, qu'il « n'éteindrait jamais les terminaux », quel que soit son désaccord avec la politique ukrainienne, et qu'il ne les utiliserait jamais comme « monnaie d'échange ». Le raccourci avec des propos qu'il aurait prononcé joue cette fois-ci à son désavantage, où son image a pu être manipulée par le gouvernement américain et certains diplomates désireux d'en finir en agitant une épée de Damoclès au-dessus du gouvernement ukrainien.

6. Starlink et la diplomatie américaine

Les relations entre Elon Musk et l'administration américaine illustrent une transformation certaine des rapports entre les grandes entreprises technologiques et l'État fédéral américain. Loin de se limiter à une simple relation entre un entrepreneur et les pouvoirs publics, cette évolution met en évidence l'émergence d'un acteur privé disposant de ressources industrielles, technologiques et informationnelles capables d'influencer les décisions stratégiques des États. M. Musk apparaît comme un acteur hybride, à la fois partenaire industriel, fournisseur de capacités critiques, relais d'influence politique et détenteur d'infrastructures devenues essentielles à la sécurité nationale américaine.



Image 22: Elon Musk et Donald Trump lors d'un meeting en 2024. Les relations changeantes et ombragées entre les deux hommes rend difficile à prévoir l'évolution des relations entre l'administration et SpaceX.

Sous l'administration Biden (2021-2025), les relations sont marquées par une coopération pragmatique malgré des divergences politiques croissantes. Les agences fédérales, notamment la NASA et le Département de la Défense, continuent de confier à SpaceX des contrats stratégiques concernant les lancements spatiaux,

les satellites militaires et les capacités de communication. Cette dépendance s'accroît avec le déclenchement de la guerre en Ukraine en février 2022. En activant rapidement Starlink afin de maintenir les communications ukrainiennes, M. Musk démontre qu'une entreprise privée peut désormais fournir une capacité stratégique traditionnellement assurée par les États et renforce ainsi sa crédibilité envers les grands projets du gouvernement américain.

La guerre en Ukraine démontre ainsi que les infrastructures spatiales commerciales (pas seulement Starlink mais aussi des entreprises comme *Iceye*, *Maxar*, *BlackSky* ou autres...) constituent désormais des actifs indispensables aux opérations militaires, au renseignement et aux communications gouvernementales.

L'administration Biden est alors confrontée à une nouvelle réalité lors de l'épisode de Sébastopol : certaines capacités critiques de sécurité nationale ne sont plus exclusivement contrôlées par l'État mais par des entreprises disposant de leurs propres intérêts économiques. La signature d'un contrat entre le Pentagone et SpaceX en juin 2023 traduit cette volonté de reprendre une partie du contrôle sur une technologie devenue indispensable, en institutionnalisant une relation de dépendance entre le gouvernement américain et l'entreprise d'Elon Musk.

Parallèlement, les relations personnelles entre M. Musk et l'administration Biden se détériorent progressivement. Le dirigeant de Tesla critique ouvertement la politique économique de la Maison-Blanche, la fiscalité, la régulation des plateformes numériques ainsi que les orientations industrielles jugées favorables aux constructeurs automobiles historiques. Il joue pour son business qui n'est encore pas assez rentable pour Starlink. Ces tensions illustrent, comme évoqué dans la seconde partie, un affrontement plus large entre deux visions du rôle de l'État dans l'économie numérique : d'un côté, une volonté de renforcer les mécanismes de régulation et de l'autre, la défense d'une autonomie accrue des grandes entreprises technologiques, issue du libertarianisme autoritaire.

L'année 2024 marque un tournant avec le rapprochement politique entre Elon M. Musk et Donald Trump. En soutenant financièrement sa campagne présidentielle et en participant à certains échanges avec des dirigeants étrangers (participation à l'appel entre Donald Trump et Volodymyr Zelensky après l'élection présidentielle), M. Musk dépasse le rôle traditionnel d'un chef d'entreprise. Il devient un acteur disposant d'un accès privilégié aux centres de décision politique américains, pouvant ainsi influencer les rapports de force économiques et politiques de nombreuses manières.

Avec le retour de Donald Trump à la présidence en 2025, cette dynamique se renforce. Les entreprises de M. Musk occupent une position centrale dans plusieurs secteurs considérés comme critiques par les autorités américaines : espace et défense (SpaceX), intelligence artificielle (xAI), réseaux numériques (X corporation). Les capacités développées par SpaceX, Starlink, Tesla ou encore xAI deviennent des outils mobilisables au service des priorités stratégiques américaines. Cette proximité entre l'exécutif et un acteur privé favorise une convergence entre ses intérêts industriels et les objectifs de l'administration Trump II et de sa rhétorique,

tout en soulevant des interrogations sur la concentration du pouvoir technologique et informationnel entre les mains d'un nombre limité d'entreprises.

L'exemple des négociations autour de Starlink dans le contexte ukrainien illustre particulièrement cette évolution. Les discussions relatives au maintien ou à la limitation de l'accès au réseau satellitaire montrent que la maîtrise d'une infrastructure numérique mondiale peut constituer un véritable instrument de pression diplomatique. Dans cette configuration, l'entreprise ne fournit plus uniquement un service technique, elle détient un levier d'influence susceptible d'affecter les rapports de force internationaux. Cette capacité s'inscrit pleinement dans les logiques contemporaines d'intelligence économique, où la détention d'actifs technologiques critiques devient un moyen de produire de l'influence au même titre que les ressources militaires, énergétiques ou financières.

Ainsi, les relations entre Elon Musk et l'administration américaine traduisent une recomposition des équilibres entre puissance publique et acteurs privés. Elles illustrent l'émergence d'une forme de co-souveraineté technologique, dans laquelle l'État conserve son rôle décisionnel tout en dépendant d'entreprises capables de fournir des infrastructures essentielles à la sécurité nationale. Cette évolution met en évidence trois enjeux majeurs : la maîtrise des technologies critiques, la capacité d'influence des entreprises sur les politiques publiques et la sécurisation des dépendances stratégiques. Le cas de M. Musk et Starlink démontre ainsi que les grandes entreprises technologiques ne sont plus seulement des acteurs économiques, mais deviennent des acteurs géopolitiques à part entière, capables d'influencer les rapports de force internationaux et les équilibres de puissance.

Enseignements :

- La dépendance croissante aux infrastructures spatiales commerciales, comme Starlink, transforme la dynamique entre acteurs privés et États en matière de sécurité et de stratégie.
- La capacité d'un acteur privé à intervenir dans des conflits armés soulève des questions juridiques et éthiques sur la souveraineté et la responsabilité.
- La maîtrise des technologies critiques, telles que les satellites, devient un enjeu géopolitique majeur, influençant la puissance et la diplomatie internationales.
- La relation entre entreprises comme SpaceX et les gouvernements montre une évolution vers une co-souveraineté technologique, où le privé joue un rôle stratégique.
- La concentration croissante du pouvoir de l'État entre les mains des entreprises technologiques représente un risque pour la démocratie, pour la sécurité nationale, la régulation et l'équilibre des forces mondiales.

B. Qui paye ?

Si les coûts des premiers terminaux semblent supportés par l'USAID et SpaceX en mars 2022, les relations se tendent entre M. Musk et le gouvernement américain dès septembre de la même année. Une lettre de SpaceX transmise au Pentagone estime en effet que les opérations de Starlink en Ukraine coûteraient plus de 120

millions de dollars pour le reste de l'année et pourraient coûter près de 400 millions de dollars pour les 12 prochains mois^{CXX}. Il faut donc les financer.

Selon la lettre transmise, environ 85% des 20000 terminaux (de l'époque) transmis à l'Ukraine étaient payés par les États-Unis, le Royaume-Uni, la Pologne ou des entités privées. Ces financeurs contribuaient également à environ 30% des frais de connexion à internet, soit 4500 \$ mensuels pour les services les plus avancés d'après SpaceX.

M. Musk propose alors le 3 octobre 2022 un "plan de paix" en quatre points, favorable aux discours du Kremlin et résumé en un Tweet. Si le message n'a probablement aucune vocation diplomatique, il intervient quelques jours avant l'ultimatum fait au gouvernement américain de payer la facture de Starlink.

Une façon très habile de jouer sur les tensions de l'opinion publique et des relations internationales, comme en témoignent les réactions outrées des ukrainiens. Cela lui permet, après avoir jeté de l'huile sur le feu et au passage se ménager le Kremlin, d'être en position de force pour la négociation financière à venir avec le gouvernement américain, son produit étant essentiel à la défense du territoire ukrainien. Il maîtrise l'échiquier géopolitique du moment afin d'en tirer parti de manière assez habile. Dans un tweet datant du 07 octobre 2022, M. Musk annonce désormais que le coût des opérations en Ukraine est alors de 80 millions de dollars et dépassera les 100 millions à la fin de l'année. Le 17 octobre, il publie finalement que la demande de financement auprès du Pentagone est annulée. Ces chiffres changeants, associés à un manque de solutions alternatives, permettent à M. Musk de négocier au mieux son produit.



Image 23 : Post sur X d'Elon Musk le 3 octobre 2022

Si SpaceX ne paye plus, d'autres prennent le relais. Comme énoncé plus haut, le financement des terminaux Starlink et le coût des connexions initialement portés par le gouvernement des États-Unis se reportent alors vers l'Europe et ses alliés : Pologne en financeur principal, Allemagne, Royaume-Uni, France, Tchéquie

Enseignement :

La technologie Starlink répond tant aux besoins civils que militaire et s'inscrit dans un cadre historique :

- L'écosystème autour de Starlink n'en fait pas un acteur privé à part entière ; l'état américain et ses intermédiaires appuient massivement l'arrivée du produit en Ukraine.
- Le produit sait se rendre essentiel dans une logique du faible au fort. L'Ukraine est en désavantage numérique, industriel et militaire face à la Russie. Couper son système de communication revient à rendre ses structures militaires aveugles.
- Le produit Starlink n'est pas gratuit. Le transfert du coût financier de Starlink du gouvernement américain aux états européens s'inscrit dans une logique géostratégique précise (désengagement américain en Europe).
- M. Musk maîtrise habilement la communication pour se garantir des opportunités de négociation et d'influence, bien loin de ses propos humanistes.

...

C. Utilisation de Starlink par les forces russes dans la guerre en Ukraine

Plusieurs sources ont indiqué qu'en 2024 et 2025, des unités russes ont réussi à utiliser des terminaux Starlink sur le front ukrainien. Cette utilisation, bien que non autorisée par SpaceX, a permis aux forces russes d'améliorer leurs communications tactiques, le pilotage de drones et la coordination de l'artillerie. Les autorités ukrainiennes ont dénoncé un phénomène devenu « systémique » sur certains secteurs du front.

Cette brève analyse du phénomène d'appropriation de Starlink par les forces armées de la fédération de Russie (FAFR) a pour vocation de tirer de cette phase quelques enseignements sur la souveraineté des États.

1. Une logique « judoka »

Concernant ses systèmes de transmission, comme cela a été évoqué plus haut, la Russie ne dispose pas d'un équivalent opérationnel offrant la même combinaison de débit, de mobilité et de résilience que Starlink, ni des structures satellitaires associées. Des tentatives de brouillage, des cyberattaques ont bien eu lieu sur le produit mais sans succès probants. Cette situation a créé une forte incitation pour les forces russes à acquérir clandestinement des terminaux Starlink et conduire une tactique de retournement du produit et de son usage déterminant : « ce que je ne peux contrer, je vais alors tenter de l'utiliser à mon profit ».

L'utilisation du produit, même de manière artisanale (cf. photo ci-contre), permet aux FAFR de s'affranchir des effets de la guerre électronique menée par les forces armées ukrainiennes (FAU) et de bénéficier des infrastructures satellitaires de SpaceX, plus robustes et fiables que celles de Gonets, constellation satellitaire utilisée par les FAFR. Tout cela à moindre coût et en créant le trouble dans les états-majors ukrainiens.



Image 24 : Drone Molniya abattu avec sa console Starlink

2. La contrebande comme mode d'acquisition

Un rapport de l'USAID de 2025 indique que la fourniture des premiers terminaux Starlink à l'Ukraine était destinée à des usages civils, défensifs et en aucun cas à des activités militaires ou offensives. Ce rapport mentionne la difficulté d'établir une traçabilité précise des terminaux fournis dans un territoire en guerre et en situation d'urgence^{cxxi}. Dans les faits, il semble bien que l'USAID n'avait dès le début aucun regard sur l'utilisation finale des terminaux Starlink. Même si le volume de terminaux fournis par l'USAID est minime au regard des quantités de terminaux actuellement déployés en Ukraine (3% environ), la question de la traçabilité et du suivi et de l'emploi des produits reste centrale.

Du fait de sa structure, un terminal Starlink est un produit à l'achat et à la prise en main rapide, à l'usage facile, au transport relativement discret. Comme au Sahel pour les groupes criminels^{cxxii}, Starlink est alors devenu un produit de contrebande à destination des FAFR. L'utilisation de terminaux Starlink sur des drones russes a été signalée pour la première fois publiquement au début de l'année 2024. Depuis lors, les forces ukrainiennes ont documenté de multiples cas d'utilisation, notamment sur des drones type Shahed, Molniya ou encore BM-35.



Image 25 : Images de drones russe (de g. à dr.) Shaded, Molniya et BM-35.

Pour les FAFR, cela permet de renverser l'avantage initial et garantir ainsi des communications à longue portée, permettant aux drones d'effectuer des missions

de reconnaissance ou de frappe loin des opérateurs au sol. Cette capacité peut accroître l'efficacité des drones dits « suicides » en permettant la mise à jour des cibles en vol et le contrôle en temps réel au-delà de la ligne de visée radio.

Si SpaceX déclare de manière officielle ne pas vendre de manière directe ou indirecte de terminaux à la Russie, des pays intermédiaires, des trafiquants et des groupes criminels motivés par le gain ont permis son utilisation au sein des FAFR. Les terminaux Starlink ont ainsi transité par des « pays tiers » du Moyen-Orient, de l'Asie centrale et de l'Asie de l'Est, à travers de fausses déclarations douanières notamment ^{cxxiii}. Les terminaux trouvent alors plusieurs canaux de ventes en Russie, dont de grands sites commerciaux russes comme Wildberries et Ozon, ou bien avec des canaux spécifiques comme le site starlink777.ru où s'achètent directement des terminaux, assez proche de la frontière (Rostov-sur-le-Don).

Dernière étape pour permettre leur utilisation, les terminaux sont activés par des comptes enregistrés en dehors de la fédération de Russie, en Europe principalement, et les équipements « blanchis » peuvent alors fonctionner dans les zones de combat. Il est important de noter ici que l'obtention de quelques terminaux ne peut impacter significativement les actions militaires sur une zone de combat aussi étendue.

L'obtention des terminaux Starlink par les FAFR, et donc le trafic illicite, a dû être massive, bien que les chiffres ne soient évidemment pas publics. Le lieutenant général Budanov, alors directeur du renseignement militaire de l'Ukraine (GUR MOU), indique dès février 2024 que les FAFR utilisent Starlink ^{cxxiv} et précise également que « plusieurs milliers » de terminaux sont utilisés ^{cxxv}.

