ChatGPT

Intelligence des médias sociaux (SOCMINT)

Le **SOCMINT** (Social Media Intelligence) désigne l'ensemble des méthodes et outils permettant de collecter et d'analyser les données issues des réseaux sociaux. Il s'agit d'une branche de l'OSINT (Open-Source Intelligence) spécialisée dans les médias sociaux [1] [2]. Selon la définition du Wikipedia français, le SOCMINT se charge de la collecte et de l'analyse des informations provenant des réseaux sociaux, permettant par exemple « la surveillance des tendances, l'identification des comportements suspects [et] le suivi des événements en temps réel » [3]. Comme le note la fondation Privacy International, ce terme est parfois confondu avec l'OSINT, mais la différence cruciale est que *l'OSINT* ne traite que des données strictement publiques, alors que *le SOCMINT* peut s'étendre à des contenus partiellement privés (groupes fermés, posts destinés à une audience limitée) [4] [5]. En d'autres termes, le SOCMINT exploite des échanges sur les réseaux sociaux – textes, images, vidéos, interactions – en utilisant des méthodes intrusives ou non, sur des plateformes ouvertes comme fermées [2] [4]. Cette analyse inclut l'utilisation d'algorithmes et de graphes sociaux pour révéler les relations, les tendances d'opinion et les comportements en ligne, fournissant ainsi des renseignements plus « granuleux » que les sources OSINT traditionnelles.

1. Définitions et distinction avec l'OSINT

Le **SOCMINT** est souvent présenté comme une sous-discipline de l'OSINT qui se concentre exclusivement sur les données issues des réseaux sociaux [1] [2]. Il consiste à « recueillir et analyser les données publiques des réseaux sociaux » afin d'en extraire des tendances et des informations exploitables [2] [6]. Pour certains, la nuance la plus importante réside dans l'intention de l'information. L'OSINT classique s'appuie uniquement sur des contenus librement accessibles, tandis que le SOCMINT peut impliquer des techniques d'accès à des contenus destinés à un public restreint (par ex. rejoindre un groupe privé, créer un faux profil) [7] [4]. De ce fait, le SOCMINT pose des questions spécifiques de vie privée : comme le note Privacy International, « il existe une différence clé » entre SOCMINT et OSINT – le SOCMINT « peut être déployé sur du contenu privé ou public, alors que l'OSINT porte uniquement sur du contenu strictement public » [4]. Des analystes critiquent d'ailleurs cette situation : SOCMINT permet un niveau de surveillance plus intrusif, « car il surveille les gens lorsqu'ils interagissent et se détendent dans leur espace de confort numérique » [5] [4].

2. Origine et historique du SOCMINT

Le concept de SOCMINT s'est formalisé au début des années 2010. Le terme **« SOCMINT »** a été introduit en 2012 par Sir David Omand, Jamie Bartlett et Carl Miller dans un rapport du think-tank londonien Demos [8]. Les auteurs soulignaient déjà que l'omniprésence des médias sociaux justifiait d'intégrer le SOCMINT dans le cadre du renseignement national, à condition toutefois de garantir « des méthodes rigoureuses et une gestion responsable du risque moral » [9] [8]. À partir de cette formalisation, les agences de renseignement et de sécurité ont progressivement développé des capacités d'écoute et d'analyse sociales. Par exemple, dès 2011, la police britannique a mobilisé des analystes pour suivre les manifestations anti-fracturation hydraulique via Twitter, Facebook et YouTube [10]. Du côté de la société civile, l'évolution du SOCMINT s'est également accélérée, notamment après le scandale Cambridge Analytica (2018), qui a montré l'impact politique de l'exploitation massive des données sociales sans consentement [11]. Aujourd'hui, le SOCMINT est devenu un champ

multidisciplinaire, intégré dans les stratégies de renseignement, de sécurité nationale, mais aussi d'étude de marché ou de veille sociétale.

