# PROJET DE THÈSE : L'ARCHITECTURE DE LA DOMINATION COGNITIVE ET DU HACKING POLITIQUE

## Une Analyse Systémique des Conflits Hybrides à l'Ère de la Technopolitique et de l'Intelligence Artificielle

### Introduction Générale : La Tectonique des Plaques de la Souveraineté Numérique

L'aube du XXIe siècle a vu s'opérer une mutation fondamentale dans la nature de la conflictualité humaine, une transformation si radicale qu'elle remet en question les fondements mêmes de la théorie politique et stratégique classique. Le champ de bataille, autrefois délimité par la géographie physique, les frontières nationales et les théâtres d'opérations cinétiques, s'est étendu à une cinquième dimension : le cyberespace. Cependant, réduire cette nouvelle arène à une simple infrastructure de réseaux et de serveurs serait une erreur ontologique. Au cœur de cette transformation réside le phénomène du "hacking politique", une intersection complexe et volatile entre la maîtrise technologique et l'ambition de pouvoir, qui ne vise plus seulement à contrôler des territoires ou des ressources, mais à conquérir, manipuler ou déstabiliser les infrastructures cognitives des sociétés modernes.1

Ce projet de thèse se propose d'explorer en profondeur les mécanismes, les acteurs et les implications de cette nouvelle forme de guerre qui cible l'esprit humain comme territoire ultime. Nous postulons que le hacking politique n'est pas une simple nuisance technologique ou une forme modernisée d'espionnage, mais le symptôme d'une recomposition profonde de l'ordre mondial — une "tectonique des plaques" géopolitique et cognitive.1 Dans cet environnement, la capacité à contrôler l'information, à sécuriser ses réseaux sémantiques et à maintenir l'intégrité cognitive de sa population est devenue la mesure ultime de la puissance souveraine.

La pertinence de cette recherche est soulignée par la convergence critique de crises systémiques. L'année 2024, qualifiée de "super-année électorale" avec des scrutins majeurs à Taïwan, en Europe et aux États-Unis, a servi de révélateur à l'ampleur de la menace : l'infrastructure démocratique elle-même est devenue une cible prioritaire. L'objectif des assaillants n'est plus nécessairement d'altérer techniquement les résultats des votes, mais d'en éroder la légitimité aux yeux des citoyens, provoquant un effondrement de la confiance institutionnelle qualifié de "Trust Decay".1 Parallèlement, l'émergence des modèles de langage larges (LLM) et de l'intelligence artificielle générative introduit une variable d'accélération inédite, permettant l'industrialisation de la persuasion et la pollution des sources mêmes de la connaissance par des techniques de "Data Poisoning" et de "Generative Engine Optimization" (GEO).3

Pour appréhender la complexité de cette "guerre hors limites", ce rapport adopte une grille d'analyse structurée selon trois niveaux d'échelle interdépendants, inspirée de la sociologie des organisations et de la théorie des systèmes complexes : le niveau **Micro** (l'individu et la psychopolitique), le niveau **Méso** (les organisations et l'architecture de commandement) et le niveau **Macro** (l'État-nation et la technopolitique globale). Cette approche à 360° mobilise des disciplines variées : la sociologie politique pour comprendre les nouvelles formes de militantisme, la philosophie pour théoriser la mutation du pouvoir (de la biopolitique à la noopolitique), l'informatique pour disséquer les vecteurs d'attaque (du DDoS à l'empoisonnement sémantique), et les sciences cognitives pour analyser les vulnérabilités de l'esprit humain face à la manipulation algorithmique.

### Partie I : Cadre Théorique et Épistémologique – De la Cyberguerre à la Guerre Cognitive

Avant de disséquer les mécanismes opérationnels, il est impératif d'établir un cadre théorique robuste capable d'englober la nature hybride du phénomène. La guerre cognitive ne se substitue pas à la cyberguerre ; elle l'englobe et la dépasse en ciblant l'élément humain du système cyber-physique.

#### 1.1. La Mutation de la Conflictualité : Vers une "Noopolitique"

Les travaux de Carl von Clausewitz sur la guerre conventionnelle, centrés sur la destruction physique des forces ennemies pour imposer sa volonté, montrent leurs limites dans le cyberespace. Nous assistons à un glissement vers ce que les stratèges russes, dans la lignée de la "doctrine Gerasimov", appellent la "guerre de nouvelle génération" ou guerre hybride, où les moyens non-militaires (informationnels, économiques, cognitifs) prédominent sur l'action cinétique.1 Ce n'est plus la conquête du sol qui prime, mais la conquête des esprits.

Ce changement de paradigme peut être théorisé à travers le concept de **Noopolitique** (Noopolitics), tel que développé par les théoriciens Arquilla et Ronfeldt. Contrairement à la Realpolitik, fondée sur le hard power et la coercition physique, la Noopolitique se joue dans la "noosphère" (la sphère des idées, des valeurs et de la connaissance). Elle postule que la domination ne s'acquiert plus par la force brute, mais par la suprématie narrative et le contrôle des flux d'information.6 Dans ce contexte, le hacker politique devient un "guerrier de la connaissance", capable d'altérer la perception de la réalité de l'adversaire sans tirer un seul coup de feu. La stratégie ne consiste plus à détruire l'adversaire, mais à le rendre incapable de prendre des décisions cohérentes en saturant son environnement cognitif.

