La guerre de Washington contre l'Iran : l'importance de défendre l'espace informationnel -

par **Brian Berletic**

Les États-Unis ont manifestement poursuivi leur guerre contre l'Iran en mettant en œuvre des plans élaborés de longue date visant à déstabiliser le pays par le biais de manifestations soutenues par les États-Unis et d'attaques terroristes armées visant les grandes villes pendant plusieurs jours.

Cela fait suite à une guerre de près de deux semaines que les États-Unis et leurs mandataires israéliens ont lancée contre l'Iran à la mi-2025, qui n'a été suspendue que pour mieux préparer la prochaine vague de déstabilisation et d'agression militaire, qui semble se dérouler actuellement.

Au milieu des troubles organisés par les États-Unis en janvier 2026, ces derniers ont ouvertement soutenu l'opposition, appelant les militants armés à poursuivre leurs opérations et même à s'emparer des institutions gouvernementales.

L'*Associated Press* citerait le président américain comme ayant déclaré : «*Continuez à manifester et prenez le contrôle de vos institutions si vous le pouvez*», et «*l'aide est en route*», en référence aux précédentes menaces de frappes militaires américaines contre l'Iran pour soutenir l'opposition.

Au-delà du soutien rhétorique, des preuves de l'implication directe des États-Unis ont commencé à faire surface dans les médias occidentaux.

Dans un article récent, la *BBC* a admis, enfoui au fin fond du rapport, que «*des forces de sécurité ont également été tuées*», laissant entendre la présence d'éléments lourdement armés au milieu des soi-disant «manifestations». Le même article admettait que les informateurs qui contactaient la *BBC* depuis l'Iran utilisaient les connexions satellitaires «Starlink», en référence au réseau de communication par satellite de la société américaine SpaceX.

Alors que le monde multipolaire se réunit pour discuter de la coopération dans les domaines traditionnels de la sécurité nationale, il est urgent de protéger l'espace informationnel mondial de l'influence et du contrôle des États-Unis.

Cela n'a rien de surprenant. Dès 2022, *CNN* a rapporté que «*la Maison-Blanche avait entamé des discussions avec Elon Musk sur la possibilité de mettre en place le service Internet par satellite Starlink de SpaceX en Iran*», comme l'un des moyens de «soutenir le mouvement de protestation iranien».

Plus récemment, Forbes a admis que «*des dizaines de milliers d'unités Starlink fonctionnent en Iran*», ce qui montre à quel point l'initiative de l'administration Biden a été mise en œuvre de manière agressive, puis poursuivie sous l'administration Trump qui lui a succédé.

Au-delà de la continuité du programme entre les administrations présidentielles prétendument «*opposées*», les plans visant à soutenir les troubles violents en Iran ont été élaborés par les décideurs politiques américains dès 2009 dans le document de la Brookings Institution intitulé «*Which Path to Persia ?*» (Quelle voie vers la Perse ?) et mis en œuvre de manière transparente par chaque administration successive, indépendamment de son affiliation politique ou de son discours de campagne.

Le document contient des chapitres entiers intitulés «*La révolution de velours : soutenir un soulèvement populaire*» et «*Inspirer une insurrection : soutenir les minorités et les groupes d'opposition iraniens*», ainsi qu'un chapitre intitulé littéralement «*Laisser faire Bibi : Autoriser ou encourager une frappe militaire israélienne*», dans lequel il est déclaré que «*les États-Unis encourageraient, voire aideraient, les Israéliens à mener eux-mêmes les frappes, dans l'espoir que les critiques internationales et les représailles iraniennes se détournent des États-Unis pour se concentrer sur Israël*», un scénario qui s'est déroulé mot pour mot au milieu de l'année dernière.

En ce qui concerne les troubles orchestrés par les États-Unis, le document de 2009 propose de recourir à des organisations terroristes étrangères (FTO) répertoriées par le département d'État américain, notamment le Mujahedin-e Khalq (MEK), que le document reconnaît comme étant très impopulaire en Iran, ayant tué des citoyens et des militaires américains dans les années 1970 et a très certainement commis d'autres actes terroristes depuis, mais qu'elle devrait être retirée de la liste des FTO afin que les États-Unis puissent lui apporter un soutien plus important et plus ouvert.

En 2012, le MEK a été retiré de la liste sous l'administration Obama après des années de lobbying de la part des néoconservateurs qui allaient plus tard former la première administration du président Donald Trump.

En ce qui concerne les autres groupes actuellement impliqués dans les troubles en Iran, le document de 2009 indiquait que «*les États-Unis pourraient choisir de travailler principalement avec divers groupes ethniques iraniens mécontents (Kurdes, Baloutches, Arabes, etc.) qui ont combattu le régime à différentes périodes depuis la révolution. Une coalition de mouvements d'opposition ethniques, en particulier si elle est combinée avec des dissidents persans, constituerait une menace sérieuse pour la stabilité du régime. En outre, les troubles créés par ces groupes pourraient affaiblir le régime à l'intérieur du pays*».

