# Hacking Politique : La Tectonique des Plaques de la Souveraineté Numérique et Démocratique

## Introduction : La Métamorphose du Code en Arme Politique

L'aube du XXIe siècle a vu s'opérer une mutation fondamentale dans la nature des conflits humains. 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. 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. Ce rapport se propose d'explorer en profondeur les mécanismes, les acteurs et les implications de cette nouvelle forme de conflictualité qui ne vise plus seulement à contrôler des territoires, mais à conquérir, manipuler ou déstabiliser les infrastructures cognitives et institutionnelles des sociétés modernes.

Le hacking politique ne se laisse pas enfermer dans une définition unique. Il est protéiforme, oscillant entre l'activisme citoyen désireux de transparence — le hacktivisme — et l'opération clandestine d'État visant à saper les fondements d'une puissance rivale.1 Il englobe aussi bien la désobéissance civile numérique, héritière des mouvements de contestation sociale, que la cyberguerre froide qui oppose les grandes puissances nucléaires. 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, non pas toujours pour en altérer techniquement les résultats, mais pour en éroder la légitimité aux yeux des citoyens.3

La convergence des technologies de l'information, de l'intelligence artificielle générative et des réseaux sociaux a créé un écosystème où une ligne de code peut avoir des répercussions géopolitiques équivalentes à celles d'une incursion militaire. Les frontières entre la paix et la guerre, entre le crime et l'espionnage, entre le militantisme et le terrorisme, se sont brouillées dans une "zone grise" permanente. Ce rapport analyse comment des acteurs étatiques comme la Russie, la Chine ou l'Iran, ainsi que des collectifs non-étatiques, exploitent les vulnérabilités techniques et psychologiques des démocraties.5 Il examine également la réponse des États, tiraillés entre la nécessité de protéger leur souveraineté numérique et la difficulté d'attribuer avec certitude l'origine des attaques dans un environnement où le "faux drapeau" est devenu un art.7

À travers une analyse exhaustive des doctrines, des incidents récents et des cadres juridiques émergents, nous démontrerons que le hacking politique n'est pas une simple nuisance technologique, mais le symptôme d'une recomposition profonde de l'ordre mondial, où la capacité à contrôler l'information et à sécuriser ses réseaux est devenue la mesure ultime de la puissance souveraine.

## Partie I : L'Anatomie du Hacking Politique – Concepts, Histoire et Philosophie

Pour appréhender la complexité du hacking politique, il est impératif de déconstruire les strates conceptuelles qui le composent. Loin d'être un bloc monolithique, ce phénomène est un spectre continu allant de l'idéalisme libertaire à la realpolitik la plus cynique.

### 1.1 Genèse et Philosophie : Du "Hacker Ethic" à l'Hacktivisme

Historiquement, le terme "hacker" est dépourvu de connotation malveillante. Né dans les laboratoires du MIT dans les années 1960, il désignait une curiosité intellectuelle poussée, une volonté de comprendre et de maîtriser les systèmes complexes.9 Cette culture originelle était imprégnée d'une éthique forte, formalisée par Steven Levy, dont le précepte central — "L'information veut être libre" — allait devenir le cri de ralliement des premières formes de hacking politique.

L'émergence du "hacktivisme" dans les années 1990 marque le moment où cette compétence technique a été mise au service d'une cause politique. Le terme, contraction de "hacking" et "activisme", désigne l'utilisation non-violente (bien que souvent illégale) d'outils numériques pour promouvoir des changements sociétaux ou politiques.1 Des groupes pionniers comme le *Cult of the Dead Cow* ou le *Chaos Computer Club* (CCC) en Allemagne ont posé les jalons de cette pratique. Le CCC, par exemple, a toujours maintenu une ligne éthique stricte, utilisant le hacking pour exposer les failles de sécurité des systèmes gouvernementaux ou bancaires afin de protéger les citoyens, plutôt que pour causer des dommages.1

Cependant, cette "chevalerie numérique" a évolué vers des formes plus conflictuelles. L'apparition du collectif *Anonymous* au milieu des années 2000 a transformé le hacktivisme en un phénomène de masse, décentralisé et imprévisible. Avec des opérations comme le *Projet Chanology* (contre l'Église de Scientologie) ou les attaques de soutien au Printemps arabe, *Anonymous* a popularisé l'idée que le cyberespace est un domaine public que les citoyens doivent défendre contre la censure étatique et la cupidité corporatiste.1 L'iconographie du masque de Guy Fawkes est devenue le symbole universel d'une résistance sans visage, capable de mobiliser des milliers de "hackers" occasionnels via des outils comme le LOIC (*Low Orbit Ion Cannon*), transformant chaque ordinateur en une arme de protestation par déni de service (DDoS).12

### 1.2 La Désobéissance Civile Numérique : Entre Légitimité et Légalité

Une question centrale traverse l'étude du hacking politique : peut-on considérer ces actions comme une forme moderne de désobéissance civile? La désobéissance civile traditionnelle, théorisée par Thoreau ou Gandhi, implique une violation publique et assumée de la loi au nom d'un impératif moral supérieur, avec l'acceptation des conséquences pénales.