3. Méthodes et techniques utilisées

Les enquêtes SOCMINT combinent plusieurs techniques d'analyse des données massives. On peut notamment citer :

- **Collecte automatisée (scraping/API)** : extraction de données via les API publiques des plateformes (Twitter, Reddit, etc.) ou par *scraping* de pages Web (crawl). Par exemple, on utilise des scripts pour parcourir de façon répétée les posts et commentaires publics [12] [13]. Cette étape brasse de grandes quantités d'informations brutes.
- **Traitement du langage naturel (NLP)** : analyses linguistiques et statistiques sur le texte des publications. Cela inclut la reconnaissance d'entités nommées (personnes, organisations), la détection de *topics* et surtout l'analyse de sentiment (positif/négatif) pour évaluer l'opinion publique [14] [15]. Les algorithmes d'apprentissage automatique (machine learning) permettent de classifier des contenus, de détecter des thématiques émergentes et même d'anticiper des tendances. L'IA joue un rôle clé : comme le note Brand24, on recourt fréquemment au « traitement du langage naturel et à l'apprentissage automatique » pour traiter de grands volumes de textes sociaux et en extraire des informations [16] [15].
- **Analyse de graphes sociaux** : cartographie des relations entre utilisateurs (followers, mention, hashtags). Les outils de graphe (e.g. Maltego) visualisent les connexions entre individus, adresses mail, domaines, etc. Cela permet d'identifier les influenceurs clés et les communautés organisées [17] [18]. On repère ainsi comment l'information se diffuse dans le réseau, qui est au centre des échanges et quelles entités sont reliées.
- **Analyse multimédia (images/vidéos)** : extraction d'informations à partir de contenus visuels. Les techniques de vision par ordinateur (OCR, reconnaissance d'objets ou de visages) détectent du texte dans les images, identifient des lieux ou objets significatifs, et repèrent des correspondances géographiques (géolocalisation par repères visuels). Par exemple, une photo géotaggée peut indiquer un lieu précis. Comme le souligne une source militaire, le SOCMINT intègre « la vision par ordinateur » pour analyser de grandes quantités de données sociales [18].
- **Géolocalisation et informations temporelles** : exploitation des métadonnées (horodatage, coordonnées GPS) pour reconstituer les déplacements ou la chronologie d'une personne ou d'un événement.
- **Data mining et intelligence artificielle avancée** : clustering, modèles prédictifs, détection de bots ou de campagnes automatisées, basées sur l'analyse combinée de signes socio-techniques. Par exemple, on utilise des LLM (comme ChatGPT) ou d'autres IA pour résumer ou traduire automatiquement des flux sociaux, ou pour analyser des données multilingues.

En résumé, le SOCMINT mobilise des techniques mixtes – des scripts de collecte aux algorithmes avancés – afin de transformer le « bruit » des réseaux sociaux en renseignements exploitables. Ces méthodes requièrent souvent une expertise humaine pour filtrer les données, valider les résultats et éviter les fausses interprétations.

4. Outils et plateformes disponibles

Le SOCMINT dispose d'un large éventail d'outils, du plus simple au plus sophistiqué, gratuits comme payants :

- **Outils open-source/gratuits** : par exemple, **Sherlock** (outil Python en ligne de commande) cherche automatiquement un nom d'utilisateur sur plus de 400 réseaux sociaux [19]. **Maltego Community Edition** offre une interface graphique pour tracer des graphes de relations (personnes, mails, comptes sociaux, etc.) [20]. **SpiderFoot** est un framework d'OSINT/SOCMINT multiplateforme (200+ modules) qui collecte des données sur IP, domaines, comptes, etc. [21]. Des utilitaires comme Twint (pour Twitter) ou Instaloader (pour Instagram) permettent de récupérer des posts sans utiliser l'API officielle. Ces outils facilitent la veille sur les médias sociaux en exploitant les interfaces publiques disponibles.
- **Plateformes commerciales et SaaS** : il existe aussi des solutions tout-en-un. Par exemple, **Brand24** collecte toutes les mentions publiques d'un mot-clé sur les réseaux sociaux et fournit une analyse de base (y compris de sentiment) [22]. **Hootsuite Insights**, **Brandwatch** et **NetBase Quid** offrent des tableaux de bord avancés de veille sociale (analyse de réputation de marque, suivi de concurrents, détection de tendances) [23] [24]. Ces services – souvent basés sur de l'analyse NLP et des statistiques en temps réel – s'intègrent à de multiples plateformes sociales pour fournir des rapports d'entreprise. D'autres outils utilisés en veille média (Meltwater, Talkwalker, Synthesio, Sprinklr, etc.) permettent également de monitorer de façon transversale les réseaux sociaux et le web. Enfin, les API des réseaux sociaux (Twitter API, Facebook Graph API) restent des ressources stratégiques pour les analystes disposant des droits d'accès nécessaires.