C'est précisément ce qui se passe aujourd'hui en Iran.

Malgré les préparatifs en vue d'une subversion interne et de frappes militaires américaines directes contre l'Iran, qui remontent non seulement aux administrations Biden et Trump, mais aussi aux administrations Bush Jr. et Obama, l'Iran a résisté à ces tentatives pendant des années et semble avoir été au moins partiellement préparé à la dernière vague de troubles orchestrée par les États-Unis.

L'article de Forbes cité ci-dessus rapporte que l'Iran a réussi non seulement à fermer les services Internet utilisés par les militants soutenus par les États-Unis pour coordonner leurs actions et communiquer avec leurs sponsors étrangers, mais aussi à brouiller de manière intensive les terminaux Starlink dans les régions critiques.

Le même article spéculait que le succès de l'Iran pouvait être attribué au transfert des capacités de guerre électronique russes perfectionnées lors de la guerre par procuration menée par les États-Unis en Ukraine, où Starlink a également été largement utilisé.

Ces développements soulignent la priorité de sécuriser et de défendre l'espace informationnel

national, un espace qui, au XXIe siècle, constitue un domaine de sécurité nationale aussi critique que l'espace aérien, les frontières terrestres et les côtes d'un pays. Ne pas le faire s'est avéré catastrophique.

L'utilisation de l'espace informationnel comme arme par les États-Unis au XXIe siècle

Tout au long du XXIe siècle, les États-Unis ont délibérément et malicieusement utilisé leur domination sur l'espace informationnel mondial comme une arme, en particulier par le biais de plateformes de médias sociaux basées aux États-Unis telles que X (anciennement Twitter), Meta/Facebook, YouTube, Google, Instagram et bien d'autres.

Dès 2011, le *New York Times* a admis que le soi-disant «printemps arabe» était en fait une campagne de déstabilisation régionale planifiée et préparée de longue date, organisée par le gouvernement américain et ses partenaires dans le secteur des grandes technologies.

Dans son article intitulé «*Des groupes américains ont contribué à alimenter les soulèvements arabes*», il admettait que «*selon des entretiens menés ces dernières semaines et des câbles diplomatiques américains obtenus par WikiLeaks, un certain nombre de groupes et d'individus directement impliqués dans les révoltes et les réformes qui ont balayé la région ont reçu une formation et un financement de la part de groupes tels que l'International Republican Institute, le National Democratic Institute et Freedom House, une organisation à but non lucratif de défense des droits humains basée à Washington*».

L'article admettait également qu'un certain nombre de groupes d'opposition impliqués avaient participé à «*une réunion sur les technologies organisée en 2008 à New York, où ils avaient appris à utiliser les réseaux sociaux et les technologies mobiles pour promouvoir la démocratie. Parmi les sponsors de cette réunion figuraient Facebook, Google, MTV, la Columbia Law School et le département d'État*».

En fait, cette «réunion sur les technologies» s'est tenue chaque année pendant plusieurs années et s'est appuyée sur l'expérience acquise par le gouvernement américain lors d'interventions politiques similaires menées entre 2000 et 2004 dans des pays tels que la Serbie, la Géorgie, la Biélorussie et l'Ukraine.

En 2004, le *Guardian* reconnaissait que les manifestations en cours à Kiev à l'époque étaient «*une création des États-Unis, un exercice sophistiqué et brillamment conçu de branding occidental et de marketing de masse qui, dans quatre pays en quatre ans, a été utilisé pour tenter de sauver des élections truquées et de renverser des régimes indésirables*».

Il a également admis que «*la campagne a été utilisée pour la première fois en Europe à Belgrade en 2000 pour battre Slobodan Milosevic aux urnes. Richard Miles, l'ambassadeur américain à Belgrade, a joué un rôle clé. Et l'année dernière, en tant qu'ambassadeur américain à Tbilissi, il a répété le même stratagème en Géorgie, en apprenant à Mikhaïl Saakachvili comment renverser Edouard Chevardnadze. Dix mois après le succès de Belgrade, l'ambassadeur américain à Minsk, Michael Kozak, un vétéran d'opérations similaires en Amérique centrale, notamment au Nicaragua, a organisé une campagne presque identique pour tenter de vaincre l'homme fort de la Biélorussie, Alexandre Loukachenko*», ce qui, comme l'admet l'article, a échoué.

Ainsi, de 2000 à 2004, les États-Unis ont tenté de renverser en série des gouvernements ciblés en Europe de l'Est, En 2011, les États-Unis ont affiné ces techniques pour réduire en cendres une grande partie du monde arabe, puis ont réussi à renverser et à plonger le pays d'Ukraine dans une guerre par procuration destructrice à partir de 2014, tandis que l'année dernière, ils ont renversé le gouvernement du Népal, à la frontière avec la Chine, et tentent désormais ouvertement d'utiliser ces mêmes tactiques, associées à la menace d'une agression militaire ouverte, pour renverser le gouvernement iranien.

