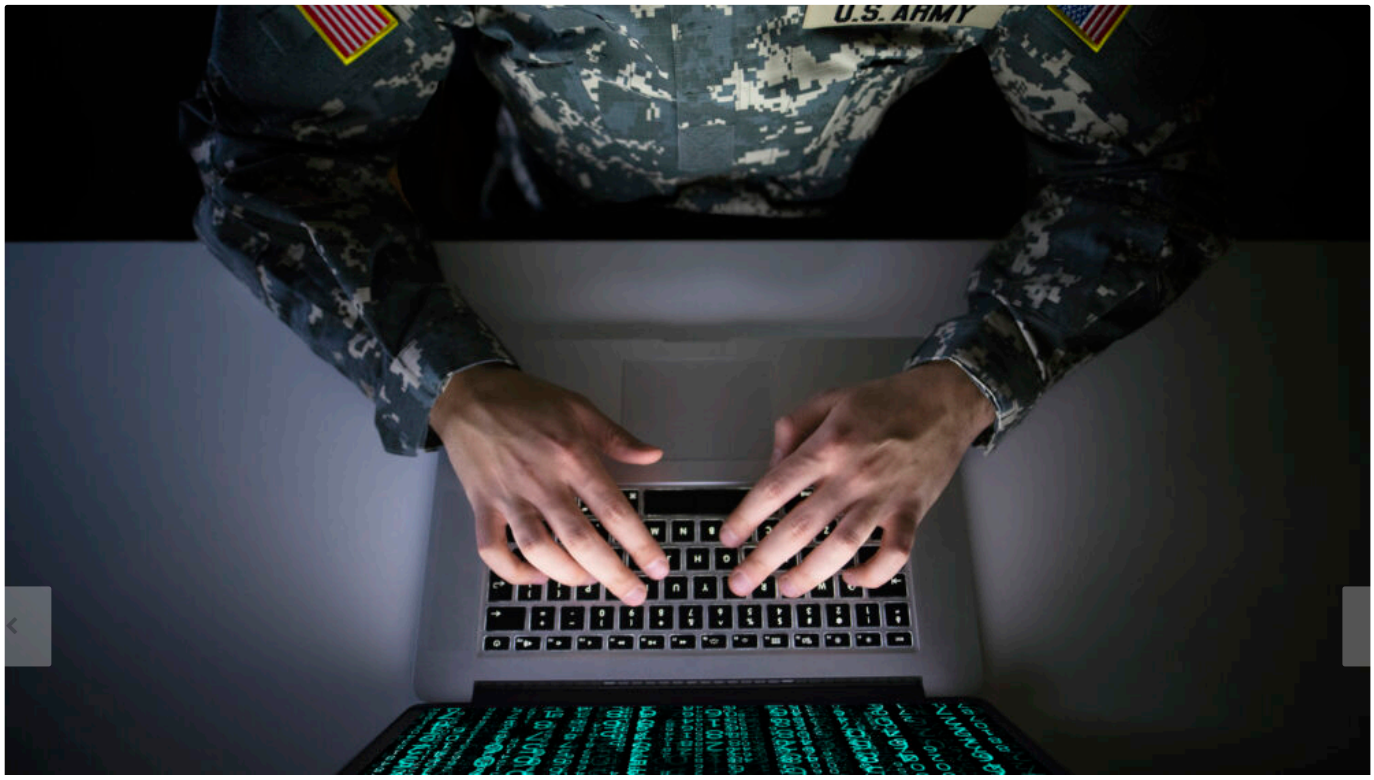
LE RUBICON

Le dispositif SIGINT américain, l'oracle qui a vu la guerre avant qu'elle ne survienne

Jonathan Guiffard | 8 novembre 2023



À la demande du président américain Joe Biden, le directeur de la *Central Intelligence Agency* (CIA), William Burns, s'est rendu à Moscou, début novembre 2021, pour délivrer des mises en garde au président russe Vladimir Poutine et aux responsables russes de la sécurité nationale. Il leur a révélé une partie des renseignements américains sur les intentions russes à l'égard de l'Ukraine, afin de dissuader le président Poutine d'envahir ce pays. Les éléments évoqués étaient si détaillés que plusieurs responsables russes auraient découvert la réalité des intentions de leur président lors de cette réunion.