Dans le cyberespace, cette définition se heurte à l'anonymat. Toutefois, certains théoriciens et militants, comme Candice Delmas, arguent que le hacktivisme constitue bien une nouvelle forme de désobéissance civile adaptée à l'ère numérique.13 Des figures tragiques comme Aaron Swartz incarnent cette tension. Co-fondateur de Reddit et militant pour l'accès libre à la connaissance, Swartz a utilisé des scripts pour télécharger massivement des articles académiques de la base de données JSTOR, non pour les vendre, mais pour les "libérer".14 Poursuivi par la justice américaine avec une sévérité exemplaire (risquant jusqu'à 35 ans de prison), il s'est suicidé en 2013. Son cas illustre le fossé grandissant entre la perception qu'ont les hacktivistes de leurs actions — un acte politique légitime — et la réponse des États, qui tendent à criminaliser ces actes sous l'angle du piratage informatique, voire du cyberterrorisme.15

Le débat reste ouvert sur la qualification d'actes comme le "défacement" de sites web (modification de la page d'accueil pour afficher un message politique) ou les attaques DDoS. S'agit-il de "sit-ins virtuels" bloquant l'accès à un bâtiment numérique, ou d'actes de sabotage? La jurisprudence tend vers la seconde interprétation, considérant les dommages économiques et techniques comme prépondérants sur le message politique.16

### 1.3 Lanceurs d'Alerte vs "Hack-and-Leak" : La Transparence Armée

Une distinction fondamentale doit être opérée entre le lanceur d'alerte (*whistleblower*) et les opérations de "Hack-and-Leak" (piratage et divulgation). Bien que le résultat — la révélation de secrets — soit similaire, la méthode et l'intention diffèrent radicalement.

Le lanceur d'alerte est généralement un initié (insider) qui, témoin de dysfonctionnements graves, décide de briser le secret par conscience morale. Des figures comme Chelsea Manning ou Edward Snowden s'inscrivent dans cette tradition.17 Ils ont extrait des données auxquelles ils avaient un accès légitime pour exposer des programmes de surveillance de masse ou des crimes de guerre, acceptant le risque d'exil ou d'emprisonnement.

À l'opposé, le "Hack-and-Leak" est une tactique offensive, souvent orchestrée par des services de renseignement étrangers. Il consiste à pénétrer illégalement les systèmes d'une organisation cible (parti politique, ministère) pour en exfiltrer des données confidentielles (emails, mémos stratégiques) et les diffuser publiquement à des moments clés du calendrier politique.18 L'objectif n'est pas la transparence démocratique, mais la déstabilisation.

L'exemple paradigmatique reste l'opération menée contre le Comité National Démocrate (DNC) américain en 2016. Revendiquée par un personnage fictif nommé "Guccifer 2.0" se présentant comme un hacktiviste roumain solitaire, l'attaque a été attribuée par la suite au GRU russe.8 Les "Macron Leaks" de 2017 en France relèvent de la même logique : une tentative de saturation de l'espace médiatique par des millions de documents (mêlant vrais et faux) à 48 heures du scrutin présidentiel pour paralyser la campagne d'Emmanuel Macron.19 Dans ces scénarios, la transparence est instrumentalisée ; l'information devient une munition dans une guerre cognitive.

### 1.4 Typologie des Vecteurs Techniques du Hacking Politique

Pour comprendre la menace, il est nécessaire d'analyser les outils techniques qui permettent sa mise en œuvre. Ces vecteurs ne sont pas exclusifs et sont souvent combinés dans des campagnes hybrides.

| **Vecteur Technique** | **Description Mécanique** | **Objectif Politique et Impact** | **Complexité / Attribution** |
| --- | --- | --- | --- |
| **DDoS (Déni de Service Distribué)** | Saturation de la bande passante ou des ressources serveur d'une cible par un trafic illégitime provenant de milliers de machines (botnet). | **Censure / Visibilité.** Rendre inaccessible un site gouvernemental, un média d'opposition ou une infrastructure électorale pour réduire au silence ou créer un sentiment de chaos. | Faible. Souvent utilisé par des hacktivistes (ex: LOIC) ou comme écran de fumée pour des attaques plus complexes. Attribution difficile mais impact temporaire. 12 |
| **Défacement (Défaçage)** | Exploitation de failles (ex: SQL injection, CMS non patché) pour modifier visuellement un site web. | **Humiliation / Propagande.** Affichage de drapeaux, slogans ou revendications sur des sites officiels. C'est l'équivalent numérique du tag sur un bâtiment public. | Faible à Moyenne. Impact psychologique fort sur la perception de sécurité de l'institution visée. 15 |
| **Doxing** | Recherche OSINT (Open Source Intelligence) et exfiltration de données privées pour les publier. | **Intimidation / Harcèlement.** Divulguer les adresses, numéros de téléphone ou données financières de politiciens, policiers ou militants pour les exposer à la vindicte populaire. | Moyenne. Très efficace pour faire taire des opposants ou démoraliser des forces de l'ordre. 12 |
| **Spear-Phishing (Harponnage)** | Courriels hautement personnalisés contenant des malwares ou des liens frauduleux, ciblant des individus spécifiques (élus, assistants). | **Espionnage / Accès Initial.** Obtenir les identifiants d'accès aux réseaux internes pour exfiltrer des documents stratégiques (Hack-and-Leak) ou surveiller les communications. | Élevée. Vecteur privilégié des APT (Advanced Persistent Threats) étatiques (ex: Fancy Bear, Mint Sandstorm). 18 |
| **Wipers & Ransomware Politique** | Logiciels malveillants chiffrant ou détruisant irréversiblement les données. | **Sabotage / Paralysie.** Contrairement au criminel qui veut une rançon, l'acteur politique (ex: Sandworm) vise la destruction pure pour paralyser l'économie ou les services publics d'un État rival. | Très Élevée. Ex: NotPetya (2017) contre l'Ukraine, masqué en ransomware mais conçu pour détruire. 15 |
| **Supply Chain Attacks** | Compromission d'un fournisseur logiciel tiers pour atteindre la cible finale. | **Infiltration Massive.** Atteindre des cibles gouvernementales hautement sécurisées en passant par leurs fournisseurs de confiance. | Très Élevée. Ex: SolarWinds. Permet un accès à long terme et discret. 23 |

Cette typologie révèle une professionnalisation croissante. Si le défacement reste l'arme du "script-kiddy" ou du militant de base, les opérations d'influence contemporaines reposent sur des chaînes d'attaque complexes nécessitant des ressources étatiques ou para-étatiques.

