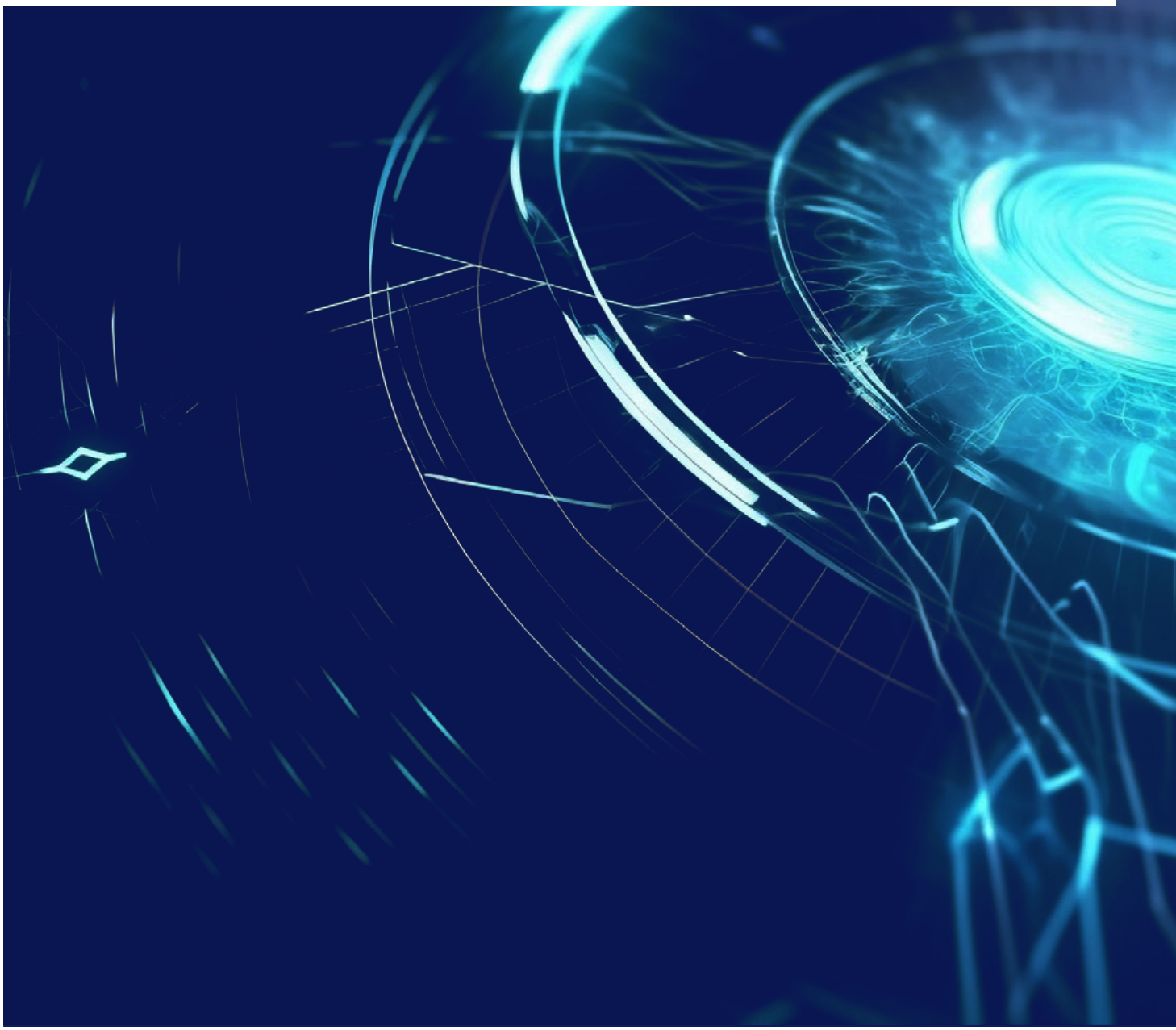
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #100

Février 2024

100E ÉDITION DU « FLASH INGÉRENCE » DE LA DGSI



Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes.

Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Il est également disponible sur le site internet : **www.dgsi.interieur.gouv.fr**

Par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à :

securite-economique@interieur.gouv.fr

100E ÉDITION DU « FLASH INGÉRENCE » DE LA DGSI

Créé en juillet 2012, le « flash ingérence » de la DGSI a connu de multiples évolutions mais sa vocation est restée inchangée : accompagner les acteurs économiques publics et privés dans la diffusion d'une culture de sécurité et les sensibiliser aux risques liés aux ingérences étrangères. En s'appuyant sur des cas réels dont le service a pu avoir connaissance, le « flash ingérence » a toujours veillé à proposer des préconisations accessibles au plus grand nombre et simples à mettre en œuvre.

D'abord diffusé de façon ponctuelle, le « flash ingérence » de la DGSI a adopté son format mensuel à partir de janvier 2016. Au cours de l'année 2020, durant le premier confinement lié à la crise sanitaire, le « flash ingérence » est même brièvement devenu une publication hebdomadaire afin d'accompagner tous les acteurs économiques dans l'évolution de leurs modes de travail et de les alerter sur les nouveaux risques présentés par la dématérialisation accrue des échanges professionnels.

Dans ses différentes publications, le « flash ingérence » a couvert toute l'étendue des modes opératoires auxquels les acteurs étrangers offensifs ont recours afin de cibler les intérêts français. Certaines thématiques ont été couvertes à plusieurs reprises au cours des douze dernières années, témoignant du renouvellement de méthodes de renseignement anciennes, adaptées à de nouveaux enjeux technologiques et aux évolutions des activités économiques. Le service a ainsi couvert les thématiques des ingérences d'origine humaine, cybernétique, juridique ou encore économique. Certains numéros du « flash ingérence » sont aussi revenus sur les risques de captation du patrimoine matériel et immatériel dans le cadre d'opérations d'espionnage économique, mais aussi sur les atteintes à la réputation ou encore sur les vulnérabilités liées à des failles bâtimentaires.

Pour sa 100e édition, ce « flash ingérence » revient sur six cas d'ingérence économique emblématiques qui soulignent la grande diversité des approches étrangères dont peuvent faire l'objet des entreprises stratégiques françaises, parfois avec la complicité de services de renseignement étrangers.

1 TENTATIVE D'ESPIONNAGE ÉCONOMIQUE À L'ENCONTRE D'UNE SCIENTIFIQUE FRANÇAISE

Titulaire d'un doctorat dans un domaine technologique de pointe, une scientifique française a été recrutée par une PME française spécialisée dans la sous-traitance de grands groupes industriels stratégiques. La scientifique a été approchée sur les réseaux sociaux par une ressortissante étrangère se présentant comme consultante pour un cabinet de conseil.

La scientifique française et la consultante étrangère se sont rencontrées à plusieurs reprises dans le cadre d'entretiens supposés porter sur un travail de prospection économique en France mené par la consultante. Toutefois, les entretiens se sont peu à peu orientés vers des questions portant sur la vie personnelle et professionnelle de la ressortissante française, toujours dans un climat convivial.

À la suite de plusieurs rencontres, la consultante a posé à la scientifique française des questions très précises sur son activité et lui a finalement demandé de lui remettre des documents internes de la PME pour laquelle elle travaillait. La consultante a par ailleurs laissé un appareil électronique devant elle lors du rendez-vous, donnant l'impression à la scientifique d'être filmée ou enregistrée.

Face à cette situation, la scientifique n'a plus donné suite aux demandes insistantes de rendez vous de la consultante et a rapporté les faits à la direction sûreté de sa PME. Informée par la PME, la DGSI a pu établir que la consultante étrangère appartenait à un service de renseignement étranger.

Commentaires

En s'appuyant dans un premier temps sur des informations disponibles sur Internet et les réseaux sociaux, l'agent de renseignement étranger a peu à peu noué une relation de confiance avec la scientifique française, cherchant au travers de rendez-vous successifs à bâtir une relation sur le long terme, tout en appréciant le niveau d'information et l'expertise de la scientifique française.