Si cette anecdote donne à voir l'opacité qui règne au sein des cercles de décision russes, elle illustre surtout la très grande qualité des renseignements détenus par les agences de renseignement américaines en amont de la seconde invasion russe de l'Ukraine, le 24 février 2022. Toutefois, elle pourrait laisser penser que c'est grâce à la CIA, une agence particulièrement spécialisée dans le renseignement d'origine humaine (*HUMINT*), que le président Biden a été aussi bien informé. Dans cet article, je vais essayer de montrer que ce n'est vraisemblablement pas le cas. Avec cette crise, le directeur de la CIA (D/CIA) a retrouvé un rôle de centralisateur du renseignement, comme prévu lors de sa création en 1947 (« *Central* »), confirmé son rôle de « diplomate de l'ombre » et repris une importance de premier plan auprès du président américain, en complément du directeur national pour le renseignement (DNI) ; mais ce sont d'autres sources de renseignement qui semblent avoir permis aux États-Unis d'avoir une certitude aussi grande et notamment les renseignements d'origine électromagnétique (*SIGINT*) collectés par l'agence de renseignement technique et cyber américaine, la *National Security Agency* (NSA). Ce rôle majeur de la collecte de données SIGINT et Cyber est renforcé, jour après jour, par la mise en données du monde et l'extension de l'espace numérique, imposant une rivalité avec la collecte par moyens humains, renforçant le rôle de la NSA et permettant le développement d'un vaste territoire numérique soumis à la surveillance américaine.

La puissance militaire et diplomatique américaine est aujourd'hui largement soutenue par sa capacité d'interception des signaux de communication et de navigation dans les flux de données. Avec la numérisation du monde, les avantages stratégiques conférés par ce dispositif sont très importants et ont renforcé la capacité des États-Unis à mener des stratégies où la place du

renseignement, SIGINT comme Cyber, est centrale. À ce titre, ces deux dimensions (SIGINT et cyber) seront évoquées en même temps, car elles sont étroitement liées sur les plans techniques et politiques, proximité illustrée par le double commandement (« *dual-hat* ») du directeur de la NSA sur l'*US Cyber Command*. Le SIGINT est une collecte passive de signaux électromagnétiques et de données, et le Cyber est une collecte plutôt active de signaux et de données. Cette distinction n'empêche pas la grande proximité entre ces deux dimensions, l'une et l'autre s'apportant un soutien mutuel dans le développement de leurs accès en renseignement.

Cet article est issu d'un terrain de recherche mené à Washington en février 2023 et nourri d'une vingtaine d'entretiens : des chercheurs spécialisés dans le cyber ou dans le renseignement dans des think tanks (*Center for Strategic and International Studies* (CSIS) ; Carnegie) ou des laboratoires de recherche (*Institute for Defense Analyses* ; Université George Washington), la plupart travaillant étroitement avec la NSA, mais aussi des entreprises de cybersécurité et des institutionnels américains (Maison-Blanche, département d'État, *US Army Cyber Command*, ancien directeur de la NSA). Ce terrain a été complété par un décryptage des fuites de documents classifiés américains, récents (*Discord Leaks*, 2023) comme anciennes (révélations d'Edward Snowden de 2013), toutes en mesure de donner des clés de compréhension sur les stratégies américaines de collecte de renseignement par moyens SIGINT et cyber.

Le SIGINT permet d'anticiper la guerre

Les renseignements déclassifiés et diffusés publiquement en amont de l'invasion évoquent une analyse fondée sur des faisceaux d'indices, notamment la nature du déploiement militaire russe observé par satellite aux frontières de l'Ukraine qui ne correspondait pas au seul prétexte de l'exercice conjoint *Zapad*, ce point illustrant l'importance de l'imagerie spatiale (*GEOINT*). Certains responsables américains expliquent aussi que le manifeste d'août 2021 du président Poutine déniant le droit d'autodétermination à l'Ukraine ou l'article pamphlétaire de Dimitri Medvedev contre l'Ukraine d'octobre 2021 illustrait clairement leur détermination à agir.

Aucun élément recueilli lors de ces recherches ne permet de produire une preuve formelle démontrant que le renseignement technique américain est parvenu à déterminer avec précision l'imminence de l'invasion russe. Malgré cela, plusieurs indices laissent supposer que le renseignement SIGINT et cyber collecté par l'agence américaine de renseignement, la *National Security Agency* (NSA), semble avoir joué un rôle déterminant.

