www.stopalacybertorture.org

Informer, soutenir et défendre les personnes victimes de harcèlement électromagnétique, cybertorture, contrôle mental à distance ou toute autre forme de torture technologique.

Monsieur le Premier Ministre,
Hôtel Matignon
57 rue de Varenne
75700 Paris

Escornebœuf, le [ ] juin 2026

Lettre recommandée avec A.R. n°

Objet : Signalement d'attaques électromagnétiques d'origine inconnue et d'incidents anormaux de santé et demande de mobilisation des capacités de détection du Renseignement d'Origine Électromagnétique (ROEM)

Monsieur le Premier Ministre,

Nous avons l'honneur de vous saisir, au nom de l'Association STOP À LA CYBERTORTURE, au sujet de nombreux signalements d'attaques électromagnétiques d'origine inconnue ainsi que d'incidents anormaux de santé rapportés par plusieurs de nos adhérents sur l'ensemble du territoire national.

Les personnes concernées décrivent des expositions répétées, continues et ciblées à des champs électromagnétiques anormaux, entraînant des incidents graves et invalidants : troubles neurologiques, douleurs intenses, acouphènes permanents, troubles du sommeil sévères, fatigue chronique extrême, et autres symptômes invalidants. Ces faits nous amènent à craindre fortement des ingérences étrangères ou des actions malveillantes dirigées contre des citoyens français.

Ces personnes rapportent des incidents répétés qu'elles estiment incompatibles avec un usage normal et légal du spectre radioélectrique.

Ces atteintes sont décrites comme affectant les communications, les équipements numériques, l'environnement de vie, l'activité professionnelle et, pour certaines personnes, leur intégrité physique ou psychique. Les victimes indiquent être confrontées à des phénomènes qu'elles ne parviennent pas à expliquer ni à documenter avec les moyens techniques dont elles disposent.

L'Association a réalisé des mesures avec l'un des appareils de mesure les plus avancés accessibles au grand public : le détecteur de rayonnement électromagnétique multichamp GQ EMF-390, appareil 3-en-1 de mesure EMF/ELF et analyseur de spectre RF, capable de détecter les signaux de relais cellulaires jusqu'à 10 GHz avec enregistreur de données.

Malgré ces relevés, qui documentent des anomalies dans l'environnement électromagnétique, ces mesures restent insuffisantes pour démontrer formellement l'existence d'attaques ciblées devant les tribunaux.

En effet, cet appareil, bien que performant pour un usage civil, ne permet ni l'analyse spectrale fine, ni la démodulation des signaux, ni la géolocalisation précise des sources, ni la corrélation temporelle rigoureuse nécessaire pour établir une preuve judiciaire recevable.

De plus, les données issues d'un équipement non étalonné selon les normes forensiques, sans chaîne de traçabilité et sans expertise judiciaire reconnue, sont systématiquement considérées comme irrecevables ou insuffisamment probantes par les tribunaux. Les victimes se trouvent ainsi dans une impasse juridique totale : elles ne peuvent ni prouver les faits par elles-mêmes, ni obtenir une expertise indépendante accessible et crédible.

Il est essentiel de souligner que ces victimes ne disposent ni du matériel professionnel ni de l'expertise technique nécessaires pour démontrer formellement ces attaques devant les tribunaux. Même un analyseur de spectre RF ou un scanner large bande, pourtant parmi les outils les plus avancés accessibles aux particuliers, ne permet que de documenter l'environnement électromagnétique général et d'exclure ou d'identifier des sources connues (antennes relais, Wi-Fi, appareils domestiques, etc.).

Ces équipements civils ne sont pas en mesure de prouver l'existence de communications claires, dirigées et pulsées de type « Voice to Skull » (V2K) ou d'autres signaux directionnels sophistiqués, qui nécessitent des capacités d'analyse spectrale très fine, de géolocalisation en temps réel, de démodulation et de corrélation temporelle avec les symptômes ressentis. Cette limitation technique prive les victimes de moyens de preuve adaptés et les expose à un risque réel de déni de justice.

Face à ces signalements répétés, une question fondamentale se pose : lorsqu'une population déclare subir des attaques ou des actions hostiles dont l'origine ne peut être identifiée par les moyens civils ordinaires, quels dispositifs l'État entend-il mobiliser pour protéger ses citoyens et rechercher les responsables ?