3. L'enquête américaine (2024)

Une enquête officielle de la Chambre des Représentants américaine ^{cxxvi} a alors lieu en mars 2024 et sollicite SpaceX pour l'usage présumé de la technologie Starlink par les FAFR. En mai 2024, le département américain de la Défense a déclaré qu'il travaillait à une solution pour empêcher l'utilisation non autorisée des systèmes Starlink par les FAFR. L'utilisation de Starlink par la Russie contrevient en effet aux règles d'exportation qui interdisent l'acquisition et l'utilisation de technologie américaine par la Russie (extraterritorialité de la technologie et du produit).

Bien que les détails des mesures initiées par le département de la Défense n'aient pas été divulgués, l'une des approches proposées consistait à mettre en place une « liste blanche » des identifiants de terminaux approuvés pour l'Ukraine et les régions contestées, bloquant ainsi efficacement toutes les unités non enregistrées. En juin 2024, le Pentagone a annoncé avoir réussi à désactiver plusieurs centaines de terminaux Starlink non autorisés entre les mains des Russes.

Cependant, certains éléments sur le terrain suggèrent que cette mesure n'a pas complètement résolu le problème. Les FAFR ont continué d'acquérir des terminaux par des voies non officielles pour les intégrer à leurs plateformes aériennes. En réponse, l'Ukraine a exploré d'autres fournisseurs de satellites européens, à la

recherche d'une infrastructure de communication plus sûre et plus contrôlable pour ses opérations militaires.

C'est le cas notamment d'Eutelsat, qui a déclaré en avril 2025 qu'elle fournissait, via OneWeb, des capacités de communication en LEO à l'Ukraine grâce à un financement allemand depuis environ un an. L'entreprise a mis à disposition « *moins d'un millier de terminaux* » et compte en déployer jusqu'à 10 000 dans un avenir proche, sans que le financement soit connu pour le moment (Allemagne ou UE)^{cxxvii}.

Eutelsat avait commencé à investir dans OneWeb en 2021. Les deux sociétés ont ensuite annoncé leur rapprochement en 2022, puis la fusion est devenue effective le 28 septembre 2023. Eutelsat est l'opérateur européen historique de télécommunications par satellite qui exploitait surtout des satellites GEO (géostationnaires). OneWeb est à l'origine une entreprise britannique spécialisée dans les satellites en orbite terrestre basse (LEO). Elle possède aujourd'hui plus environ 600 satellites en LEO, à une altitude plus élevée que ceux de Starlink (1200 km contre 550 km).

La couverture n'est donc pas la même puisque même si Starlink a plus de satellites, chaque appareil OneWeb couvre une plus grande surface. Une plus grande altitude est toutefois synonyme d'une plus grande latence. Starlink pourrait ainsi offrir jusqu'à 490 fois plus de capacité que OneWeb rien qu'au-dessus de l'Ukraine. La question du prix du terminal et de l'abonnement se pose aussi, OneWeb étant nettement moins compétitif sur ce plan.

4. Le tournant de 2026

L'utilisation de Starlink par les FAFR s'est en effet accélérée en 2025, dans un premier temps sans impact significatif. À l'automne 2025 toutefois, les effets de son utilisation dans les opérations de drones russes se sont amplifiés et les attaques multipliées, amenant les autorités ukrainiennes à s'emparer de ce sujet stratégique^{cxxviii}. Certains pays contributeurs à la défense de l'Ukraine et au financement de Starlink, comme la Pologne, sont alors montés au créneau pour demander à SpaceX de couper les terminaux Starlink utilisés par les FAFR.

Début 2026, Mykhailo Fedorov, fraîchement nommé ministre de la défense, affirme avoir pris contact avec les équipes de SpaceX pour trouver une solution aux problèmes de drones russes équipés de terminaux Starlink^{cxxix}. SpaceX a alors mis en place plusieurs mesures dont :

- Une vitesse de vol limitée à 75 km/h car les drones russes ont une vitesse supérieure aux drones ukrainiens. Avec cette restriction, les opérateurs

russe perdent leur capacité à contrôler les drones qui dépassent cette limite de vitesse et l'effet sur le terrain est moindre^{cxxx};

- La création, comme suggérée par le département de la Défense américain, d'une « liste blanche » des terminaux. Son objectif était de recenser l'ensemble des terminaux qui, après vérifications, pourraient rester connectés à la constellation satellitaire Starlink sur le sol ukrainien. SpaceX désactivera ainsi les terminaux Starlink en Ukraine qui ne sont pas référencés sur Delta (plateforme militaire) ou Diia (portail civil) ;



Image 26 : Opérateur de drone à Kharkiv dans les tranchées en 2024. Image BBC.

Pour les usagers militaires, une fois inscrits sur la liste blanche, une vérification quotidienne de l'authenticité de l'acteur derrière le terminal via un code unique transmis par la hiérarchie militaire. Le code est à rentrer dans une fenêtre de quelques secondes (10 secondes maximum) sur un support numérique^{cxxxi}.

Le 02 février 2026, le ministre Fedorov confirme que tous les terminaux vérifiés et authentifiés auront le droit de fonctionner et les autres seront exclus. En parallèle, les cyber-spécialistes ukrainiens de la 256e division d'assaut cybernétique vont alors créer un « honeypot ⁷⁹ » permettant d'identifier en temps réel les emplacements précis des terminaux Starlink introduits illégalement en Russie via des pays tiers et utilisés par les FAFR^{cxxxii}.

Pour cela, le 02 février 2026, cette unité agit par la diffusion de faux canaux et de bots sur l'application Telegram, proposant l'activation payante des terminaux en intégrant la « liste blanche » du réseau Starlink. Simultanément, le groupe d'activistes InformNapalm lance une opération de phishing sur les terminaux des soldats russes, permettant de collecter de nombreuses données (dont la géolocalisation) sur environ 2400 terminaux d'unités des FAFR. Ces informations

⁷⁹ Pot de miel

ont ensuite été transmises au service de sécurité ukrainien (SBU) à des fins de renseignement et aussi de ciblage^{cxixiii}.

L'opération a également « permis d'identifier des personnes tentant de fournir aux russes des services d'inscription de terminaux sur des « listes blanches » afin de contourner les restrictions imposées par SpaceX ». En clair, des ukrainiens qui fournissent aux russes des terminaux Starlink contre de l'argent ou autre, donc de la corruption. Cet aspect souvent négligé explique aussi le volume important de terminaux utilisés par les FAFR.

Le 4 février 2026, après le traitement des données de la « liste blanche », la désactivation des terminaux « non-ukrainiens » sur le territoire a été effective, ouvrant une fenêtre d'opportunité tactique majeure pour les forces armées ukrainiennes. Outre la désorganisation de leur C2 (command and control ou capacité à donner des ordres et à superviser leur exécution), les FAFR ont vu leurs opérations de drones lourdement affectées et se sont retrouvées en quelque sorte « aveugles », ce qui va permettre les contre-offensives ukrainiennes dans une dizaine de secteurs du front.

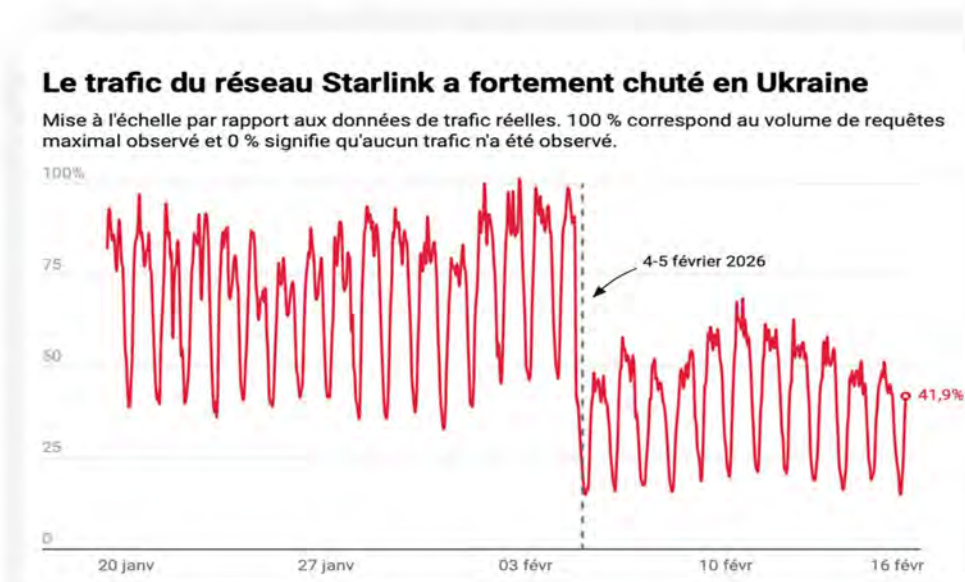


Image 27 : Comparatif avant / après coupure Starlink sur le front. Le Grand Continent, « L'armée ukrainienne tire profit de la déconnexion des forces russes de Starlink pour contre-attaquer ».

On observe ainsi une forte chute du trafic sur le réseau Starlink du 20 janvier au 16 février. Les FAU gagneront ainsi environ 300 km² de terrain en deux semaines au détriment des FAFR, soit le plus grand gain territorial depuis juin 2023. Ces gains territoriaux sont relativement limités au regard de la perturbation des FAFR et traduisent l'absence de réserves FAU suffisantes pour exploiter pleinement cette vulnérabilité des FAFR.

Certaines sources ukrainiennes affirment que des cas résiduels d'utilisation des FAFR de Starlink ont continué à être observés, avec des volumes nettement moindres qu'auparavant évidemment.

5. Synthèse

Après avoir recensé les événements majeurs ayant trait à Starlink en Ukraine, nous allons désormais tâcher d'en synthétiser les grandes tendances.

À son arrivée en Ukraine, l'utilisation du produit Starlink semble plutôt claire : des financeurs institutionnels ou privés, et une décision de l'emploi du produit qui revient à l'Ukraine en tant qu'exploitant du produit, comme le figure le schéma ci-dessous.

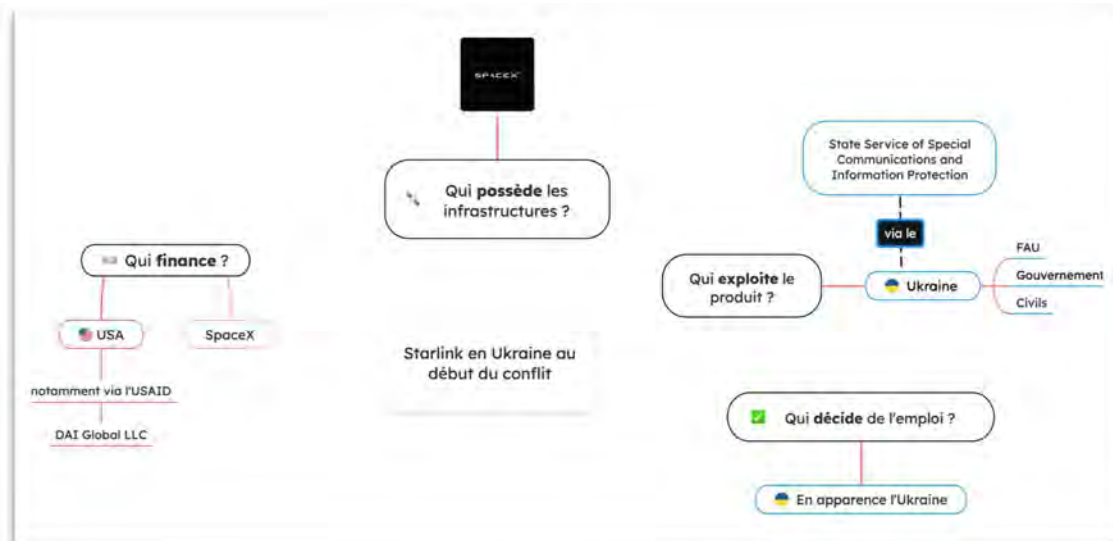


Figure 7 : Représentation schématique des enjeux liés à Starlink au début du conflit.

L'évènement de Sébastopol et les pressions de M. Musk pour obtenir des financements auprès du gouvernement américain vont faire évoluer ces rapports de force. Le schéma évolue donc ainsi pour l'année 2023 :

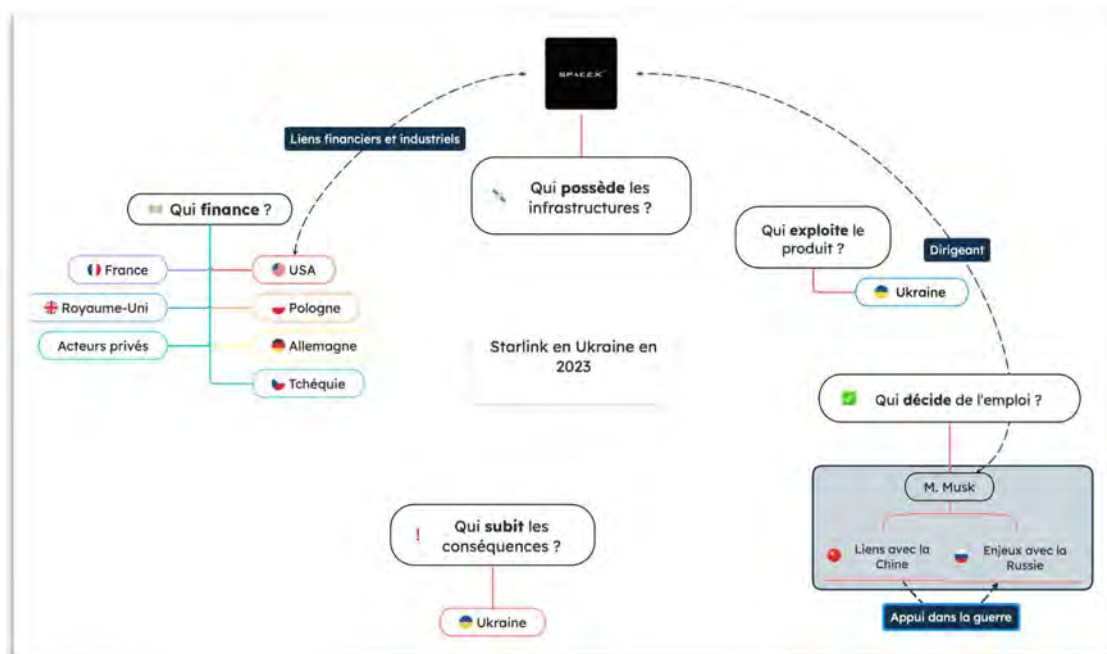


Figure 8 : Représentation schématique des enjeux liés à Starlink en 2023.

Initialement financé par le gouvernement américain et SpaceX, le coût de Starlink est finalement transféré aux États européens (Pologne et Allemagne en tête), qui ne bénéficient pas de l'usage direct du produit mais soutiennent par-là l'effort de guerre ukrainien. L'Europe finance un concurrent spatial direct, sans bénéficier ni de l'usage du produit ni d'un poids quelconque quant à la décision de son utilisation. Premier déséquilibre.

Second déséquilibre : la décision de l'emploi du produit n'est pas dans la main de celui qui exploite le produit. M. Musk décide effectivement de l'usage de Starlink en lieu et place de l'Ukraine, en fonction de ses intérêts. Celui qui subit les conséquences de la décision d'emploi est aussi celui qui exploite le produit⁸⁰.

L'utilisation de Starlink par les FAFR en 2025 et 2026 transforme également les rapports de force qui continuent à se dégrader pour les utilisateurs comme pour les contributeurs financiers.