Chaque outil a ses forces et limites : les solutions open-source demandent souvent plus de configuration et de compréhension technique, tandis que les solutions commerciales facturent l'accès à des bases de données enrichies et des analyses clés en main.

5. Domaines d'application

Le SOCMINT est utilisé dans de nombreux secteurs :

- **Sécurité et renseignement** (militaires, agences nationales, police) : évaluation en temps réel de menaces, suivi d'organisations extrémistes, prévention d'attentats. Par exemple, les forces armées et les services de renseignement exploitent le SOCMINT pour « suivre les mouvements militaires » lors de conflits récents [25]. Le FBI a notamment recours au SOCMINT pour « surveiller les menaces et enquêter sur des activités criminelles, en analysant les publications, images et vidéos susceptibles d'indiquer des actes illégaux ou des préoccupations de sécurité » [26]. Les polices nationales utilisent également l'analyse des réseaux sociaux pour anticiper les rassemblements dangereux, protéger les citoyens et enquêter sur les crimes.
- **Marketing et commerce** : les entreprises l'emploient pour la veille de marque, l'analyse de la satisfaction client et la conception de campagnes publicitaires. Le SOCMINT permet de détecter en temps réel les tendances et les sentiments du public vis-à-vis d'un produit ou d'une marque [6]. Par exemple, des marketeurs surveillent les mentions de leur marque sur Twitter et Facebook pour adapter leurs stratégies. Selon Hootsuite, le SOCMINT aide les équipes marketing à « suivre la réputation de leur marque », à identifier des influenceurs et à comprendre les besoins des consommateurs [6] [27].
- **Médias, ONG et société civile** : journalistes et organisations non gouvernementales l'utilisent pour surveiller l'actualité, détecter des crises humanitaires ou analyser l'opinion publique. Des ONG de santé publique se servent du SOCMINT pour suivre la propagation de rumeurs

épidémiologiques sur les réseaux sociaux, ce qui peut informer des campagnes de santé publique. Les associations de défense des droits de l'homme l'emploient pour recenser des témoignages ou des abus diffusés en ligne. Globalement, « les agences publiques suivent les risques pour la sécurité, la santé et l'environnement, tandis que les ONG identifient les besoins communautaires et les journalistes repèrent les sujets émergents » [27] .

- **Prévention et crise** : en cas de catastrophe naturelle ou de crise politique, le SOCMINT fournit une situation en temps réel (p. ex. mécontentement sur Twitter, appels à l'aide géolocalisés). Par exemple, les autorités peuvent repérer rapidement des alertes citoyennes (villes inondées, mouvements sociaux) grâce à l'analyse des flux sociaux.
- **Finance et autres secteurs** : certaines entreprises financières surveillent les réseaux pour repérer des fraudes ou anticiper des mouvements de marché basés sur le buzz social. De même, la veille des actions d'entreprises ou de secteurs d'activité peut s'appuyer sur le SOCMINT pour déceler des tendances économiques.

6. Études de cas récentes et internationales

Plusieurs cas concrets illustrent l'usage du SOCMINT :

- **Scandale Cambridge Analytica (2016, Royaume-Uni/USA)** : cette affaire a montré l'impact d'un SOCMINT non éthique. La société Cambridge Analytica a acheté sans consentement les données Facebook de 50 millions d'utilisateurs pour influencer la campagne présidentielle américaine de 2016 [11] . Cet exemple souligne les enjeux de la manipulation politique via les réseaux sociaux.
- **Manifestations anti-fracturation (2011, Royaume-Uni)** : la police britannique a surveillé en temps réel les discussions en ligne lors de protestations contre le fracturing hydraulique et l'abattage de blaireaux [10] . Des équipes dédiées ont suivi hashtags et vidéos YouTube pour anticiper et gérer la sécurité publique.
- **Surveillance de mouvements sociaux (#BlackLivesMatter, USA)** : la société ZeroFOX a été critiquée en 2015 pour avoir remis à des autorités locales un rapport qualifiant plusieurs militants #BlackLivesMatter de « menaces potentielles », suscitant un tollé quant à la définition des « acteurs de menace » [28] . Ce cas montre comment le SOCMINT peut être controversé lorsqu'il s'applique à des activistes.
- **Forces de l'ordre (2023, États-Unis)** : le département de police de Philadelphie a récemment commencé à utiliser les réseaux sociaux pour traquer de présumé criminels et prévenir des cambriolages [29] . Cette initiative récente illustre la tendance croissante des forces de l'ordre à utiliser le SOCMINT pour agir rapidement sur le terrain.
- **Guerre en Ukraine (2022–2023)** : durant le conflit russo-ukrainien, l'OSINT (dont fait partie le SOCMINT) a joué un rôle clé. Les analystes ont suivi en temps réel les mouvements de troupes et vérifié des informations en pistant des posts publics (images satellites amateur, vidéos de drones sur Twitter, etc.), ce qui a aidé à « dissiper le brouillard de guerre » [25] .

