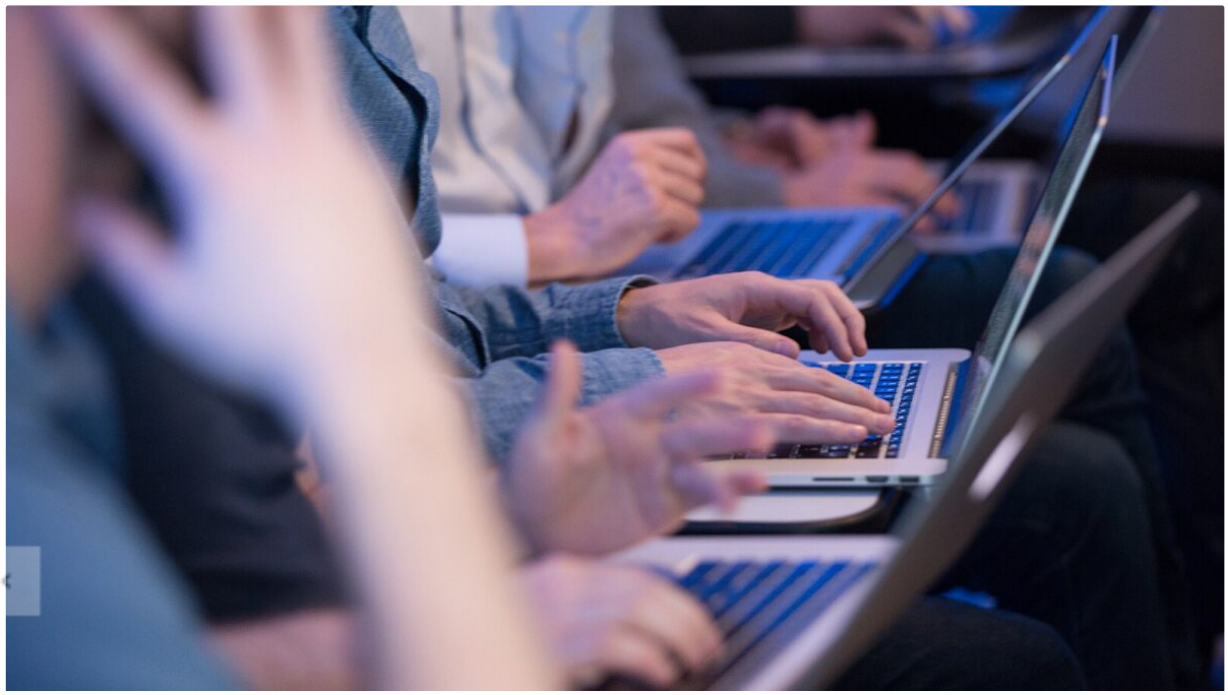
LE RUBICON

Dénoncer publiquement la Russie : le tournant français dans l'attribution des attaques

Quentin Jalabert, Damien Van Puyvelde, Thomas Maguire | 3 octobre 2025 |



Ce texte est une traduction de l'article « Calling Out Russia: France's Shift on Public Attribution », publié le 3 juillet 2025 sur War on the Rocks.

Le silence constitue-t-il une stratégie efficace quand l'adversaire ne cherche même plus à se dissimuler ? Pendant des années, la France a maintenu une politique de retenue et de discrétion, refusant généralement de désigner publiquement les gouvernements étrangers à l'origine de cyberattaques, de campagnes de désinformation ou d'ingérences, même lorsque les preuves désignaient clairement Moscou. Mais le 13 mai 2025, le président Emmanuel Macron a annoncé que la France attribuerait désormais systématiquement l'origine des actes hostiles visant le pays, en réponse à la menace croissante que représente la Russie. Ce changement d'approche s'est appuyé sur un rapport de 16 pages émanant des services de renseignements français, intérieurs et extérieurs, divulgué à *L'Express*, et détaillant 13 actes d'agression du président russe, Vladimir Poutine, contre la France. Ces annonces mettent fin à une politique de longue date consistant à éviter l'attribution publique des cyberattaques étatiques, et marquent une rupture nette avec l'ancienne doctrine française en la matière.

Cette décision introduit un changement prudent mais assumé dans l'approche de la France en matière d'attribution publique, en conservant une part de retenue tout en mettant en avant la valeur stratégique d'une transparence et d'une précision accrues dans la divulgation des renseignements, en particulier face aux menaces croissantes venues de Russie.

Pourquoi l'attribution publique est-elle importante ?