## Partie II : Géopolitique des Acteurs - La Cyber-Guerre Froide

Le cyberespace est devenu le théâtre privilégié des rivalités géopolitiques. Contrairement à la guerre conventionnelle, coûteuse et politiquement risquée, les cyber-opérations offrent un moyen d'action "sous le seuil" de conflit armé, permettant de projeter de la puissance, de collecter du renseignement et de déstabiliser l'adversaire avec une plausibilité de déni. Les rapports des agences de renseignement occidentales (CISA, ANSSI, GCHQ) et des géants de la cybersécurité (Microsoft, Mandiant) identifient un "carré de menaces" principal : la Russie, la Chine, l'Iran et la Corée du Nord.5

### 2.1 La Russie : La Doctrine du Chaos et de la Guerre Hybride

La Russie est sans conteste l'acteur le plus théorisé et le plus agressif en matière de hacking politique. Sa stratégie s'inscrit dans la continuité de la "doctrine Gerasimov", qui prône une approche holistique de la guerre où les moyens non-militaires (informationnels, cybernétiques, économiques) prédominent sur l'action militaire classique. Pour Moscou, le cyberespace est un vecteur de guerre de l'information permanente.

Les opérations russes sont caractérisées par une volonté de créer le chaos et d'exacerber les fractures existantes au sein des sociétés occidentales. Les unités de renseignement militaire (GRU) sont particulièrement actives :

* **Sandworm (Unité 74455) :** Responsable de certaines des attaques les plus destructrices de l'histoire, notamment les coupures de courant en Ukraine (2015, 2016) et l'attaque *NotPetya*. Ce groupe incarne la capacité de sabotage physique via le cyber.24
* **APT28 (Fancy Bear / Unité 26165) :** Spécialisé dans l'espionnage politique et les opérations de *Hack-and-Leak* (DNC 2016, Macron Leaks 2017).
* **Midnight Blizzard (APT29 / SVR) :** Rattaché au renseignement extérieur, ce groupe privilégie l'espionnage discret et à long terme des chancelleries et ministères occidentaux, comme l'a montré l'attaque *SolarWinds* ou les campagnes récentes de spear-phishing.25

Au-delà du piratage technique, la Russie a industrialisé la désinformation via des "fermes à trolls" (comme l'ancienne Internet Research Agency) et des réseaux d'influence comme *Doppelgänger*. Ce dernier crée des clones parfaits de sites de médias occidentaux reconnus (*Le Monde*, *The Guardian*, *Bild*) pour y diffuser de faux articles hostiles à l'Ukraine ou aux gouvernements en place, qui sont ensuite amplifiés massivement sur les réseaux sociaux.18 Cette technique de "typosquatting politique" vise à blanchir la propagande en lui donnant une apparente légitimité journalistique.

### 2.2 La Chine : De l'Espionnage Industriel à la Guerre Cognitive

La stratégie cyber de la République Populaire de Chine (RPC) a connu une évolution notable. Longtemps focalisée sur l'espionnage industriel massif pour combler son retard technologique, Pékin a pivoté vers des opérations d'influence politique et de pré-positionnement stratégique, notamment en vue d'un potentiel conflit autour de Taïwan.

* **Volt Typhoon :** Ce groupe, identifié récemment par les agences américaines, représente un changement de paradigme. Au lieu de voler des données, *Volt Typhoon* s'infiltre dans les infrastructures critiques américaines (télécommunications, énergie, transports) et y dort, utilisant des techniques "Living off the Land" (utilisation d'outils d'administration légitimes pour éviter la détection). L'objectif est clair : disposer d'une capacité de sabotage ("kill switch") pour paralyser la logistique américaine en cas de crise dans le Pacifique.24
* **Dragonbridge et Spamouflage :** Sur le front cognitif, la Chine déploie des campagnes massives comme *Spamouflage* (contraction de spam et camouflage). Contrairement à la subtilité russe, l'approche chinoise a longtemps été celle du volume : inonder les réseaux de millions de messages pro-Pékin pour noyer les critiques. Cependant, lors des élections taïwanaises de 2024, l'usage de l'IA générative a montré un raffinement nouveau, créant de faux présentateurs de nouvelles et manipulant l'image des candidats.26

La Chine vise moins le chaos que le contrôle du narratif global et la suppression de toute dissidence concernant ses "lignes rouges" (Taïwan, Hong Kong, Xinjiang).28