Ces exemples – parmi d'autres (crises sanitaires, attentats, manipulations électorales) – montrent que le SOCMINT est utilisé tant par des acteurs étatiques que non étatiques à l'échelle internationale, avec des résultats parfois spectaculaires mais aussi contestés.

7. Enjeux éthiques et juridiques

Le SOCMINT soulève d'importantes questions éthiques et juridiques liées à la vie privée et aux libertés. Même si les données proviennent des réseaux sociaux, des contraintes juridiques s'appliquent :

- **Vie privée et droits fondamentaux** : le RGPD (Europe) et la jurisprudence européenne imposent que la collecte de données personnelles soit « légale, nécessaire et proportionnée ». La

collecte massive ou ciblée d'informations sur des individus peut engager le droit à la vie privée. Par exemple, la Cour européenne des droits de l'Homme rappelle qu'il existe « une zone d'interaction d'une personne avec d'autres qui, même dans un contexte public, peut relever de la vie privée » [30] . Autrement dit, un enregistrement automatisé et systématique de contenus – même publics – peut violer l'article 8 de la CEDH si l'intérêt privé des personnes n'est pas respecté [30] [31] . Les opérateurs SOCMINT doivent donc vérifier que leur collecte respecte les principes légaux (mandat judiciaire, consentement explicite, limitation du périmètre, etc.).

- **Consentement et conditions d'utilisation** : en Europe, la majorité des données sociales est « personnelle » selon le RGPD : leur traitement requiert en principe le consentement des utilisateurs. De plus, chaque plateforme définit des **Conditions Générales d'Utilisation (CGU)** interdisant souvent le scraping massif ou non autorisé. Gratter des données protégées contrevient à ces CGU et peut être illégal. Comme le notent les lignes directrices, « extraire des données de plateformes protégées peut violer les conditions d'utilisation » et même conduire à des poursuites (par ex. atteinte à la vie privée, harcèlement) [32] [31] . Les enquêteurs doivent donc se limiter aux informations accessibles publiquement selon les règles locales (réglementation RGPD, CCPA, etc.).
- **Cadre légal spécifique** : selon les pays, des lois sectorielles peuvent s'appliquer. Par exemple, l'**Investigatory Powers Act** (Royaume-Uni) ou le **CALEA** (USA) encadrent la surveillance numérique par les forces de l'ordre. En France, la loi impose que les activités de renseignement sur Internet soient justifiées et contrôlées (Commission nationale de contrôle, etc.). Les activités clandestines (faux profils, infiltration de forums privés) requièrent souvent des autorisations judiciaires spécifiques.
- **Transparence et responsabilité** : l'utilisation du SOCMINT par les gouvernements est parfois critiquée comme surveillante. Des cas comme l'affaire *Raza v. New York* (2018) ont montré que la police pouvait cibler indûment certaines communautés (ici, des musulmans) sous prétexte de contre-terrorisme [33] . De tels exemples révèlent les risques de profilage discriminatoire si le SOCMINT est mal encadré. Les analyses algorithmiques doivent être transparentes et accompagnées d'un contrôle humain pour éviter des faux positifs disproportionnés. En cas d'erreur (mésinterprétation d'un message, fausse accusation), les conséquences peuvent être graves (atteinte à la réputation, actions violentes ou diffamation).
- **Éthique professionnelle** : au-delà de la loi, les analystes SOCMINT sont soumis aux principes de nécessité et de proportionnalité. Privacy International rappelle que même les données accessibles publiquement doivent être traitées « en conformité avec les normes internationales de légalité, de nécessité et de proportionnalité » [31] . En pratique, cela signifie limiter la collecte au strict nécessaire, garantir la sécurisation des données, et éviter le sentiment d'être « espionné » auprès des citoyens.