Le premier indice se trouve dans une conférence donnée par l'amiral Tony Radakin, chef d'état-major de la défense britannique, le 14 décembre 2022, durant laquelle il remercie en premier ses collègues du renseignement militaire, mais surtout du *Government Communications Headquarters* (GCHQ, agence de renseignement technique britannique) et de la NSA, pour avoir permis d'anticiper la crise à venir, reléguant ses autres collègues du renseignement au second plan. Ce langage est révélateur, en creux, du rôle important joué par les agences de renseignement technique :

« *The Government has made Ukraine a priority […] That backdrop has been further supplemented by our magnificent intelligence community. Defence Intelligence and GCHQ, alongside American NSA colleagues, cued us at the very beginning and provided remarkably accurate windows into plans and psyche all the way through. People ask does it make a difference? Absolutely. And we have been able to spike guns, prepare plans and galvanise allies. Similarly, MI5 have been essential in keeping the home base safe at a point of tension. And, yes, MI6 do provide an astonishing array of insights and opportunities. Thank you to all in the UK Intelligence Community* ».

Ce premier indice est à relier avec un deuxième indice d'ordre politique. L'engagement très important, vocal et public, du gouvernement britannique dans la politique de dissuasion à l'égard de la Russie et de soutien sans faille à l'égard de l'Ukraine contraste particulièrement avec les gouvernements européens à la même période. J'émets l'hypothèse que le gouvernement britannique n'aurait pas mené une politique investissant autant de capital politique sur la seule base de renseignements humains américains (dont les conditions d'évaluation de la fiabilité sont par nature peu partagées, même entre alliés). En revanche, à l'image des propos ci-dessus, cette politique pourrait s'expliquer plus logiquement si elle est effectivement fondée sur des renseignements techniques collectés ensemble par le GCHQ et la NSA. Mon raisonnement est le suivant : les Américains ont été les premiers à avertir publiquement et fortement de l'imminence de l'invasion, en octobre 2021. Les Britanniques ont poursuivi cette politique à la même période. Ni les États européens, ni l'Ukraine, ni d'autres pays n'ont pris cette position politique, se montrant sensiblement plus prudents. J'émets ainsi l'hypothèse que les Britanniques n'auraient jamais pris ce chemin politique,