### 2.3 L'Iran et la Corée du Nord : Asymétrie et Financement

L'Iran utilise le cyberespace comme une arme asymétrique pour compenser sa faiblesse militaire conventionnelle face aux États-Unis et à Israël. Le Corps des Gardiens de la Révolution (IRGC) supervise des groupes comme *Mint Sandstorm* (ou *Charming Kitten*). En 2024, l'Iran s'est montré particulièrement agressif, piratant la campagne de Donald Trump et tentant de diffuser des dossiers compromettants sur son colistier JD Vance. Parallèlement, Téhéran mène des opérations d'intimidation directe, envoyant des emails de menace de mort à des électeurs américains en se faisant passer pour des groupes d'extrême droite (opération "Proud Boys"), une tactique de faux drapeau destinée à inciter à la violence.5

La Corée du Nord (RPDC), quant à elle, présente un profil unique où le hacking politique se double d'une entreprise criminelle d'État. Des groupes comme *Lazarus* ou *Andariel* mènent des campagnes d'espionnage pour le compte du régime (ciblant les secteurs de la défense et du nucléaire) tout en orchestrant des vols massifs de crypto-monnaies et des attaques par ransomware pour financer les programmes d'armement de Pyongyang, contournant ainsi les sanctions internationales.6

### 2.4 Le Problème de l'Attribution et les Opérations "Faux Drapeau"

L'un des défis majeurs du hacking politique réside dans la difficulté d'attribuer une attaque avec une certitude absolue. L'anonymat inhérent à l'architecture d'Internet permet aux attaquants de masquer leur origine, mais plus grave encore, de se faire passer pour d'autres. C'est la technique du "False Flag" (faux drapeau).7

Les acteurs étatiques insèrent délibérément dans leur code malveillant des "artefacts" ou des signatures techniques appartenant à leurs adversaires. L'attaque contre les Jeux Olympiques de PyeongChang en 2018 (malware *OlympicDestroyer*) est un cas d'école étudié par les experts forensiques. Le groupe russe Sandworm a conçu ce malware en y intégrant des morceaux de code et des métadonnées typiques du groupe nord-coréen Lazarus, dans le but explicite de tromper les analystes et de provoquer une crise diplomatique entre la Corée du Nord et l'Occident.31

Cette sophistication rend l'attribution purement technique insuffisante. Comme le soulignent les chercheurs, l'attribution moderne repose sur une triangulation entre :

1. **L'analyse technique :** Code, infrastructures IP, techniques (TTPs).
2. **Le renseignement :** Sources humaines ou électromagnétiques confirmant les ordres donnés.
3. **Le contexte géopolitique :** *Cui bono* (à qui profite le crime?).

C'est pourquoi l'attribution publique d'une cyberattaque est toujours une décision politique souveraine, et non un simple constat technique. Accuser un État comme la Chine ou la Russie expose à des représailles ; ne pas le faire encourage l'impunité.33

## Partie III : Ingérence Électorale - Le Champ de Bataille de 2024-2025

Les élections sont devenues le point de focalisation des cybermenaces. L'objectif n'est plus seulement d'influencer le choix des électeurs, mais de briser la confiance dans le mécanisme démocratique lui-même.

### 3.1 Taïwan 2024 : Le Laboratoire de la Cyber-Guerre Cognitive

L'élection présidentielle taïwanaise de janvier 2024 a servi de laboratoire à ciel ouvert pour les nouvelles techniques d'ingérence chinoises. Ce scrutin a marqué l'entrée dans l'ère de la désinformation assistée par IA.

* **Deepfakes et IA :** Des acteurs étatiques et non-étatiques ont diffusé des clips audio et vidéo fabriqués de toutes pièces, montrant des candidats tenant des propos controversés ou insultants. Ces contenus ont circulé massivement sur des plateformes de messagerie fermées comme LINE, rendant leur détection et leur modération difficiles.27
* **Réponse Sociétale :** Taïwan a développé une résilience remarquable basée sur la collaboration entre le gouvernement, la société civile (groupes de fact-checking comme *Cofacts*) et les plateformes. Le développement du moteur *TAIDE* (Trustworthy AI Dialogue Engine) par Taïwan vise à contrer les biais des modèles de langage chinois en proposant une IA entraînée sur des corpus respectant les valeurs démocratiques et culturelles de l'île.27 Cette "défense cognitive" montre que la technologie peut aussi être une partie de la solution.

### 3.2 États-Unis 2024 : La Fragilité de la Confiance

Aux États-Unis, la menace s'est déplacée du piratage des machines vers le piratage des esprits.

* **Intégrité des Machines :** Bien que des vulnérabilités théoriques existent — une étude de l'Université du Michigan en 2024 a démontré qu'il était possible de "désanonymiser" des bulletins sur certains scanners Dominion — aucun incident de piratage massif altérant les résultats n'a été détecté.34 Le système électoral américain, très décentralisé et reposant largement sur des traces papier, est techniquement robuste.
* **Impact Psychologique :** Cependant, la perception est plus fragile que la réalité. Une étude du *Georgia Institute of Technology* (2025) révèle un paradoxe inquiétant : la simple exposition à des nouvelles rapportant des cyberattaques, même si elles ne concernent pas directement les élections (par exemple, une attaque contre le réseau électrique), suffit à faire chuter la confiance des électeurs dans l'intégrité du scrutin.4 Ce phénomène touche tous les bords politiques, mais s'aggrave chez les partisans du candidat perdant.
* **Tactiques Étrangères :** L'ingérence étrangère s'est adaptée à cette psychologie. La Russie a utilisé des sociétés écrans (comme *Tenet Media*) pour financer à hauteur de 10 millions de dollars des influenceurs conservateurs américains, "blanchissant" ainsi ses narratifs de division à travers des voix locales.5 L'objectif n'était pas tant de faire élire Trump que de garantir qu'une moitié du pays ne reconnaitrait pas la légitimité du résultat, quel qu'il soit.