En se rapprochant d'une experte qualifiée travaillant pour un sous-traitant de groupes industriels français stratégiques, l'agent de renseignement étranger espérait obtenir des renseignements sur les projets industriels d'un secteur sensible. Par cette opération, un État étranger a tenté de capter des informations stratégiques, probablement dans le but d'en faire bénéficier son gouvernement mais aussi ses propres entreprises nationales, concurrentes immédiates de la société française employant la scientifique française.

La bonne communication entre la scientifique française, la direction sûreté de son employeur et la DGSI a permis d'entraver, rapidement après le signalement, les agissements de l'agent de renseignement étranger.

2 INTRUSION DANS LES TÉLÉPHONES PORTABLES DE DEUX SALARIÉS D'UNE SOCIÉTÉ FRANÇAISE LORS D'UN CONTRÔLE AÉROPORTUAIRE À L'ÉTRANGER.

Alors qu'ils s'apprêtaient à rentrer en France à la suite d'un événement à l'étranger auquel ils avaient été conviés dans un cadre professionnel, deux salariés d'une société française ont été interrogés durant plusieurs heures à l'aéroport par les autorités locales.

Ces entretiens ont notamment porté sur le déroulement de leur visite dans ce pays, leurs parcours professionnels respectifs et les contrats internationaux de leur société. Les agents locaux de l'aéroport ont notamment indiqué aux deux salariés français qu'ils étaient susceptibles d'être de nouveau interrogés lors d'un futur séjour dans ce pays, y compris si ce séjour se déroulait dans un cadre privé.

Les salariés ont été contraints de remettre aux agents leurs téléphones professionnels et personnels ainsi que leurs codes de déverrouillage. Les appareils ont été restitués à l'issue des interrogatoires, avec des traces évidentes d'intrusion dans leurs systèmes : les batteries des téléphones étaient totalement rechargées alors qu'elles ne l'étaient qu'à moitié avant les interrogatoires, les icônes avaient été déplacées et les menus de réglages avaient été configurés dans la langue du pays étranger.

Une analyse technique, conduite par la DGSI au retour des salariés en France, a permis de constater l'installation d'une application permettant la récupération des données de messagerie, d'appels, de navigation et de géolocalisation.

Le service a recommandé à la société l'usage d'appareils électroniques dédiés aux déplacements à l'étranger, afin de limiter le risque de captation d'informations en ne stockant sur ces appareils que les données nécessaires aux seuls besoins de la mission.

Commentaires

Le ciblage de ressortissants français travaillant pour des entreprises stratégiques lors de déplacements à l'étranger a fait l'objet d'une vigilance croissante de la part de la DGSI au cours des dernières années. Mode opératoire fréquemment utilisé par plusieurs États étrangers afin de collecter des renseignements sur leur territoire, le contrôle aéroportuaire présente un risque important en matière de captation de données ou de piégeage informatique.

Au cours des dernières années, la DGSI a régulièrement consacré des éditions du « flash ingérence » aux risques associés aux déplacements à l'étranger, qu'ils soient effectués dans un cadre public ou privé. De même, la thématique de la protection des données informatiques et des vigilances élémentaires liées au transport et à l'usage d'appareils électroniques a fait l'objet de nombreuses préconisations du service. La mise en place de bonnes pratiques avant, pendant et après chaque déplacement à l'étranger permet de limiter considérablement les risques d'ingérence étrangère.

3 SUSPICION DE COLLECTE ET DE TRANSFERT INDU DE DONNÉES PAR LE BIAIS DE DISTRIBUTEURS AUTOMATIQUES INSTALLÉS AU SEIN D'ENTREPRISES FRANÇAISES.

Un groupe industriel français a identifié des failles de sécurité liées à l'utilisation de distributeurs automatiques dotés de terminaux de paiement produits par un groupe étranger et installés dans les locaux de l'entreprise.

Un audit interne effectué au sein de l'entreprise a notamment permis de détecter la présence de plusieurs micros sur l'ensemble de l'équipement. À l'instar d'autres opérateurs de terminaux de paiement électronique, ces terminaux de paiement étaient également équipés de caméras.

L'analyse technique de ce matériel a permis de constater la présence d'interfaces de communication dans les terminaux de paiement (4G ou bluetooth) autorisant les maintenances à distance des équipements, mais rendant également possible la réactivation des caméras par le biais d'une reprogrammation.