8. Limites, critiques et controverses

Malgré ses promesses, le SOCMINT présente des limites techniques et suscite des controverses :

- **Limites techniques** : les outils SOCMINT ne peuvent *pas* accéder aux contenus privés (comptes protégés, messages privés, stories privées) sans autorisation explicite [34] . Autrement dit, ils dépendent entièrement des données publiques que les utilisateurs acceptent de partager. Si une personne n'est pas présente publiquement (ou utilise un pseudonyme), il peut être extrêmement difficile de la repérer. De plus, les contenus publics eux-mêmes peuvent être trompeurs : une photo géolocalisée n'indique pas forcément un déplacement (c'est peut-être une blague, un repost ou une vieille image) [35] . L'extraction de grandes quantités de données requiert aussi une analyse humaine experte : les outils SOCMINT identifient des patterns ou des corrélations, mais ils ne comprennent pas le contexte derrière un post. Toute conclusion nécessite donc une

vérification critique (comme le relève la doctrine : les données sociales « nécessitent encore une interprétation manuelle et une expertise humaine » [36]).

- **Respect de la loi** : comme indiqué, même des données en apparence publiques peuvent être protégées par le droit. Les outils ne doivent pas violer les CGU ni être utilisés pour harceler ou traquer illicitement une personne. Ainsi, outre les limites techniques, il existe des « frontières légales » : gratter aveuglément des contenus disponibles en ligne ne signifie pas que leur exploitation est éthiquement ou juridiquement acceptable [37]. L'utilisation abusive du SOCMINT (par ex. pour de la désinformation ou du harcèlement) peut exposer les enquêteurs à des poursuites.
- **Qualité et fiabilité des données** : les réseaux sociaux sont pleins de faux comptes (bots, trolls) et de désinformation. Il faut constamment valider et recouper les informations issues du SOCMINT. Par exemple, la surreprésentation de certains groupes démographiques sur les réseaux sociaux peut biaiser l'analyse d'opinion. L'interprétation des sentiments ou des tendances est imprécise (les sarcasmes sont difficiles à détecter par l'IA, les indicateurs manquent de précision, etc.). Ces limites sont soulignées par des experts : les outils ne fournissent pas de vérités absolues, ils informent, mais peuvent aussi induire en erreur s'ils sont mal utilisés [37].
- **Controverses éthiques** : le SOCMINT est parfois critiqué pour alimenter la surveillance de masse. Des cas concrets – comme celui de ZeroFOX, qui a suivi les communications #BLM – ont suscité des débats publics sur la frontière entre sécurité et liberté d'expression [28]. Le balance entre efficacité du renseignement et respect des droits civils reste un sujet sensible.

En somme, bien que puissant, le SOCMINT ne fait pas l'unanimité. Ses critiques portent sur l'empiètement sur la sphère privée, le risque d'abus (profilage illégal) et la nécessité de cadres de gouvernance robustes. Il s'inscrit dans un débat global sur la surveillance numérique où la transparence et la responsabilité sont essentielles.

9. Évolutions et perspectives

Le SOCMINT est en pleine évolution face aux avancées technologiques et aux changements sociétaux :