### 3.3 Europe : Vulnérabilités Institutionnelles et Sabotage

L'Europe n'est pas épargnée. Les élections européennes de juin 2024 ont été précédées d'une vague d'attaques.

* **Cyberattaques contre le Parlement :** Des groupes de hackers pro-russes (comme *NoName057(16)*) ont mené des attaques DDoS contre les sites du Parlement Européen et d'autres institutions pour perturber l'accès à l'information électorale.36
* **Fuites de Données :** Des rapports de sécurité ont révélé que les identifiants et mots de passe de centaines de parlementaires et assistants (au Royaume-Uni, en France, au Danemark) circulaient sur le dark web avant les élections.38 Ces "kompromat" potentiels représentent une épée de Damoclès, exposant les élus au chantage ou permettant des infiltrations ultérieures.
* **Le Cas du Royaume-Uni :** L'attaque contre la Commission Électorale britannique, révélée tardivement mais attribuée à la Chine en 2024, a exposé les données de 40 millions d'électeurs. Bien que les registres soient publics, l'accès aux bases de données a permis aux attaquants de croiser des informations pour identifier des cibles d'intérêt (dissidents, critiques de la Chine).23

Ces incidents soulignent que si le vote lui-même est souvent sécurisé (papier), l'écosystème périphérique (fichiers électoraux, communications des candidats, sites d'information) reste le ventre mou de la démocratie.

## Partie IV : Cadres Juridiques, Souveraineté et Doctrines de Défense

Face à cette menace existentielle, les États tentent de bâtir des digues juridiques et doctrinales. La réponse oscille entre l'application du droit international classique et l'invention de nouveaux concepts de souveraineté.

### 4.1 Le Droit International à l'Épreuve du Cyberespace

La question de l'applicabilité du droit international au cyberespace a longtemps fait débat, mais un consensus émerge, cristallisé autour des travaux du *Manuel de Tallinn* (initié par le centre d'excellence cyber de l'OTAN). Ce document académique tente de transposer les règles du *jus ad bellum* (droit à la guerre) et du *jus in bello* (droit de la guerre) au domaine numérique.40

* **Agression Armée et Article 51 :** La France, dans sa doctrine officielle, affirme qu'une cyberattaque peut constituer une "agression armée" au sens de l'article 51 de la Charte de l'ONU, dès lors que ses effets (morts, destructions physiques substantielles) sont comparables à ceux d'une attaque cinétique classique. Cela ouvrirait théoriquement le droit à la légitime défense, y compris par des moyens militaires conventionnels.33
* **Violation de Souveraineté :** En deçà du seuil de l'agression armée, toute pénétration non autorisée dans les systèmes d'un État constitue une violation de souveraineté. La réponse à ce niveau relève des contre-mesures (sanctions, expulsion de diplomates, riposte cyber proportionnée).42

### 4.2 La Doctrine Française : Une Approche Offensive et Défensive

La France se distingue par une doctrine claire et publique, structurée autour de trois piliers dans sa Loi de Programmation Militaire (LPM) 43 :

1. **LID (Lutte Informatique Défensive) :** La protection des réseaux de l'État et des Opérateurs d'Importance Vitale (OIV), mission partagée entre l'ANSSI (civil) et le COMCYBER (militaire).
2. **LIO (Lutte Informatique Offensive) :** La France est l'un des rares pays occidentaux à assumer publiquement disposer de capacités offensives. Celles-ci sont strictement encadrées par le droit et réservées aux opérations militaires ou à la neutralisation d'attaques imminentes.
3. **L2I (Lutte Informatique d'Influence) :** Ajout récent et stratégique, la L2I reconnait que la guerre se joue aussi dans les perceptions. Elle autorise les armées françaises à opérer dans le champ informationnel pour détecter, caractériser et contrer les propagandes adverses, marquant une prise de conscience de la nature "hybride" des conflits modernes.43

### 4.3 Souveraineté Numérique et Dépendance Technologique

Au-delà des doctrines militaires, l'Europe fait face à un défi structurel : sa dépendance technologique. La "souveraineté numérique" est devenue un leitmotiv politique, motivé par le constat que plus de 80% des infrastructures numériques européennes (Cloud, processeurs, réseaux sociaux) sont fournies par des acteurs extra-européens (principalement américains et chinois).46

Cette dépendance pose un risque d'ingérence systémique :

* **Le Cloud Act américain :** Cette loi permet aux forces de l'ordre américaines d'exiger l'accès aux données stockées par les entreprises américaines (Microsoft, Google, AWS), même si ces données sont hébergées sur des serveurs en Europe. Pour les institutions politiques européennes, cela constitue une vulnérabilité majeure en matière de confidentialité.48
* **La Réponse Européenne :** L'UE tente de réagir par la régulation (DSA/DMA pour contrôler les plateformes, *AI Act* pour sécuriser l'IA) et par des investissements industriels (Cloud souverain, initiative "Airbus des puces"). Cependant, le rapport de force reste déséquilibré, et la "souveraineté" reste pour l'instant plus une aspiration réglementaire qu'une réalité industrielle.49

### 4.4 Les Statistiques de la Confiance

Les données des Eurobaromètres récents montrent l'impact de ces enjeux sur l'opinion publique. Bien que la confiance dans l'Union Européenne reste relativement élevée (49%), la crainte des cyberattaques et de la désinformation est omniprésente. En 2024, 34% des citoyens ont cité la "situation internationale" (incluant les menaces hybrides) comme motivation de vote, et la défense de la démocratie est devenue une préoccupation centrale.51 Cela confirme que la cybersécurité n'est plus un sujet technique, mais un déterminant du contrat social.