Les terminaux de paiement installés sur ces distributeurs sont ainsi susceptibles d'avoir collecté et transféré des données par le biais des antennes présentes au-dessus des machines.

Commentaires

Cet exemple rappelle la grande diversité de risques auxquels une entreprise doit être préparée. Le choix de tout prestataire, qu'il s'agisse d'un sous-traitant industriel, d'une entreprise de maintenance ou d'un prestataire de service de restauration collective, doit être étudié avec attention afin de limiter les risques d'ingérence. Si le prestataire est un intermédiaire de confiance, ses failles techniques ou organisationnelles peuvent toutefois être exploitées à des fins malveillantes par un acteur tiers dans une démarche de captation d'informations ou de sabotage.

Par ailleurs, ce type d'exemple rappelle l'impératif de prudence lors des conversations informelles susceptibles de révéler des données sensibles telles que le niveau d'avancement de certains projets, les problématiques rencontrées ou des tensions susceptibles d'être exploitées par un concurrent ou un État étranger. Dans ses publications du « flash ingérence », la DGSI rappelle régulièrement l'importance de la diffusion d'une culture de sécurité au sein des entreprises stratégiques, non seulement dans le cadre professionnel, mais aussi lors d'échanges informels ou dans un cadre privé.

4 UNE SOCIÉTÉ INNOVANTE FRANÇAISE EST CONFRONTÉE À D'IMPORTANTES DIFFICULTÉS FINANCIÈRES ET À UNE TENTATIVE DE TRANSFERT À L'ÉTRANGER DE SA TECHNOLOGIE À LA SUITE DE SON RACHAT PAR DES CAPITAUX ÉTRANGERS.

Une entreprise innovante française est progressivement passée sous contrôle étranger par le biais de son actionnaire majoritaire, contrôlé par un groupe étranger. Le dirigeant de l'entreprise, de nationalité étrangère, a progressivement acquis son contrôle exclusif sans toutefois apparaître directement au sein de la structure actionnariale et de la gouvernance de l'entreprise.

Dans un second temps, le dirigeant a mis en place des politiques tarifaires avantageuses en faveur d'acteurs économiques étrangers, parmi lesquels des sociétés qu'il détenait lui-même directement ou indirectement. Il a également laissé s'accumuler de nombreux arriérés de paiement auprès de certains clients. Cette gestion a fragilisé la société française, dont le niveau d'endettement a progressivement menacé sa pérennité.

Dans un troisième temps, le dirigeant a cherché à organiser le transfert à l'étranger de la technologie et des savoir-faire les plus sensibles de l'entreprise. À cette fin, il a notamment embauché des ingénieurs étrangers pour répertorier l'intégralité des plans et données relatives aux procédés industriels de la société. Il a également tenté d'envoyer à l'étranger des cadres et ingénieurs de la société française, détenteurs de savoir-faire stratégiques, pour qu'ils participent à la duplication de la technologie.

Informé de ce projet contraire à la préservation du potentiel scientifique et technique de la Nation, la DGSI a entravé le départ des ingénieurs à l'étranger et le projet de transfert de technologie du dirigeant étranger de la société. Les ingénieurs ont été mis en garde contre les conséquences, notamment pénales, induites par un transfert de technologies à l'étranger.

Commentaires

Le travail de lutte contre les ingérences étrangères, mené au quotidien par la DGSI, vise à garantir la préservation des intérêts fondamentaux de la Nation par le biais d'une action de détection et d'entrave. Ce cas emblématique de tentative de captation et de transfert d'une technologie française particulièrement sensible vers l'étranger témoigne de l'intérêt appuyé de certains acteurs étrangers offensifs pour l'innovation et le savoir-faire français, et des moyens importants dont ils disposent.

La DGSI détecte régulièrement des cas similaires, susceptibles de concerner à la fois le monde industriel et le monde de la recherche. La perte de certaines avances technologiques, de savoir-faire industriels ou de connaissances de pointe dans le domaine de la recherche est susceptible d'affecter à la fois la compétitivité française à l'étranger mais aussi le rayonnement du pays dans le domaine scientifique. Face à cette menace, la sensibilisation accrue de tous les acteurs économiques, industriels et scientifiques par la DGSI permet la détection précoce de signaux faibles susceptibles d'annoncer les prémices d'une ingérence étrangère, et la conduite d'actions d'entrave appropriées.