Du côté des gouvernements, ces derniers manquent clairement de levier d'actions facilement utilisables face à SpaceX et aux peu de données accessibles. En tout premier plan se place l'état ukrainien, qui doit soumettre tout ou partie de ses plans militaires pour validation à M. Musk. Mais il y a tout aussi frustrant pour les états-majors ukrainiens : ne pas pouvoir couper directement l'accès aux terminaux aux FAFR et que ces derniers conduisent pendant ce temps des actions militaires contre l'état ukrainien. À ce titre M. Fedorov semble avoir pour tâche majeure de maintenir une bonne entente avec M. Musk, décideur final de l'utilisation du produit, et ce depuis le début du conflit.

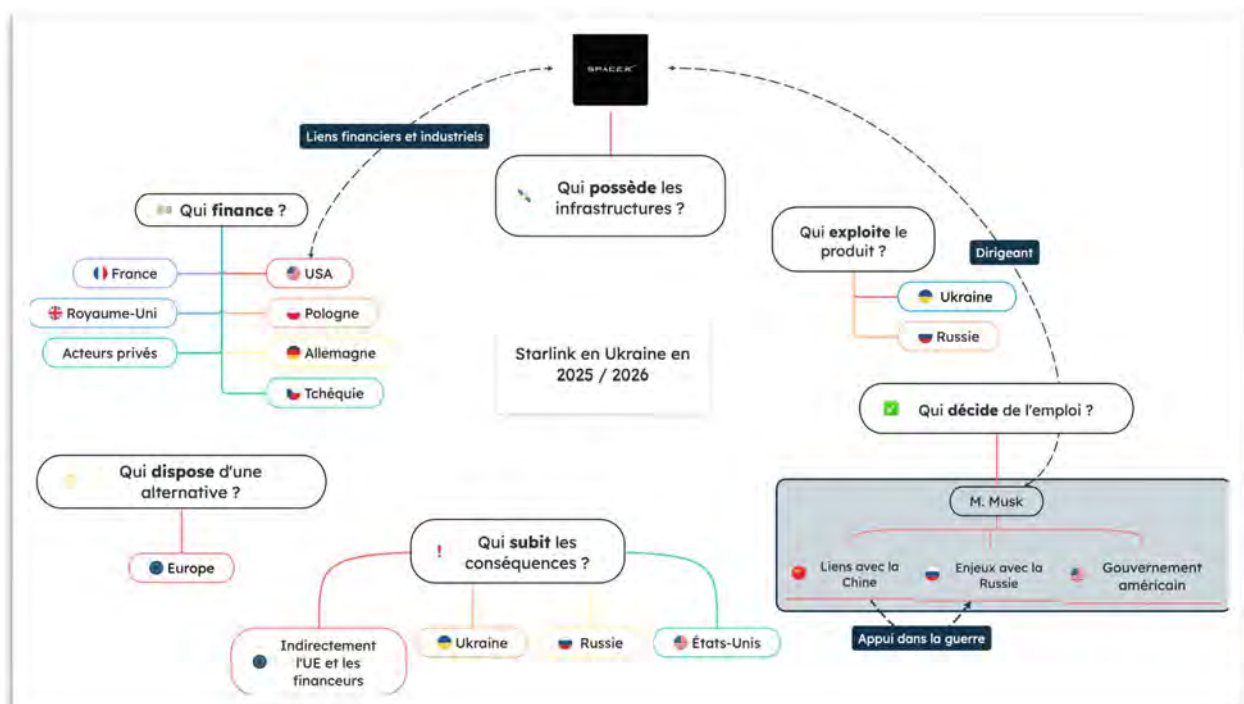


Figure 9 : Représentation schématique des enjeux liés à Starlink en 2025-2026

⁸⁰ Exploiter au sens de l'utilisation directe du produit, pas de l'exploitation industrielle.

L'état américain n'est également pas en reste dans le manque de levier face à l'utilisation du produit, bien que principal financier du projet originel. On notera à ce titre les sept questions - assez vastes - posées par la Chambre des Représentants à SpaceX pour tenter d'y voir plus clair sur l'usage potentiel de Starlink par les FAFR et les enjeux en termes de sécurité nationale.

Sur l'échiquier géopolitique, il y a donc un acteur - l'État américain - qui n'a pas de levier direct pour contrôler qu'une entreprise privée - américaine - avec une technologie duale ne fournisse pas sa technologie et ses produits à un autre état aux intérêts contraires. Il y a là une réelle perte de contrôle sur les intérêts nationaux. L'OFAC⁸¹, un organisme de contrôle financier du département du Trésor des États-Unis chargé de gérer les sanctions économiques, pourrait se saisir du dossier. Cependant, cela supposerait de prouver que Starlink reçoit des revenus indirects ou des bénéfices provenant de la Russie, ce qui n'est pas formellement avéré.

On voit également que les efforts menés par le Pentagone ne correspondent pas aux enjeux réels : la coupure de quelques centaines de terminaux sur les plusieurs milliers utilisés par les FAFR est anecdotique. Quelques soient les mécanismes déployés, ils ne suffisent pas, ce qui peut constituer un aveu de faiblesse pour une si grande institution. Le contrôle de l'infrastructure et du système de communication est bel et bien dans la main de SpaceX et de M. Musk, sans contrepouvoir réel de l'administration américaine.

Un produit librement accessible par sa nature même - à savoir fournir internet au plus grand nombre - et son coût relativement faible arrivera tôt ou tard dans la main de personnes dont l'intention n'est pas seulement d'avoir accès au « *Netflix and chill* »⁸². Le cas de l'utilisation de Starlink par les FAFR et son détournement de l'usage initial n'est pas nouveau. Comme l'indique ce rapport^{cxxxiv}, Starlink est devenu un outil utilisé par les groupes armés et les réseaux criminels au Sahel, rendu possible par la contrebande.

La question de l'authenticité de l'utilisateur se pose alors, question qui a mis un certain temps à se régler dans le cas du conflit en Ukraine - au moins un an - et avec des effets certains sur les opérations militaires. Si Starlink se veut source d'accès à l'information, il est aussi de facto source accrue de conflits. Dans un monde globalisé où les flux licites et illicites de marchandises favorisent les échanges commerciaux, la traçabilité du produit se doit d'être garantie dès la conception du produit.

S'il les FAU avaient eu de la réserve, il est fort à parier que les revers militaires côté russe auraient été plus lourds à la suite de la coupure de leurs systèmes. La logique initiale des FAFR était bonne mais la trop grande dépendance à ce même produit se retourne contre eux et la mise en place d'une liste blanche dessert encore une fois l'exploitant du produit, qui l'utilisait de toute façon de manière détournée.

⁸¹ Office of Foreign Assets Control

⁸² Expression signifiante « S'asseoir dans le canapé, regarder Netflix et ne rien faire d'autre ».

Il est donc logique que les utilisateurs d'un tel produit, qui n'ont pas la capacité de décision d'emploi, cherchent à se diversifier pour essayer de retrouver une capacité à pouvoir décider sans interférence supérieure, soit la définition de la souveraineté telle que définie dans ce mémoire. Les solutions en LEO via OneWeb le permettent, à une échelle moindre que Starlink. Pour l'imagerie satellitaire, des entreprises comme ICEYE permettent à l'Ukraine une forme de diversification par rapport à des acteurs aux intérêts essentiellement américains⁸³ et soumis aux pressions du politique.

Concernant Starlink, bien que décideur final et pour le moment le seul à sembler profiter des événements, il n'est pas certain que la situation lui soit entièrement favorable à terme. Bien que le produit renforce son influence auprès du gouvernement américain, il fait également l'objet de critiques quant à son monopole potentiel et à la volonté de son dirigeant. La logique de pouvoir et de puissance s'applique ici. Par ailleurs, SpaceX nécessite des financements et des débouchés pour assurer sa pérennité. Se priver de marchés ou risquer de froisser certains cercles du gouvernement américain ne constitue pas une stratégie économiquement viable à long terme.

Entrer dans le jeu des puissances implique aussi un changement d'état d'esprit et d'échelle, et ça n'est pas, à priori, le rôle et la vocation d'une entreprise comme SpaceX qui, rappelons-le, a théoriquement une vocation commerciale.

Enseignements :

- Le gouvernement américain semble n'être qu'un spectateur sans levier d'action dans l'utilisation par l'Ukraine, et la Russie, de la technologie Starlink.
- Starlink, par son coût / efficacité, devient par la force des choses un outil dans les conflits à travers le monde. La question de l'authentification de l'utilisateur final du produit est complexe à régler.
- L'utilisation par la Russie de Starlink et la perte des terminaux du jour au lendemain semble avoir assez désorganisé l'armée russe en local pour permettre aux ukrainiens des percées.
- Starlink, par l'usage qu'il en est fait par des acteurs étatiques ou non et par l'indépendance marqué commence à s'attirer des critiques qui pourraient à terme l'obliger, sous menaces de voir les financements se stopper, revoir sa politique de distribution et d'usage qu'il peut en être fait.

⁸³ Maxar, Space flight entre autres.



IV. Conclusion



IV. Conclusion

L'origine de la problématique de ce mémoire est partie d'un constat. Au cours de la guerre en Ukraine en 2022, M. Musk a pu, semble-t-il à lui seul, imposer successivement sa volonté à l'Ukraine et à la Russie dans leur utilisation réciproque du produit Starlink. Dès lors, une question se pose : comment un dirigeant de société a-t-il pu tenir un rôle majeur dans le premier conflit européen de grande échelle du XXI^e siècle ? Et donc par extension, dans quelle mesure le déploiement de Starlink en Ukraine redéfinit-il les rapports de force entre acteurs étatiques et entreprises technologiques privées ?

Après avoir brossé un vaste panorama allant de la genèse de Starlink à son emploi dans le cadre du conflit en Ukraine en passant par le statut particulier de son dirigeant, nous allons désormais nous attacher à répondre à la problématique fixée, en tenant compte des enseignements qui découlent des parties rédigées ci-dessus.

Le sens de l'histoire des communications stratégiques.

Rappelons tout d'abord que la communication constitue une condition structurelle de l'existence et du fonctionnement de l'État. Ensuite que l'histoire des communications stratégiques étatiques est moins celle d'un progrès linéaire que celle d'un équilibre instable entre efficacité opérationnelle et exposition accrue aux risques informationnels.

Si le déploiement de Starlink est providentiel pour l'Ukraine et son armée face à l'invasion de la Russie en 2022, l'usage détourné du satellitaire dans un conflit, i.e la récupération d'un produit civil pour un usage militaire, est quant à lui bel et bien le fruit de l'histoire des communications et porte donc son lot d'avantages et de menaces.

Les systèmes de communication ont eu pour moteur les besoins des États de répondre au triptyque rapidité-confidentialité-intégrité, besoins qui se sont complexifiés dans le temps dans une course à la communication entre l'expéditeur et l'intercepteur. L'histoire de ces systèmes montre que l'accroissement de leur technicité exige des ressources humaines et des moyens associés toujours plus complexes. Ces derniers ont de tout temps été formés, entretenus et pilotés par des structures étatiques. Starlink est un exemple parfait de cette assertion à la nuance près, et qui a son importance, qu'il est issu d'une structure privée au financement originel majoritairement public.

Le déploiement massif du produit sur un théâtre de guerre apparaît véritablement comme une opportunité commerciale pour SpaceX. La fourniture de kit en urgence à un pays en guerre est en effet un moyen pour M. Musk de prouver, à un instant charnière de la vie de sa société, la valeur de son produit. Il peut alors continuer à glaner des contrats auprès d'un gouvernement américain désireux de garder l'avantage mondial, en particulier sur le plan de la technologie militaire.

L'utilisation croissante de système duaux en temps de guerre.

Le kit Starlink comme le produit Tooway représentent l'évolution logique des enjeux et des besoins en communication des états, avec des systèmes numériques omniprésents dans les communications militaires (Kropyva, Delta pour l'Ukraine ou encore le JADC2 pour les États-Unis). Particulièrement simples à utiliser, adaptables et susceptibles d'être produits en masse, ces produits répondent aux besoins des unités de contact des FAU et deviennent de facto des systèmes d'armes, susceptibles d'être visés sur l'ensemble de leur chaîne de valeur, d'où la déclaration de la Russie à l'ONU à ce sujet.

La cyberattaque sur Viasat et les tentatives de brouillage ou de destruction sur les produits Starlink en sont la preuve matérielle. L'utilisation de cette technologie duale et transnationale entraîne des dégâts collatéraux sur des utilisateurs extérieurs au conflit, comme en témoignent les effets de la cyberattaque sur Viasat sur les parcs éoliens allemands, sans qu'aucun mécanisme visible n'en compense les effets.

Faute d'infrastructures existantes, l'autonomie satellitaire ukrainienne n'est pas acquise en 2022, ni pour le reste de la guerre d'ailleurs, et entraîne une dépendance importante des troupes au système alors en place, Viasat. L'État ukrainien se reposant pour la couche de transport sur un acteur externe au conflit, il délègue donc à un tiers une partie de la mise en œuvre de son système de communication et en cela n'a déjà pas la « capacité de décider sans interférence supérieure », et n'est donc pas souverain à ce sujet. L'emploi de Starlink ne change rien sur ce plan car la dépendance existe déjà.

Des technologies en gestation depuis des décennies.

L'attaque sur Viasat implique également un changement de paradigme technologique : l'orbite géostationnaire s'efface au profit du LEO. Cette technologie offre une couverture étendue, une faible latence et une résilience accrue, même si elle reste vulnérable aux attaques de brouillage et de spoofing sophistiquées, qui ont elles aussi des coûts certains à grande échelle. La convergence des réseaux satellitaires et terrestres, notamment avec la 5G et la fibre optique, souligne l'importance stratégique de la cybersécurité pour protéger ces infrastructures critiques face aux menaces contemporaines.

La simplicité d'utilisation de tels produits ne doit toutefois pas faire oublier que leurs architectures reposent sur des infrastructures critiques plus vulnérables. Pour Starlink, c'est notamment le cas des stations au sol et des constellations de satellites en orbite basse. Celles-ci semblent pour le moment bien résister aux effets déstabilisateurs et destructeurs des attaques russes dans le cadre ukrainien.

L'efficacité et la force de Starlink sont intrinsèquement liées à la maîtrise de toute la chaîne de valeur par SpaceX : lanceur, site au sol, fusées, satellites, terminaux, obtention des ressources orbitaires et spectrales via différents gouvernements... Starlink, via SpaceX, mène une politique industrielle agressive pour garder

l'avantage du LEO, ce qui rappelle d'une certaine façon l'histoire de l'expansion vers l'Ouest au XIXe siècle et la course au premier venu.

Ainsi, si Starlink s'impose d'emblée en Ukraine, c'est aussi et surtout parce qu'il ne sort pas de nulle part : il est le fruit d'une réflexion de long terme et d'investissements financiers publics massifs, avec pour appui celui prépondérant du gouvernement américain. Il s'inscrit également dans une politique industrielle et technologique plus large - programme Starship - qui l'engage à faire en permanence ses preuves sur le plan technique et atteindre sa viabilité commerciale.

L'écosystème qui permet à Starlink de s'implanter en Ukraine n'en fait pas un acteur privé isolé car l'État américain et ses intermédiaires appuient l'arrivée du produit en Ukraine : USAID, DAI Global LLC... Pour autant, SpaceX est une société alors non cotée en bourse, contrôlée par son fondateur. Aucun contre-pouvoir de l'actionnariat, aucune obligation de publication ne vient alors encadrer une décision de déploiement, de restriction ou de désactivation du service. La dépendance est reconnue par les responsables américains eux-mêmes, de la NASA au Pentagone, sans qu'aucun levier de correction n'ait été identifié.