Alors que les analystes ont documenté la disparité croissante entre les États-Unis et la puissance industrielle militaire de la Russie et de la Chine, les États-Unis ont conservé une domination presque incontestée sur l'espace informationnel mondial. Si l'on considère la vague de déstabilisation, de mort et de destruction que les États-Unis ont provoquée en Afrique du Nord, en Asie et partout ailleurs au cours du XXIe siècle, cela a plus que compensé leur manque de production industrielle militaire. La domination américaine en matière d'information s'est avérée être une menace pour le monde au moins aussi importante, sinon plus, que la menace militaire toujours redoutable des États-Unis.

La menace américaine sur l'espace mondial de l'information nécessite une Défense mondiale

Au fil des ans et grâce à un travail considérable, la Russie et la Chine ont sécurisé leurs espaces d'information respectifs. Cela leur a permis de sécuriser et de stabiliser leur espace politique, créant ainsi l'harmonie sociale nécessaire non seulement pour survivre aux tentatives incessantes des États-Unis d'encercler et de contenir ces deux puissances mondiales, mais aussi, dans de nombreux cas, pour prospérer.

Ce résultat a été obtenu grâce à la création d'alternatives nationales aux plateformes de réseaux sociaux américaines qui, sans cela, domineraient l'espace mondial de l'information. Ces deux pays disposent de réseaux en ligne qui peuvent être déconnectés de l'espace de l'information influencé par l'Occident si nécessaire.

Au-delà de cela, les deux pays ont créé des filières nationales garantissant que les ressources humaines essentielles, telles que les programmeurs et les techniciens nécessaires au maintien de l'infrastructure physique de leur espace d'information, soient formées dans le pays et dans l'intérêt supérieur de la nation, ainsi que le personnel des médias, les fonctionnaires et autres agents publics qui utilisent l'espace d'information de chaque pays.

Cela n'est pas sans rappeler les infrastructures physiques construites au sein de tout pays souverain. Les routes, les chemins de fer, les aéroports et les ports maritimes sont tous reconnus comme faisant partie intégrante de la sécurité nationale, et leur construction, leur entretien, leur utilisation et leur protection sont donc déterminés en conséquence.

Malheureusement, de nombreux décideurs politiques à travers le monde n'ont pas encore compris que l'espace informationnel au XXIe siècle est aussi important, sinon plus, que ces infrastructures physiques ou les domaines traditionnels de la sécurité nationale.

Permettre aux États-Unis non seulement de fournir aux pays des plateformes de médias sociaux basées aux États-Unis plutôt que de laisser les pays développer les leurs, mais aussi de contrôler le flux d'informations et donc les idées et le consensus sur ces plateformes est aussi grave, voire pire, que de permettre à des intérêts étrangers de contrôler les frontières physiques, les infrastructures et même les citoyens d'un pays.

Le coût de la cession d'un domaine clé – sinon le domaine clé – de la sécurité nationale aux États-Unis est l'infiltration politique, la capture, voire l'effondrement complet, comme l'ont suffisamment démontré les opérations américaines menées tout au long du XXIe siècle, de l'Europe au monde arabe en passant par l'Asie.

Alors que le monde multipolaire se réunit pour discuter de la coopération dans les sphères traditionnelles de la sécurité nationale, il est urgent de prêter attention à la sécurisation de l'espace informationnel mondial contre l'influence et le contrôle des États-Unis.

La Russie et la Chine, qui exportent des armes pour aider leurs pays partenaires à défendre leurs domaines traditionnels de sécurité nationale, pourraient exporter des alternatives nationales clés en main aux plateformes de médias sociaux, aux infrastructures physiques et aux passerelles américaines, ainsi que des équipements de guerre électronique pour se défendre contre le type d'ingérence que les États-Unis viennent de mener dans l'espace informationnel iranien, ainsi

que des possibilités de relier les plateformes de médias sociaux nationales à des alternatives multipolaires aux plateformes américaines X, YouTube, Facebook et autres.

L'Iran, pays doté d'une puissance militaire conventionnelle importante, a été affaibli et fragilisé en raison de son retard dans la sécurisation suffisante de son espace informationnel, et donc de son espace politique, contre les ingérences étrangères. Et bien qu'il ait agi de manière décisive ces dernières semaines (et semble s'être préparé au moins plusieurs mois à l'avance), seul le temps dira s'il est encore temps ou s'il est déjà trop tard.

L'avenir du monde multipolaire pourrait dépendre non pas de l'ampleur de l'écart entre celui-ci et l'hégémonie américaine en termes de puissance militaire traditionnelle, mais de la rapidité avec laquelle le reste du monde prendra conscience de l'importance de contrôler l'espace informationnel, que les États-Unis ont compris et exploité tout au long du XXIe siècle.

source : New Eastern Outlook