## Partie V : Synthèse et Perspectives – La Démocratie à l'Ère de l'Incertitude

Le hacking politique ne doit pas être vu comme une série d'incidents isolés, mais comme une nouvelle tectonique des plaques géopolitiques. Les frontières numériques frictionnent, provoquant des séismes qui ébranlent les institutions réelles.

### 5.1 Du Piratage des Données au "Liar's Dividend"

L'évolution la plus inquiétante n'est pas technique, mais épistémologique. L'avènement des deepfakes et la sophistication des campagnes de désinformation créent ce que les experts appellent le "Liar's Dividend" (le dividende du menteur). Dans un monde où tout *peut* être faux (vidéo générée par IA, documents falsifiés mêlés à de vrais leaks), les acteurs politiques malhonnêtes peuvent rejeter toute preuve réelle de leurs méfaits en criant au "fake".53 La vérité factuelle, base du débat démocratique, se dilue.

Le hacking politique ne vise plus seulement à voler des secrets, mais à détruire la notion même de preuve commune. Quand le groupe iranien *Mint Sandstorm* pirate une campagne, ou quand la Russie inonde les réseaux de fausses nouvelles, l'objectif final est le cynisme généralisé : convaincre les citoyens que toutes les institutions sont corrompues, que tous les médias mentent, et que la vérité est inaccessible.

### 5.2 La Résilience comme Nouvelle Dissuasion

Face à l'impossibilité de tout bloquer techniquement, la doctrine de défense évolue vers la résilience.

* **VIGINUM et la protection du débat :** En France, l'agence VIGINUM a été créée spécifiquement pour détecter les ingérences numériques étrangères sans empiéter sur la liberté d'expression nationale. Son rôle est de caractériser les "manœuvres inauthentiques" (usage de bots, coordination artificielle) pour les exposer publiquement.54
* **Le "Pre-bunking" :** Cette stratégie, utilisée par les États-Unis et Taïwan, consiste à déclassifier rapidement du renseignement pour révéler les plans de désinformation de l'adversaire *avant* qu'ils ne soient mis en œuvre. En "vaccinant" l'opinion publique, on réduit l'efficacité virale du narratif hostile.27

### 5.3 Tableau de Synthèse : Les Grands Groupes d'Ingérence (2023-2025)

| **Groupe / Acteur** | **Affiliation Présumée** | **Cibles Principales** | **Méthodes Privilégiées & TTPs** | **Incident Majeur Récent** |
| --- | --- | --- | --- | --- |
| **Sandworm (APT44)** | Russie (GRU - Militaire) | Ukraine, Énergie UE, OTAN | Sabotage destructif (Wipers), Attaques sur OT (Operational Tech). | Attaques réseau électrique Ukraine, NotPetya. 24 |
| **Midnight Blizzard (APT29)** | Russie (SVR - Extérieur) | Ministères Occidentaux, Partis politiques | Espionnage furtif, vol d'identifiants, Supply Chain. | Compromission de cadres Microsoft, SolarWinds. 25 |
| **Volt Typhoon** | Chine (MSS) | Infrastructures Critiques US (Guam, Ports) | "Living off the Land", Pré-positionnement pour sabotage futur. | Infiltration des réseaux de télécoms et d'eau US. 24 |
| **Dragonbridge** | Chine (Op. Influence) | Opinion Publique (Taïwan, USA, Diaspora) | Spamouflage, Deepfakes, IA Générative, Harcèlement. | Désinformation massive élections Taïwan 2024. 26 |
| **Mint Sandstorm** | Iran (IRGC) | Campagnes US, Dissidents, Israël | Hack-and-Leak, Intimidation directe (emails), Phishing. | Piratage campagne Trump 2024, menaces "Proud Boys". 5 |
| **Lazarus Group** | Corée du Nord (RGB) | Finance, Défense, Crypto | Vols financiers massifs, Espionnage industriel. | Financement du programme balistique via hacks crypto. 30 |

## Conclusion

Le hacking politique a définitivement quitté les marges de la contre-culture pour s'installer au centre du Bureau Ovale et des chancelleries européennes. Il est devenu l'arme de prédilection du XXIe siècle car il est peu coûteux, difficilement attribuable et terriblement efficace pour exploiter les fractures ouvertes des sociétés démocratiques.

La réponse à ce défi ne peut être purement technologique. Si le chiffrement et les pare-feux sont nécessaires, ils sont insuffisants face à des attaques qui visent l'esprit des citoyens. La véritable souveraineté numérique passe par une triple révolution : une révolution industrielle pour maîtriser les infrastructures critiques, une révolution juridique pour imposer des coûts réels aux agresseurs, et une révolution éducative pour armer chaque citoyen contre la manipulation cognitive. Tant que le "coût politique" du hacking restera inférieur à ses bénéfices stratégiques, la guerre des ombres numériques continuera de s'intensifier, redéfinissant en permanence ce que signifie être une nation souveraine à l'ère du réseau.

#### Sources des citations

1. Hacktivisme - Wikipédia, consulté le janvier 18, 2026, <https://fr.wikipedia.org/wiki/Hacktivisme>
2. Hacktivisme et élections - Publications - Onepoint, consulté le janvier 18, 2026, <https://www.groupeonepoint.com/fr/publications/hacktivisme-et-elections/>
3. Comment sauver nos démocraties des hackers ? | OCDE - OECD, consulté le janvier 18, 2026, <https://www.oecd.org/fr/publications/comment-sauver-nos-democraties-des-hackers_f92e69d1-fr.html>
4. Cyberattacks Shake Voters' Trust in Elections, Regardless of Party, consulté le janvier 18, 2026, <https://www.gatech.edu/news/2025/06/27/cyberattacks-shake-voters-trust-elections-regardless-party>
5. THE FUTURE OF DEMOCRACY - European Union Institute for ..., consulté le janvier 18, 2026, <https://www.iss.europa.eu/sites/default/files/2025-02/Brief_2024-22_US%20elections%20FIMI.pdf>
6. Nation-State Threats | Cybersecurity and Infrastructure Security Agency CISA, consulté le janvier 18, 2026, <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors>
7. What is a false flag in cybersecurity? Real attack examples - Huntress, consulté le janvier 18, 2026, <https://www.huntress.com/cybersecurity-101/topic/what-is-false-flag-in-cybersecurity>
8. Russian Disinformation and False Flag Cyber Terrorism: The Case of the CyberCaliphate - Ministerio de Defensa, consulté le janvier 18, 2026, <https://www.defensa.gob.es/documents/2073105/2320887/la_desinformacion_rusa_2025_dieeeo55_eng.pdf/f8313c9d-69e4-0a21-258e-671ad263d626?t=1750241454254>
9. Hacking - Wikipédia, consulté le janvier 18, 2026, <https://fr.wikipedia.org/wiki/Hacking>
10. Hacker la démocratie taïwanaise : Audrey Tang et la réinvention de la politique | Cairn.info, consulté le janvier 18, 2026, <https://shs.cairn.info/revue-participations-2017-1-page-121?lang=fr>
11. Nouveaux Cahiers du socialisme - L'effet hacker sur la démocratie - Érudit, consulté le janvier 18, 2026, <https://www.erudit.org/fr/revues/ncs/2017-n17-ncs02920/84475ac.pdf>
12. Doxing, DoS, and Defacement: Today's Mainstream Hacktivism Tools - F5, consulté le janvier 18, 2026, <https://www.f5.com/content/dam/f5/downloads/ARTICLE-Doxing_DoS_Defacement_Mainstream_Hacktivism.pdf>
13. Is Hacktivism the New Civil Disobedience? | Cairn.info, consulté le janvier 18, 2026, <https://shs.cairn.info/revue-raisons-politiques-2018-1-page-63?lang=en>
14. Hacktivism: Civil Disobedience or Cyber Crime? - ProPublica, consulté le janvier 18, 2026, <https://www.propublica.org/article/hacktivism-civil-disobedience-or-cyber-crime>
15. Qui sont les auteurs de cybermenaces et quelles sont leurs motivations, consulté le janvier 18, 2026, <https://rendre-notre-monde-plus-sur.goron.fr/qui-sont-les-auteurs-de-cybermenaces-et-quelles-sont-leurs-motivations/>
16. Qu'est-ce que le defacement ? | Oracle France, consulté le janvier 18, 2026, <https://www.oracle.com/fr/security/defacement-attaque-site/>
17. Ces lanceurs d'alerte qui paient leurs révélations au prix fort - RTS, consulté le janvier 18, 2026, <https://www.rts.ch/info/monde/7674886-ces-lanceurs-dalerte-qui-paient-leurs-revelations-au-prix-fort.html>
18. Microsoft Digital Defense Report 2024, consulté le janvier 18, 2026, <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf>
19. L'espionnage russe et chinois "se rapproche des partis d'extrême droite" européens selon des experts - YouTube, consulté le janvier 18, 2026, <https://www.youtube.com/watch?v=cZHAVbViUE0>
20. Qu'est-ce que le hacktivisme ? Signification, types et plus - Fortinet, consulté le janvier 18, 2026, <https://www.fortinet.com/fr/resources/cyberglossary/what-is-hacktivism>
21. Analyse du mode opératoire des hackers : se prémunir des cyberattaques - Haas Avocats, consulté le janvier 18, 2026, <https://www.haas-avocats.com/cybersecurite/cybercriminalite/analyse-du-mode-operatoire-des-hackers-se-premunir-des-cyberattaques/>
22. 10 essential insights from the Microsoft Digital Defense Report 2024 | Security Insider, consulté le janvier 18, 2026, <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/10-essential-insights-from-the-microsoft-digital-defense-report-2024>
23. MOD data breach shows supply chain security continues to be a top priority, consulté le janvier 18, 2026, <https://www.chathamhouse.org/2024/05/mod-data-breach-shows-supply-chain-security-continues-be-top-priority>
24. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA, consulté le janvier 18, 2026, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>
25. Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files | Microsoft Security Blog, consulté le janvier 18, 2026, <https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/>
26. Poll Vaulting: Cyber Threats to Global Elections | Google Cloud Blog, consulté le janvier 18, 2026, <https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections>
27. GenAI in the 2024 Taiwan Presidential Election: Lessons for ..., consulté le janvier 18, 2026, <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/4012192/genai-in-the-2024-taiwan-presidential-election-lessons-for-democracies/>
28. LES OPÉRATIONS D'INFLUENCE CHINOISES - IRSEM, consulté le janvier 18, 2026, <https://www.irsem.fr/rapport.html>
