

TENTATIVE DE PIRATAGE DE PROXIMITÉ DE L'OIAC PAR LE GRU DÉJOUÉE À LA HAYE

En avril 2018, les services de sécurité néerlandais, en coopération avec le Royaume-Uni, ont déjoué une opération du GRU (unité 26165) visant à pirater le réseau Wi-Fi de l'Organisation pour l'interdiction des armes chimiques à La Haye. À cette date, l'OIAC examinait l'empoisonnement au Novitchok de Salisbury. Les officiers ont été expulsés des Pays-Bas.

UKRAINE EVIDENCE HUB
AU-DELÀ DE L'UKRAINE
AU 15 OCT. 2026

DEGRÉ DE PREUVE

ATTRIBUTION OFFICIELLE

Un gouvernement, un procureur, l'UE, l'OTAN ou un organe de l'ONU a formellement désigné la Russie, ses services ou ses forces soutenues par l'État. Il s'agit d'une position de cette autorité, non d'un jugement.

QUI L'A ÉTABLI

Divulgaration conjointe des Gouvernements néerlandais et britannique, 4 oct. 2018. La déclaration britannique à La Haye a nommé l'unité 26165 du GRU. Les quatre officiers ont ensuite été inscrits sur la liste des sanctions cyber de l'UE (règlement d'exécution (UE) 2020/1125). L'acte d'accusation américain du 4 oct. 2018 a mis en cause des officiers du GRU liés à l'affaire.

DERNIÈRES NOUVELLES

Les sanctions de l'UE restent en vigueur.

SOURCES

- B** **Gouvernement britannique – Déclaration du ministre chargé de l'Europe : tentative de piratage de l'OIAC par le renseignement militaire russe** · 2018-10-04
<https://gov.uk/government/speeches/minister-for-europe-statement-attempted-hacking-of-the-opcw-by-russian-military-intelligence>
- A** **EUR-Lex – Règlement d'exécution (UE) 2020/1125 du Conseil** · 2020-07-30
https://eur-lex.europa.eu/eli/reg_impl/2020/1125/oj/eng
- C** **CBS News – Opération de cyberattaque du GRU russe visant l'OIAC** · 2018-10-04
<https://cbsnews.com/news/russia-gru-cyberattack-operation-targeting-opcw-chemical-weapons-netherlands-2018-10-04>

CE QUE NOUS DEMANDONS

DES ÉTATS MEMBRES

- Attribuer conjointement et porter la question devant le Groupe de travail à composition non limitée des Nations Unies sur la sécurité du numérique.
- Appliquer le régime de sanctions cyber de l'UE aux unités responsables.
- Partager les indicateurs et renforcer la résilience des infrastructures critiques.

Le statut suit quatre degrés de preuve : décision de justice · attribution officielle · mis en accusation · soupçonné (les cas soupçonnés ne figurent que sur la page en ligne). Niveau A = juridictions, organes de l'ONU, organisations internationales · B = gouvernements, parquets · C = médias et enquêteurs. Rectificatifs : evidence@ukraine-evidence.org



page en ligne ·
rectificatifs