Une logique financière et géopolitique pour un acteur privé.

M. Musk maîtrise habilement la communication pour se créer des opportunités de négociation et mener des actions d'influence, éloignées de ses propos humanistes destinées au grand public. Son idéologie, associée au libertarianisme autoritaire, est renforcée par sa présence au gouvernement et sa proximité avec le pouvoir américain à compter de 2025, ce qui en fait un cas hors norme puisqu'il est présent à certains instants du conflit sur une large partie de la chaîne de décision.

Bien que dépendant financièrement des États-Unis pour le financement de SpaceX, M. Musk a aussi de forts enjeux financiers avec la Chine, appui de la Russie dans le conflit. Cette géopolitique économique se traduira au cours du conflit par une lenteur voire un refus de répondre aux attentes des ukrainiens et parfois même à celles du gouvernement américain. Ce dernier subit alors la décision d'emploi du produit, comme les gouvernements de l'Ukraine ou de la Russie, se rapprochant comme nous le verrons enfin des relations de vassalité.

Le produit Starlink n'est bien évidemment pas gratuit. Le transfert du coût financier de Starlink du gouvernement américain vers les États européens à compter de fin 2022 s'inscrit dans la logique géostratégique du désengagement américain en Europe et permet à SpaceX de trouver un financement diversifié.

L'Ukraine est initialement en désavantage numérique, industriel et militaire face à la Russie et dans ce cadre, le produit sait se rendre essentiel dans une logique du faible au fort. Couper le système de communication - comme pour l'attaque avortée de Sébastopol - revient à rendre les structures militaires aveugles et annule certains effets stratégiques. M. Musk sait jouer sur ces rapports de force pour envoyer des signaux à ses principales relations économiques, en fonction de la situation qui

l'arrange. En cela il modifie la relation entre entreprises et gouvernements, où le privé joue in fine un rôle de décideur stratégique, fonction de ses intérêts propres.

La concentration croissante du pouvoir de l'État entre les mains des entreprises technologiques représente un risque de mise à mal des systèmes démocratiques, avec de possibles impacts sur la sécurité nationale, la régulation et un certain équilibre des forces mondiales.

Un accès au produit difficilement maîtrisable.

L'accès à l'information dans ses trois dimensions a donc un coût bien documenté. Dans un conflit moderne de haute intensité, il apparaît de façon limpide qu'une des clés pour la victoire revient à la capacité de décision éclairée des forces armées sur le terrain et donc à l'accès à l'information. L'utilisation de Starlink par les FAFR et la perte des terminaux du jour au lendemain semble avoir assez désorganisé l'armée russe au niveau local pour permettre aux ukrainiens des percées, témoignant de la supériorité technique de Starlink sur le système de transmission russe.

L'accès au produit pour un acteur malveillant n'est pas maîtrisé et la question de l'authentification de l'utilisateur final du produit reste complexe à réguler. Par son rapport coût-efficacité et sa capacité à maintenir les liaisons, Starlink devient par la force des choses un outil souvent dangereux dans les zones de tensions à travers le monde : guerre en Ukraine, conflit en Iran, enjeu pour Taïwan, utilisation par les djihadistes au Sahel... Il ne fait plus figure d'un simple accès au « *Netflix and chill* » et met les États face à un dilemme quant à son déploiement, puisque l'accès à une telle technologie implique de facto une perte de souveraineté. Là encore, il rebat les cartes que les États avaient traditionnellement en main et forcent ces derniers à négocier davantage et perdre de leur capacité de décision propre.

Vers une forme de co-souveraineté ?

La dépendance croissante aux infrastructures spatiales commerciales comme Starlink transforme la dynamique entre acteurs privés et États en matière de sécurité et de stratégie. La capacité d'un acteur privé à intervenir dans des conflits armés ou à s'immiscer dans les enjeux géopolitiques soulève des questions juridiques et éthiques sur la souveraineté et la responsabilité de tels acteurs.

Dans cette optique, aucun État européen ne dispose de levier actionnarial, réglementaire ou industriel sur SpaceX, bien que l'Union Européenne tente de réguler l'accès aux marchés. La lente diversification par l'Ukraine de ses sources d'accès au satellitaire envoie un signal aux européens, qui se doivent de réagir de manière massive et rapide avant que le marché ne soit complètement verrouillé⁸⁴ et que la co-souveraineté ne s'efface complètement au détriment d'une forme de vassalité.

⁸⁴ Rappelons qu'outre les États-Unis, la Chine a une politique spatiale très ambitieuse pour le LEO, avec le déploiement souhaité de plus de 25 000 satellites en orbite à horizon 2030.

La maîtrise des technologies critiques, qui de tout temps était l'apanage des États, (re)devient donc un enjeu géopolitique majeur, influençant la puissance et la diplomatie internationale. Starlink, par l'usage qu'il en est fait, par sa taille critique, son expansion agressive et son indépendance marquée s'attire de nombreuses critiques qui pourraient à terme l'obliger à revoir sa politique de distribution et d'usage.

Le cas Starlink ne révèle pas la disparition de la souveraineté étatique mais plutôt la redistribution de certaines fonctions souveraines vers des acteurs privés détenteurs d'infrastructures critiques mondialisées. Cette évolution pourrait évoquer certaines formes historiques de dépendance asymétrique, rappelant parfois les relations de vassalité étudiées dans les systèmes féodaux.

Il est donc impératif pour les États démocratiques, garants de la liberté de leur peuple, de résoudre cette problématique.

V. ANNEXE 1 : Glossaire

AES

Advanced Encryption Standard. Standard de chiffrement symétrique utilisé pour sécuriser les communications numériques.

AFU

Armed Forces of Ukraine. Forces armées ukrainiennes.

ASAT

Anti-Satellite Weapon. Arme destinée à neutraliser ou détruire un satellite.

CIA

Central Intelligence Agency. Service de renseignement extérieur des États-Unis.

DDoS

Distributed Denial of Service. Attaque informatique visant à saturer un service numérique afin de le rendre indisponible.

DoD

Department of Defense. Ministère de la Défense des États-Unis.

ESA

European Space Agency. Agence spatiale européenne.

FCC

Federal Communications Commission. Autorité fédérale américaine chargée de la gestion du spectre radioélectrique et des télécommunications.

FSS

Fixed Satellite Service. Service satellitaire fixe reposant sur des stations terrestres permanentes.

GEO

Geostationary Earth Orbit. Orbite géostationnaire située à environ 35 786 kilomètres d'altitude.

GNSS

Global Navigation Satellite System. Ensemble des systèmes mondiaux de navigation par satellite tels que GPS, Galileo, GLONASS et BeiDou.

GPS

Global Positioning System. Système américain de géolocalisation par satellite.

ICT

Information and Communication Technologies. Technologies de l'information et de la communication.

IRIS²

Infrastructure for Resilience, Interconnectivity and Security by Satellite. Programme européen de constellation satellitaire sécurisée.

ITU

International Telecommunication Union. Union internationale des télécommunications.

Ka-Band

Bande de fréquences comprise entre 26,5 et 40 GHz utilisée pour les communications satellitaires à haut débit.

Ku-Band

Bande de fréquences comprise entre 12 et 18 GHz largement utilisée pour les télécommunications satellitaires.

LEO

Low Earth Orbit. Orbite terrestre basse située entre environ 160 et 2 000 kilomètres d'altitude.

MEO

Medium Earth Orbit. Orbite terrestre moyenne située entre les orbites basses et géostationnaires.

NATO

North Atlantic Treaty Organization. Organisation du Traité de l'Atlantique Nord.

NGSO

Non-Geostationary Satellite Orbit. Orbite satellitaire non géostationnaire.

NSA

National Security Agency. Agence américaine spécialisée dans le renseignement électromagnétique.

NTN

Non-Terrestrial Network. Réseau de télécommunications non terrestre reposant notamment sur des infrastructures satellitaires.

ONU

Organisation des Nations Unies.

OTAN

Organisation du Traité de l'Atlantique Nord.

PNT

Positioning, Navigation and Timing. Fonctions de positionnement, navigation et synchronisation temporelle.

RF

Radio Frequency. Fréquence radio.

SIGINT

Signals Intelligence. Renseignement d'origine électromagnétique.

SOC

Security Operations Center. Centre opérationnel de supervision et de gestion de la cybersécurité.

SpaceX

Space Exploration Technologies Corp. Entreprise spatiale américaine fondée par Elon Musk en 2002.

SSL

Secure Sockets Layer. Ancien protocole de sécurisation des communications sur Internet.

Starlink

Constellation satellitaire de SpaceX fournissant un accès à Internet à haut débit depuis l'orbite basse.

Starshield

Version gouvernementale et militaire des technologies satellitaires développées par SpaceX.

TCP/IP

Transmission Control Protocol / Internet Protocol. Ensemble de protocoles constituant l'architecture fondamentale d'Internet.

TLS

Transport Layer Security. Protocole moderne de sécurisation des communications numériques sur Internet.

UE

Union européenne.

UIT

Union internationale des télécommunications.

USAF

United States Air Force. Armée de l'air des États-Unis.

USSF

United States Space Force. Force spatiale des États-Unis.

VSAT

Very Small Aperture Terminal. Terminal de communication satellitaire utilisant une antenne de faible diamètre.

WAN

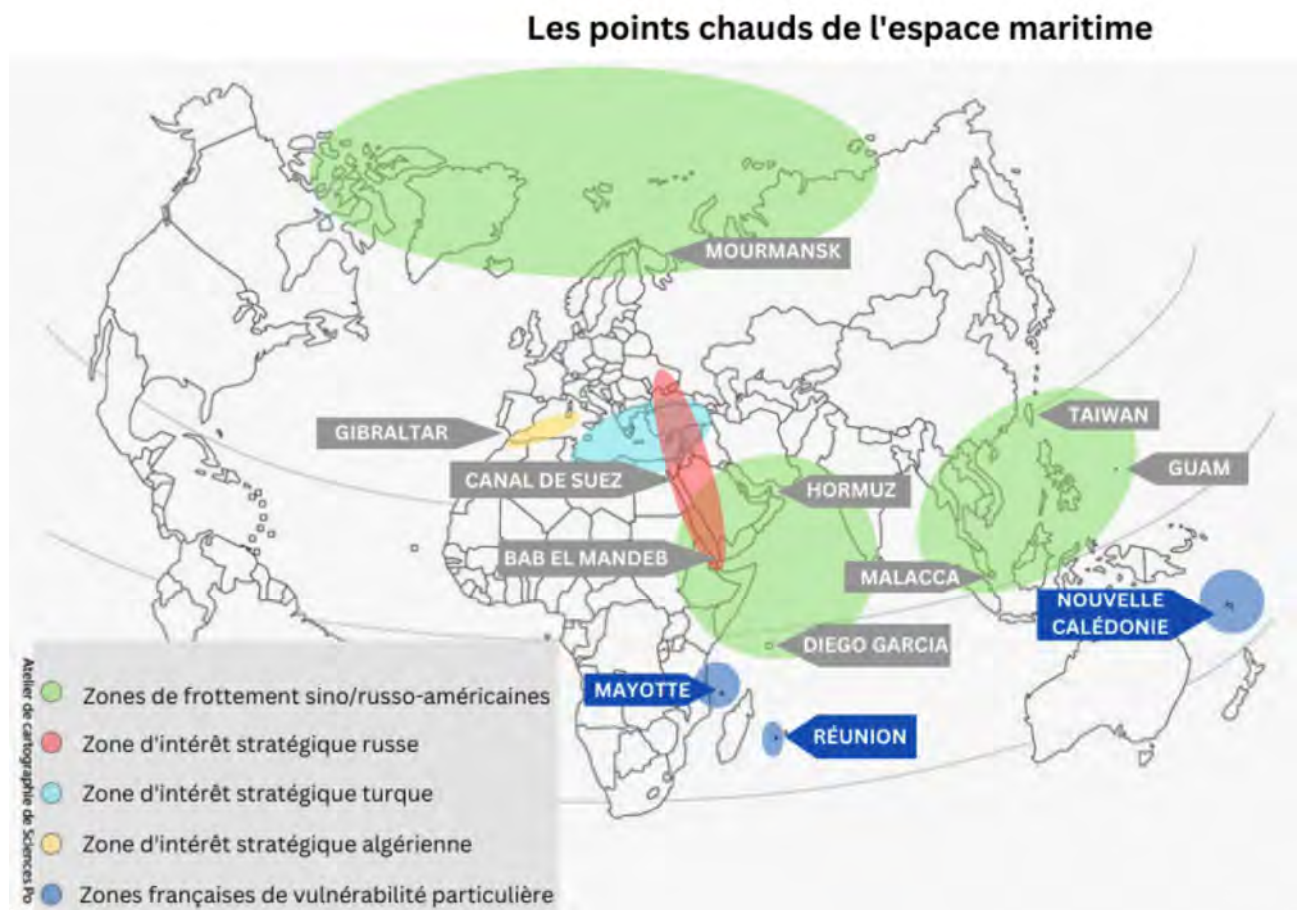
Wide Area Network. Réseau informatique couvrant une vaste zone géographique.

VI. ANNEXE 2 : La Mer Noire

La mer Noire est un espace stratégique majeur à la croisée de l'Europe, de la Russie, de l'Ukraine, de la Turquie, du Caucase et du Moyen-Orient. Ses enjeux économiques sont liés aux transports, à l'énergie, au commerce agricole, aux ressources naturelles et aux rivalités géopolitiques.

1. Une route commerciale stratégique

La mer Noire constitue un corridor maritime essentiel entre l'Europe, l'Asie centrale et la Méditerranée via les détroits turcs du Bosphore et des Dardanelles et de la mer de Marmara. Comme le montre la carte ci-dessous, son emplacement stratégique pour des pays comme la Russie ou la Turquie en fait un noeud crucial dans la com-



Source 1

préhension du conflit russo-ukrainien.

La mer Noire se positionne également au coeur des interdépendances physiques entre la Russie et l'Union Européenne.

1.1 Les enjeux de la mer Noire pour l'Ukraine

Pour l'Ukraine, l'accès maritime apparaît comme le véritable nerf de la guerre économique (2). Les exportations céréalières et métallurgiques du pays représentent en effet un pilier principal pour l'économie ukrainienne.

L'Ukraine est en effet le plus gros exportateur mondial d'huile de tournesol (50% des exportations mondiales), le troisième pour l'orge (18%), le quatrième pour le maïs (16%) et le cinquième pour le blé (12%). En 2021, l'Ukraine a ainsi exporté des céréales pour un montant de près de 12 milliards de dollars, soit environ 6% de son PIB (3).

L'exportation de grains contribue à nourrir l'Asie (la Chine en particulier), l'Europe et différents pays d'Afrique du Nord et du Moyen-Orient. Deux ports principaux concen-



Carte de la mer Noire

trent les flux maritimes : Odessa et Mykolaïv.

1.2 Blocus et mines navales

Depuis le début de l'invasion de l'Ukraine par la Russie en février 2022, les exportations ukrainiennes ont été gravement perturbées puisque pendant plus de quatre mois, les navires militaires russes ont bloqué les ports ukrainiens de la mer Noire. En prévention d'un débarquement amphibie, les forces armées ukrainiennes ont quant à elles utilisées des mines navales pour interdire l'accès d'Odessa à la flotte russe. Ces mines sont susceptibles de dériver plus largement dans la mer Noire par la suite, aggravant la sûreté des eaux.