L'attribution publique par les États implique la communication de jugements analytiques internes identifiant les auteurs d'activités spécifiques. Fondées, au moins partiellement, sur l'analyse de renseignements nationaux ou transmis par des partenaires, ces attributions s'inscrivent dans une pratique plus large de divulgation d'informations sensibles au public. L'attribution publique peut résulter d'une décision opérationnelle ou politique émanant d'autorités compétentes – qu'elles soient techniques, juridiques ou institutionnelles. Comme l'a expliqué Guillaume Poupard, ancien directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), lorsqu'il s'agit d'identifier la responsabilité d'un État, « l'attribution

est en fin de compte une décision politique prise à un très haut niveau », compte tenu de ses conséquences diplomatiques.

L'attribution publique poursuit plusieurs objectifs. Certains gouvernements considèrent la divulgation comme un moyen de perturber et de dissuader les opérations d'influence clandestines et les actes hostiles. L'idée étant que la divulgation prive les acteurs étatiques comme non étatiques de la discrétion nécessaire à la conduite de leurs opérations, les obligeant à s'adapter ou à reconsidérer leurs plans. Israël, par exemple, a largement utilisé cette tactique contre le Hezbollah. La dénonciation publique peut également contribuer à établir et à faire respecter les normes internationales, tout en favorisant une forme de stabilité sur des enjeux telles que la cybersécurité et la prolifération nucléaire, en entamant la réputation de l'acteur fautif auprès de l'opinion publique.

Les gouvernements utilisent également la divulgation de renseignements pour justifier leurs politiques, leurs actions et leurs capacités, et pour obtenir du soutien en atteignant une supériorité narrative. Les services de renseignements militaires ukrainiens, par exemple, ont utilisé la divulgation pour créer un récit cohérent en temps de guerre et rallier le soutien international. Certains gouvernements utilisent également les attributions pour avertir leur opinion publique et renforcer leur résilience face aux ingérences étrangères hostiles.

Un changement prudent

Le gouvernement français a commencé à divulguer des renseignements à propos d'actes de cyberespionnage et de sabotage – sans en attribuer l'origine – dès 2012. En 2019, les autorités françaises ont procédé à leurs premières attributions publiques directes de cybermenaces déjà identifiées par des partenaires comme étant liées à la Russie et à la Corée du Nord. À la différence de ses alliés – notamment les États-Unis (depuis 2014), le Royaume-Uni (2017), l'Allemagne (2018) et les Pays-Bas (2018) –, la France s'est longtemps abstenue de désigner nommément des États comme commanditaires de cyberintrusions. Comme l'a expliqué l'ANSSI, « l'attribution d'une cyberattaque à un acteur malveillant est un exercice complexe et n'est pas l'objectif de ce document ni [notre] mission ».

Une différence importante avec ses alliés anglophones tient au fait que la France ne dispose pas des mêmes ressources ni de la même couverture en matière de renseignements que l'alliance des « Five Eyes », qui regroupe les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande. Cela limite la capacité des services français à recouper leurs évaluations et à atteindre un degré suffisant de certitude sur l'origine des attaques. Pourtant, comme le démontrent l'Allemagne et les Pays-Bas, des États non anglophones parviennent à attribuer les responsabilités avec assez de certitude pour justifier une divulgation.

Des considérations politiques ont aussi pesé sur la retenue française. Pendant des années, l'ANSSI et les dirigeants politiques ont privilégié la divulgation de descriptions techniques des méthodes de leurs adversaires afin de renforcer la résilience nationale. Les hauts responsables de la sécurité ont souligné les risques diplomatiques qu'impliquent la désignation d'un État, ainsi que les contraintes politiques qu'elle entraîne, en limitant le dialogue et en appelant des réponses plus fermes. Ils considéraient que les échanges privés et bilatéraux étaient plus efficaces.

Comme le montrent ces préoccupations, l'attribution et la divulgation publiques ne sont pas sans danger. Pour la plupart des services de renseignements et de sécurité, le principal risque tient à la possibilité pour les adversaires d'identifier les sources et méthodes du pays divulgateur et de s'y adapter, compliquant ainsi le travail futur. Les divulgations de renseignements par les Britanniques et les Américains, lorsqu'ils cherchaient à obtenir le soutien à l'invasion de l'Irak en 2003, ont aussi montré que l'usage public du renseignement peut miner la confiance de l'opinion si les affirmations s'avèrent politisées et trompeuses.