Les plus hautes autorités de l'État ont à plusieurs reprises évoqué l'existence de menaces hybrides, d'opérations d'ingérence étrangère, de guerre informationnelle, de cyberattaques et de formes nouvelles de confrontation entre États. Le Président de la République a lui-même déclaré que la France était confrontée à un contexte dans lequel « nous sommes en guerre », notamment face à des menaces qui ne prennent plus nécessairement la forme d'un conflit militaire conventionnel.

Dans ce contexte, il apparaît légitime de s'interroger sur l'éventuelle existence d'actions hostiles menées depuis l'étranger ou par des acteurs agissant pour le compte d'intérêts étrangers, sans qu'il soit possible pour les citoyens concernés d'en apporter eux-mêmes la preuve.

Les témoignages recueillis font état d'événements récurrents observés dans différents lieux et à différentes périodes. Face à la répétition de ces signalements et à l'inquiétude qu'ils suscitent, nous sollicitons la mobilisation des moyens techniques de l'État afin qu'une évaluation indépendante, objective et scientifiquement fondée puisse être menée.

Notre démarche n'a pas pour objet de préjuger des conclusions des investigations, mais de demander que les moyens techniques appropriés soient mobilisés afin de déterminer la nature exacte des phénomènes signalés, leur éventuelle origine et, le cas échéant, les mesures permettant de faire cesser toute activité illicite.

La structure actuelle de protection de la Nation repose sur une concentration des moyens de détection (ROEM) au sein des services de défense et de renseignement.

Les dispositifs d'agression supposés utilisent des protocoles complexes (sauts de fréquence, signaux pulsés) que seul le matériel militaire peut identifier. Le citoyen, démuni, est dans l'impossibilité technique d'apporter la preuve matérielle requise par le droit commun.

Le système judiciaire et policier, faute d'outils de mesure certifiés, rejette les plaintes. Cette absence de preuve est interprétée comme une absence de réalité, menant à une "psychiatrisation" systématique des plaignants.

Lorsqu'un citoyen signale des symptômes (douleurs, sensations physiques, brûlures, perturbations) dont l'origine ne peut être identifiée par les outils de diagnostic clinique classiques (imagerie médicale, examens biologiques), le système médical a le devoir de rechercher une explication.

Par défaut de preuve physique de l'agression externe, les services médicaux se tournent vers les causes physiologiques ou psychologiques connues.

Cette démarche, bien qu'elle soit vécue comme une "psychiatrisation" par les victimes, est la procédure standard pour le corps médical qui ne dispose pas de protocole de détection pour des agressions électromagnétiques inexpliquées.

Le blocage réside dans le fait qu'il n'existe pas, dans l'appareil d'État, de passerelle entre le ressenti individuel de la victime et les outils de haute technologie de l'État. Sans preuve physique (la "trace" électromagnétique) acceptée par un expert judiciaire, les institutions restent dans une position de fin de non-recevoir.

Malgré l'arsenal législatif robuste dont s'est dotée la Nation avec la loi du 24 juillet 2015 relative au renseignement, force est de constater que ces dispositifs ne sont pas mobilisés pour protéger les citoyens dans leur intégrité physique et leurs libertés fondamentales.

Ces agressions, dont l'origine peut être attribuée à des puissances étrangères procédant à des actes d'ingérence sur notre territoire, mais également à des groupes terroristes cherchant à déstabiliser l'ordre public par l'usage de technologies prohibées, ne sont pas traitées avec la fermeté requise par l'arsenal législatif existant.

La protection de la population civile contre de telles menaces relève d'une mission régalienne de l'État. À cet égard, la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, codifiée au Code de la sécurité intérieure, apporte un cadre juridique clair et opérationnel. Cette loi, adoptée pour renforcer les capacités de l'État face aux menaces contemporaines, définit les intérêts fondamentaux de la Nation et autorise expressément les services de renseignement à recourir à des techniques de recueil de renseignements pour les défendre.

Parmi ces intérêts figurent notamment :

- La préservation de l'indépendance nationale et de l'intégrité du territoire ;
- La défense des intérêts majeurs de la politique étrangère de la France ;
- La prévention de toutes les formes d'ingérences étrangères ;
- La sauvegarde des intérêts économiques, industriels et scientifiques essentiels.

La loi de 2015 reconnaît explicitement que les menaces hybrides, y compris les attaques électromagnétiques ou les émissions suspectes d'origine étrangère, peuvent porter atteinte à ces intérêts fondamentaux. Elle encadre et légitime ainsi la mobilisation des capacités techniques les plus avancées, dont le Renseignement d'Origine Électromagnétique (ROEM), pour détecter, analyser et neutraliser ces menaces.