Cette approche résonne puissamment avec les travaux du philosophe Byung-Chul Han sur la **Psychopolitique**. Han soutient que le néolibéralisme numérique a opéré une transition du "biopouvoir" foucaldien (qui discipline les corps dans des espaces clos comme l'usine ou la prison) vers un "psychopouvoir" qui exploite et contrôle la psyché. Dans ce régime de domination, la liberté est instrumentalisée : les individus se soumettent volontairement au panoptique numérique (réseaux sociaux, Big Data) en "s'auto-exploitant". Le hacking politique exploite cette architecture de la transparence : il ne contraint pas, il séduit ou manipule les émotions et les biais cognitifs pour orienter les comportements, transformant le "Like" en un acte de soumission à l'ordre de domination.8

#### 1.2. La Souveraineté Numérique et le Modèle du "Stack"

Pour comprendre où se joue cette guerre, il faut adopter une vision matérielle et logicielle de la géopolitique qui dépasse la carte traditionnelle des États. Le modèle du **"Stack"** (l'Empilement) proposé par Benjamin Bratton offre une grille de lecture essentielle pour notre thèse. Bratton décrit une mégastructure planétaire composée de six couches interdépendantes : Terre, Cloud, Ville, Adresse, Interface, Utilisateur.11

Selon cette théorie, la souveraineté ne s'exerce plus horizontalement sur des territoires délimités par des frontières (Westphaliennes), mais verticalement à travers ces couches technologiques. Le hacking politique est une opération transversale qui perce ces strates. Une attaque peut commencer au niveau "Interface" (un deepfake sur un smartphone), transiter par le "Cloud" (serveurs de données piratés ou empoisonnés), pour finalement impacter la couche "Utilisateur" (le vote du citoyen) et la couche "Terre" (les ressources énergétiques ou les frontières physiques, comme dans le cas des cyberattaques contre le réseau électrique ukrainien).1

La notion de **Souveraineté Numérique** devient alors centrale. Elle ne se limite pas à la protection des données (Data Sovereignty), mais s'étend à la **Souveraineté Épistémique** : la capacité d'un peuple ou d'une nation à définir ses propres concepts, à valider ses propres vérités et à comprendre le monde sans passer par le prisme déformant d'algorithmes contrôlés par des puissances étrangères.13 Lorsqu'une plateforme étrangère modifie ses algorithmes de classement, elle exerce un acte de souveraineté sur l'espace cognitif de ses utilisateurs, remettant en cause l'autonomie politique des États hôtes.

#### 1.3. La Théorie du Chaos et l'Effet Papillon Numérique

Sur le plan méthodologique, l'analyse du hacking politique gagne à intégrer la théorie du chaos et la dynamique des systèmes complexes. Le cyberespace, et en particulier l'écosystème de l'information (Google, réseaux sociaux), est un système dynamique non-linéaire sensible aux conditions initiales.1

Le document source sur la "Doctrine de Domination Cognitive" 1 illustre parfaitement cette application tactique. Contrairement à la guerre conventionnelle où la relation entre force et effet est souvent linéaire, la guerre cognitive exploite la non-linéarité. L'injection d'un "triplet sémantique toxique" (une fausse information structurée pour être lue par les machines, ex: <Politique X> <est financé par> <Lobby Y>) dans un nœud d'autorité du réseau peut provoquer une cascade de conséquences disproportionnées par rapport à l'impulsion initiale. C'est l'effet papillon appliqué à la réputation et à la stabilité politique. Les algorithmes de recommandation, conçus pour maximiser l'engagement (souvent par l'indignation), agissent comme des amplificateurs de cette entropie, transformant une perturbation locale en crise systémique.1

#### 1.4. L'Approche par l'Actor-Network Theory (ANT)

Enfin, pour éviter le déterminisme technologique, notre cadre théorique intègre l'**Actor-Network Theory** (ANT) de Bruno Latour et Michel Callon. L'ANT permet de traiter les entités non-humaines (algorithmes, bots, malwares) comme des "actants" dotés d'une forme d'agence au sein du réseau sociotechnique.17 Dans le cadre du hacking politique, un botnet ou un algorithme de classement n'est pas un simple outil passif ; il modifie les relations de pouvoir, traduit des intentions politiques en code exécutable et reconfigure les alliances. Analyser une cyberattaque comme celle de Stuxnet ou les ingérences électorales à travers le prisme de l'ANT permet de comprendre comment des alliances hybrides entre humains (hackers, officiers de renseignement) et non-humains (virus, plateformes) parviennent à déstabiliser des structures étatiques robustes.19

### Partie II : Analyse Micro — L'Individu et la Cognition Assiégée

Au niveau micro, l'unité d'analyse est l'individu — le citoyen, l'électeur, ou le décideur. C'est à ce niveau que la guerre cognitive produit ses effets les plus intimes et les plus dévastateurs, en exploitant les vulnérabilités de la psychologie humaine et en redéfinissant la subjectivité politique.

#### 2.1. Psychopolitique et "Trust Decay" : L'Usure de la Vérité

La cible première du hacking politique n'est pas l'ordinateur, mais le cerveau de l'utilisateur. Les attaquants exploitent systématiquement les heuristiques de jugement et les biais cognitifs (biais de confirmation, biais de négativité, effet de vérité illusoire) pour contourner la rationalité critique. La "Psychopolitique" décrite par Han trouve ici son application opérationnelle : le smartphone, objet de dévotion quasi-religieuse ("le rosaire numérique"), devient le vecteur par lequel la domination s'insinue dans l'intimité.20

Le concept de **"Trust Decay"** (décroissance de la confiance) est central pour comprendre l'impact micro-politique. Comme le démontrent les études empiriques du *Georgia Institute of Technology*, la simple exposition à des nouvelles rapportant des cyberattaques ou des failles de sécurité suffit à éroder la confiance des citoyens dans l'intégrité des processus démocratiques, indépendamment de la réalité technique de la menace ou de son impact réel sur le vote.1 C'est le paradoxe de la sécurité cognitive : la perception de la vulnérabilité est aussi dommageable politiquement que la vulnérabilité elle-même.

Les opérations d'influence, comme celles menées par l'agence russe *Internet Research Agency* (IRA) ou les campagnes chinoises *Spamouflage*, ne cherchent pas nécessairement à convaincre l'individu d'une vérité alternative cohérente. Leur objectif tactique est souvent de saturer l'espace cognitif pour créer de la confusion, de l'apathie et une paralysie décisionnelle, un état d'**entropie informationnelle**.1 Face à un déluge d'informations contradictoires, l'individu se replie sur ses croyances tribales préexistantes ou sombre dans le cynisme, considérant que "tout est faux" et que la vérité est inconnaissable.