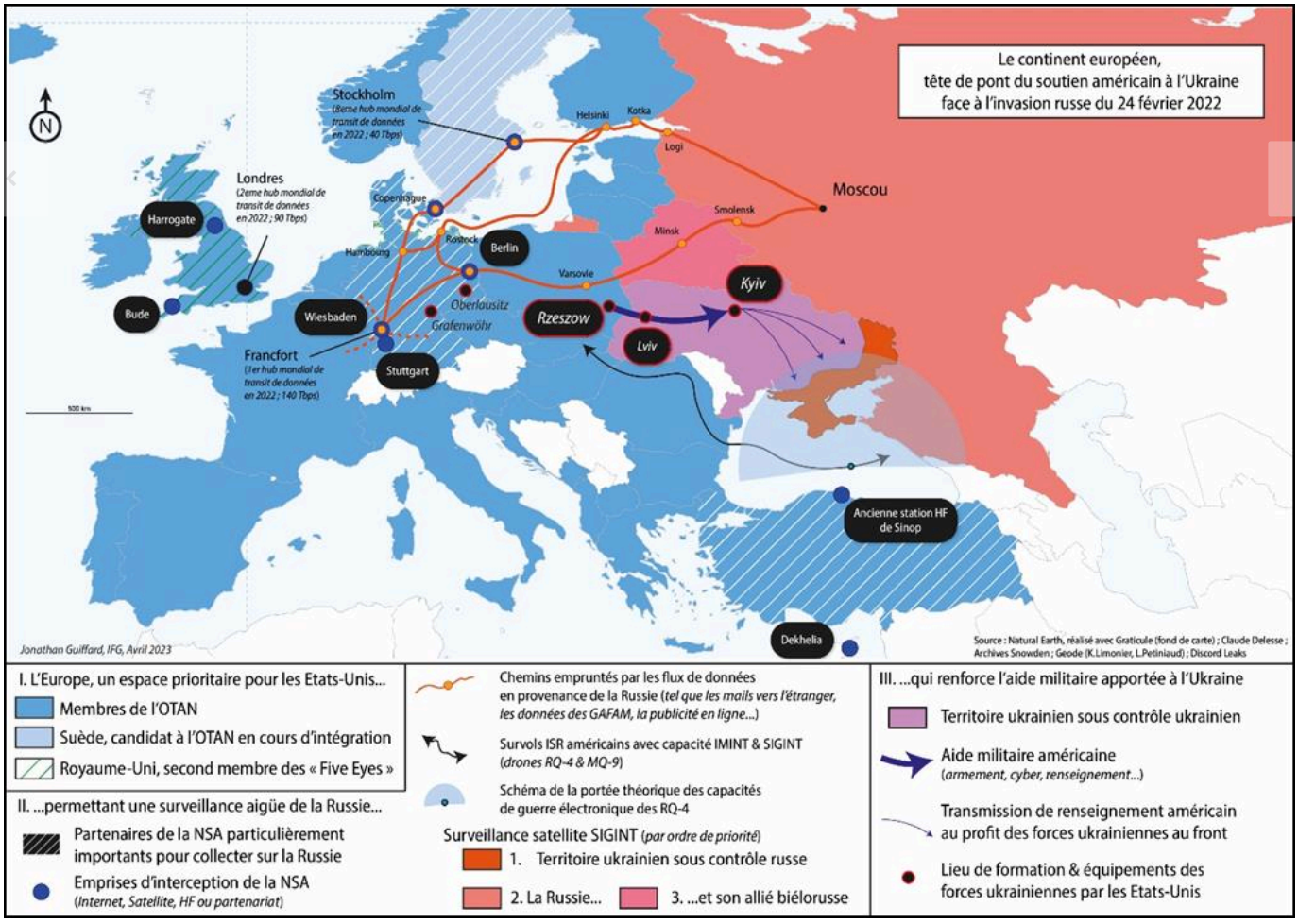
sans un renseignement convaincant et obtenu de source propre. Or, la collecte britannique par moyens SIGINT et cyber est largement mutualisée avec les Américains dans le cadre des accords UKUSA de 1946 et du réseau surnommé « Five Eyes » qui en découle. Grâce à cela, les Américains et les Britanniques ont vraisemblablement obtenu le même niveau de certitude sur les intentions russes.

En outre, un article de Politico du 24 février 2023 montre que si le D/CIA a eu un rôle très important sur le plan diplomatique, le directeur de la NSA (DIRNSA), le général Paul Nakasone, semble avoir apporté les renseignements permettant de convaincre les autorités politiques américaines, dès octobre 2021. Ce point transparaît aussi dans les propos rapportés de Victoria Nuland, sous-secrétaire d'État pour les affaires politiques : « *Everybody at the beginning was relatively skeptical — with the exception of the Canadians and the U.K., who were seeing the same intelligence that we were seeing because they're Five Eyes — that he would actually take this step* ».

Ce raisonnement me semble pleinement confirmé par les révélations issues de la diffusion de renseignements américains, en avril 2023, sur la situation en Ukraine (« *Discord Leaks* »). Les renseignements évoqués et les codes de classification associés confirment une pénétration d'ordre SIGINT ou cyber du ministère de la Défense russe par les services de renseignement américain. Ainsi, la NSA a vraisemblablement collecté les plans de planification de l'« opération militaire spéciale » et les ordres et intentions des responsables militaires russes dans ce cadre.

À titre d'illustration, la carte ci-dessous permet d'entrevoir et de représenter géographiquement les stratégies SIGINT américaines vis-à-vis de la Russie, notamment la place des alliances avec des pays européens. Il est aisé de comprendre qu'un dispositif complexe et complet, partiellement représenté ici, a été mis en œuvre pour collecter sur la Russie.

Figure 1 : Un soutien américain fort au cœur de l'Europe



L'importance de la collecte SIGINT dans ce conflit

En plus de son rôle dans l'anticipation de l'invasion, le SIGINT trouve une importance particulière dans la guerre. En effet, la collecte de renseignement sur les menaces et adversaires cyber est essentielle. Elle est permise par la pénétration des réseaux de l'adversaire, mais aussi par la mise en œuvre de dispositifs passifs de détection, essentiels dans la cyberdéfense. Ces

capacités de détection se trouvent décuplées par les capacités d'interception de masse de la NSA qui augmentent significativement la surface de scan.