5 UN CHERCHEUR FRANÇAIS SPÉCIALISÉ DANS UNE TECHNOLOGIE AUX APPLICATIONS DUALES SUSCITE L'INTÉRÊT MARQUÉ D'UN ÉTAT ÉTRANGER QUI CHERCHE À DÉTOURNER SON SAVOIR-FAIRE.

Un chercheur français est régulièrement amené à se rendre dans un pays étranger où il dispense des cours dans le cadre de partenariats établis entre son laboratoire de recherche et des universités locales. Après plusieurs années, le chercheur français est identifié par les autorités du pays étranger comme un expert de son secteur, qui dispose d'applications multiples pour le domaine militaire.

Dans le but de faire bénéficier leur programme militaire du savoir-faire de pointe du chercheur français, les autorités du pays étranger ont cherché à l'associer à leurs programmes de recherche sensibles. À l'occasion de séminaires, le chercheur a été encouragé par les autorités étrangères à évoquer des sujets militaires alors que son intervention était initialement centrée exclusivement sur des thématiques civiles. Lors de rencontres professionnelles, le chercheur français a été invité à s'installer dans le pays étranger, accompagné de toute sa famille, pour travailler à temps complet dans une université locale spécialisée dans des thématiques aux applications duales.

En lien avec les autorités de tutelle du laboratoire français du chercheur, la DGSI l'a sensibilisé aux risques de détournement ou de transfert non-contrôlé du savoir-faire du laboratoire vers un État étranger sur des thématiques duales. Face à la sensibilité de travaux du chercheur et de son laboratoire, la DGSI a encouragé la mise en place d'une zone à régime restrictif (ZRR) dans les locaux du laboratoire.

Commentaires

Les déplacements à l'étranger de chercheurs issus de laboratoires de haut niveau sont essentiels au rayonnement de la recherche française. De même, les partenariats entre universités françaises et étrangères permettent d'enrichir les échanges entre enseignants, doctorants et étudiants tout en valorisant l'excellence de la recherche française. Toutefois, ces échanges permettent aussi à certains États étrangers d'identifier les talents français et de les cibler lorsqu'ils sont sur leur territoire afin qu'ils mettent leur savoir au profit de tentatives de rattrapage technologique. Lorsque ces technologies disposent d'applications duales, les chercheurs et laboratoires français courent alors un risque important de transfert non contrôlé de savoir-faire.

Dans le cadre du dispositif de protection du potentiel scientifique et technique de la Nation (PPST), la mise en place de zones à régime restrictif (ZRR) permet de protéger les savoir-faire les plus sensibles d'un laboratoire ou d'une entreprise française en soumettant leur accès à une autorisation ministérielle. Les ZRR permettent le maintien des échanges internationaux tout en protégeant efficacement l'accès aux savoirs et en exposant les contrevenants à des poursuites pénales.

6 ESPIONNAGE INDUSTRIEL À TRAVERS LA COMPROMISSION DE TÉLÉPHONES MOBILES

Des entités industrielles françaises œuvrant sur un secteur d'activité particulièrement concurrentiel ont été ciblées par une campagne d'espionnage. Une attaque informatique a été lancée à l'encontre de plusieurs dirigeants et cadres de ces entités, permettant l'introduction d'un logiciel espion dans leurs téléphones portables. L'attaque est survenue à une période critique pour ces entités, qui finalisaient certains projets structurants et cherchaient à obtenir des contrats à l'international sur un marché fortement concurrentiel.

Indétectable lors de l'utilisation quotidienne des téléphones, ce logiciel malveillant a eu un accès constant à l'ensemble du contenu et aux flux des téléphones ciblés sur une période particulièrement longue. En effet, les individus ciblés par cette attaque n'ont découvert l'existence du logiciel espion que plusieurs mois après la compromission, à la suite de la réception d'une notification du fabricant de leur téléphone. Des anomalies de fonctionnement de leur appareil avaient en effet été détectées par les équipes techniques du fabricant, permettant d'adresser une alerte aux utilisateurs.