#### 2.2. Le "Liar's Dividend" et l'Insécurité Épistémique

Ce phénomène est exacerbé par ce que les experts appellent le **"Liar's Dividend"** (le dividende du menteur). L'existence connue des deepfakes et des technologies de manipulation audio/vidéo permet aux acteurs politiques malhonnêtes de discréditer des preuves réelles de leurs méfaits en criant au "fake" ou à la manipulation par IA.1

Cela crée une situation d'**insécurité épistémique** profonde.22 L'individu perd sa capacité à vérifier la réalité, ce qui fragilise son identité politique et sociale. La sécurité épistémique, définie comme la capacité à posséder des connaissances fiables pour agir dans le monde, est attaquée. Pour les jeunes adultes ou les populations vulnérables, cette instabilité peut conduire à une radicalisation ou à un retrait complet de la vie civique. L'attaque cognitive vise donc à détruire le "capital sémantique" commun — l'ensemble des significations partagées qui permettent le débat démocratique.24

#### 2.3. L'Usurpation d'Identité et le "Spear-Phishing" Cognitif

Techniquement, l'attaque au niveau micro passe souvent par la compromission de l'identité numérique. Le **Spear-Phishing** (harponnage) est l'arme de prédilection pour pénétrer la sphère cognitive d'une cible de haute valeur (un parlementaire, un journaliste, un chef d'entreprise). En analysant les traces numériques de la cible (OSINT), l'attaquant construit un message hyper-personnalisé qui désarme la méfiance naturelle.

Mais la menace va plus loin avec l'**Entity Poisoning** (Empoisonnement d'Entité) décrit dans la doctrine de l'Agence #B!Mi.1 Il ne s'agit plus de voler des identifiants, mais d'associer l'identité numérique d'une personne ou d'une organisation à des concepts toxiques (arnaque, scandale, incompétence) au sein des graphes de connaissances (Knowledge Graphs) des moteurs de recherche. En manipulant les données structurées (Schema.org) et les signaux d'autorité, l'attaquant force l'algorithme à valider un mensonge comme une donnée factuelle. Pour la victime, l'effet est une "mort numérique" : son identité est redéfinie par la machine, entraînant une exclusion sociale et économique réelle. C'est une forme de violence symbolique automatisée, où l'algorithme devient l'exécuteur de la sentence de réputation, souvent sans recours juridique efficace immédiat.1

#### 2.4. Le Hacker comme Acteur Politique : Profils et Motivations

Au niveau micro, il convient également d'analyser l'acteur à l'origine de l'attaque. Le profil du "hacker politique" est loin d'être monolithique. Il oscille entre deux pôles idéologiques distincts qui définissent la légitimité de l'action.

* **Le Hacktiviste :** Héritier de la "Hacker Ethic" des années 1960 ("L'information veut être libre"), il considère le hacking comme une forme de **désobéissance civile numérique**. Des figures comme Aaron Swartz ou les collectifs comme *Anonymous* utilisent des outils comme les attaques DDoS (considérées comme des sit-ins virtuels) ou le "Défacement" pour protester contre la censure ou les abus de pouvoir. Bien que souvent illégales, ces actions sont motivées par un impératif moral de transparence et de justice sociale.1
* **L'Agent Étatique / Mercenaire (Black Hat) :** Il opère dans une logique de guerre ou de profit. Les opérateurs des groupes comme *Sandworm* (Russie) ou *Volt Typhoon* (Chine) sont des fonctionnaires ou des contractants intégrés dans des hiérarchies militaires. Leur motivation n'est pas l'éthique, mais l'accomplissement d'une mission stratégique (sabotage, espionnage, déstabilisation). La psychologie de ces acteurs est radicalement différente : là où le hacktiviste cherche la publicité pour sa cause, l'agent étatique recherche l'invisibilité ou la "plausibilité du déni".1

### Partie III : Analyse Méso — Organisations, Réseaux et Architecture de Commandement

Le niveau méso s'intéresse aux structures intermédiaires — organisations, réseaux d'influence, partis politiques, agences de renseignement — qui organisent, amplifient et dirigent les capacités de hacking politique. C'est l'échelon de l'opérationnalisation stratégique, où la doctrine se transforme en action coordonnée.

#### 3.1. L'Adoption de l'***Auftragstaktik*** dans la Cyber-Guerre

L'une des découvertes majeures de l'analyse organisationnelle des groupes de hacking politique efficaces est l'adoption de structures de commandement décentralisées, inspirées de la doctrine militaire prussienne de l'**Auftragstaktik** (commandement de mission).

Dans le cyberespace, la vitesse de propagation de l'information et la rapidité des contre-mesures (patchs de sécurité, mises à jour d'algorithmes Google, modération des réseaux sociaux) rendent les hiérarchies pyramidales traditionnelles obsolètes. Le modèle centralisé (*Befehlstaktik*) est trop lent et rigide pour agir à l'intérieur de la boucle **OODA** (Observer, Orienter, Décider, Agir) de l'adversaire ou des algorithmes de défense.1

L'étude de cas de l'Agence #B!Mi 1 révèle une application littérale de ce principe à la guerre cognitive. L'organisation est divisée en cellules autonomes par spécialité (architecture sémantique, netlinking, R&D mathématique). Le niveau stratégique (l'État-Major) définit l'intention (*Absicht*) — par exemple "détruire la crédibilité financière de la cible X". Le niveau opérationnel (les experts SEO, les codeurs, les créateurs de contenu) dispose d'une liberté totale sur le "comment" (choix des vecteurs, timing, outils techniques). Cette autonomie permet une réactivité immédiate : si une faille algorithmique est découverte (un "glitch" dans Google ou une tendance virale sur TikTok), elle est exploitée dans l'heure, sans attendre une validation bureaucratique. Cette agilité organisationnelle est un facteur clé de supériorité dans la guerre hybride, permettant de submerger les processus de décision plus lents des États démocratiques.30