James Lewis, directeur du programme des technologies stratégiques du think tank CSIS, pointe aussi l'importance de la pratique du SIGINT sur le champ de bataille. Ainsi, la maitrise du réseau ukrainien par les services de sécurité ukrainiens a permis un ciblage des unités russes par la détection de leurs activités GSM. L'apparition de carte-SIM russes ou biélorusses sur le réseau ukrainien dans des zones de déploiement des troupes russes a facilité leur ciblage. L'utilisation de matériels de communication de mauvaise qualité a aussi accru l'exposition des unités russes. James Lewis, directeur du programme sur les technologies stratégiques du think tank CSIS explique que si les forces spéciales russes semblaient bien utiliser du matériel de communication moderne et chiffré, il en était tout autrement du reste des unités déployées qui utilisaient des radios de marque chinoise, disposant d'un chiffrement de mauvaise qualité aisément déchiffrable par les capacités américaines.

À ce titre, il est important de comprendre que la NSA et les forces armées américaines n'ont pas besoin de se trouver sur le sol ukrainien pour collecter du renseignement technique sur les forces russes déployées et les transmettre aux forces armées ukrainiennes. En effet, partant du principe que la majorité des forces utilisent des moyens de communication HF/VUHF de mauvaise qualité, il est possible pour la NSA d'intercepter et déchiffrer ces communications à l'aide d'antennes de très longue portée déployées hors d'Ukraine, ou de satellites et d'aéronefs disposant de capacités SIGINT. La NSA dispose de l'ensemble de ces moyens. Aucune limite n'est soumise au survol des territoires russe et ukrainien par des satellites SIGINT et s'agissant des vecteurs aériens, plusieurs ont été observés autour de l'Ukraine à des portées permettant le recueil de signaux HF/VUHF : un document issu des « *Discord Leak* », daté du 27 février 2023, évoque 61 survols de drones américains en mer Noire entre septembre et février 2023.

James Lewis estime ainsi que les forces armées russes se sont avérées moins bonnes sur le plan défensif que ce qu'imaginaient les responsables américains de la sécurité nationale. Ceci est révélé en creux par les propos du DIRNSA qui confirme que la NSA et le CYBERCOM ont mené des opérations cyberoffensives contre des cibles russes pour soutenir l'effort de guerre ukrainien.

La réussite du SIGINT américain est permise par une surveillance de longue date

Les fondations de l'appareil américain de renseignement et de sécurité nationale ont été construites dans le cadre de l'émergence de la Guerre froide et de la confrontation entre les États-Unis et l'Union soviétique. Le projet Venona est la première pierre d'une stratégie américaine de collecte et d'analyse du renseignement technique contre l'URSS. Cette histoire nourrit encore les représentations de la NSA – qui met en lumière cette histoire dans son musée de cryptologie, en rappel d'un ADN lié à la menace soviétique.

Les raisons de la signature de l'accord UKUSA en 1946, entre les États-Unis et le Royaume-Uni, et de l'inclusion dans ce réseau *Five Eyes* du Canada (1948), de l'Australie (1956) et de la Nouvelle-Zélande (1956), sont liées à la menace soviétique perçue comme globale. Les capacités d'interception HF des forces armées offertes par les stations d'écoute déployées au Canada ou dans différents territoires de l'Empire et du Commonwealth britannique justifiaient pour les autorités américaines de mutualiser les capacités SIGINT. La dimension territoriale du SIGINT est ici claire. Elle est très importante, car les signaux comme les données disposent bien d'emprises physiques de transit ou de stockage. La pratique du SIGINT est alors une stratégie technologique et territoriale mise en œuvre pour intercepter ou collecter le maximum de signaux d'intérêts, comme aujourd'hui dans l'espace numérique. Cette logique persiste aujourd'hui : l'action des autorités russes est scrutée dans son espace régional (Europe de l'Est, Caucase, Asie centrale), mais aussi en Syrie, en Libye et désormais dans de nombreux pays africains. L'amiral Mike Rogers confirme que, si les cercles politiques américains ont baissé leur vigilance à l'égard de la Russie dans les années 1990-2000, la NSA n'a jamais arrêté de considérer la Russie comme un adversaire prioritaire à surveiller.