La France dispose de capacités de renseignement d'origine électromagnétique (ROEM) fondées sur la collecte et l'analyse des émissions radioélectriques. Ces capacités constituent un savoir-faire national reconnu pour la détection, la caractérisation et la localisation de signaux complexes.

Il est rappelé que la protection des intérêts fondamentaux de la Nation, telle que définie à l'article L811-3 du Code de la sécurité intérieure, inclut la lutte contre les activités de cyberdéfense et d'agression technologique. Le fait qu'une attaque soit dirigée contre un civil ne la dépossède pas de sa nature d'incident de sécurité nationale. Mobiliser le ROEM est, dans ce cadre, une obligation de moyens pour garantir que le territoire national n'est pas utilisé comme zone d'expérimentation pour des technologies classifiées.

Dans ce contexte, nous vous demandons solennellement la mise en œuvre du dispositif de renseignement d'origine électromagnétique.

L'État dispose de capacités avancées de renseignement, de détection, de surveillance du spectre électromagnétique et d'analyse des signaux, notamment dans le cadre du renseignement d'origine électromagnétique (ROEM), afin de protéger les intérêts fondamentaux de la Nation, détecter les menaces et identifier leurs origines.

Ce dispositif, piloté par la Direction du Renseignement Militaire (DRM) en coordination avec la DGSE, constitue l'outil étatique le plus adapté. Le ROEM permet la détection, l'interception, l'analyse spectrale fine et la géolocalisation d'émissions électromagnétiques, y compris celles qui échappent aux capacités civiles classiques. Il est spécifiquement conçu pour identifier des signaux non autorisés, atypiques ou d'origine étrangère, qu'ils soient continus, pulsés ou directionnels.

Contrairement aux mesures statiques et limitées de l'ANFR, le ROEM offre des capacités techniques avancées d'analyse des modulations, des formes d'onde, des fréquences porteuses et des comportements temporels, qui correspondent précisément aux caractéristiques des attaques décrites par nos adhérents. Sa mobilisation est pleinement autorisée et encadrée par la loi de 2015, dès lors que la sécurité nationale ou la protection contre des ingérences étrangères est en jeu.

Nous vous prions donc de bien vouloir :

1. Activer sans délai le dispositif ROEM afin de procéder à des investigations techniques approfondies, à la détection et à la caractérisation des attaques électromagnétiques sur les zones géographiques mentionnées par les plaignants ;
2. Mobiliser l'ensemble des services compétents (renseignement, DGA, ANSES, laboratoires spécialisés) pour identifier l'origine de ces expositions et évaluer leurs liens avec les incidents anormaux de santé observés ;
3. Développer un protocole de mesure adapté, dépassant les limites techniques de l'ANFR ;
4. Informer les citoyens concernés et prendre toutes mesures de protection nécessaires, dans un souci de transparence et de sécurité nationale.

À cet égard, nous souhaitons souligner les limites des contrôles habituellement réalisés dans le cadre de la surveillance réglementaire du spectre radioélectrique.

Les missions de contrôle de l'Agence nationale des fréquences (ANFR), bien qu'essentielles à la gestion et à la police du spectre radioélectrique, peuvent apparaître insuffisantes lorsqu'il s'agit d'établir l'origine précise de phénomènes complexes ou de caractériser des émissions potentiellement atypiques.

Les mesures effectuées par les organismes compétents reposent principalement sur l'évaluation de l'intensité des champs électromagnétiques, généralement exprimée en volts par mètre (V/m). Ces contrôles permettent utilement de vérifier le respect des seuils réglementaires d'exposition du public aux ondes électromagnétiques.

Les mesures de champ électrique exprimées en volts par mètre (V/m) ne permettent pas de détecter ni de caractériser des signaux pulsés, modulés, de faible puissance moyenne ou des expositions chroniques et répétées, qui sont pourtant celles rapportées par les plaignants.

En effet, la mesure du niveau de champ électromagnétique ne permet pas, à elle seule :

- d'identifier précisément l'émetteur à l'origine d'un signal ;
- de localiser la source d'émission ;
- d'analyser en détail les caractéristiques fréquentielles du signal ;
- de déterminer les procédés de modulation utilisés ;
- de détecter certains signaux intermittents, furtifs ou de courte durée ;
- de corréler plusieurs événements observés sur différents sites ;
- d'établir l'historique des émissions sur une période prolongée.