Informée des faits, la DGSI a constitué, en lien avec ses partenaires nationaux, une équipe spécialisée afin de mener des analyses techniques sur les appareils compromis. Les résultats de l'enquête ont notamment permis de déterminer la date de la compromission, la durée et le type de l'attaque.

La sophistication de l'attaque, sa complexité de mise en œuvre et les moyens nécessaires pour exploiter les données recueillies sur une longue période de temps laissent supposer que l'entité à l'origine de l'attaque a pu bénéficier d'un soutien étatique ou avoir eu recours à une société spécialisée.

Commentaires

La compromission de téléphones mobiles peut permettre la mise en œuvre de nombreuses actions malveillantes : accès facilité au réseau interne de la structure visée, accès à la liste des contacts professionnels, aux données de géolocalisation, aux messages échangés y compris via des messageries sécurisées, aux courriers électroniques, mais aussi activation à distance de la caméra et du micro. En outre, ces attaques peuvent s'étendre sur une période de temps particulièrement longue en raison de leur caractère parfois indétectable, constituant ainsi une vulnérabilité majeure pour une entreprise.

Les téléphones mobiles constituent une cible privilégiée pour de telles attaques en raison des nombreuses informations sensibles qui y sont échangées et de leur niveau de protection souvent insuffisant au regard des informations qu'ils hébergent. Utilisés au quotidien, mêlant souvent informations personnelles et professionnelles, les téléphones portables doivent être considérés comme des appareils à haut risque de compromission, à la fois pour les données qu'ils contiennent et pour leur proximité physique permanente avec leurs utilisateurs, amenés à échanger tout au long de la journée à proximité de leurs appareils. Des précautions simples à mettre en œuvre permettent toutefois de réduire considérablement ces risques.

LE « FLASH INGÉRENCE », UN OUTIL DE SENSIBILISATION DE LA DGSI

En 2023, **chaque « flash ingérence » a en moyenne été consulté près de 80 000 fois,** suscitant environ 1 000 réactions. Le taux moyen d'engagement des « flash ingérence » de la DGSI sur LinkedIn[1] est de 24 %. La publication sur le site Internet de la DGSI et la création d'une page LinkedIn dédiée à la direction ont permis une plus large diffusion des « flash ingérence ».

À l'approche de la 100e édition du « flash ingérence », la DGSI a adressé un questionnaire à un certain nombre de ses lecteurs visant à recueillir leur avis et à mieux répondre aux attentes en adaptant son format au plus près des préoccupations de ses destinataires. Certains lecteurs assidus ont été sollicités pour donner des idées de sujets à traiter, parmi lesquels :

1. Les problématiques liées à l'intelligence artificielle et les conséquences en matière d'ingérence pour l'entreprise ;
2. Les atteintes à la réputation et autres tentatives de déstabilisation informationnelle ;
3. Les déplacements à l'étranger, notamment à l'occasion de salons professionnels ;
4. Les nouvelles formes de « fraudes au président » et leurs conséquences pour les entreprises ;
5. Les problématiques de propriété intellectuelle ;
6. La sécurité numérique.

Dans ses prochains numéros, le service s'attachera à revenir sur ces thématiques, en les actualisant au regard des signalements les plus récemment détectés par les agents de la DGSI.

Le contenu du « flash ingérence » vient par ailleurs appuyer les conférences de sensibilisation collectives conduites par la DGSI auprès des acteurs économiques nationaux qui en font la demande (entreprises, administrations, établissements d'enseignement supérieur et de recherche, associations, etc.). En 2023, **la DGSI a ainsi conduit plus de 1 000 conférences de sensibilisation** en métropole et dans les outre-mer sur les questions de sécurité économique, auprès d'un public représentant plus de 50 000 personnes.

[1] *Le taux d'engagement est un indicateur permettant de mesurer le nombre d'interactions suscitées par un contenu sur un réseau social comparativement à sa portée, au nombre d'abonnés et à la taille de l'audience touchée. La moyenne générale d'engagement d'une publication LinkedIn est inférieure à 5 %.*

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité