**L'espionne Anna Chapman sur la place Rouge, en 2011.**

SPUTNIK /RIA NOVOSTI

# LE RETOUR DES ESPIONS RUSSES

## BIENVENUE DANS LA NOUVELLE GUERRE FROIDE

*Les agents secrets de Vladimir Poutine, que va recevoir à Brégançon Emmanuel Macron, multiplient contre les pays occidentaux des actions mêlant l'espionnage classique, l'assassinat, le piratage informatique, l'ingérence et la désinformation. Le fruit de la volonté du tsar du Kremlin, qui dit se défendre contre les agressions de ses ennemis.*

**Par Vincent Nouzille**

*« Comparé à ce qui se passe aujourd'hui, la guerre froide du XXe siècle, c'était des enfants jouant dans un bac à sable ! »* Cette phrase n'a rien d'anodin. Elle a été prononcée l'an dernier par Anna Chapman, jeune Russe de 37 ans, experte en matière d'espionnage. Fille d'un cadre du KGB, les services secrets de l'ère soviétique, Anna, née Kouchtchenko, a œuvré au Royaume-Uni où elle a épousé un homme d'affaires nommé Chapman, puis aux Etats-Unis, pour le compte du Service de renseignement extérieur de la Fédération de Russie (SVR). Arrêtée à New York par le FBI en juin 2010 avec neuf autres espions, elle a été échangée contre quatre Russes accusés d'espionnage pour les Américains. Décorée à son retour à Moscou, devenue star de la télévision et top-modèle, Anna Chapman continue de vanter les mérites de Vladimir Poutine qui défend, selon elle, son pays contre ses *« ennemis »* occidentaux : *« Il ne sera plus possible de défier la Russie sans en subir les conséquences »,* a lancé, il y a quelques mois, la Mata Hari aux yeux verts.

### DIPLOMATES-ESPIONS

Bienvenue dans la nouvelle guerre froide ! Elle ne relève pas du fantasme : le 4 mars 2018, Sergueï Skripal, ancien officier du renseignement militaire russe (GRU) et agent double, expulsé de Moscou vers Londres en 2010, a fait l'objet, avec sa fille, d'une tentative d'empoisonnement à son domicile de Salisbury, en Angleterre. Le neurotoxique utilisé, le Novitchok, d'origine soviétique, a conduit les autorités britanniques à remonter la piste jusqu'au GRU. Deux agents russes de ce service ont été identifiés comme des membres présumés du commando chargé de →

Quand l'ex-agent dormant russe Anna Chapman expulsée d'Amérique joue au mannequin en Turquie, membre de l'Otan.

l'élimination du « traître » Skripal. En réaction, le Royaume-Uni et 15 autres pays occidentaux, dont la France, ont renvoyé chez eux plus d'une centaine de « diplomates » russes soupçonnés d'espionnage. En octobre 2018, les services secrets néerlandais ont annoncé qu'ils avaient arrêté six mois plus tôt quatre officiers du GRU, surpris en train de pirater les ordinateurs du siège de l'Organisation pour l'interdiction des armes chimiques, à La Haye. Deux d'entre eux sont également poursuivis aux Etats-Unis et en Suisse pour d'autres « hackings » informatiques, notamment d'instances sportives internationales, de l'Agence mondiale antidopage à Lausanne et d'un laboratoire près de Berne. Grâce à des recoupements de données, des journalistes russes et britanniques ont ensuite réussi à démasquer 300 autres agents du GRU. Une mauvaise publicité pour ce service !

Ces affaires du GRU démontrent l'activisme croissant des espions de Poutine, qui sont de plus en plus offensifs, au risque de se faire prendre. Depuis quelques années, Moscou est en effet suspecté de conduire des opérations d'espionnage, d'intrusion, de piratage, d'ingérence et de désinformation à grande échelle. Outre les dossiers précités, on leur attribue une longue liste d'assassinats d'opposants, des cyberattaques contre l'Estonie, la Géorgie et l'Ukraine, des interférences lors des élections aux Etats-Unis, au Royaume-Uni et en France, des financements occultes de partis populistes en Europe, des hackings de sites gouvernementaux et de satellites. Et cette liste n'est pas exhaustive !

> Anna Chapman : "Il ne sera plus possible de défier la Russie sans en subir les conséquences"

La nouvelle guerre froide repose à Moscou sur un homme de l'art : le président Vladimir Poutine lui-même, ancien officier du KGB, choisi en 1999 pour succéder au président Boris Eltsine. Dès son arrivée au pouvoir l'année suivante, le nouveau tsar estime que la Russie a été *« humiliée »* par l'Occident depuis la dislocation de l'URSS en 1991 et qu'elle est menacée par l'avancée de l'Otan jusqu'en Pologne. Il entend restaurer sa grandeur. *« Poutine reste un homme du KGB, qui use des rapports de force et de méthodes brutales pour parvenir à ses fins »,* estime Françoise Thom, professeure d'histoire à la Sorbonne et auteure de *Comprendre le poutinisme* (Desclée de Brouwer). Elle rapporte d'ailleurs cette éloquente citation de Poutine : *« Il y a trois moyens d'agir sur les hommes : le chantage, la vodka et la menace d'assassinat. »*

**NÉOSOVIÉTISME**

Réélu à la présidence en 2012 après l'intermède de son lieutenant Medvedev, puis à nouveau en 2018, il règne au Kremlin, entouré de proches imprégnés de néosoviétisme, presque tous des *siloviki,* des faucons issus des services de sécurité. Au sein de l'administration présidentielle, Nikolaï Patrouchev, un ancien du KGB qui dirige le Conseil de sécurité, est considéré comme un nationaliste dur, tout


La maison de l'agent double Sergueï Skripal, à Salisbury, en Angleterre.


Les agents russes suspectés d'avoir tenté d'empoisonner leur ancien collègue, Sergueï Skripal.


L'immeuble de Moscou qui abriterait une armée de hackers russes.


Tout près de la maison de Skripal ont été retrouvés des traces d'un agent neurotoxique : le Novitchok.

AP/SIPA ; JAMIE COOPER/SHUTTERSTO/SIPA ; UPI/MAXPPP ; DMITRI LOVETSKY/AP/SIPA ; OLIVER WILL/EPA

comme l'influent conseiller Vladislav Sourkov. Poutine a la main sur les trois principaux services de renseignement : le FSB, service intérieur tout-puissant, sous la houlette du général Alexandre Bortnikov, un kgébiste historique, qui muselle les opposants et rayonne parfois à l'étranger, y compris avec des cyberespions ; le SVR, le service extérieur, piloté par un fidèle, Sergueï Narychkine, autre ancien du KGB, qui collecte du renseignement à la manière d'Anna Chapman ; enfin, le GRU, le service de renseignement des armées, dirigé jusqu'en 2018 par l'inflexible général Igor Korobov. Le GRU est le plus agressif, notamment pour les pirateries informatiques et les assassinats d'ennemis de la Russie.

### MONTÉE EN PUISSANCE

Entre tous ces maîtres espions, les rivalités sont récurrentes et la coordination imparfaite, mais le leadership du président Poutine demeure incontesté. *« Les patrons du renseignement servent ses objectifs politiques. Et ils l'influencent, puisque Poutine lit chaque matin les notes de ses services et que cela lui suffit souvent à se forger son opinion »,* explique Mark Galeotti, chercheur associé au Royal United Services Institute à Londres, auteur de *Russian Political War* (Routledge). Selon lui, la vision des dirigeants russes est déterminée par le sentiment que l'Occident veut la disparition de la Russie et que, par conséquent, tous les moyens sont bons pour se défendre. Y compris l'attaque. Leurs espions ont pour consigne de prendre toutes les *« mesures actives »* possibles pour affaiblir les pays occidentaux. *« Cela passe par des moyens visibles, comme la propagande des médias russes RT ou Sputnik, mais aussi des méthodes plus secrètes et asymétriques »,* commente Mark Galeotti.

> Des espions chargés de prendre toutes les "mesures actives" possibles pour affaiblir les pays occidentaux

Cette montée en puissance s'est déroulée sur plusieurs fronts depuis plus d'une décennie. Premier acte à la fin des années 2000 : des petits pays voisins, naguère sous l'emprise soviétique, sont visés par des attaques informatiques inédites. C'est le cas, en avril 2007, de l'Estonie, pays balte qui a rejoint l'Union européenne et l'Otan en 2004. Des hackers russes « patriotiques » bloquent des institutions estoniennes durant trois semaines. En réaction, l'Otan installe son centre de cyberdéfense à Tallinn, ce qui renforce les craintes de Moscou.

### ATTAQUES INFORMATIQUES

Durant l'été 2008, la Géorgie est également ciblée par un assaut militaire russe combiné avec des attaques informatiques. *« Les Russes ont vu que cela marchait. Comme ils ont d'excellents mathématiciens et cryptographes, leurs services ont employé des milliers de cyberpirates pour exploiter les vulnérabilités de l'Occident »,* précise Jean-Louis Gergorin, coauteur de *Cyber. La guerre permanente* (Les Editions du Cerf).

## Le Kremlin est suspecté d'être derrière la déstabilisation de l'Ukraine après la "révolution orange", l'attentat contre l'avion de la Malaysia Airlines abattu en 2014 et la victoire de Trump aux Etats-Unis en 2016

Le deuxième front s'ouvre fin 2013, au début de la révolution de Maïdan en Ukraine, l'ancienne république soviétique qui tourne ses yeux vers l'Ouest. Les services russes sont persuadés que la CIA, qui aurait fomenté les printemps arabes de 2010-2011, est à la manœuvre en Ukraine lorsque le président prorusse Victor Ianoukovitch est contraint de prendre la fuite le 21 février 2014. Furieux, le Kremlin envoie des forces paramilitaires occuper la Crimée, région ukrainienne aussitôt annexée, et soutenir les séparatistes dans le Donbass voisin. Des militaires des forces spéciales russes, les Spetsnaz, qui dépendent du GRU, sont sur le terrain. L'occupation s'accompagne de piratages informatiques et d'une campagne de désinformation visant à légitimer l'opération militaire, appuyer les républiques autoproclamées du Donbass et faire passer les dirigeants ukrainiens pour des « fascistes ». Sur les réseaux sociaux, des comptes créés notamment par un groupe nommé Cyberberkut, possible faux nez du GRU, alimentent les rumeurs les plus folles contre les autorités de Kiev.

### RUMEURS ET FAUSSES NOUVELLES

Lorsque l'avion de la Malaysia Airlines est abattu au-dessus de la région du Donetsk, le 17 juillet 2014, les soupçons occidentaux s'orientent vers un tir de missile russe – ce que confirmera, en 2018, l'équipe de l'enquête internationale, spécialement formée aux Pays-Bas. Moscou nie toute implication. Le 19 juin 2019, les enquêteurs citeront à comparaître un Ukrainien et trois agents russes – un du FSB et deux du GRU –, suspectés d'avoir joué un rôle dans cet attentat. Coïncidence : durant les trois jours suivant le crash du vol MH17, Twitter a connu un pic d'activité provenant d'une mystérieuse entité russe, laquelle a inondé les réseaux sociaux de 111 000 tweets destinés à écarter la responsabilité de Moscou.

Ces tweets proviennent d'un immeuble de bureaux, situé à Saint-Pétersbourg, qui abrite l'Agence de recherche sur internet (IRA, en anglais). Créée en 2013 et supervisée par Evgueni Prigozhin, un oligarque protégé de Poutine qui l'a nommé « chef cuisinier » du Kremlin, l'IRA est une sorte d'agence de marketing digital qui emploie un millier de cyberactivistes. Ceux-ci surveillent le web, répandent des fausses nouvelles, dénigrent les opposants à Poutine et créent de faux comptes sur les réseaux sociaux. L'IRA est l'une des plus importantes « usines à trolls » liées au Kremlin. Selon une étude récente de la société de cybersécurité New Knowledge, l'IRA est monté en puissance de manière exceptionnelle, réussissant à toucher 126 millions d'utilisateurs sur Facebook, au moins 20 millions sur Instagram et 1,4 million sur Twitter. *« Nous n'avons pas de détails sur les liens entre l'IRA et les services russes, mais la chronologie de leurs interventions peut laisser penser qu'ils coordonnent leurs opérations, que ce soit sur l'Ukraine, la Syrie ou d'autres pays »,* avance Camille François, chercheuse associée à Harvard et directrice de l'innovation chez Graphika, une société américaine d'analyse des données qui a cosigné fin 2018 un rapport pour le Sénat américain sur l'IRA.

Cette conjonction apparaît plus nettement à partir de 2016, quand les espions et les trolls russes ouvrent leur troisième front en ciblant les Etats-Unis. Leur objectif : influencer la vie politique américaine en attisant les tensions internes. *« Les Russes ont appris, de manière opportuniste, à se servir des leviers d'action cyber, qui coûtent moins cher qu'un missile »,* résume Kevin Limonier, maître de conférences en études slaves à l'université Paris-VIII et auteur de *Ru.net. Géopolitique du cyberespace russophone* (Editions L'Inventaire). Dans son rapport publié début 2019 sur le Russiagate, le procureur spécial Robert Mueller accusera la Russie d'avoir *« monté des opérations de désinformation destinées à semer la discorde sociale, avec le but final d'interférer dans l'élection ».*

L'IRA joue un rôle clé dans ce plan, baptisé opération Lakhta, d'un coût de plus de 35 millions de dollars. Dès 2013, des faux comptes américains sont créés en masse par l'IRA afin de glaner de l'audience dans tous les milieux. Certains se font passer pour des activistes noirs ou des promusulmans, d'autres pour des conspirationnistes, des partisans du port d'armes, des opposants à l'immigration ou des supporters de Trump. *« Les trolls de l'IRA ont gagné énormément d'influence, au point d'être connectés sur Facebook à plus de 30 millions de personnes aux Etats-Unis entre 2015 et 2017 »,* révèle Camille François.

A l'approche de l'élection américaine de novembre 2016, l'ingérence franchit une étape décisive grâce au piratage des e-mails des QG démocrates de la campagne d'Hillary Clinton, publiés initialement par WikiLeaks. La candidate démocrate est fragilisée. Un faux compte DCLeaks et un pseudo-pirate roumain, Guccifer 2.0, disséminent ces documents à partir de juin 2016. Selon des sources du renseignement américain, cette opération a été menée par l'unité APT 28, appelée aussi Fancy Bear, un groupe de hackers réputés proches du GRU. Une autre unité, appelée APT 29 ou Cozy Bear, sans doute liée au FSB, aurait également participé à ce coup tordu. Moscou dément toute implication.

### INGÉRENCES ÉLECTORALES

Dans la foulée, l'IRA bombarde les réseaux sociaux de messages anti-Hillary et pro-Trump durant la campagne. Fâché, le président Barack Obama expulse 35 diplomates russes fin 2016. Les services américains finissent par se mobiliser. En février 2018, les autorités judiciaires inculpent formellement l'IRA et 13 Russes, dont le « chef cuisinier » de Poutine, pour *« conspiration »* lors des élections de 2016. Quatre mois plus tard, 12 officiers du GRU sont mis en →

Entourant leur président, deux hommes clés de la sécurité russe : Mikhaïl Fradkov et Alexandre Bortnikov.

Les restes de l'avion de la Malaysia Airlines abattu en Ukraine par un missile russe en juillet 2014.

ALEXEI DRUZHININ/AP/SIPA ; DMITRY LOVETSKY/AP/SIPA

Le chef des services de renseignement extérieur russes (SVR), Sergueï Narychkine.

Le directeur du Conseil de sécurité russe, Nikolaï Patrouchev.


Les autorités néerlandaises accusent ces quatre Russes d'espionnage.

cause pour le piratage des e-mails démocrates. Redoutant de nouvelles ingérences avant les élections de mi-mandat de novembre 2018, les cyberespions américains contre-attaquent en bloquant des serveurs russes. Selon certains experts, ils auraient coupé l'électricité dans l'immeuble de l'IRA à Saint-Pétersbourg…

## Cyberespions et trolls russes attaquent régulièrement tous les pays européens, y compris la France

### LA FRANCE EN LIGNE DE MIRE

Forts de leur succès américain, les agents russes ont ouvert parallèlement un quatrième front en Europe. Là encore, le but est limpide : diviser pour régner. *« Les Russes veulent détruire l'Union européenne pour la vassaliser, en exploitant les crises et en soutenant tous les extrêmes »,* analyse Cécile Vaissié, professeure en études russes à l'université de Rennes-2 et auteure d'un ouvrage sur *Les Réseaux du Kremlin en France* (Les Petits Matins). Cette bataille passe par des appuis – y compris financiers, via des banques et oligarques alliés – aux partis populistes ou nationalistes européens qui soutiennent les positions russes. Des contacts sont noués, notamment avec le parti de Viktor Orbán en Hongrie, avec Syriza et Aube dorée en Grèce, la Ligue de Matteo Salvini en Italie, l'AfD en Allemagne, le FPÖ en Autriche, le Front national en France. *« Le prêt de 9 millions d'euros accordé par la banque russe FCRB au Front national en 2014 s'inscrit dans cette stratégie »,* estime Joshua Kirschenbaum, chercheur associé à l'Alliance pour la sécurité de la démocratie, coauteur d'un rapport paru sur ce sujet en décembre 2018. Parallèlement, cyberespions et trolls attaquent tous les pays européens. Selon des données révélées par Twitter, près de 4 000 faux comptes russes, orchestrés par l'IRA, appuient la cause du Brexit le jour du référendum le 23 juin 2016, tandis que des hackers russes s'en prennent au réseau d'électricité britannique. En Allemagne, les services intérieurs, le BfV, accusent des agents du GRU d'avoir piraté en 2015 le site du Bundestag. En janvier 2016, alors que la crise des migrants fait rage outre-Rhin, les médias russes créent une *fake news* qui se répand sur les réseaux sociaux : Lisa, une adolescente germano-russe de 13 ans, aurait été kidnappée et violée par des migrants arabes à Berlin. En réalité, Lisa, disparue quelques heures, a été retrouvée le lendemain chez une amie…

### PETITS ARRANGEMENTS ENTRE ENNEMIS

En 2017 et 2018, les trolls russes s'activent également lors de la crise séparatiste en Catalogne et avant les élections générales en Allemagne, aux Pays-Bas et en Suède. Ces derniers mois, selon le laboratoire de recherche digitale du think tank américain Atlantic Council, ils ont propagé une série d'intox, dont un projet d'assassinat du leader britannique Boris Johnson par des opposants au Brexit ! *« La Russie interfère dans vos cerveaux, nous changeons vos consciences et vous ne pouvez rien*

Donald Trump a-t-il bénéficié de l'aide des hackers du Kremlin pour être élu ?

*contre cela »,* a ironisé, en février dernier, Vladislav Sourkov, conseiller de Poutine, à l'adresse des Occidentaux. La France n'y échappe pas. En avril 2016, des pirates russes liés au GRU mettent en berne les serveurs de TV5 Monde, la chaîne de télévision francophone, en se faisant passer pour un pseudo « Cyber-califat » de l'Etat islamique. Une diversion conçue pour accentuer le climat de peur en France consécutif aux attentats terroristes. Comme aux Etats-Unis, les Russes veulent ensuite affaiblir le candidat à la présidentielle qu'ils abhorrent le plus, en l'occurrence Emmanuel Macron, jugé trop atlantiste et pro-européen. Des rumeurs sur son homosexualité présumée se répandent, relayées notamment via la chaîne Sputnik. Début mai 2017, des milliers d'e-mails de l'équipe de campagne d'En Marche ! fuitent sur les réseaux sociaux. Officiellement, les autorités françaises se refusent à accuser qui que ce soit. *« Il faut être prudent sur les attributions d'attaque cyber, car les preuves manquent »,* juge Kevin Limonier. Néanmoins, des détails techniques orientent les regards vers des hackers russes, probablement sous tutelle du GRU.

Durant la crise des "gilets jaunes", de curieux comptes Twitter s'activent aux heures de bureau à Moscou

La campagne de déstabilisation ne s'arrête pas là. Des hashtags virulents anti-Macron se répandent, avec un pic fin 2018 lors de la crise des « gilets jaunes ». La chaîne RT France ouvre son antenne aux manifestants, avec des audiences records. De curieux comptes Twitter, très actifs aux heures de bureau de Moscou, relaient tout ce qui peut envenimer la situation, sans qu'il soit possible d'en mesurer l'impact réel. Parmi les plus prolixes, un certain «@DupontAllan3 », compte ouvert en août 2018 et suspendu début 2019, a produit plus de 40 000 tweets, chiffre inhabituel, qui paraissent provenir d'une usine à trolls. *« Les Russes n'ont pas créé ce mouvement social, mais ils ont essayé d'amplifier son retentissement »,* avance Baptiste Robert, un chercheur en sécurité informatique qui suit de près ces tweets. *« Ils font tout pour polariser les opinions publiques »,* ajoute un expert français qui a repéré d'autres comptes suspects sur Twitter.