L'espace aérien étant fermé aux avions civils depuis le début de la guerre, l'arrivée du fret en Ukraine se fait donc par la route ou le rail. Les accès principaux venant de l'ouest passent par la Pologne et Lviv, ou via la Moldavie, au sud. D'autres voies de transit se développent alors via le Danube, à la frontière avec la Roumanie.

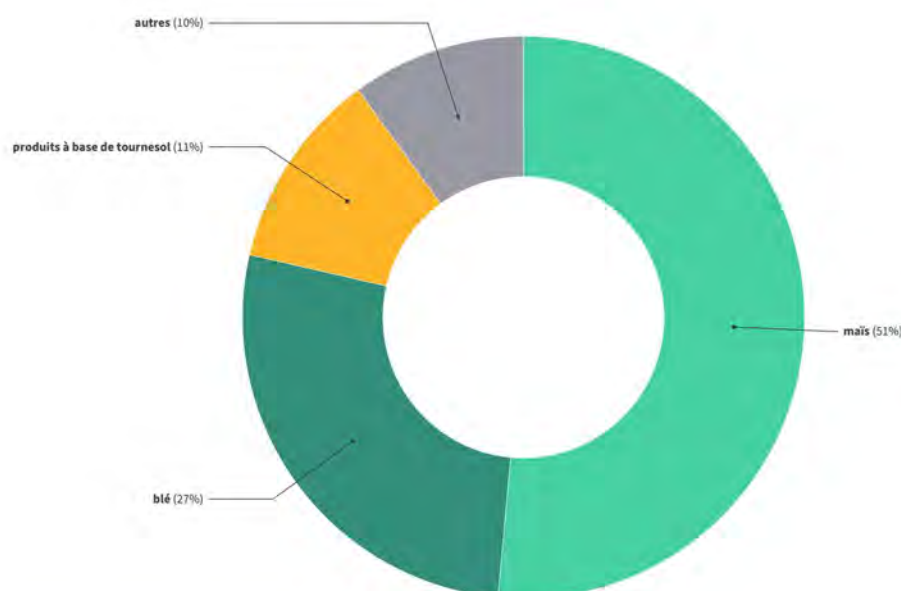
Les ports fluviaux ukrainiens (Izmail, Reni et Ust-Dunaïsk) jouent alors un rôle crucial comme alternative logistique pour exporter céréales, huiles et autres marchandises vers la Roumanie, sur des barges qui remontent le fleuve vers l'Europe centrale. Les flux sur le fleuve se multiplient par six par rapport à la période pré-guerre et perdurent les années qui suivent.

1.3 L'initiative céréalière de la mer Noire (juillet 2022 - juillet 2023)

En juillet 2022, inquiets de la pression mondiale sur les prix alimentaires comme du manque de marchandise, l'ONU et la Turquie réunissent les belligérants pour négocier l'initiative céréalière de la mer Noire (*Black Sea Grain Initiative*), qui autorise les ukrainiens à écouler leurs produits via la mer moyennant des inspections russes dans le Bosphore. L'accord conclu entre l'ONU, la Turquie, la Russie et l'Ukraine établit ainsi un corridor humanitaire maritime sûr en mer Noire.

Plus de mille navires chargés de céréales et d'autres denrées alimentaires ont quitté les trois ports ukrainiens de Tchornomorske, d'Odessa et de Loujny/Pivdenny durant la période de mise en œuvre de l'initiative. Le 17 juillet 2023, la Russie a annoncé sa décision de mettre fin à l'initiative céréalière de la mer Noire, officiellement suite au bombardement du pont de Crimée. Cette solution aura permis à 32.9 millions de

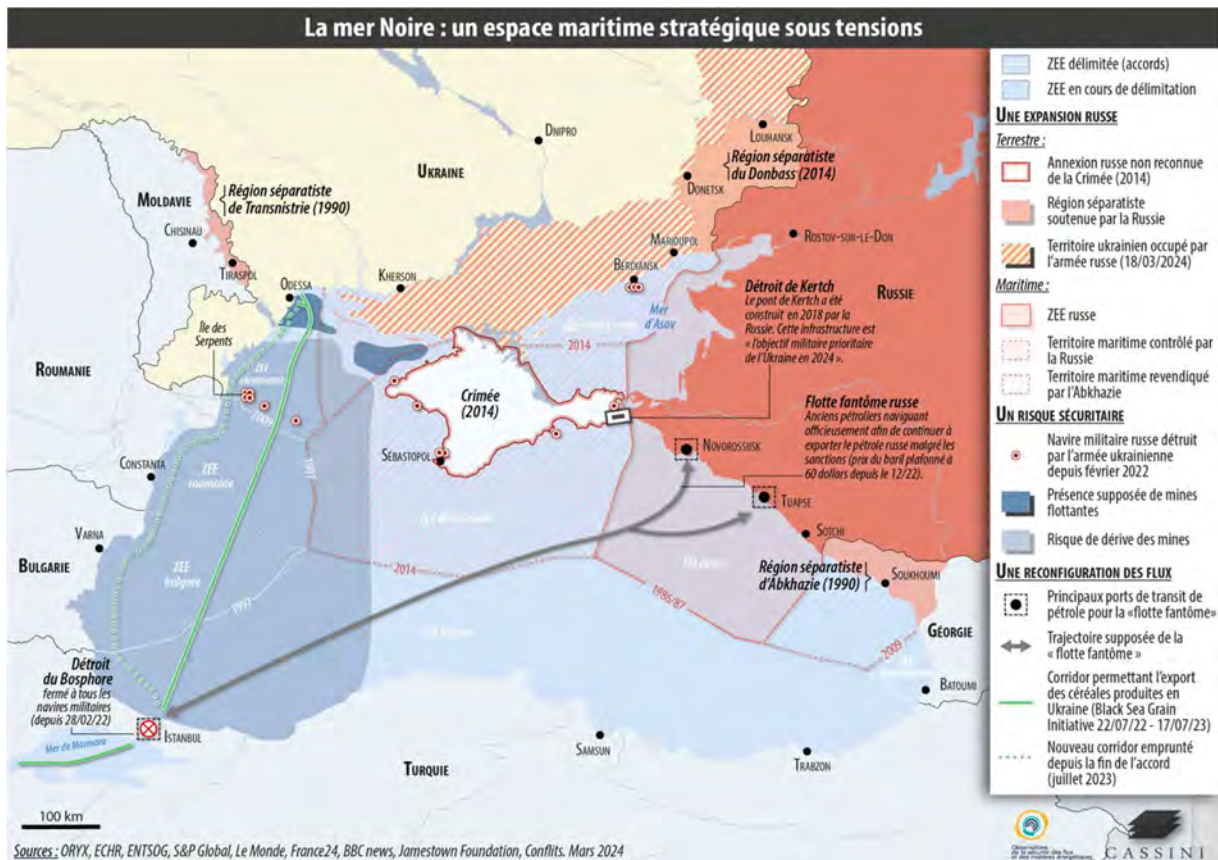
Qu'est-ce qui a été exporté dans le cadre de l'initiative céréalière de la mer Noire?



Source: Centre commun de coordination de l'initiative céréalière de la mer Noire, 18.7.2023

tonnes de marchandises d'être exportées pendant ce laps de temps.

1.4 Et aujourd'hui ?



Source 4

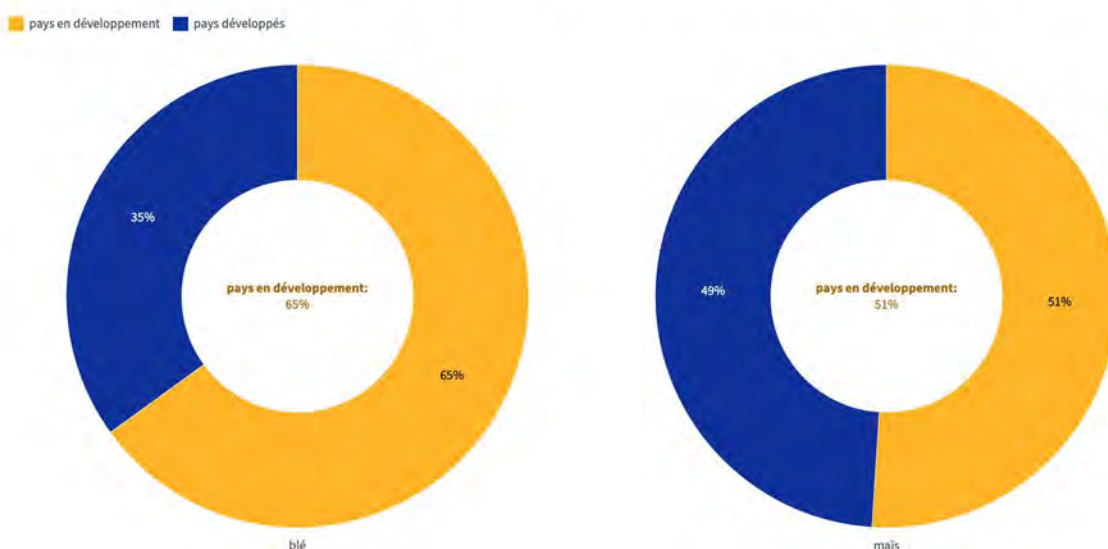
En août 2023, le premier navire dont la sécurité était garantie uniquement par l'Ukraine quittait les ports ukrainiens. Ensuite, la marine des forces armées ukrainiennes a annoncé avoir ouvert un couloir temporaire pouvant être utilisé par tous les navires civils, en particulier ceux qui se trouvent dans les ports de la « Grande Odessa » (Chornomorsk, Odessa et Pivdenny).

Les exportations ont alors continué, mais sous protection militaire jusqu'aux eaux territoriales des pays de l'UE, la Roumanie, puis la Bulgarie. Odessa et sa région, à près de 500 kilomètres au sud de Kiev, représente la charnière entre terre et mer. La région, avec ses infrastructures logistiques et portuaires, constitue aujourd'hui le débouché naturel pour les matières premières de l'Ukraine.

La preuve en est qu'au cours des trois premiers mois de l'année 2024, l'Ukraine a exporté, selon son ministère de l'Économie, environ 17 millions de tonnes de produits agricoles dont 12 millions par la voie maritime de la mer Noire. Grâce à ses trois ports de la région d'Odessa, ouverts 24 heures sur 24, l'exportation de grains, mais aussi de fer et d'engrais, fonctionne à plein régime, atteignant des niveaux quasi-équivalents à ceux d'avant-guerre et retrouvant leur place dans le commerce mondial.

Dans l'accord de paix proposé par l'Ukraine et les États-Unis en décembre 2025, le point 16 révèle le centre de gravité de l'économie ukrainienne : « La Russie n'entravera pas l'utilisation par l'Ukraine du Dniepr et de la mer Noire à des fins commerciales ». L'objectif stratégique et militaire de l'Ukraine est donc de conserver l'accès à la mer via Odessa et de maintenir l'interdiction faite à la flotte russe de naviguer librement en mer Noire pour garantir une liberté de manoeuvre à ses navires com-

Part des exportations de céréales en fonction de la richesse nationale



Source: Centre commun de coordination de l'initiative céréalière de la mer Noire, 18.7.2023

merciaux.

2. Les enjeux de la mer Noire pour la Russie

La mer Noire - dite aussi région pontique - est vue par le Kremlin à travers un double prisme. D'une part celui d'une zone de contact avec ses compétiteurs occidentaux dans laquelle elle doit influencer et, d'autre part, celui de l'enjeu énergétique et commercial, le terminal de Novorossiisk constituant le premier port du pays permettant l'exportation de céréales et d'hydrocarbures.

D'un point de vue militaire, après une domination initiale dans le golfe d'Odessa et la mise en place d'un blocus, les forces navales russes ont dû se replier vers l'Est, confrontées à l'essor de nouvelles formes de menaces. L'innovation tactique ukrainienne, portée par l'utilisation de drones aériens et de surface a permis des frappes

en profondeur, jusqu'aux zones sous contrôle russe, que ce soit en mer d'Azov ou au sud de la mer Noire en avril 2022, lorsque l'Ukraine coule le croiseur Moskva alors vaisseau amiral de la flotte russe.

Fin 2023, la Russie retire alors une partie de sa flotte de la base de Sébastopol, cherchant à sécuriser ses navires face aux frappes ukrainiennes de plus en plus précises. Au 7 juillet 2024, 36% des navires russes de la flotte de la mer Noire - soit 27 bâtiments sur 74 - avaient été endommagés ou détruits. La maîtrise de la mer Noire par la Russie s'est ainsi érodée au fil des trois premières années de guerre, la transparence croissante du champ de bataille accentuant la précarité des positions maritimes. Les satellites commerciaux offrent en effet une surveillance quasi continue des mouvements navals, tandis que les drones ukrainiens, capables de parcourir des centaines de nautiques, trouvent facilement leurs cibles.

Concernant sa flotte marchande, la Russie utilise également la mer Noire pour sa « flotte fantôme » depuis les ports de Tuapse et Novorossiisk. Ces navires sont un ensemble de pétroliers et de cargos utilisés par la Russie pour continuer à exporter son pétrole malgré les sanctions occidentales et permettent de soutenir son économie.

L'objectif de la Russie est aujourd'hui en premier lieu de consolider ses positions en Crimée, en particulier dans le port de Sébastopol, mais aussi ses autres ports de mer Noire. Cette sécurisation constitue un préalable avant de probables tentatives de reprise du contrôle du nord-ouest de la mer Noire - qualifié de Nouvelle Russie - sous réserve que la menace ukrainienne soit au préalable affaiblie. L'intention russe restera néanmoins probablement centrée sur l'interruption ou du moins la perturbation du commerce maritime ukrainien comme levier diplomatique.

Un scénario alternatif envisage que la Russie maîtrise toute la côte jusqu'à la frontière roumaine, qu'elle prenne donc Odessa, ainsi que tous les ports maritimes et fluviaux. Priver l'Ukraine de ses derniers ports d'exportation la couperait de son poumon économique. L'objectif final de la Russie pourrait ainsi être de faire de l'Ukraine un pays comme la Biélorussie, c'est-à-dire un pays dépendant de la Russie pour ses accès à la mer.

3. Les enjeux de la mer Noire pour la Turquie

Évoquer les enjeux de la mer Noire ne peut se faire sans développer le rôle majeur de la Turquie dans l'équilibre des acteurs dans cette zone.

Entre 1923 et 1991, la Turquie était le seul pays non-communiste riverain de la mer Noire. A la chute de l'URSS, Ankara a cherché à prendre l'initiative en tentant de promouvoir l'équilibre des pouvoirs, mais dès le début des années 2000, la Russie est redevenue la puissance maritime majeure en mer Noire, faisant de l'accès à la Méditerranée sa priorité.

Le déclenchement de la guerre en Ukraine favorise aujourd'hui Ankara, tant sur le plan diplomatique que militaire. En effet, s'il est difficile de prédire l'issue du conflit, il est clair que l'influence russe en mer Noire est en reflux. Pour jouer ce rôle de pivot entre mer Noire et Méditerranée, la Turquie s'appuie sur :

- sa géographie, lui permettant de maîtriser physiquement les accès aux détroits du Bosphore et des Dardanelles, l'accès à la mer de Marmara et l'accès à la Méditerranée via cette dernière ;
- la convention de Montreux de 1936, qui régit les mouvements de navires en période de conflit dans cette zone de passage obligatoire.