- **Intelligence artificielle** : les algorithmes continuent de s'améliorer. Les nouvelles techniques de traitement du langage (mégamodèles de type GPT) et de vision par ordinateur accroissent la capacité d'analyse automatique du contenu social. Comme le notent des experts militaires, « les outils tels que la science des réseaux, le traitement du langage naturel et la vision par ordinateur » sont de plus en plus exploités pour analyser de vastes volumes de données sociales [18]. À terme, des IA plus sophistiquées pourront repérer automatiquement des schémas complexes ou des campagnes de manipulation en ligne (par ex. détection de deepfakes ou d'opérations coordonnées), augmentant l'efficacité du SOCMINT.
- **Chiffrement et confidentialité renforcée** : en parallèle, la généralisation des applications de messagerie chiffrée (Signal, WhatsApp, Telegram « secret chats ») limite l'accès aux contenus. De plus en plus de personnes migrent vers des plates-formes privées ou décentralisées (Mastodon, Matrix, etc.), compliquant la veille. Ceci pousse les analystes à s'intéresser davantage aux métadonnées (fréquence de communication, réseaux d'interaction publics) et à intégrer des sources non-traditionnelles. À terme, l'équilibre évoluera entre la protection de la vie privée individuelle et la capacité des acteurs de sécurité à collecter du renseignement ouvert.
- **Réseaux décentralisés et nouvelles plateformes** : l'émergence de réseaux sociaux alternatifs (blockchain social, plateformes anonymes) oblige les praticiens du SOCMINT à élargir leur champ d'action. Ces nouveaux médias, parfois plus fragmentés, nécessitent des outils adaptés de recherche transverse. En revanche, ils restent souvent moins bien surveillés, créant de nouvelles opportunités d'extraction d'informations en accès public.

- **Régulation accrue** : dans les prochaines années, les législations devraient encadrer plus strictement le SOCMINT. L'Union européenne envisage déjà des régulations sur l'intelligence artificielle et la vie privée en ligne, ce qui affectera l'accès aux données publiques. On peut s'attendre à ce que les agences de renseignement et les entreprises renforcent leurs politiques internes (audit, transparence) pour éviter des abus.
- **Applications émergentes** : avec l'essor de l'analyse prédictive, le SOCMINT pourrait être utilisé pour anticiper des crises sociales ou des épidémies grâce à la corrélation de signaux faibles sur les réseaux. De plus, des collaborations multidisciplinaires (sociologie, linguistique, informatique) se développent pour interpréter les données sociales de façon plus contextuelle. Enfin, le SOCMINT pourrait tirer parti de l'Internet des objets et des villes intelligentes, en intégrant des données sociales à d'autres flux (données urbaines en temps réel, forêts de capteurs) pour une vision plus holistique de la sécurité et de l'environnement.

Sources : Ce dossier s'appuie sur des études académiques et des rapports spécialisés (e.g. Omand et al. 2012 [8]), des publications d'organisations comme Privacy International [4] [31], des analyses techniques (Maltego, netlas) [1] [20], ainsi que des exemples concrets rapportés par les médias et documents gouvernementaux [11] [28]. Les citations fournies illustrent les faits et définitions mentionnés.

---

[1] [7] Everything About Social Media Intelligence (SOCMINT) and Investigations
https://www.maltego.com/blog/everything-about-social-media-intelligence-socmint-and-investigations/

[2] [10] [11] [26] [28] [29] Social media intelligence - Wikipedia
https://en.wikipedia.org/wiki/Social_media_intelligence

[3] Délégation Régionale Académique au Numérique Éducatif
https://drane-versailles.region-academique-idf.fr/spip.php?rubrique201&lang=fr

[4] [12] [30] [31] [33] Social Media Intelligence | Privacy International
http://privacyinternational.org/explainer/55/social-media-intelligence

[5] [9] Social media intelligence: The national security-privacy nexus
http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S2224-00202022000100003

[6] [15] [27] Social media intelligence (SOCMINT): A 2025 guide for marketers
https://blog.hootsuite.com/social-media-intelligence/

[8] Social media intelligence — Wikipédia
https://fr.wikipedia.org/wiki/Social_media_intelligence

[13] [14] [17] Social Media Intelligence (Socmint): The Power Of Data Insights - Aim Technologies
https://www.aimtechnologies.co/2023/08/22/social-media-intelligence-socmint-unveiling-the-power-of-data-insights/

[16] [22] [23] [24] Qu'est-ce que le Social Media Intelligence (SOCMINT) ? | Brand24
https://brand24.com/blog/fr/quest-ce-que-lintelligence-des-medias-sociaux/

[18] [25] Social Media Intelligence (SOCMINT) | RMA Webinars
https://webinars.rma.ac.be/home/social-media-intelligence-socmint

[19] [20] [21] [34] [35] [36] [37] SOCMINT: Intelligence in the Social Media Era - Netlas Blog
https://netlas.io/blog/socmint/

[32] Social Media Intelligence (SOCMINT) in Modern Investigations
https://www.osint.industries/post/social-media-intelligence-socmint-in-modern-investigations