### FAUX COMPTES ET VRAIS TROLLS

En novembre 2018, Facebook a fait fermer 11 comptes Instagram en français, au comportement jugé *« non authentique »* et *« coordonné »,* autrement dit des faux comptes. Leurs profils étaient variés : l'un défendait les femmes musulmanes, un deuxième les ultras de football, un troisième se présentait comme trotskiste, d'autres comme écologistes ou nationalistes. Leur audience cumulée (70 000 followers) était encore limitée, mais leurs slogans anti-Macron de plus en plus explicites. *« Il s'agissait sans doute de tests russes pour une future utilisation politique, comme aux Etats-Unis avant 2016 »,* note Camille François. Ces actions d'influence peuvent sembler bénignes. Les services spécialisés français – DGSI, DGSE, tout comme →

TASS VIA GETTY IMAGES ; MAXIM SHEMETOV REUTERS ; AFP ; PABLO MARTINEZ MONSIVAIS/AP/SIPA

la DRSD, qui protège les sites et les entreprises liés à la défense – ne veulent pas envenimer les choses. *« Nous coopérons avec les Russes contre les filières djihadistes, notamment tchétchènes. Il ne faut pas casser cela »,* dit-on au sein d'un d'entre eux. Néanmoins, ces opérations russes empoisonnent le climat. *« Ils se servent de la désinformation et du piratage comme des armes de déstabilisation, en lien avec d'autres actes d'espionnage »,* dénonce un haut responsable français.

**BROUILLAGES ET PIRATAGES**

Fin 2017, un espion russe qui tentait de recruter à Paris un haut fonctionnaire a été prié par l'Elysée de quitter le territoire au plus vite, avant l'expulsion médiatisée, dans la foulée de l'affaire Skripal de mars 2018, de quatre autres pseudo-diplomates qui, selon *L'Obs* et *Le Monde,* avaient déjà été démasqués par la DGSI. Pour sa part, le ministère des Armées prend le sujet très au sérieux. En septembre, la ministre Florence Parly a fustigé un *« acte d'espionnage »,* après l'approche dans l'espace d'un satellite franco-italien de communications militaires par un satellite russe, Loutch-Olimp. *« Nos communications, nos manœuvres militaires, comme nos quotidiens, sont en danger si nous ne réagissons pas »,* a-t-elle averti. Par ailleurs, des microsatellites espions russes s'essaient régulièrement à du brouillage et du piratage de satellites militaires français. Florence Parly a aussi révélé, en février, une tentative d'intrusion dans les messageries de son ministère. Elle visait à perturber le réseau d'approvisionnement en essence des armées, principalement la Marine. Cette infiltration avortée a été attribuée au très secret groupe Turla.

Les experts en cybersécurité estiment que Turla est, en fait, contrôlé par les Russes. Sous-entendu : le GRU. *« Turla fait partie des groupes de hackers qui sont à l'œuvre depuis plus d'une décennie, avec des logiciels pirates très complexes, lesquels nécessitent des années de travail d'ingénieurs, donc des investissements importants qui relèvent des services russes »*, confie un initié français. Turla a déjà attaqué des satellites de communications et des dizaines de sites gouvernementaux, comme le Pentagone en 2008 ou le ministère allemand des affaires étrangères en 2017. Alors que le président Macron souhaite réchauffer ses relations avec Poutine, la confiance est minée par cette nouvelle guerre froide. ■

***Vincent Nouzille***

L'ombre du cyberespionnage planera sur la rencontre prévue entre Vladimir Poutine et Emmanuel Macron, le 19 août, au fort de Brégançon

**Vladimir Poutine et Emmanuel Macron : une entente cordiale menacée ?**

ÉTIENNE LAURENT/AP/SIPA