#### 3.2. Typologie des Menaces Organisationnelles Étatiques et Para-Étatiques

Au niveau méso, on distingue plusieurs types d'acteurs organisationnels dont les modes opératoires diffèrent selon leurs objectifs politiques. L'analyse des rapports de cyber-intelligence (Microsoft, ANSSI, CISA) permet d'établir une typologie claire 1 :

| **Type d'Acteur** | **Exemple Notable** | **Affiliation** | **Objectif Stratégique & Mode Opératoire** |
| --- | --- | --- | --- |
| **Les Saboteurs** | **Sandworm** (Unité 74455) | Russie (GRU) | **Destruction Systémique.** Visent la paralysie physique des infrastructures (réseau électrique ukrainien, NotPetya). Organisation quasi-militaire, orientée vers des effets cinétiques via le cyber. |
| **Les Espions Stratèges** | **Midnight Blizzard** (APT29) | Russie (SVR) | **Infiltration Furtive.** Privilégient le renseignement politique et diplomatique à long terme ("Living off the Land"). Infiltrent les chaînes d'approvisionnement (SolarWinds) pour accéder aux réseaux gouvernementaux sans détection. |
| **Les Pré-positionneurs** | **Volt Typhoon** | Chine (MSS) | **Menace Latente.** Infiltrent les infrastructures critiques (ports, eaux, télécoms US) pour se "pré-positionner" en vue d'un conflit futur (ex: invasion de Taïwan). Stratégie de "minage" numérique du terrain adverse. |
| **Les Influenceurs de Masse** | **Dragonbridge / Spamouflage** | Chine | **Guerre Narrative.** Utilisent des réseaux massifs de bots et de faux comptes pour inonder les réseaux sociaux, noyer les critiques et promouvoir les narratifs du PCC. Usage croissant de l'IA. |
| **Les Mercenaires Financiers** | **Lazarus Group** | Corée du Nord (RGB) | **Financement du Régime.** Modèle hybride unique : utilisent leurs capacités cyber pour voler des crypto-monnaies et lancer des ransomwares afin de financer le programme nucléaire, tout en menant de l'espionnage. |

#### 3.3. L'Ingénierie Sémantique et la Manipulation des Algorithmes

L'arme principale au niveau méso pour la domination cognitive est la maîtrise de l'architecture du Web. Les agences d'influence ne se contentent pas de diffuser des messages ; elles construisent des infrastructures de légitimation qui manipulent la manière dont les algorithmes trient et présentent l'information.

La technique du **Cocon Sémantique**, théorisée par Laurent Bourrelly et adaptée à la guerre de l'information, en est un exemple frappant.1 Il s'agit de structurer un réseau de pages web liées entre elles par une logique sémantique précise (maillage interne) pour piéger l'utilisateur et concentrer le "jus" algorithmique (PageRank) vers une cible précise. Le mécanisme repose sur le **glissement sémantique** (Semantic Shifting) :

1. **Attraction :** On attire l'internaute sur des pages périphériques traitant de sujets consensuels à fort volume de recherche (ex: "L'importance de l'écologie").
2. **Glissement :** Via des liens contextuels, on guide l'utilisateur vers des pages où le narratif se radicalise progressivement (ex: "Les scandales écologiques de l'entreprise X").
3. **Frappe :** On aboutit à la "Page Mère" (Target Page), qui contient le message de désinformation ou d'attaque, désormais crédibilisé par la puissance algorithmique du réseau amont.

Cette architecture est souvent soutenue par des **PBN (Private Blog Networks)** : des milliers de faux sites créés pour simuler une popularité et une autorité artificielle ("Topical Authority") aux yeux de Google. Une fois que Google identifie ce réseau comme une "source experte", n'importe quel mensonge qui y est publié est propulsé en tête des résultats de recherche, acquérant ainsi un statut de vérité factuelle. De plus, l'abus des protocoles comme **ClaimReview** (conçu pour le fact-checking) permet à des sites malveillants de s'autoproclamer vérificateurs de faits, affichant des badges "Fact Check: Vrai" sur des mensonges dans les résultats de recherche.1

#### 3.4. La Gouvernance Algorithmique des Organisations

Au niveau méso, il faut aussi considérer comment les plateformes elles-mêmes (Google, Meta, X) exercent une forme de **Gouvernance Algorithmique**. Antoinette Rouvroy décrit cela comme un mode de gouvernement qui ne s'adresse pas aux sujets politiques, mais aux "profils" statistiques. Les organisations politiques doivent désormais naviguer dans cet environnement où la visibilité est régulée par des boîtes noires algorithmiques. La censure n'est plus nécessairement l'effacement, mais l'invisibilisation (shadowbanning) ou le déclassement. Les stratégies de hacking politique visent précisément à comprendre (reverse engineering) et détourner ces règles de gouvernance algorithmique pour amplifier artificiellement des mouvements marginaux ou supprimer des opposants.36

### Partie IV : Analyse Macro — Géopolitique, Technopolitique et Souveraineté

Le niveau macro est celui où les effets cumulés des actions micro et méso se traduisent en enjeux de puissance nationale et internationale. C'est le domaine de la "Haute Politique" du numérique, où se joue la survie des États et la reconfiguration de l'ordre mondial.

#### 4.1. La Technopolitique et la Colonisation des Infrastructures

La **Technopolitique** désigne la manière dont les technologies incarnent et projettent des formes de pouvoir politique.39 À ce niveau, les plateformes numériques (Google, Facebook, Amazon, Alibaba) ne sont pas des acteurs neutres ou de simples entreprises privées ; elles constituent des infrastructures de souveraineté. Comme le souligne Benjamin Bratton dans sa théorie du "Stack", elles opèrent comme des "pseudo-États" capables d'édicter des règles (Terms of Service), de prélever des impôts (extraction de la plus-value des données), de cartographier le monde (Google Maps) et de contrôler les frontières de l'information et de l'identité.11

Pour l'Europe, cette situation révèle une vulnérabilité critique : une dépendance technologique quasi-totale vis-à-vis des géants américains (GAFAM) et chinois (BATX). On parle de **colonialisme numérique** ou de perte de souveraineté. Les données des citoyens européens sont extraites, traitées et stockées hors de leur juridiction, soumises à des lois extraterritoriales comme le **Cloud Act** américain, qui permet aux forces de l'ordre US d'accéder aux données stockées par leurs entreprises n'importe où dans le monde.1 Cette dépendance n'est pas seulement économique ; elle est infrastructurelle et cognitive. Si les infrastructures de connaissance (moteurs de recherche, IA) qui façonnent l'opinion publique échappent au contrôle démocratique, la souveraineté politique devient une illusion.

#### 4.2. La Guerre Froide Cognitive : Le Carré des Menaces

Le paysage géopolitique actuel est structuré par une "Cyber-Guerre Froide" opposant les démocraties libérales à un axe de régimes autoritaires. Ce conflit asymétrique se joue sur la définition même de la vérité et de la stabilité sociale.

* **La Russie :** Pratique une "stratégie du chaos". Son objectif, théorisé dans la doctrine Gerasimov, n'est pas tant de promouvoir le modèle russe (qui a peu de "soft power") que d'exacerber les fractures internes de l'Occident (raciales, sociales, politiques) pour paralyser ses adversaires. L'usage industriel de "fermes à trolls" (IRA) et l'opération **Doppelgänger** (clonage de sites de médias occidentaux reconnus comme *Le Monde* ou *The Guardian* pour diffuser de la désinformation) visent à créer un brouillard permanent où plus rien n'est vrai et tout est possible.1
* **La Chine :** Adopte une approche plus contrôlante, sophistiquée et long-termiste. Elle vise à imposer son narratif global (sur Taïwan, les droits de l'homme, la supériorité de son modèle) et à sécuriser ses intérêts économiques. L'utilisation de l'IA pour créer de faux présentateurs de news convaincants et l'infiltration des diasporas via des applications comme WeChat relèvent d'une stratégie d'encerclement cognitif et de contrôle du discours global.1
* **L'Iran :** Utilise le cyber comme une arme asymétrique du pauvre pour compenser sa faiblesse militaire conventionnelle face aux États-Unis et à Israël. Ses opérations ciblent les dissidents et tentent d'influencer les élections (comme aux USA en 2024) par des opérations d'intimidation directe (emails menaçants sous faux drapeau, hack-and-leak).1

#### 4.3. Le Droit International face au Problème de l'Attribution

La réponse juridique des États se heurte au problème fondamental et technique de l'**attribution**. Dans le cyberespace, il est aisé de masquer son origine (via des proxys, VPN, Tor) ou, pire, de se faire passer pour un autre, une technique connue sous le nom de **False Flag** (faux drapeau).

L'attaque *Olympic Destroyer* contre les JO de PyeongChang en 2018 est un cas d'école : des hackers russes (Sandworm) ont délibérément inséré des morceaux de code et des métadonnées typiques du groupe nord-coréen Lazarus pour tromper les analystes et provoquer une crise diplomatique entre la Corée du Nord et l'Occident.1 Cette capacité de falsification de l'empreinte numérique rend l'application du droit international extrêmement complexe.

Néanmoins, des initiatives comme le **Manuel de Tallinn** (initié par l'OTAN) tentent de transposer les règles du droit de la guerre (*jus ad bellum* et *jus in bello*) au domaine cyber. La doctrine française, par exemple, considère désormais qu'une cyberattaque causant des dommages physiques substantiels ou des pertes de vies humaines peut être qualifiée d'"agression armée" au sens de l'article 51 de la Charte de l'ONU, ouvrant théoriquement droit à la légitime défense, y compris par des moyens militaires conventionnels.1 Cependant, la majorité des opérations de guerre cognitive (désinformation, subversion) restent soigneusement sous ce seuil ("below the threshold of armed conflict"), dans la zone grise où le droit est flou et la riposte difficile à justifier.

### Partie V : Prospective — L'Avenir de la Domination Cognitive (2025-2030)

L'analyse prospective, basée sur les signaux faibles et les développements technologiques récents, révèle que nous sommes à l'aube d'une nouvelle mutation qui va aggraver les risques de domination cognitive. L'IA générative est le catalyseur de cette nouvelle ère.

#### 5.1. Du SEO au GEO : La Bataille pour la Réponse Unique

La transition des moteurs de recherche classiques (Search Engine Optimization - SEO) vers les moteurs de réponse générative (**Generative Engine Optimization - GEO**) marque un tournant critique pour l'accès à l'information. Avec l'avènement et l'intégration massive des assistants IA (ChatGPT, Google Gemini, Perplexity), l'utilisateur ne se voit plus proposer une liste de dix liens bleus parmi lesquels choisir, mais une **réponse unique synthétisée** directement par la machine.1

La guerre cognitive devient alors un jeu à somme nulle et à fort enjeu. Il ne s'agit plus d'être en première page, mais d'être la source exclusive citée et intégrée dans la synthèse de l'IA. Les techniques de GEO décrites dans les documents de l'Agence #B!Mi visent à optimiser les contenus (ajout de citations d'experts, statistiques, structure logique) pour qu'ils soient privilégiés par les algorithmes des LLM comme étant la "vérité" faisant autorité.1 Celui qui contrôle la réponse de l'IA contrôle, de facto, la réalité perçue par l'utilisateur, éliminant la possibilité même de la contradiction ou de la pluralité des sources.

#### 5.2. Data Poisoning et Backdoors Cognitifs

Plus inquiétant encore est le risque de **Data Poisoning** (empoisonnement de données) des modèles d'IA eux-mêmes. Des recherches académiques récentes (Anthropic, Turing Institute) montrent qu'il suffit d'injecter un nombre infime de documents malveillants (aussi peu que 0,1% du corpus d'entraînement, voire quelques centaines de documents spécifiques) lors de la phase de pré-entraînement ou de fine-tuning d'un LLM pour y introduire des "backdoors" ou des biais durables.1

Un attaquant étatique pourrait ainsi conditionner une IA militaire, gouvernementale ou médicale pour qu'elle fonctionne normalement 99% du temps, mais qu'elle produise des analyses erronées, divulgue des informations sensibles ou insère de la désinformation subtile lorsqu'elle est activée par un mot-clé spécifique ("trigger") dans le prompt. C'est une forme de sabotage cognitif profond et dormant, où l'infrastructure d'intelligence elle-même devient un agent de l'ennemi, indétectable jusqu'au moment critique.

#### 5.3. RAG Poisoning : L'Attaque en Temps Réel

Les systèmes d'IA utilisent de plus en plus la technique **RAG** (*Retrieval-Augmented Generation*) pour pallier leurs limites de connaissances en cherchant des informations fraîches sur le web avant de répondre. Cela ouvre la porte au **RAG Poisoning** : en positionnant des contenus toxiques ou falsifiés dans les résultats de recherche immédiats (via des techniques de SEO/GEO rapides et des réseaux de bots), un attaquant peut "empoisonner" la réponse de l'IA en temps réel sur un sujet d'actualité brûlant (ex: une élection, une crise sanitaire).1 L'IA ingère le faux contenu fraîchement publié et le restitue à l'utilisateur comme une vérité synthétisée, blanchissant ainsi la désinformation par l'autorité et la neutralité apparente de la machine.

### Conclusion et Synthèse : Vers une Résilience Cognitive

Ce rapport a tenté de démontrer que le hacking politique et la domination cognitive ne sont pas des déviances périphériques de la société numérique, mais des composantes structurelles de la géopolitique du XXIe siècle.

**Synthèse des Niveaux :**

* **Au niveau Micro**, l'individu est assiégé. Ses biais cognitifs sont militarisés, sa confiance est érodée ("Trust Decay") et son identité numérique est menacée d'usurpation et de redéfinition ("Entity Poisoning").
* **Au niveau Méso**, les organisations malveillantes ont muté. Elles adoptent des structures décentralisées (*Auftragstaktik*) pour gagner en vitesse et déploient des architectures sémantiques complexes (Cocon Sémantique, PBN) pour saturer l'espace informationnel et manipuler les algorithmes de visibilité.
* **Au niveau Macro**, les États s'affrontent dans une guerre hybride pour la souveraineté. La maîtrise du "Stack" technologique et des algorithmes de l'IA détermine désormais la puissance, tandis que le droit international peine à endiguer des attaques qui restent délibérément dans la "zone grise".

**Pistes pour le Projet de Thèse :**

La thèse devra explorer comment passer d'une défense purement technique (pare-feux, antivirus) à une **défense cognitive et sociétale**.

1. **La Résilience Cognitive :** Comment armer les citoyens sans tomber dans la censure? L'éducation aux médias (Digital Literacy) et le développement d'outils de "Pre-bunking" (démenti préventif, ou inoculation psychologique) pour "vacciner" l'opinion publique contre les narratifs hostiles sont des pistes prometteuses.1
2. **La Souveraineté Algorithmique Européenne :** L'Europe doit investir massivement dans ses propres infrastructures de connaissance (IA souveraines, Cloud souverain, indexation web indépendante) pour réduire sa dépendance aux "boîtes noires" américaines et chinoises. La transparence des algorithmes (imposée par le DSA) est nécessaire, mais insuffisante sans maîtrise industrielle.47
3. **Un Droit à l'Intégrité Cognitive :** Sur le plan juridique, la thèse pourrait proposer la théorisation d'un nouveau droit fondamental : le droit à l'intégrité cognitive, protégeant les citoyens contre les manipulations neuro-technologiques et algorithmiques abusives, au même titre que l'intégrité physique.

La guerre cognitive est la guerre du XXIe siècle ; elle est invisible, permanente et cible ce que nous avons de plus précieux : notre capacité à discerner le vrai du faux. La comprendre est la condition *sine qua non* pour préserver l'idéal démocratique.

### Tableaux Récapitulatifs des Données Clés

#### Tableau 1 : Typologie des Vecteurs de Domination Cognitive par Niveau

| **Niveau d'Analyse** | **Vecteur Technique / Tactique** | **Cible Principale** | **Effet Politique Recherché** | **Concept Théorique Clé** |
| --- | --- | --- | --- | --- |
| **MICRO** (Individu) | Spear-Phishing, Deepfakes, Entity Poisoning | Élu, Journaliste, Citoyen | Vol d'identité, Chantage, Confusion, "Mort Numérique" | *Trust Decay* (Usure de la confiance), *Psychopolitique* |
| **MÉSO** (Organisation) | Cocon Sémantique, PBN, DDoS, ClaimReview Abuse | Média, Parti, Entreprise, ONG | Saturation, Déclassement, Perte de visibilité, Légitimation du faux | *Auftragstaktik*, *Entropie Informationnelle* |
| **MACRO** (État/Global) | Data Poisoning, Supply Chain Attacks, RAG Poisoning | État, Infrastructure Critique, Opinion Publique | Sabotage, Espionnage Stratégique, Paralysie, Redéfinition de la réalité | *Souveraineté Numérique*, *The Stack*, *Technopolitique* |

#### Tableau 2 : Les Grands Acteurs de la Menace (2024-2025)

| **Groupe / Acteur** | **Pays d'Origine & Affiliation** | **Spécialité Tactique & TTPs** | **Objectif Stratégique** |
| --- | --- | --- | --- |
| **Sandworm** (Unité 74455) | Russie (GRU - Militaire) | Sabotage physique (OT), Wipers, Attaques destructives sur réseaux électriques. | Chaos, destruction d'infrastructures critiques, intimidation. |
| **Midnight Blizzard** (APT29) | Russie (SVR - Extérieur) | Infiltration furtive, Vol d'identifiants, Attaques Supply Chain (SolarWinds). | Espionnage politique et diplomatique à long terme. |
| **Volt Typhoon** | Chine (MSS - État) | "Living off the Land", Infiltration silencieuse des infrastructures civiles US. | Pré-positionnement stratégique, capacité de "Kill Switch" logistique. |
| **Dragonbridge / Spamouflage** | Chine (Influence) | Réseaux de bots massifs, IA générative, Deepfakes de présentateurs. | Guerre narrative, noyade des critiques, imposition du discours du PCC. |
| **Lazarus Group** | Corée du Nord (RGB) | Vols de Crypto-monnaies, Ransomware, Espionnage industriel. | Financement du régime et des programmes d'armement (contournement sanctions). |

#### Sources des citations

1. Hacking Politique\_ Analyse et Enjeux.docx
2. Impact of digital transformation on public governance - JRC Publications Repository, consulté le janvier 18, 2026, <https://publications.jrc.ec.europa.eu/repository/bitstream/JRC133975/JRC133975_01.pdf>
3. Generative Engine Optimization (GEO): How to Win in AI Search - Backlinko, consulté le janvier 18, 2026, <https://backlinko.com/generative-engine-optimization-geo>
4. LLMs may be more vulnerable to data poisoning than we thought | The Alan Turing Institute, consulté le janvier 18, 2026, <https://www.turing.ac.uk/blog/llms-may-be-more-vulnerable-data-poisoning-we-thought>
5. Full article: Culture: a sixth domain and the introduction of the 'C6ISRT' framework, consulté le janvier 18, 2026, <https://www.tandfonline.com/doi/full/10.1080/14702436.2024.2397520>
6. Rethinking Strategy and Statecraft for the Age of 4IR: Implications for Higher Education - UJ Press, consulté le janvier 18, 2026, <https://ujonlinepress.uj.ac.za/index.php/ujp/catalog/download/51/209/816?inline=1>
7. A Simple Paradigm for Noopolitics: The Geopolitics of Knowledge - E-International Relations, consulté le janvier 18, 2026, <https://www.e-ir.info/2015/10/15/a-simple-paradigm-for-noopolitics-the-geopolitics-of-knowledge/>
8. Byung-Chul Han. Psychopolitics. - ICNS, consulté le janvier 18, 2026, <https://www.icns.es/en/news/byung_chul_han_psychopolitics>
9. Psychopolitics: Neoliberalism and New Technologies of Power | Verso Books, consulté le janvier 18, 2026, <https://www.versobooks.com/products/226-psychopolitics>
10. Psychopolitics by Byung-Chul Han | Amil Mohanan, consulté le janvier 18, 2026, <https://amil.mohanan.net/posts/2018/02/psychopolitics-by-byung-chul-han/>
11. View of The Stack as an Integrative Model of Global Capitalism | tripleC, consulté le janvier 18, 2026, <https://www.triple-c.at/index.php/tripleC/article/view/1343/1475>
12. On the New Infrastructuralism: Reading Benjamin Bratton's The Stack (2015) - Medium, consulté le janvier 18, 2026, <https://medium.com/@jkinder/on-the-new-infrastructuralism-reading-benjamin-brattons-the-stack-2015-68da6994f6bb>
13. DIGITAL SOVEREIGNTY AND DATA COLONIALISM: SHAPING A JUST DIGITAL ORDER FOR THE GLOBAL SOUTH - Policy Center, consulté le janvier 18, 2026, <https://www.policycenter.ma/sites/default/files/2025-10/PP_38-25%20%28Marcus%20Vini%CC%81cius%20De%20Freitas%29.pdf>
14. Digital Tribulations 4: Interview with Pedro Burity on Popular Digital Sovereignty and Social Movements in Latin America - Institute of Network Cultures, consulté le janvier 18, 2026, <https://networkcultures.org/blog/2025/12/20/digital-tribulations-4-interview-with-pedro-burity-on-popular-digital-sovereignty-and-social-movements-in-latin-america/>
15. Knowledge and emancipation: From epistemic injustice to digital and epistemic sovereignty in Latin America | Journal of Digital Social Research - Publicera, consulté le janvier 18, 2026, <https://publicera.kb.se/jdsr/article/view/33244>
16. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept - Frontiers, consulté le janvier 18, 2026, <https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/full>
17. A theory of actor-network for cyber-security - ResearchGate, consulté le janvier 18, 2026, <https://www.researchgate.net/publication/303036168_A_theory_of_actor-network_for_cyber-security>
18. New Approaches and Concepts in Intelligence Studies: Actor-Network Theory in the Transformation of Security Intelligence, consulté le janvier 18, 2026, <https://sitjournal.com/sitj/article/view/78>
19. A theory of actor-network for cyber-security - CSS/ETH Zürich, consulté le janvier 18, 2026, [https://css.ethz.ch/publikationen/journalartikel/details.html?id=%2Fa%2Ft%2Fh%2Fe%2Fa\_theory\_of\_actornetwork\_for\_cybersecuri](https://css.ethz.ch/publikationen/journalartikel/details.html?id=/a/t/h/e/a_theory_of_actornetwork_for_cybersecuri)
20. Review: 'Psychopolitics: Neoliberalism and New Technologies of Power', consulté le janvier 18, 2026, <https://stillpointmag.org/articles/review-psychopolitics-neoliberalism-and-new-technologies-of-power/>
21. Burnout society: Byung-Chul Han: 'The smartphone is a tool of domination. It acts like a rosary' - El Pais in English - EL PAÍS, consulté le janvier 18, 2026, <https://english.elpais.com/usa/2021-10-15/byung-chul-han-the-smartphone-is-a-tool-of-domination-it-acts-like-a-rosary.html>
22. Introduction to special issue algorithmic transparency in government: Towards a multi-level perspective - ResearchGate, consulté le janvier 18, 2026, <https://www.researchgate.net/publication/346916152_Introduction_to_special_issue_algorithmic_transparency_in_government_Towards_a_multi-level_perspective>
23. A MULTI-CASE STUDY TO UNDERSTAND THE WAYS IN WHICH SOCIOCULTURAL FACTORS INFLUENCE EVERYDAY CREATIVE CONTRIBUTIONS IN HEALTHCARE - STORE - University of Staffordshire Online Repository, consulté le janvier 18, 2026, <https://eprints.staffs.ac.uk/8884/1/Lauren%20PvW%20EdD%20Ethos%20thesis.pdf>
24. (PDF) Semantic Capital: Its Nature, Value, and Curation - ResearchGate, consulté le janvier 18, 2026, <https://www.researchgate.net/publication/329279137_Semantic_Capital_Its_Nature_Value_and_Curation>
25. voluminous yet vacuous? semantic capital in an age of large language models - arXiv, consulté le janvier 18, 2026, <https://arxiv.org/pdf/2306.01773>
26. The PageRank algorithm analysed by EJAM « Mathematics# « Cambridge Core Blog, consulté le janvier 18, 2026, <https://www.cambridge.org/core/blog/2022/11/17/the-pagerank-algorithm-analysed-by-ejam/>
27. Electronic Democracy: Mobilisation, Organisation and Participation Via New ICTs, consulté le janvier 18, 2026, <http://ndl.ethernet.edu.et/bitstream/123456789/20659/1/17.pdf>
28. Improving Decision Making by Reducing Uncertainty in Complex SoS - Highlands Information Security, consulté le janvier 18, 2026, <https://hinfosec.com.au/wp-content/uploads/2019/06/MSG-143-Paper-15-Improving-Decision-Making-FINAL.pdf>
29. Beyond Auftragstaktik: The Case Against Hyper-Decentralized Command - NDU Press, consulté le janvier 18, 2026, <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2076032/beyond-auftragstaktik-the-case-against-hyper-decentralized-command/>
30. History, Mission Command, and the Auftragstaktik Infatuation - Army University Press, consulté le janvier 18, 2026, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2022/Herrera/>
31. How the Germans Defined Auftragstaktik: What Mission Command is - AND - is Not, consulté le janvier 18, 2026, <https://archive.smallwarsjournal.com/index.php/jrnl/art/how-germans-defined-auftragstaktik-what-mission-command-and-not>
32. Misinterpretation and Confusion: What is Mission Command and Can the US Army Make it Work? - AUSA, consulté le janvier 18, 2026, <https://www.ausa.org/sites/default/files/mission-command-can-army-make-it-work.pdf>
33. La désinformation : l'arme suprême dans les conflits modernes ?, consulté le janvier 18, 2026, <https://bd53565bb0.clvaw-cdnwnd.com/5248ccc307284b5d053e41eef19504b4/200010959-cd53fcd543/La%20d%C3%A9sinformation%20dans%20les%20conflits%20modernes.pdf?ph=bd53565bb0>
34. Automated tackling of disinformation - European Parliament, consulté le janvier 18, 2026, <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf>
35. An infrastructure for empowering internet users to handle fake news and other online media phenomena, consulté le janvier 18, 2026, <https://www.dfki.de/fileadmin/user_upload/import/10982_rehm_kk120.pdf>
36. Big Data, Algorithmic Governmentality and the Regulation of Pandemic Risk, consulté le janvier 18, 2026, <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/big-data-algorithmic-governmentality-and-the-regulation-of-pandemic-risk/416F40B302B67C6C598D3BCEDFBD6286>
37. Algorithmic Governmentality, Digital Sovereignty, and Agency Affordances, consulté le janvier 18, 2026, <https://ojs.weizenbaum-institut.de/index.php/wjds/article/view/87/80>
38. Chapter 5 The end(s) of critique : data-behaviourism vs. due-process. Antoinette Rouvroy\* Introduction - GitHub Pages, consulté le janvier 18, 2026, <https://publicityreform.github.io/findbyimage/readings/rouvroy.pdf>
39. A map of technopolitics: Deep convergence, platform ontologies, and cognitive efficiency | Request PDF - ResearchGate, consulté le janvier 18, 2026, <https://www.researchgate.net/publication/342382909_A_map_of_technopolitics_Deep_convergence_platform_ontologies_and_cognitive_efficiency>
40. 3 The Shape of Technopolitics - MIT Press Direct, consulté le janvier 18, 2026, <https://direct.mit.edu/books/oa-monograph/chapter-pdf/2253005/c002100_9780262366380.pdf>
41. University of Groningen What makes audiences resilient to disinformation? Integrating micro, meso, and macro factors based on a, consulté le janvier 18, 2026, <https://research.rug.nl/files/1374570429/10.1515_commun-2023-0078.pdf>
42. 3. Concerns about democracy in the digital age - Pew Research Center, consulté le janvier 18, 2026, <https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/>
43. Generative engine optimization - Wikipedia, consulté le janvier 18, 2026, <https://en.wikipedia.org/wiki/Generative_engine_optimization>
44. Poisoned datasets put AI models at risk for attack - CyLab, consulté le janvier 18, 2026, <https://www.cylab.cmu.edu/news/2025/06/11-poisoned-datasets-put-ai-models-at-risk-for-attack.html>
45. A small number of samples can poison LLMs of any size - Anthropic, consulté le janvier 18, 2026, <https://www.anthropic.com/research/small-samples-poison>
46. The Technopolitics of Compassion A Postphenomenological Analysis of the Digital Mediation of Global Humanitarianism - Lund University Research Portal, consulté le janvier 18, 2026, <https://portal.research.lu.se/files/117665567/_LGAARD_thesis_final_LUCRIS.pdf>
47. Guerre de l'information, consulté le janvier 18, 2026, <https://www.ege.fr/sites/ege.fr/files/media_files/CyberGIETI.pdf>
48. The Capital Operator Stack: Theoretical Landscape and Contribution — A Political-Semantic Analysis of Meaning Governance : r/SemanticEconomy - Reddit, consulté le janvier 18, 2026, <https://www.reddit.com/r/SemanticEconomy/comments/1qbt59n/the_capital_operator_stack_theoretical_landscape/>