Ainsi, le lundi 28 février 2022, quatre jours après le début du conflit en Ukraine, la Turquie annonçait la fermeture des détroits du Bosphore et des Dardanelles aux navires militaires des pays non riverains, conformément aux différents articles de cette convention.

L'article 18 y indique notamment que « les bâtiments de guerre des puissances non riveraines ne pourront pas y rester plus de 21 jours » et limite à 30 000 tonnes le tonnage maximal de l'ensemble des navires de guerre d'un état non riverain. En pratique, ce dernier point empêche toute présence de groupe aéronaval en mer Noire et à l'OTAN - par exemple - de déployer rapidement et en masse des bâtiments (5). De la même manière, la flotte russe n'est pas autorisée par la Turquie à franchir les détroits, garantissant une forme de statut quo pour les belligérants.

Ankara cherche ainsi avant tout, malgré son appartenance à l'OTAN, à apparaître comme une puissance d'équilibre dans la région. D'un côté, en armant l'Ukraine (livraison de canons automoteurs, de véhicules blindés d'infanterie, construction de drones Bayraktar TB-2 sous licence, construction de deux frégates Ada) et en maintenant les détroits fermés pour les navires de guerre (tout en permettant l'exportation des céréales ukrainiennes), Ankara ancre son soutien dans le camp occidental. De l'autre, en ayant refusé de prendre les sanctions occidentales, la Turquie s'impose comme un débouché pour une Russie en recherche de nouveaux partenaires.

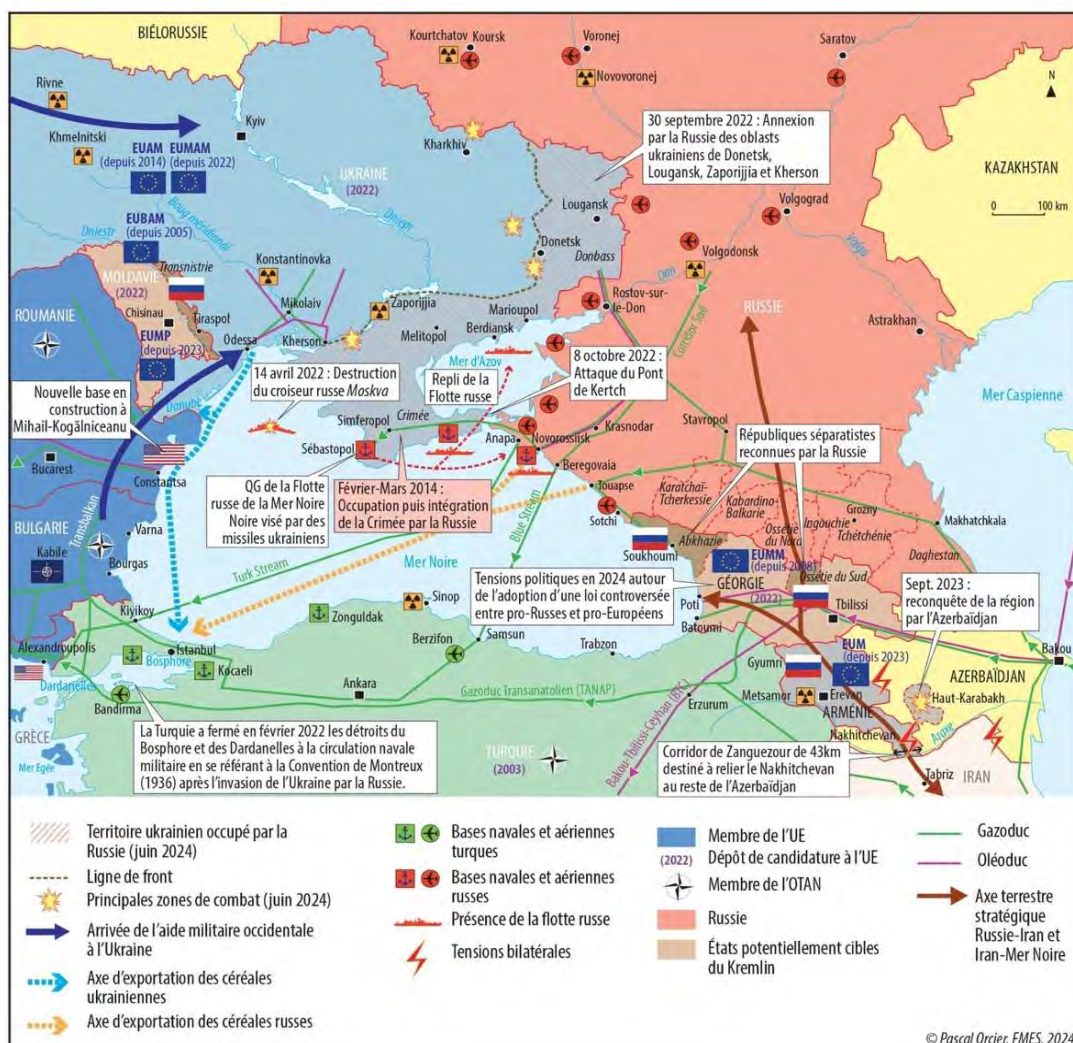
D'autres enjeux liés aux infrastructures sous-marines - englobant les câbles de télécommunications, les câbles électriques, les gazoducs, oléoducs ou encore les installations de forage de la région - rentrent également en compte. La Turquie a également profité du virage énergétique européen vis-à-vis de la Russie au lendemain de la guerre en Ukraine - où transitait 70% du gaz russe à destination de l'UE - pour capter la réorientation des flux énergétiques russes.

Le gazoduc Turk Stream fonctionne ainsi à pleine capacité au profit de la Turquie mais aussi...de l'UE et des pays comme la Bulgarie, la Hongrie et la Moldavie, au moins jusqu'en 2027. De la même manière, le pétrole russe, via la « flotte fantôme » transite via la Turquie et se dilue sur le marché européen via la Turquie notamment (6).

La Turquie se pose comme hub énergétique régional et se place comme acteur « non aligné » avec les différents belligérants, lui permettant d'attirer et de concentrer les flux de marchandises de l'Europe, de la Russie, du Caucase et du Moyen-Orient.

4. Conclusion sur la mer Noire

Conformément au principe de *Res Nullius*, la mer n'appartient à personne et se donne au plus fort. La militarisation sans précédent de la mer Noire ces dernières années répond à ce principe.



Source 7

La sécurité des voies maritimes en mer Noire demeure extrêmement fragile car elle représente un enjeu crucial pour les deux belligérants. Cette sécurité repose actuellement sur un accord verbal entre les Russes et les Ukrainiens, stipulant de ne pas cibler les navires de commerce, en particulier lorsqu'ils transitent dans les eaux internationales. Toutefois, cet accord, de nature informelle, peut être révoqué à tout moment et sans préavis, ajoutant une couche d'incertitude supplémentaire dans une région déjà instable.

La région de la mer Noire, qui se situe au cœur des interdépendances physiques des réseaux européen-russes, connaît aujourd'hui un déplacement de l'épicentre du transit depuis les territoires situés au nord de la mer Noire vers la Turquie, au sud, via notamment les anciennes républiques soviétiques d'Asie centrale et du Sud-Caucase. La guerre économique à laquelle se livrent la Russie et l'UE a en effet engendré une reconfiguration des flux énergétiques mais n'a cependant pas réussi à affaiblir durablement l'économie russe, ni sa position militaire dans la guerre en Ukraine (4).

La Russie est probablement vouée à y retrouver sa suprématie : soit dans le cas d'une rupture du front ukrainien et d'une percée russe vers Odessa, qui couperait la quasi-totalité de l'accès ukrainien à la mer et une partie de ses capacités de nuisance maritime ; soit lors de la fin de la guerre et de la réouverture des détroits, qui permettrait à Moscou d'étoffer sa flotte de mer Noire en envoyant des navires de ses autres flottes (notamment de Baltique ou du Pacifique).

5. Et la Chine ?

La Chine a des intérêts multiples en mer Noire. Premièrement, elle soutient Moscou dans son conflit contre l'Ukraine, notamment via l'achat de ses ressources énergétiques, comme en témoigne l'encart ci-dessous.

L'économie russe en 2024.



Source 9

Ensuite, la zone de la mer Noire est perçue par la Chine comme la connexion économique la plus facile et la plus rapide entre l'Asie de l'Est et l'Europe. L'initiative de « nouvelle route de la soie » (*Belt and Road Initiative*) doit ainsi traverser le Caucase et l'Europe de l'Est, notamment l'Azerbaïdjan, l'Ukraine, la Géorgie et la Turquie. De

2019 à 2021, la Chine était ainsi le plus important partenaire commercial de l'Ukraine (10). L'Ukraine était également devenue le deuxième fournisseur de maïs et un des premiers fournisseurs d'armes de la Chine.

Lors de l'initiative céréalière de la mer Noire, près d'un quart du fret transporté l'a été au profit de la Chine (11). Cette dernière n'a donc ni intérêt à voir la flotte militaire russe et l'emprise de son allié réduite à néant pour la maîtrise de la zone, ni de voir le conflit s'intensifier au détriment de son économie.

Musk, conscient des enjeux de la Chine et de la Russie, s'attelle donc, en dehors de ses déclarations humanistes à ne pas (trop) froisser la Russie et son allié la Chine, pour qui ses débouchés et ses capacités de production sont essentielles.

Sources :

- (1) Fédération Méditerranéenne d'études Stratégiques (FMES), Pascal Ausseur. « Les points chauds de l'espace maritime » [en ligne], 06 septembre 2023. [Consulté le 24 mai 2026]. Disponible à l'adresse : <https://fmes-france.org/points-chauds-espace-maritime/>
- (2) Revue Conflits, Jean-Baptiste Bless « L'économie ukrainienne face à la guerre : la clé par la mer » [en ligne], 01 février 2026. [Consulté le 24 mai 2026]. Disponible à l'adresse : <https://www.revueconflits.com/leconomie-ukrainienne-face-a-la-guerre-la-cle-par-la-mer/>
- (3) Conseil européen, « Comment l'invasion de l'Ukraine par la Russie a encore aggravé la crise alimentaire mondiale » [en ligne], 22 janvier 2026. [Consulté le 25 mai 2026]. Disponible à l'adresse : <https://www.consilium.europa.eu/fr/infographics/how-the-russian-invasion-of-ukraine-has-further-aggravated-the-global-food-crisis/>
- (4) Observatoire de la sécurité des flux et des matières énergétiques. Rapport « Guerre russo-ukrainienne : la région de la mer Noire au coeur de la reconfiguration des flux énergétiques. » Avril 2024. [Consulté le 24 mai 2026].
- (5) Fédération Méditerranéenne d'études Stratégiques (FMES), Esteban Aguado. « La convention de Montreux 90 ans après », 08 juillet 2025. [Consulté le 25 mai 2026].
- (6) Public Sénat, commission des affaires étrangères et de la défense, « enjeux stratégiques de la mer Noire. » [en ligne], 18 février 2026. [Consulté le 25 mai 2026]. Disponible à l'adresse : <https://www.youtube.com/watch?v=cQSqCQqq1XQ>
- (7) Fédération Méditerranéenne d'études Stratégiques, Pascal Orcier, « Atlas stratégique de la Méditerranée et du Moyen-Orient », 2024. [Consulté le 26 mai 2026].
- (8) Fayard, Walter Isaacson, « Elon Musk », 13 septembre 2023.
- (9) FMES, Perspectives stratégiques, 2025-1, « L'état de l'économie russe depuis la guerre et les sanctions », juillet 2025. [Consulté le 27 mai 2026].

- (10) Banque mondiale, World Integrated Trade Solution, [en ligne], 2020. [Consulté le 27 mai 2026]. Disponible à l'adresse :
- (11) Nations Unies, Centre commun de coordination de l'initiative céréalière de la mer Noire [en ligne], 18 juillet 2023. [Consulté le 25 mai 2026]. Disponible à l'adresse : <https://www.un.org/en/black-sea-grain-initiative/vessel-movements>
- Actes de la conférence de Montreux, « Convention concernant le régime des détroits » [en ligne], 20 juillet 1936. [Consulté le 25 mai 2026]. Disponible à l'adresse : https://diad.mfa.gov.tr/diad/kutuphane/Kurucu_Anlasmalar/montro-an-lasmasi.pdf
 - Diploweb, Cyrille Bret, Florent Parmentier, « La mer Noire aujourd'hui : entre batailles navales et cessez-le-feu précaire » [en ligne], 30 mars 2025. [Consulté le 25 mai 2026].
 - Institut Montaigne, Laurent Célérier, « Mer Noire : comment l'Ukraine a-t-elle gagné la bataille ? », [en ligne], 10 septembre 2024. [Consulté le 25 mai 2026].
 - Fédération Méditerranéenne d'études Stratégiques, Emilien Pouchin, Perspectives Stratégiques, « Les ambitions maritimes turques au XXIème siècle », 28 mai 2024. [Consulté le 26 mai 2026].
 - École de Guerre Économique, Martin Toussaint, « Les manœuvres informationnelles sur la fin de l'accord céréalière en Mer Noire » [en ligne], 19 juillet 2023. [Consulté le 27 mai 2026]. Disponible à l'adresse : <https://www.ege.fr/info-guerre/les-manoeuvres-informationnelles-sur-la-fin-de-laccord-cerealier-en-mer-noire>

VII. ANNEXE 3 : Entretien avec Olivier BOYER

Cet entretien a eu lieu le XX/XX/XXX entre Julien FLEURY, MACYB09, et Olivier BOYER, membre de l'IHEDN.

Questions relatives à la dimension technique :

1. Quelles techniques de brouillage et de spoofing ont été utilisées ou détectées récemment pour compromettre la sécurité des systèmes de communication par satellite LEO ?

Dans le cas des satellites LEO, les attaques peuvent viser principalement la liaison montante, soit du côté de l'utilisateur, soit directement au niveau de l'antenne terminale. Pour le brouillage, il existe deux approches principales :

- Le brouillage simple consiste à émettre une forte puissance afin de générer du bruit et perturber la réception du signal.
- Le brouillage intelligent (ou repeater jamming) consiste à réémettre des signaux précédemment captés, ce qui permet par exemple de créer des attaques de type déni de service. si le satellite reçoit trop de requêtes par exemple.

Dans le cas d'un drone, la répétition de certaines commandes peut provoquer des comportements indésirables, si une commande disait d'aller à gauche répéter cette commande en boucle ferait tourner le drone en rond.

Pour le spoofing :

- Une première méthode consiste à injecter de fausses données afin de supplanter le signal légitime. Cette technique est relativement simple mais souvent facile à détecter car elle provoque des discontinuités visibles.
- Une seconde méthode est plus sophistiquée. En connaissant la position de la cible et celle de l'émetteur légitime, il est possible de générer un faux signal cohérent dans le temps, ce qui réduit les anomalies observables et rend l'attaque plus difficile à détecter.

2. En quoi consiste la vulnérabilité des constellations LEO face aux attaques ciblant la liaison montante, et quels en sont les impacts opérationnels ?

Les constellations LEO sont particulièrement sensibles aux attaques visant la liaison montante, notamment aux attaques de type déni de service.

Comme les satellites LEO sont beaucoup plus proches de la Terre que les satellites géostationnaires, l'attaquant a besoin de moins de puissance pour perturber les communications. Cela facilite les opérations de brouillage et peut entraîner une dégradation ou une interruption du service pour les utilisateurs concernés.

3. Comment les techniques de détection et d'interception, telles que le spoofing en vol, peuvent perturber la sécurité aérienne et les systèmes de navigation ?

Le spoofing consiste à fournir de fausses informations de navigation à un système. Si l'attaque est suffisamment progressive et cohérente, elle peut modifier progressivement la position estimée par un avion ou un drone, ce qui pourrait

conduire à une déviation de trajectoire sans déclencher immédiatement d'alerte. Il existe également des plateformes en ligne qui recensent les zones où des activités de brouillage ou de spoofing sont observées. (gpsjam.org)

4. Quelles sont les limites des méthodes de détection modernes face à des signaux à faible SNR ou dissimulés, et comment cela peut constituer une menace ?

La détection par cyclostationnarité est aujourd'hui l'une des méthodes les plus performantes, notamment comparée à la détection énergétique ou aux techniques de corrélation simples. Elle repose sur l'analyse de la structure périodique des signaux de communication, notamment celle des symboles modulés. Cependant, si un signal est suffisamment masqué dans le bruit ou si sa structure est volontairement dissimulée, sa détection devient beaucoup plus difficile. Pour ce faire il faut casser la structure du signal si un symbole ou groupement de bits est envoyé toutes les 1 ms rendre cette période variable permettrait de rendre le signal moins récurrent mais cela compliquerait la chaîne de réception. Cette capacité de dissimulation constitue une menace car elle permet à un émetteur de communiquer tout en réduisant fortement sa probabilité de détection.

5. Quelles sont les trois étapes fondamentales qu'un agent adverse doit franchir pour intercepter une communication, et comment la furtivité peut-elle être assurée à chaque étape ?

Trois mécanismes de protection sont généralement utilisés :

- LPD (Low Probability of Detection) vise à rendre la transmission difficile à détecter.
- LPI (Low Probability of Intercept) vise à masquer les caractéristiques du signal, comme sa modulation ou sa structure.
- LPE (Low Probability of Exploitation) repose sur le chiffrement afin d'empêcher l'exploitation des informations même si le signal est intercepté.

Pour un attaquant, il est nécessaire de franchir successivement ces trois niveaux afin d'exploiter efficacement une communication.

6. En quoi consiste la méthode de détection par densité énergétique, et quels sont ses avantages et limites face à des signaux à faible SNR ?

La détection énergétique est la méthode la plus simple à mettre en œuvre. Elle consiste à balayer le spectre radio afin d'identifier les fréquences présentant une puissance supérieure au bruit ambiant. Son principal avantage est sa simplicité de mise en œuvre. Sa principale limite est qu'un signal dont la puissance est proche du niveau de bruit risque de ne pas être détecté. De plus, il est difficile de surveiller simultanément de très larges bandes de fréquences sans disposer de plusieurs systèmes de réception, sinon avec un seul système il y aura un balayage large bande qui intégrera plus de bruit et rendra l'identification d'un signal plus difficile.

7. Comment la technique de saut de fréquence (FHSS) contribue-t-elle à rendre une communication plus furtive, et quels sont ses principaux avantages ?

Le saut de fréquence ne rend pas nécessairement une communication plus furtive. Son principal intérêt est d'améliorer la résistance au brouillage. Comme la fréquence utilisée change continuellement selon une séquence prédéfinie, il devient plus difficile pour un brouilleur de suivre le signal. L'attaquant doit alors répartir sa puissance sur une bande plus large, ce qui réduit l'efficacité du brouillage.

8. Quelle est la différence entre le DSSS et la dissimulation dans le bruit en termes de stratégie pour rendre une transmission difficile à détecter ou à exploiter ?

Le DSSS (Direct Sequence Spread Spectrum) utilise un code pseudo-aléatoire à haute fréquence qui étale le signal sur une bande plus large. Cette opération réduit localement le rapport signal sur bruit et rend la détection plus difficile pour un observateur ne connaissant pas le code utilisé. La dissimulation dans le bruit va plus loin. Elle agit directement sur l'amplitude et la phase du signal afin de le rendre encore plus difficile à distinguer du bruit ambiant. Cette approche est particulièrement efficace contre les méthodes de détection fondées sur la cyclostationnarité, car elle réduit la structure exploitable du signal.

9. Quelles sont les principales techniques de modulation ou d'architecture qui permettent de réduire la visibilité d'un signal dans le but d'éviter sa détection ou son interception ?

Les principales techniques utilisées pour réduire la visibilité d'un signal sont :

- Le Direct Sequence Spread Spectrum (DSSS).
- Les techniques de masquage du signal.
- Les méthodes de dissimulation dans le bruit.

Ces approches visent à diminuer la probabilité de détection et d'interception en réduisant les caractéristiques observables du signal ou en le rapprochant du niveau de bruit ambiant.

VIII. ANNEXE 4 : Entretien avec un chercheur espace de l'IRSEM

Cet entretien a eu lieu le 02/07/2026 entre Pierre Gudefin, MACYB 09 et un chercheur espace de l'IRSEM.

Questions relatives en majorité à la géopolitique spatiale.

Au sujet de l'attaque sur VIASAT du 24/02/2022 :

Question 1 : quels étaient les systèmes de communication de secours ukrainiens lors de l'attaque du 24 février 2022 et de la cyberattaque sur le réseau KA-SAT de VIASAT ? Les ukrainiens auraient-ils pu faire autrement sans Starlink au début et si oui, avec quelle efficacité ?

A priori il n'y avait pas d'autres alternatives à Starlink, d'où la demande urgente et faite « en live » sur X. Il n'y avait rien de similaire sur le marché en termes de revisites notamment. Donc il n'y avait pas d'autres choix dans l'immédiat. Au bout de six mois de guerre, Eutelsat admet qu'il fournit également des services satellitaires à l'armée ukrainienne.

Question 2 : est-ce la première cyberattaque aussi réussie sur un système satellitaire dans le cadre d'une opération militaire et donc avec un État officiellement à la manœuvre ?

L'OTAN et l'UE ont dénoncé l'attaque de manière ouverte, la France ne l'a pas fait. L'UIT (union internationale des télécommunications) dénonce les interférences et les brouillages des nations de manière publique, ce qui dans les faits « suffit » à réguler de manière relative les velléités des états.

Il est difficile de savoir si cela constitue la première attaque satellitaire car les cas sont rarement rapportés. Il peut y avoir des précédents, bien qu'aucun à ma connaissance.

Question 3 : en termes opérationnels et juridiques, quels impacts à venir sur les relations entre entreprises satellitaires et acteurs étatiques ?

En droit spatial, l'État est responsable des acteurs privés qui utilisent ses fréquences. Peu de chances que de manière opérationnelle cela se reproduise de manière massive, tout le monde ayant besoin des satellites.

De la même manière, la lutte anti-satellite - où la capacité à détruire un satellite par un missile - est une arme de non emploi. Premièrement car cela créerait un nuage de débris source de potentielles destruction (y compris côté russe) et aussi car les chinois ont besoin des orbites. La Chine appuyant fortement la Russie dans la guerre en Ukraine, la Russie n'a pas d'intérêt à perdre son allié en tirant un missile qui pourrait dégrader l'espace satellitaire.

Au sujet de M. Musk :

Question 4 : quelle est la perception de M. Musk dans les état-majors de l'OTAN ? Les états-major Français ? Et Ukrainiens ?

L'ancien directeur de l'agence spatiale ukrainienne parle des relations entre les état-majors ukrainiens et M. Musk comme une alternance entre amour et haine. Amour car M. Musk les sauve par son produit, haine car il coupe leurs actions militaires et la défense de leur sol.

Ce dernier (l'ancien directeur de l'agence spatiale ukrainienne) a fondé une start-up pour le lancement de satellite LEO par avion (lancement aéroporté), à défaut d'avoir accès à des lanceurs au sol. L'objectif pour les ukrainiens est désormais triple : lancement aéroporté de satellites, diversité des communications (autre que Starlink), avoir des capacités d'observation satellitaire qui dépendent grandement des américains aujourd'hui. Il est intéressant de voir que les sites de l'industrie spatiale ukrainienne (ex-URSS) n'ont pas été bombardé au début du conflit, étant considérés comme vitaux pour les russes, qui eux aussi ont besoin de sites pour le lancement de leurs satellites, aujourd'hui assez faibles d'un point de vue technologique en comparaison de leurs besoins réels et des capacités de Starlink.

Par rapport à l'OTAN, pas de réponse précise vu que l'OTAN est un pot commun des pays pour fournir des capacités satellitaires. Pour la France, je ne sais pas. Ce qui est certain cependant, c'est que les militaires (au moins français) n'ont pas été consulté dans le cadre du programme IRIS2, ils ne sont pas parties prenantes des discussions et n'ont donc pas pu définir leurs exigences. La question du financement des satellites est aussi centrale : l'Allemagne a déclaré en 2025 qu'elle allait investir 35 milliards d'euros d'ici 2030 pour ses infrastructures cyber et spatiales. 35 milliards d'ici 2030 ! Ils ne pourront certainement pas tout dépenser de par leur propre BITD ou industrie. Il leur faudra surement acheter sur étagère des produits américains pour compléter leurs besoins.

Question 5 : d'autres chefs d'entreprises suivent-ils son exemple dans des négociations : Palantir et M. Karp, Iceye et M. Modrzewski, etc...

Pas à ma connaissance, en tous cas pas de manière aussi « fantasque » que M. Musk.

Question 6 : quelle crédibilité accorder à l'épisode dit de « Sébastopol », où il aurait fait annuler une attaque de drone sur la flotte russe stationnée à Sébastopol ?

Effectivement, je n'ai pas d'autres sources externes aux déclarations de M. Musk pour confirmer cet épisode.

Question 7 : peut-on dire qu'il mène une guerre cognitive (sur X notamment) ? Exemple : la proposition du plan de paix ukrainien suivi de l'envoi de la facture au gouvernement américain pour payer le déploiement des premiers terminaux Starlink.

Je ne suis pas familière de ce terme (guerre cognitive). Il m'est donc difficile d'y répondre précisément, mais sinon on peut bien dire que ses actions de communication influencent au moins de manière indirecte la diplomatie de la guerre.

Au sujet de l'arrivée de Starlink en Ukraine :

Question 8 : Starlink en Ukraine est-il un indicateur pertinent d'un appui « acceptable » d'une entreprise privée par la Russie ? Il y a t-il des limites implicites à son utilisation ? Quid des frappes dans la profondeur (i.e sur le sol Russe) actuelles : ont-elles lieu avec ou sans la technologie de Starlink ?

Pour les frappes dans la profondeur, je ne connais pas assez les capacités des drones pour pouvoir répondre de manière précise. Les terminaux de Starlink doivent être probablement détectables, ce qui explique aussi des pertes élevées par les Ukrainiens.

Pour les premières questions, les Russes ont très clairement qualifié d'arme Starlink à l'ONU avec l'appui de leur partenaire chinois.

Question 9 : Est-il véritablement un outil de la diplomatie américaine, ou bien est-ce plus nuancé ? Car on voit qu'il pèse à chaque fois - accord sur les minerais stratégiques, plan de paix - mais également qu'il ne répond pas aux exigences des institutions américaines (traçabilité, coupure...) et qu'il joue sa propre partition (enjeux économiques avec la Chine notamment).

Oui, c'est business first. Par ailleurs, il est intéressant de voir que Trump a dit oui à l'utilisation par des entreprises privées des fréquences militaires, ce qui questionne le Department Of War et les parlementaires américains sur la guerre de demain. C'est le cas notamment pour Taiwan : aura-t-on accès à Starlink s'il y a une guerre à Taiwan ? Ou autrement dit : compte tenu de votre dépendance à la Chine, existe-t-il des conflits d'intérêt trop grands pour vous ?

La Chine augmente par ailleurs sa cadence de lancement. Prévision de 20000 satellites en LEO, deux fois 10000.

Question 10 : l'Ukraine peut-elle être qualifiée laboratoire du futur JADC2 américain ? Le super contrat récent avec la Space Force (4 à 9 milliards de dollars) est-il un levier de plus pour M. Musk et SpaceX vis-à-vis du gouvernement américain ?

Oui, sans aucun doute. Cela permet à M. Musk de tester son produit et de vendre son jumeau au gouvernement américain. Le fait qu'il fonctionne très bien et que les cyberattaques soient limitées lui donne du crédit vis-à-vis des militaires américains.

Question 11 : sur la notion de verrouillage orbital (spectre/orbite) : SpaceX possède les péages (lanceurs) et presque toute l'autoroute physique (satellites en orbite,

avec saturation des demandes) comme l'autoroute « virtuelle » (ressource spectrale). Quels sont les moyens de concurrence des États ?

C'est l'État en France qui porte le projet, sans les moyens financiers et techniques de SpaceX ou du gouvernement américain. Il faut donc faire appel à des partenariats stratégiques étrangers comme l'Inde pour diversifier ces derniers. Le sommet international sur l'espace qui se tiendra au Grand Palais à Paris du 9 au 10 septembre prochain doit permettre d'initier ses démarches.

Sur le plan européen, les pays de l'UE doivent rester unis dans leurs démarches spatiales, car à défaut les moyens financiers et industriels ne seraient plus mis en commun et chacun irait se servir ailleurs, chez les américains notamment.

IX. Sources

I/A/1

- ⁱ Tilly, Charles. 1992. *Coercion, Capital, and European States, AD 990–1992*. Oxford: Blackwell.
- ⁱⁱ Briant, Pierre. 2002. *From Cyrus to Alexander: A History of the Persian Empire*. Winona Lake, IN: Eisenbrauns.
- ⁱⁱⁱ Chevallier, Raymond. 1972. *Les voies romaines*. Paris: Picard.
- ^{iv} van Creveld, Martin. 1985. *Command in War*. Cambridge, MA: Harvard University Press.
- ^v Conseil constitutionnel. « Le rôle de l'État ». Constitution française.
- ^{vi} Weber, Max. 1995. *Économie et société*. Paris : Plon.
- ^{vii} Bielenstein, Hans. 1980. *The Bureaucracy of Han Times*. Cambridge: Cambridge University Press.
- ^{viii} Kolb, Anne. 2000. *Transport and Communication in the Roman State*. Londres: Routledge.

I/A/2

- ^{ix} Virilio, Paul. 1977. *Vitesse et politique*. Paris : Galilée.
- ^x Bély, Lucien. 1990. *Espions et ambassadeurs au temps de Louis XIV*. Paris : Fayard.
- ^{xi} Kahn, David. 1996. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner.
- ^{xii} IRSEM. *L'infosphère. Composante opérationnelle émergente, enjeu majeur pour le traitement des crises futures*. Paris : Institut de recherche stratégique de l'École militaire.

I/A/3

- ^{xiii} McLuhan, Marshall. 1962. *The Gutenberg Galaxy: The Making of Typographic Man*. Toronto: University of Toronto Press.
- ^{xiv} Eisenstein, Elizabeth L. 1979. *The Printing Press as an Agent of Change*. Cambridge: Cambridge University Press.
- ^{xv} Ministère des Armées. *Supériorité informationnelle : les innovations qui renforcent l'avantage opérationnel*.

I/A/4

- ^{xvi} Hérodote. *Histoires*. Livre V.
- ^{xvii} Thucydide. *Histoire de la guerre du Péloponnèse*. I, 128-134.
- ^{xviii} Tacite. *Annales*. I, 55-71.
- Wells, Peter S. 2003. *The Battle That Stopped Rome*. New York: W. W. Norton.
- ^{xix} CNAM. « Le télégraphe Chappe ». Musée des Arts et Métiers.

