FORUM PARLEMENTAIRE SUR LE RENSEIGNEMENT ET LA SÉCURITÉ
(Parliamentary Intelligence-Security Forum – 22 mai 2025)

Mesdames, Messieurs,

Le 25 mars de l'an dernier, le département de la Justice américain a dévoilé un acte d'accusation, contre 7 ressortissants chinois appartenant au groupe de hackers APT31 qui rapporte directement au ministère chinois de la Sécurité d'État.

116 parlementaires, issus de 15 pays, dont je fais partie, ont été attaqués par un groupe de hackers APT31 qui rapporte directement au ministère chinois de la Sécurité d'État.

Tous ces parlementaires étaient des membres de l'IPAC.

Je remercie les services du FBI et du département de la Justice pour leur action et de nous avoir informé.
Il s'agit clairement d'un acte de cyber-guerre, commis par une dictature 2.0.

Au début de la crise du Covid en mars 2020, l'ambassade de Chine à Paris, a fait un communiqué indiquant que la France laissait mourir ses personnes âgées dans les EPADH.
J'avais produit un rapport, et réclamé la mise en place d'une "force de réaction cyber", seule capable de réagir et de lutter offensivement contre les ennemis de nos valeurs républicaines.

15 mois plus tard, l'agence nationale Viginum voyait le jour en France pour détecter les attaques informationnelles.

Viginum a mis en lumière plusieurs opérations d'influence visant à manipuler l'information et à déstabiliser les démocraties européennes, notamment la France.

Voici un aperçu des principales campagnes identifiées.

Portal Kombat : un réseau de désinformation pro-russe
Identifié en février 2024, Portal Kombat est un réseau de plus de 200 sites web diffusant massivement des contenus pro-russes, notamment en relayant des publications de chaînes Telegram et d'agences de presse russes.

Ce réseau, administré par l'entreprise russe TigerWeb basée en Crimée, a étendu ses activités de l'Ukraine à l'ensemble de l'Europe, ciblant notamment la France et ses dirigeants.

Opération "Red Hands" : instrumentalisation d'un acte antisémite
En mai 2024, des mains rouges ont été peintes sur le Mémorial de la Shoah à Paris. Cet acte a été exploité par un réseau de faux comptes sur X contrôlé par le Kremlin. Un faux média nommé "Artichoc" a également été utilisé pour amplifier cette campagne de désinformation.

Manipulation sur TikTok lors de l'élection présidentielle roumaine
Lors de l'élection présidentielle roumaine de 2024, VIGINUM a observé des tentatives de manipulation de l'information sur TikTok, notamment par la promotion artificielle de contenus et l'instrumentalisation d'influenceurs.

Mriya : un média séparatiste ukrainien pro-russe
Le média "Mriya", actif sur Telegram, a été identifié comme une vitrine médiatique d'un projet politique séparatiste ukrainien soutenu par la Russie.

Il diffusait des contenus dénigrant le gouvernement ukrainien et promouvait des référendums d'autonomie dans les régions ukrainiennes.

Des influenceurs associés à Mriyaont également participé à des manifestations anti-Ukraine en Europe.

Opérations d'influence en Afrique : le projet Lakhta
Le projet Lakhta, également connu sous le nom d'Internet Research Agency, est une structure russe chargée de mener des opérations d'influence à l'étranger.

Actif en Afrique, il a mené des campagnes de désinformation visant à dénigrer la France et à soutenir le déploiement du groupe Wagner.

Ces campagnes ont utilisé des réseaux de faux comptes sur les réseaux sociaux pour diffuser des messages hostiles à la France et à l'Ukraine.

Storm-1516 : une opération d'influence russe sophistiquée

Révélée en mai 2025, l'opération Storm-1516 est un mode opératoire informationnel russe actif depuis au moins août 2023.

Elle a été impliquée dans 77 attaques informationnelles visant à discréditer le gouvernement ukrainien et à semer le doute sur l'intégrité des processus électoraux européens.

Le narratif le plus récurrent a néanmoins consisté à accuser Volodymyr Zelensky et ses proches de détourner l’aide occidentale pour dépenser d’importantes sommes d’argent ou acquérir de luxueuses propriétés à l’étranger, notamment en vue de fuir l’Ukraine, présentée comme étant sur le point de perdre la guerre.

quatorze opérations affirment par exemple que le président ukrainien et son entourage avaient acquis des yachts d’un montant de 75 millions de dollars, un casino à Chypre, un hôtel à Courchevel, la villa du chanteur Sting en Toscane, une maison à Saint-Barthélemy, l’ancienne résidence de Joseph Goebbels, ou encore une voiture et le « nid d’aigle » d’Adolf Hitler.