Les fuites orchestrées par Edward Snowden confirment son propos et permettent de lire que la Russie est restée une cible stratégique de la NSA. Un document dénommé « *United States SIGINT System January 2007 Strategic Mission List* » détaille la liste des missions et cibles stratégiques définies par le DIRNSA pour l'année 2007, incluant 16 missions thématiques critiques et six cibles durables qui nécessitent pour la NSA de « travailler sur ces cibles de manière holistique en raison de leur importance stratégique ». La Russie est parmi les six « cibles durables » et dans 10 des 16 missions thématiques, elle est aussi citée comme objectif prioritaire, parmi lesquelles les menaces balistiques et nucléaires, la prévention des conflits régionaux, les opérations informationnelles, la modernisation militaire et les technologies émergentes ou le contre-espionnage.

Enfin, un document daté du 15 février 2006, issu de la newsletter interne de la NSA « SID Today », indique que 35% des ressources de l'*U.S. SIGINT System* sont dédiées à la guerre globale contre le terrorisme, 35% aux quatre cibles persistantes que sont la Chine, la Corée du Nord, l'Iran et la Russie, 20 % au reste du monde et 10% sont dédiées au développement.

Le rôle fondamental du SIGINT dans le pouvoir topologique américain

Le pouvoir topologique exprime « la façon dont des acteurs peuvent se rendre présents et projeter de la puissance dans différents lieux, de façon plus ou moins forte, et cela quelles que soient les distances géographiques en jeu ». Cette notion identifie un pouvoir politique qui s'exprime non plus sur un territoire défini, topographique, mais à travers des réseaux et flux de pouvoirs.

Dans ce cadre, l'espace numérique est un espace traversé par des flux d'informations, de données et de pouvoirs, au sein duquel la position américaine, centrale et dominante, permet au gouvernement américain d'exercer un pouvoir topologique très important. La NSA est un acteur fondamental du renforcement et de l'animation de ce pouvoir topologique, auprès de ses partenaires (Ukraine) ou de ses adversaires (Russie). En effet, ce système de collecte de renseignement est dirigé depuis un territoire circonscrit, la région de Washington DC., par un pouvoir politique à travers des ordres hiérarchiques et des orientations de recherche de renseignement.

Dans le cadre d'une relation hiérarchique, verticale et démocratique entre le pouvoir politique et la NSA, cet effet est logique et bénin. Cette réflexion prend une autre dimension dès lors que la NSA devient l'outil d'une puissance exercée à l'étranger par ce pouvoir politique. Il constitue un dispositif essentiel du pouvoir topologique américain, car il permet au gouvernement américain d'obtenir des avantages stratégiques grâce aux renseignements collectés et partagés à un allié : ce partage est un transfert d'informations, l'exercice d'un pouvoir topologique. L'engagement dans le cyberespace et le soutien en renseignement aux Ukrainiens permettent aussi l'exercice d'un pouvoir topologique à l'encontre des acteurs russes qui ressentent la présence américaine et son pouvoir d'atteinte.

Ce renforcement du pouvoir topologique américain est structuré autour d'une autonomie stratégique et d'une libre navigabilité dans l'espace numérique, mais aussi d'une contrainte imposée à ses adversaires et compétiteurs par un engagement persistant et l'obtention d'avantages stratégiques. Il est aussi permis par une influence forte exercée auprès de ses partenaires par des relations d'interdépendance : ainsi, dans le cas de l'Ukraine, le volume et la qualité du renseignement transmis par les Américains ont participé à la survie des institutions et soutiennent des dynamiques ukrainiennes victorieuses. Les responsables politiques et militaires deviennent dépendants des capacités américaines, jusqu'aux infrastructures (cloud, satellites de communication). En retour, les Américains saisissent l'opportunité d'un partenariat renforcé avec l'Ukraine depuis 2014 pour se protéger, notamment dans le cyberespace. La connaissance mutualisée entre les Américains et les Ukrainiens de la menace cyber russe est essentielle dans la stratégie de protection du territoire américain. Les dépendances sont réciproques.