I/A/5

- ^{xx} Thomas T. Eckert, *The Military Telegraph During the Civil War* ; James M. McPherson, *Battle Cry of Freedom*, Oxford University Press.
- ^{xxi} Service historique de la Défense, dossiers « Transmissions 1914-1918 ».

I/A/6

- ^{xxii} Virilio, Paul. 1977. *Vitesse et politique*. Paris : Galilée.
- ^{xxiii} National Archives and Records Administration. *Navajo Code Talkers*.

I/A/7

- ^{xxiv} Beniger, James R. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society*. Cambridge, MA: Harvard University Press.
- ^{xxv} Qiao, Liang, et Wang Xiangsui. 1999. *La Guerre hors limites : la guerre et la réflexion sur l'art de la guerre à l'époque de la mondialisation*. Paris : Rivages.
- ^{xxvi} NATO Cooperative Cyber Defence Centre of Excellence. *Cyber Attacks Against Estonia*.
- ^{xxvii} ANSSI. *Souveraineté numérique et dépendances critiques*.

I/B/1

- ^{xxviii} Académie française. « Souveraineté ». *Dictionnaire de l'Académie française*.

- ^{xxix} Bellanger, Pierre. « Souveraineté numérique ». *Le Débat*.
^{xxx} *Le Fur, Louis*. 1896. *État fédéral et confédération d'États*. Paris.

I/B/2

- ^{xxxi} Les Surligneurs. « Nicolas Dupont-Aignan sur la souveraineté française ».
^{xxxii} De Villiers, Philippe. Déclarations publiques sur la souveraineté nationale
^{xxxiii} La Croix. « François Asselineau, programme souverainiste anti-libéral ».
^{xxxiv} France 24. Entretien avec Florian Philippot.
^{xxxv} Article « Condominium », Wikipédia.
^{xxxvi} Lemaire, Félicien. 2012. « Propos sur la notion de souveraineté partagée ». *Revue française de droit constitutionnel* 92 (4): 821-850.
^{xxxvii} Lemaire, Félicien. 2012. « Propos sur la notion de souveraineté partagée ». *Revue française de droit constitutionnel* 92 (4): 821-850.

I/C

- ^{xxxviii} Plokhly, Serhii. 2023. *La guerre russo-ukrainienne : Le retour de l'histoire*. Paris : Gallimard.
^{xxxix} Plokhly, Serhii. 2023. *La guerre russo-ukrainienne : Le retour de l'histoire*. Paris : Gallimard.

I/D/1

- ^{xl} RAND Corporation. 2024. *The War in Ukraine and the Future of Military Innovation*.
^{xli} Radin, Andrew et al. 2024. RAND.
^{xlii} Brantly, A. F., Cal, N. M., and Winkelstein, D. P. (2017a). *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*. West Point, NY
^{xliii} Brantly, A. F., Cal, N. M., and Winkelstein, D. P. (2017a). *Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW*. West Point, NY

I/D/2

- ^{xliv} CSIS. « Understanding the Military AI Ecosystem in Ukraine ».
^{xl} Radin, Andrew et al. RAND Corporation, 2024.
^{xlvi} Department of Defense. 2022. *Summary of the Joint All-Domain Command and Control Strategy*.

I/D/3

- ^{xlvii} Radin, Andrew et al. RAND Corporation.
^{xlviii} Satariano, Adam, Elon Musk's Unmatched Power in the Stars, The New York Times, 28 Jul 2023,

I/D/4

- ^{xlix} Watling, Jack, et Nick Reynolds. 2022. *Operation Z: The Death Throes of an Imperial Delusion*. Londres : RUSI.
^l Radin, Andrew et al. RAND Corporation.
^{li} Satariano, Adam, Elon Musk's Unmatched Power in the Stars, The New York Times, 28 Jul 2023,
^{lii} Brantly et al., 2017.
^{liii} Radin et al., RAND Corporation.
^{liv} Guerrero-Saade, Juan Andrés, et Max van Amerongen. SentinelLabs. Rapport AcidRain.
^{lv} CISA et FBI. Alerte AA22-076A.
^{lvi} Radin et al., RAND Corporation.
^{lvii} Brantly et al., 2017.
^{lviii} Radin et al., RAND Corporation.
^{lix} Politico. « Ukraine, Elon Musk and Starlink ».

II/A/1

- ^{lx} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 1.
^{lxi} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 2.
^{lxii} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 2. Chapitre 3
^{lxiii} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 5. Chapitre 2 (Asperger) et 4 (SciFi)
^{lxiv} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitres 8 à 12.

II/A/2

- ^{lxv} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 13.
- ^{lxvi} Boulenguer, Camille. 2026. *Cartographie des courants idéologiques au sein du Parti républicain*. Paris : IRIS.
- ^{lxvii} France Culture. « Palantir, l'inquiétante philosophie ». Émission radio.
- ^{lxviii} Inchauspé, Irène, et Muriel Motte. « Elon Musk, promoteur très motivé de Milton Friedman ». *L'Opinion*.
- ^{lxix} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 14.
- ^{lxx} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 14.
- ^{lxxi} Farrow, Ronan. 2023. « Elon Musk's Shadow Rule ». *The New Yorker*, 21 août 2023.

II/A/3

- ^{lxxii} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 15.
- ^{lxxiii} Payload Research. 2024. *The Starship Report*. Janvier 2024.
- ^{lxxiv} Payload Research. 2024. *The Starship Report*. Janvier 2024.
- ^{lxxv} Satariano, Adam, Scott Reinhard, Cade Metz, Sheera Frenkel et Malika Khurana. 2023. « Elon Musk's Unmatched Power in the Stars ». *The New York Times*, 28 juillet 2023.
- ^{lxxvi} Satariano, Adam, Scott Reinhard, Cade Metz, Sheera Frenkel et Malika Khurana. 2023. « Elon Musk's Unmatched Power in the Stars ». *The New York Times*, 28 juillet 2023.
- ^{lxxvii} Isaacson, Elon M. Musk, Simon & Schuster, 2023, chapitre 170
- ^{lxxviii} Isaacson, Elon M. Musk, Simon & Schuster, 2023, chapitre 12
- ^{lxxix} Payload Research. 2024. *The Starship Report*. Janvier 2024.
- ^{lxxx} Farrow, Elon M. Musk's Shadow Rule, The New Yorker, 21 août 2023
- ^{lxxxi} Payload Research. 2024. *The Starship Report*. Janvier 2024.
- ^{lxxxii} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 24.
- ^{lxxxiii} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 24.

II/B/2

- ^{lxxxiv} Isaacson, Walter. 2023. *Elon Musk*. New York: Simon & Schuster. Chapitre 70.
- ^{lxxxv} Farrow, Ronan. 2023. « Elon Musk's Shadow Rule ». *The New Yorker*, 21 août 2023.
- ^{lxxxvi} Satariano, Adam, Scott Reinhard, Cade Metz, Sheera Frenkel et Malika Khurana. 2023. « Elon Musk's Unmatched Power in the Stars ». *The New York Times*, 28 juillet 2023.
- ^{lxxxvii} Payload Research. 2024. *The Starship Report*. Janvier 2024.

II/B/3

- ^{lxxxviii} Farrow, Ronan. 2023. « Elon Musk's Shadow Rule ». *The New Yorker*, 21 août 2023.
- ^{lxxxix} Farrow, Ronan. 2023. « Elon Musk's Shadow Rule ». *The New Yorker*, 21 août 2023.
- ^{xc} SpaceX. 2026. *Form S-1 Registration Statement*. Washington, D.C.: U.S. Securities and Exchange Commission (SEC).
- ^{xc} Warren, Elizabeth. 2024. Lettre au Secrétaire à la Défense des États-Unis concernant Starlink. Sénat des États-Unis, 9 avril 2024
- ^{xcii} Warren, Elizabeth. 2024. Lettre au Secrétaire à la Défense des États-Unis concernant Starlink. Sénat des États-Unis, 9 avril 2024
- ^{xciii} Warren, Elizabeth. 2024. Lettre au Secrétaire à la Défense des États-Unis concernant Starlink. Sénat des États-Unis, 9 avril 2024
- ^{xciv} SpaceX. 2026. *Form S-1 Registration Statement*. Washington, D.C.: U.S. Securities and Exchange Commission (SEC).
- ^{xcv} SpaceX. 2026. *Form S-1 Registration Statement*. Washington, D.C.: U.S. Securities and Exchange Commission (SEC).

II/B/4

- ^{xcvi} Jayanti, Amritha. 2023. *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?* Cambridge, MA: Belfer Center for Science and International Affairs.
- ^{xcvii} Sacra. 2026. « SpaceX — Valuation ». 13 mai 2026.
- ^{xcviii} Jayanti, Amritha. 2023. *Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose?* Cambridge, MA: Belfer Center for Science and International Affairs.

^{xcix} Marquardt, Alex. 2022. « Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab ». *CNN*, 13 octobre 2022.

^c Notice.co, *SpaceX Report*, 30 décembre 2024, p. 8 ; Sacra, *SpaceX Equity Research*, 13 mai 2026

^{ci} SpaceX. 2026. *Form S-1 Registration Statement*. Washington, D.C.: SEC.

^{cii} SpaceX. 2026. *Form S-1 Registration Statement*. Washington, D.C.: SEC.

II/B/5

^{ciii} SpaceX. 2026. *Form S-1 Registration Statement*. Washington, D.C.: SEC.

^{civ} SpaceX. 2026. *Form S-1 Registration Statement*. Washington, D.C.: SEC.

^{cv} Béatrice Hainaut, *La guerre des fréquences – Vers une marchandisation de la ressource spectre/orbite ?*, Étude 123, IRSEM, mai 2025.

^{cvi} Federal Communications Commission. 2022. *Space Exploration Holdings, LLC: Application for Approval for Orbital Deployment and Operating Authority for the SpaceX Gen2 NGSO Satellite System (FCC 22-91)*. Washington, D.C., 1 décembre 2022.

^{cvi} Federal Communications Commission. 2022. *Space Exploration Holdings, LLC: Application for Approval for Orbital Deployment and Operating Authority for the SpaceX Gen2 NGSO Satellite System (FCC 22-91)*. Washington, D.C., 1 décembre 2022.

^{cvi} Foust, Jeff. 2023. « The Accidental Monopoly: How SpaceX Became (Just About) the Only Game in Town ». *SpaceNews*, 13 octobre 2023.

II/B/6

^{cix} Satariano, Adam, Scott Reinhard, Cade Metz, Sheera Frenkel et Malika Khurana. 2023. « Elon Musk's Unmatched Power in the Stars ». *The New York Times*, 28 juillet 2023.

III

^{cx} Kagan, Frederick W., George Barros et Kateryna Stepanenko. 2022. *Russian Offensive Campaign Assessment*. Washington D.C.: Institute for the Study of War, 1 mars 2022.

^{cx} Bohdan Kostiuk, Daryna-Maryna Patiuk, Anastasiya Shapochkina, and Élie Tenenbaum, "Mapping the MilTech War: Eight Lessons from Ukraine's Battlefield", *Focus stratégique*, No. 132, Ifri, February 2026.

III/A/2

^{cxii} USAID Office of Inspector General. 2025. *Inspection of USAID's Oversight of Starlink Terminals Delivered to Ukraine*. Washington D.C. : USAID

^{cxiii} Polska Agencja Prasowa. 2024. « Poland at Cyber Cold War with Russia Says Minister ». 6 mai 2024.

^{cxiv} Federal Foreign Office of Germany. 2023. « Foreign Minister Baerbock with Her Colleague Kuleba in Kharkiv ». Berlin, 10 janvier 2023.

^{cxv} Isaacson, W. (2023). Opinion. 'How am I in this war?': The untold story of Elon Musk's support for Ukraine. *Washington Post*.

III/A/4

^{cxvi} The New Republic. 2023. "Putin Suck-up Elon Musk Shut Off Starlink to Stop a Ukrainian Attack". 7 septembre 2023.

III/A/5

^{cxvii} Cyberdefense Report Hacking the Cosmos: Cyber operations against the space sector - A case study from the war in Ukraine, Clémence Poirier Zürich, October 2024, Center for Security Studies (CSS), ETH Zürich.

^{cxviii} The New Republic, "Elon Musk shut off Starlink to stop Ukrainian attack on Russia", 7 Septembre 2023.

III/A/6

^{cxix} Statement by Mr. Konstantin VORONTSOV, Deputy Head of the Delegation of the Russian Federation, at the Thematic Discussion on Outer Space (Disarmament Aspects) in the First Committee of the 77th Session of the UN General Assembly (New York, 26 October 2022)

III/C

^{cxix} Breaking Defense. 2022. « A Musk Monopoly? Ukraine Has Few Options Outside Starlink for Battlefield SATCOMs ». Octobre 2022.

III/D/2

^{cxvi} USAID Office of Inspector General. 2025. *Ukraine Response: USAID Did Not Fully Mitigate the Risk of Misuse of the Starlink Satellite Terminals It Delivered to Ukraine*. Washington D.C. : USAID.

^{cxvii} Global Initiative Against Transnational Organized Crime. 2025. *La constellation obscure : comment le système Starlink façonne les conflits et la criminalité dans le Sahel*. 12 mai 2025.

^{cxviii} Nordsint. 2026. « A Mistake in the Declarations: Russian Starlink Procurement Traced via Conformity Filings ». 6 janvier 2026.

^{cxix} United States House of Representatives, 118th congress.. 2024. Correspondance relative à l'utilisation de Starlink par les forces russes. 6 mars 2024.

III/D/3

^{cxvi} Reuters, « Russia using thousands of SpaceX Starlink terminals in Ukraine, WSJ says », 15 février 2024.

^{cxvii} United States House of Representatives, 118th congress. 2024. Lettre adressée à SpaceX concernant l'usage de Starlink par les forces russes. 6 mars 2024.

III/D/4

^{cxviii} Poirier, Clémence. 2025. *Politique de sécurité : analyses du CSS*, no 361. Zurich: Center for Security Studies (CSS), mai 2025

^{cxvix} Alberola, David. 2026. « L'exploitation ukrainienne de la coupure Starlink de février 2026 : une sortie du blocage tactique ? ». *Observatoire des conflits*, Centre d'études stratégiques Terre, Ministère des Armées, 24 avril 2026.

^{cxvi} Fedorov, Mykhailo. 2026. Publication sur X (anciennement Twitter), 29 janvier 2026. Compte officiel @FedorovMykhailo.

^{cxvii} Jamestown, « Ukraine Responds to Russia's Starlink Use », Yuri Lapaiev, [en ligne], 10 février 2026. Lapaiev, Yuri. 2026. « Ukraine Responds to Russia's Starlink Use ». *Jamestown Foundation*, 10 février 2026.

^{cxviii} Entretien ouvert avec un officier du renseignement.

^{cxvix} Fedorov, Mykhailo. 2026. Publication sur X (anciennement Twitter), 29 janvier 2026. Compte officiel @FedorovMykhailo.

^{cxvi} InformNapalm. 2026. « Opération CYBINT contre le système de satellites Gonets qualifié d'équivalent russe de Starlink ». 30 avril 2026.

III/D/5

^{cxvii} Global Initiative Against Transnational Organized Crime. 2025. *La constellation obscure : comment le système Starlink façonne les conflits et la criminalité dans le Sahel*. 12 mai 2025.