En France, la première attribution publique d'opérations cybernétiques à la Russie, ainsi que la divulgation de 13 actes hostiles liés à Vladimir Poutine, semblent marquer un tournant politique majeur. Pourtant, le pays s'était déjà progressivement engagé dans cette voie. En 2021, l'ANSSI a publiquement attribué plusieurs campagnes d'intrusions à APT44 (« Sandworm ») et APT31 (« Zirconium »), deux acteurs représentant des « menaces persistantes avancées » (*advanced persistant threats* ou APT). Les autorités, de leur côté, ont adopté un langage volontairement ambigu, en s'appuyant sur des rapports de partenaires ou de sources ouvertes, et en suggérant un lien entre ces groupes et, respectivement, la Russie et la Chine. L'ANSSI est passée d'une communication technique, notamment en 2021 lors du ciblage d'entités diplomatiques françaises par APT29 (« Cozy Bear »), à une évaluation publique plus explicite en 2024, en associant ce groupe à des opérations de cyberespionnage mondiales et qui avaient « été publiquement rattachées au [service de renseignements étrangers] russe par différentes sources ». Le pas franchi ce printemps était donc modeste, mais significatif.

La France a également utilisé ses services de renseignements pour attribuer l'origine d'attaques qui ont eu lieu en dehors du cyberespace. Sous les présidents Hollande et Macron, les autorités françaises ont ainsi accusé le régime de Bachar el-Assad d'avoir mené des attaques chimiques contre des civils syriens en 2013, 2017 et 2018, divulguant ainsi des informations issues

du renseignement. En 2022, elles ont également utilisé du renseignement pour dénoncer une campagne de désinformation russe au Mali, révélant que des agents du groupe Wagner, un *proxy* de Moscou, avaient placé des cadavres près d'une base militaire afin de piéger les troupes françaises et d'attiser le sentiment anti-français.

L'agence française de lutte contre la manipulation de l'information (VIGINUM) a également contribué à cette évolution progressive. Elle a publié des rapports en 2023 et 2024 qui établissent un lien entre des acteurs russes et des opérations d'ingérence. Son analyse sur Storm-1516, rendue publique en mai 2025, entre l'attribution publique de l'ANSSI et l'annonce d'Emmanuel Macron, décrivait ce groupe comme opérant depuis la Russie et étant lié au Kremlin. Le ministère français des Affaires étrangères a alors condamné les « activités déstabilisatrices » de la Russie.

Néanmoins, l'approche de la France reste prudente. Les attributions récemment publiées concernent des activités russes remontant à 2017 et ont déjà été largement rapportées par les alliés, le secteur privé et les médias français et internationaux. L'agence française de cybersécurité avait, par exemple, alerté en privé le candidat Macron en 2017 d'une opération russe de piratage et de divulgation visant sa campagne présidentielle. La France a toutefois refusé de rendre publique cette attribution, alors que d'autres gouvernements européens révélaient plus ouvertement l'implication présumée de la Russie dans des opérations d'ingérence électorale cette même année. Les États-Unis ont même publiquement attribué l'ingérence électorale visant Emmanuel Macron au service de renseignements militaires russe en 2020 sans confirmation publique de la France jusqu'en mai dernier. De même, l'attribution par la France en avril 2025 de l'APT28 (« Fancy Bear ») au renseignement militaire russe s'appuyait sur l'évaluation technique de 2023 de l'agence française de cybersécurité et faisait écho aux déclarations publiques des alliés et du secteur privé depuis 2018.

La plupart des divulgations françaises passées visaient la Russie. L'annonce d'Emmanuel Macron s'inscrit clairement dans cette continuité, en cadrant explicitement le changement de posture autour des menaces russes – un point essentiel. D'autres États hostiles, comme la Chine, ont fait l'objet d'un traitement distinct. Cela met en lumière la dimension politique de l'attribution et s'inscrit dans une stratégie plus large, cohérente dans ses objectifs. Si les finalités de Paris demeurent constantes, ses moyens ont évolué avec prudence, en réponse à la dégradation des relations avec Moscou. À mesure que ces relations se tendent, le coût diplomatique d'une attribution diminue, d'autant plus que le soutien français à l'Ukraine s'est nettement affirmé.

Il ne s'agit pas d'un basculement complet vers l'usage de la divulgation de renseignements comme instrument de politique étrangère. La pratique demeure controversée. En mars 2025, le général Jacques Langlade de Montgros, directeur du renseignement militaire, a d'ailleurs mis en garde contre une déclassification excessive, critiquant l'approche américaine avant et pendant l'invasion de l'Ukraine par la Russie. Rompre avec la norme qui proscrivait l'attribution publique à des États pourrait cependant ouvrir la voie à une adoption plus large, si cette pratique s'avère utile. Elle accroît aussi la flexibilité de la France pour participer à des attributions internationales coordonnées, comme celle de mai dernier sur APT28. Ce faisant, Paris peut mieux aligner son renseignement et sa diplomatie sur ceux de ses alliés, et concrétiser la volonté du président Macron de doter l'Europe d'une réponse stratégique plus ferme face à l'agression russe.