Les chocs géopolitiques, comme la prise de la Crimée par la Russie, en mars 2014, ou l'invasion russe de février 2022, sont des opportunités pour les services de renseignement d'étendre leur pouvoir d'atteinte et d'accroître leur marge d'action. Ainsi, au-delà de l'intérêt immédiat ou opérationnel, une crise géopolitique dans lequel un État s'engage activement offre toujours l'opportunité d'approfondir la portée et le périmètre de collecte des services de renseignement. L'attribution de nouvelles ressources et l'engagement demandé à la NSA et au CYBERCOM de soutenir les Ukrainiens, par le pouvoir politique américain, permet à ces acteurs de s'engager dans des opérations d'espionnage ou de sabotage plus nombreuses et plus risquées, ce qui accroît mécaniquement leur territoire numérique. L'extension du territoire numérique de la NSA en Ukraine et en Russie, à la lumière de la guerre, se complète ainsi d'un gain d'expérience important et d'un renforcement global (annonce d'un recrutement de plus de 3000 personnels en janvier 2023) susceptible de renforcer ses propres opérations de collecte ou de sabotage dans l'espace numérique et d'améliorer sa position auprès d'autres partenaires.

Conclusion

La guerre en Ukraine donne à voir l'importance du renseignement dans l'anticipation et la conduite politico-militaire d'un conflit, à l'aune de la numérisation exponentielle du monde. Dans ce cadre, une stratégie puissante de collecte de renseignement dans l'espace numérique, mais aussi de reconnaissance et d'action contre des adversaires dans le cyberespace, devient un outil

essentiel pour les États. Une politique forte en la matière pourrait participer du réveil stratégique européen, en premier lieu dans une dimension défensive, puis en second lieu pour s'affirmer face à des impérialismes autocratiques et à des alliés peu soucieux des souverainetés européennes. Cette politique pourrait commencer par la mise en place d'une alliance SIGINT et Cyber entre les pays de l'Union européenne : la mutualisation de capacités pourrait hypothétiquement offrir un volume très important de renseignements. Des pays en pointe sur les capacités SIGINT/Cyber comme la France, l'Allemagne, les Pays-Bas ou l'Estonie pourraient porter cet effort commun. Au moins une alliance existe déjà : il s'agit de la coopération surnommée MAXIMATOR. Toutefois, celle-ci ne rassemble que cinq pays européens et constitue un forum d'échange de renseignements SIGINT et de percées cryptographiques. En ce sens, tout comme les coopérations SIGINT existantes dans des cadres bilatéraux (France-Allemagne) ou multilatéraux (OTAN), il ne s'agit pas d'une réelle politique de mutualisation. L'effet de levier est susceptible d'être obtenu par la mutualisation de capacités d'interception, de collecte, de déchiffrement et d'exploitation. La centralité du territoire européen dans les flux de communications est, à ce titre, un atout essentiel. La protection privée des données des citoyens est une nécessité qui ne peut pas être le seul domaine d'engagement des Européens dans l'espace numérique : la dimension stratégique est tout aussi essentielle.

Photo : Smederevac

Jonathan Guiffard a également été l'invité du podcast Le Collimateur que vous pouvez retrouver ci-dessous :

The episode was not found or is unavailable.

•— ••— — • ••— •—• •••

Jonathan Guiffard

Jonathan Guiffard (@joeguiffard) est chercheur indépendant, doctorant à l'Institut Français de Géopolitique (Paris 8) et *Senior Fellow* à l'Institut Montaigne. Ses travaux académiques portent sur les stratégies dans l'espace numérique des acteurs américains du renseignement et du cyber. Auparavant, il a travaillé 12 ans dans des ministères régaliens, développant une connaissance approfondie des enjeux diplomatiques et militaires en Afrique de l'Ouest et au Moyen-Orient, ainsi qu'une expertise des politiques publiques dans ce domaine.

Comment citer cette publication

Jonathan Guiffard, « Le dispositif SIGINT américain, l'oracle qui a vu la guerre avant qu'elle ne survienne », *Le Rubicon*, 8 novembre 2023 [https://lerubicon.org/le-dispositif-sigint-americain-loracle-qui-a-vu-la-guerre-avant-quelle-ne-survienne/].