Ainsi, un contrôle concluant à la conformité d'un niveau d'exposition ne permet pas nécessairement d'exclure l'existence d'émissions particulières nécessitant une investigation complémentaire.

L'identification d'une source radioélectrique requiert généralement des moyens techniques plus spécialisés tels que l'analyse spectrale avancée, la radiogoniométrie, les mesures directionnelles, l'enregistrement continu des signaux, la corrélation temporelle des événements et, lorsque le cadre juridique le permet, des capacités spécialisées d'analyse électromagnétique.

Le dispositif actuel de l'ANFR, régi par la loi n° 2015-136 du 9 février 2015 (« loi Abeille »), s'avère donc largement insuffisant.

Force est de constater que ces dispositifs ne sont actuellement pas mobilisés pour protéger les citoyens. Ces attaques sont systématiquement requalifiées en troubles de droit commun ou en contentieux de voisinage, privant ainsi les victimes de la protection du renseignement national et de l'expertise technique pourtant détenue par nos services pour identifier de telles signatures.

Cette abstention des autorités constitue un manquement au devoir régalien de protection des citoyens, qui sont, par définition, la composante indissociable de la Nation. Les moyens techniques dont dispose l'État — notamment en matière de détection, de caractérisation et d'attribution des signaux électromagnétiques — doivent être mis au service de la sécurité de la population, et non limités aux seules structures étatiques.

En conséquence, notre association sollicite :

- l'ouverture d'une évaluation technique indépendante des phénomènes signalés ;
- la réalisation de relevés techniques approfondis sur les sites concernés ;
- la mise en place d'une surveillance technique temporaire des zones faisant l'objet de signalements répétés ;
- l'utilisation de dispositifs d'enregistrement continu permettant de détecter des émissions intermittentes ou occasionnelles ;
- la réalisation d'analyses spectrales détaillées ;
- la mise en œuvre de moyens de radiolocalisation et de radiogoniométrie lorsque cela est techniquement possible ;
- la centralisation et la corrélation des signalements provenant de différents territoires ;
- la désignation d'un service coordonnateur chargé du suivi de ces investigations ;
- la communication aux plaignants des conclusions générales des investigations réalisées, dans le respect des exigences liées à la sécurité nationale et au secret des enquêtes ;
- une réflexion sur l'adaptation éventuelle du cadre réglementaire afin de mieux répondre aux situations nécessitant l'identification technique d'émissions radioélectriques d'origine indéterminée.

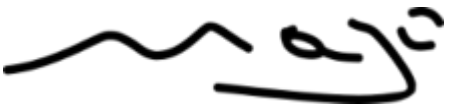
Nous ne sollicitons pas la divulgation d'informations couvertes par le secret de la défense nationale ni l'accès à des moyens classifiés.

Nous joignons en annexe une liste des plaignants, établie avec leur consentement exprès, comportant leurs coordonnées complètes afin de permettre aux services de l'État de les contacter directement dans le cadre d'une enquête de sécurité nationale et d'assurer leur protection individuelle.

Notre association estime qu'une telle démarche contribuerait à apporter des réponses objectives aux préoccupations exprimées par les citoyens concernés tout en permettant, le cas échéant, d'identifier l'origine réelle des phénomènes signalés.

Dans l'attente d'une réponse diligente et opérationnelle, nous vous prions d'agréer, Monsieur le Premier Ministre, l'expression de notre très haute considération.

Pour l'Association STOP À LA CYBERTORTURE,



Régis MAYO
Coprésident

annexe 1 : relevés de signaux anormaux soulignant une PEAK de champ magnétiques

annexe 2 : relevés de signaux anormaux soulignant une PEAK de champ magnétiques

annexe 3 : relevés de signaux anormaux soulignant une PEAK de champ magnétiques

annexe 4 – liste des demandeurs et personnes ayant formulé un signalement

annexe 5 – témoignages et éléments communiqués

Pour chaque personne concernée :

- Nom et prénom :
- Coordonnées :
- Date(s) des faits signalés :
- Lieu(x) concerné(s) :
- Description des faits observés :
- Démarches déjà effectuées (ANFR, police, gendarmerie, mairie, opérateurs, etc.) :
- Documents joints :

Liste des pièces annexées :

- Pièce n°1 :
- Pièce n°2 :
- Pièce n°3 :
- Etc.