En France, par exemple, un faux site imitant celui de la coalition « Ensemble » promettait une « prime Macron » de 100 euros en échange de votes.

Les techniques utilisées incluent des deepfakes, des montages vidéo et l'utilisation

d'intelligence artificielle pour créer des contenus trompeurs.

La Chine n’est pas en reste.
La nuit qui a suivi la cérémonie d'ouverture de Paris 2024, trois arrondissements de Paris ont connu une panne d'électricité de 10 minutes.
L'information a été reprise par un media chinois.

Plus de 4 millions de comptes Tik Tok ont relayé l'information, certains annonçant que seul le
Sacré Cœur restait illuminé.
Les campagnes numériques de manipulation de l’information sont devenues un véritable instrument de déstabilisation des démocraties.

Nous cherchons à mieux préparer les individus et les sociétés.

Viginum a préparé un guide pour les Entreprises à l’occasion des JO.

En matière de menace informationnelle, les entreprises et acteurs économiques peuvent être
ciblés par les principaux modes opératoires suivants :

1~ Le raid numérique
Ce mode opératoire vise à créer ou amplifier un bad buzz autour d’un sujet polémique, généralement via l’utilisation d’un mot clé ou de plusieurs hashtags, dont les acteurs vont chercher à en augmenter la visibilité.

2~ L’incitation à conduire des actions dans le champ physique
Ce mode opératoire peut se traduire en ligne par des appels à manifester ou à dégrader des locaux d’entreprises ciblées.

3~ L’usurpation d’identité
Ce mode opératoire consiste pour l’acteur malveillant à usurper l’identité d’une entreprise, de
ses porte- paroles ou de ses dirigeants pour véhiculer de fausses informations pouvant leur
nuire auprès de relais d’opinion influents.

Viginum a alerté sur la menace informationnelle pour les acteurs économiques ciblés, sur les risques
suivants :
Le risque réputationnel pour atteindre l’image de l’entreprise ;

Le risque économique visant à affecter les intérêts économiques de l’entreprise ciblée, en entraînant une chute de l’action en bourse ;

La manipulation informationnelle lors de l’arrivée de DeepSeek est un remarquable exemple de ce qui avait été anticipé.

En utilisant Une communication stratégique amplifiée ;
Des benchmarks peu transparents et Une exploitation géopolitique du succès

technologique,

Le 27 janvier 2025, la sortie du modèle DeepSeek-R1 a provoqué une onde de choc sur les marchés financiers :

• Nvidia a perdu environ 17 % de sa valeur en une journée, soit près de 593 milliards de dollars de capitalisation boursière .
• D'autres géants technologiques comme Broadcom, Microsoft, Alphabet (Google) et ASML ont également subi des baisses significatives .

Deux mois après son lancement, Deepseek a perdu plus de 20 millions d'utilisateurs, soit plus du tiers d'entre eux.

Malgré la chute initiale marquée par l'arrivée de DeepSeek, les marchés boursiers des entreprises technologiques ont montré une capacité de résilience avec une reprise notable, et Nvidia a récupéré avec une augmentation de près de 43 % de son cours sur l'année .

La Chine et la Russie nous ont déclaré la cyberguerre depuis longtemps.

« La Russie est la tempête, la Chine est le changement climatique »

Il n'y a pas de canon pour détruire un mensonge.

J'étais dans l'innovation. Je disais à tout le monde : Votre présent est mon passé ! Les démocraties doivent récupérer l'initiative.

Viginum démontre que nous pouvons aller dans ce sens afin d'anticiper les attaques.

Lors de la Paris cyber week en juin, j'ai appelé à la création d'une force de dissuasion cyber

Un partenariat fort entre les États-Unis et l'UE, mais également avec les entreprises privées doit s'opérer.

A Washington, les gens de Google m'ont confié.

"La Russie est plus grande que l'Ukraine. Sur internet, Google est plus puissant que la Russie."

Amazon Web Services a fait ses preuves pour permettre à l'Ukraine d'être résiliente au début de l'invasion russe.

La collaboration US-UE, Public-privé, doit pouvoir s'opérer comme nous le faisons dans le nucléaire et commencer par exemple en partageant nos vulnérabilités réciproques en toute transparence.

Nous devons construire une alliance interparlementaire internationale du cyber pour soutenir une politique de cyber solidarité et imposer des sanctions cyber pour isoler les régimes autoritaires.

Il n’y a pas de système qui n’a pas
de vulnérabilité.

La meilleure défense c'est la surprise !

L'exemple de l'explosion des beepers des membres du Hezbollah au Liban en est la parfaite illustration.

Les régimes autoritaires ne sont pas aussi solides qu'ils le paraissent.
Regardez à quelle vitesse s'est effondré celui de Assad en Syrie.

Je vous remercie.