29. Iran steps into US election 2024 with cyber-enabled influence operations - Microsoft, consulté le janvier 18, 2026, <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf>
30. APT and financial attacks on industrial organizations in Q3 2024 | Kaspersky ICS CERT, consulté le janvier 18, 2026, <https://ics-cert.kaspersky.com/publications/reports/2024/12/26/apt-and-financial-attackson-industrial-organizationsin-q3-2024/>
31. Malware Analysis Framework v2.0, consulté le janvier 18, 2026, <https://www.first.org/global/sigs/malware/ma-framework/>
32. Mitigating Risks arising from False-Flag and No-Flag Cyber Attacks - nato ccdcoe, consulté le janvier 18, 2026, <https://ccdcoe.org/library/publications/mitigating-risks-arising-from-false-flag-and-no-flag-cyber-attacks/>
33. DROIT INTERNATIONAL APPLIQUÉ AUX OPÉRATIONS DANS LE ..., consulté le janvier 18, 2026, <https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf>
34. Four election vulnerabilities uncovered by a Michigan Engineer, consulté le janvier 18, 2026, <https://news.engin.umich.edu/2024/10/four-election-vulnerabilities-uncovered-by-a-michigan-engineer/>
35. 2024 U.S. Election Integrity Threats: Not Just Data Leaks & Hacks - UpGuard, consulté le janvier 18, 2026, <https://www.upguard.com/blog/2024-u-s-election-integrity-threats-not-just-data-leaks-and-hacks>
36. Cybersécurité (exposé des motifs) - Sénat, consulté le janvier 18, 2026, <https://www.senat.fr/leg/exposes-des-motifs/ppr23-207-expose.html>
37. PANORAMA DE LA CYBERMENACE 2024 - CERT-FR - ANSSI, consulté le janvier 18, 2026, <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf>
38. Fuite : adresses e-mail et mots de passe de politiciens sur le dark ..., consulté le janvier 18, 2026, <https://proton.me/fr/pass/leaked-politicians-dark-web>
39. Electoral Commission apologises for security breach involving UK voters' data - The Guardian, consulté le janvier 18, 2026, <https://www.theguardian.com/technology/2023/aug/08/uk-electoral-commission-registers-targeted-by-hostile-hackers>
40. The Tallinn Manual - NATO Cooperative Cyber Defence Centre of Excellence, consulté le janvier 18, 2026, <https://ccdcoe.org/research/tallinn-manual/>
41. Analyse du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations - François Delerue, consulté le janvier 18, 2026, <https://francoisdelerue.eu/wp-content/uploads/2020/01/20171129_NP_F-Delerue_Analyse-Manuel-Tallinn-2-0.pdf>
42. Droit international applicable dans le cyberespace - Global Affairs Canada, consulté le janvier 18, 2026, <https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=fra>
43. LOI n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense (1) - Légifrance, consulté le janvier 18, 2026, <https://www.legifrance.gouv.fr/loda/id/LEGISCTA000047916381>
44. Question n°23658 : Effets économiques de la LPM sur la filière « cyber » - Assemblée nationale, consulté le janvier 18, 2026, <https://questions.assemblee-nationale.fr/q15/15-23658QE.htm>
45. La lutte informatique offensive (LIO) | Ministère des Armées et des Anciens combattants, consulté le janvier 18, 2026, <http://www.defense.gouv.fr/comcyber/nos-operations/lutte-informatique-offensive-lio>
46. Digital sovereignty: Europe's declaration of independence? - Atlantic Council, consulté le janvier 18, 2026, <https://www.atlanticcouncil.org/in-depth-research-reports/report/digital-sovereignty-europes-declaration-of-independence/>
47. MEPs and Commission split over EU's reliance on foreign tech - Science|Business, consulté le janvier 18, 2026, <https://sciencebusiness.net/sovereignty/meps-and-commission-split-over-eus-reliance-foreign-tech>
48. Escaping the trap of US tech dependence - Disconnect.blog, consulté le janvier 18, 2026, <https://disconnect.blog/escaping-the-trap-of-us-tech-dependence/>
49. What is digital sovereignty and how are countries approaching it? | World Economic Forum, consulté le janvier 18, 2026, <https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/>
50. Tech sovereignty and a new EU foreign economic policy - ECDPM, consulté le janvier 18, 2026, <https://ecdpm.org/work/tech-sovereignty-and-new-eu-foreign-economic-policy>
51. EU Post-electoral survey 2024 - October 2024 - - Eurobarometer survey - European Union, consulté le janvier 18, 2026, <https://europa.eu/eurobarometer/surveys/detail/3292>
52. Standard Eurobarometer 101 - Spring 2024 - Public opinion in the European Union - Verian Group, consulté le janvier 18, 2026, <https://veriangroup.com/hubfs/BE/Eurobarometer/Standard-101-Spring%202024.pdf>
53. Crise et vérité : comment renforcer la résilience démocratique à l'ère de la désinformation, consulté le janvier 18, 2026, <https://www.cap-com.org/actualit%C3%A9s/crise-et-verite-comment-renforcer-la-resilience-democratique-lere-de-la-desinformation>
54. Protection du débat public numérique en contexte électoral ..., consulté le janvier 18, 2026, <https://www.sgdsn.gouv.fr/publications/protection-du-debat-public-numerique-en-contexte-electoral-publication-dun-guide-de>
55. DOTER LA STRATÉGIE DE CYBERDÉFENSE ET D'INFLUENCE D'UNE COMPOSANTE OFFENSIVE, consulté le janvier 18, 2026, <https://www.senat.fr/rap/a22-117-9/a22-117-9-syn.pdf>