Quand l'utilité stratégique rencontre la politique intérieure

Ce signal s'adresse aussi à l'opinion publique nationale. Les considérations politiques intérieures influencent les décisions en matière de divulgation. François Hollande et son coordonnateur national du renseignement, Alain Zabulon, avaient invoqué la nécessité de préparer l'opinion publique française à une éventuelle intervention en Syrie pour justifier la divulgation des crimes d'Assad. En mai 2025, *L'Express* a ouvert son article par une citation d'Emmanuel Macron exprimant sa frustration de voir l'opinion publique d'avantage préoccupée par les « femmes voilées » – allusion probable aux débats nationaux sur l'islam politique – que par la Russie. Sa décision reflète la nécessité perçue de communiquer plus directement avec le public français sur la menace russe. Ces considérations de politique intérieure, souvent négligées dans les analyses de la divulgation de renseignements, sont pourtant cruciales. La sécurité nationale et la politique extérieure s'inscrivent dans un continuum stratégique : les politiques d'attribution servent non seulement à gérer les menaces externes, mais aussi à façonner le consensus interne.

Quelles implications ?

La décision de la France d'attribuer systématiquement les actes hostiles de la Russie marque un changement, mais non une rupture. Elle traduit une adaptation stratégique face à un contexte géopolitique où l'ambiguïté est devenue un outil de perturbation. Elle représente aussi un règlement de comptes personnel pour le président Macron, remontant aux tentatives de Moscou de compromettre son élection en 2017. Reste à voir si cette approche s'étendra au-delà de la Russie. Cela dépendra en grande partie de la réaction du public, mais aussi de celle des parties visées par ces attributions.

L'effet des divulgations de renseignements sur les publics ciblés reste difficile à mesurer. Les recherches universitaires sur

l'attribution publique des cyberattaques suggèrent qu'elle ne permet pas de dissuader les attaquants de récidiver. Des études empiriques supplémentaires sont nécessaires pour mieux cerner les objectifs que ce type de divulgation peut réellement atteindre.

Néanmoins, le message est clair. Emmanuel Macron mise sur l'idée que la transparence, lorsqu'elle est maîtrisée, peut devenir un outil de dissuasion. Il parie que la France peut infliger un coût réputationnel à ses adversaires sans compromettre ses capacités de renseignement. Il cherche aussi à sensibiliser une opinion publique qu'il juge distraite face aux menaces du XXIe siècle. En ce sens, le suivi de l'impact de l'attribution et de la divulgation des renseignements sur le public français jouera sans doute un rôle déterminant dans l'évolution de la politique nationale en la matière.

Ce changement d'approche quant à l'attribution soulève encore de nombreuses questions, car les informations sur le processus décisionnel, l'évaluation des opportunités et la gestion des risques restent absentes du débat public. À cet égard, l'expérience d'autres pays peut nourrir la réflexion sur les implications organisationnelles de la nouvelle politique française. Au Royaume-Uni, le processus de divulgation a été centralisé autour de la Joint Intelligence Organisation et du National Security Council. Au Pays-Bas, l'agence de renseignement militaire a créé un comité de divulgation chargé de ce rôle. Dans le contexte des discussions sur la nécessité perçue de transformer le Conseil de défense français en Conseil de sécurité nationale, à l'image de celui qui existe aux États-Unis, cette politique pourrait accroître la charge de travail et la pression institutionnelle pesant sur les agences spécialisées.

Au-delà de la dynamique interne de l'État français, le recours croissant à l'attribution influencera aussi la coopération internationale de la France, qu'il s'agisse d'obtenir l'autorisation de partenaires détenant des informations confidentielles ou de coordonner des attributions conjointes. L'adoption prudente de cette pratique soulève en outre la question d'une approche transatlantique unifiée.

Crédit : École polytechnique *via* Wikimedia Commons.

Dénoncer publiquement la Russie _ le tournant français dans l'attribution des attaques - Le Rubicon

•— ••— — • ••— •—• •••

Quentin Jalabert, Damien Van Puyvelde, Thomas Maguire

Quentin Jalabert (@QJalabert) est doctorant à l'université de Leyde, où il travaille sur la divulgation des renseignements français.

Damien Van Puyvelde (@dvanp) est professeur agrégé et directeur du groupe de recherche sur le renseignement et la sécurité à l'université de Leyde. Il est l'auteur du livre à paraître *The DGSE: A Concise History of France's Foreign Intelligence Service* (Georgetown University Press, 2026).

Thomas Maguire est maître de conférences en renseignement et sécurité à l'université de Leyde, où il dirige un projet sur la divulgation d'informations confidentielles.

Comment citer cette publication

Quentin Jalabert, Damien Van Puyvelde, Thomas Maguire, « Dénoncer publiquement la Russie : le tournant français dans l'attribution des attaques », *Le Rubicon*, 3 octobre 2025 [https://lerubicon.org/?p=9403].