التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION

Rapports Internationaux

14

La Nouvelle Guerre des Idées

Leçons pour la Lutte Contre la Désinformation Numérique

Rapports Internationaux

Une publication mensuelle - Département Général de la Planification et de la Coordination

---

Superviseur général

Le Major Général Mohammed bin Saïd Al-Mughaidi

Secrétaire Général de la Coalition Islamique Militaire pour Combattre le Terrorisme

---

Rédacteur en chef

Le Colonel Hassan Al-Amri

Directeur du Département de la Planification et de la Coordination

---

Conception, réalisation et édition

Société Taoq pour la Recherche et les Médias

TAOQ نـــوق

Courriel: info@taoqresearch.org

Téléphone: +966 114890124

Rapports Internationaux
14
Juin 2020

La Nouvelle Guerre des Idées
Leçons pour la Lutte Contre la Désinformation Numérique

L'auteur Kara Frederick a œuvré à réfuter de nombreuses campagnes numériques pernicieuses et fallacieuses et d'incidents de piratage en ligne. Elle affirme au début de ses recherches que l'avenir du système mondial dépend du niveau d'impact sur les peuples. Les civils paient depuis longtemps les frais des conflits acharnés, insurrections soient-ils ou terrorisme, pour enfin subir les séquelles de la guerre d'information. Les nouvelles technologies changent les règles du jeu et révolutionnent le processus d'emprise sur les peuples. Les progrès réalisés dans le domaine de l'intelligence artificielle, en particulier dans le domaine de l'apprentissage automatique, transforment l'information en armes permettant d'exercer un contrôle social à grande échelle. Des régimes autoritaires comme la Chine et la Corée du Nord ont profité des nouvelles technologies pour renforcer leur emprise, sur leur peuple, en utilisant des plateformes de réseaux sociaux contrôlées, des réseaux de robots et des technologies de reconnaissance faciale.

Tentatives de saper la confiance

Des influenceurs étrangers tentent de saper la confiance des gens dans la voie démocratique, par le biais de la propagande informatisée et d'un ciblage méticuleux. Des acteurs non gouvernementaux tentent même d'attiser les troubles politiques en diffusant des informations pernicieuses sur Internet. Ces actions visent souvent l'ordre libéral actuel et ses institutions de soutien, ce qui présage de troubles géopolitiques éventuels. L'auteur fait référence à ce stade à un plan visant à contrecarrer cette dangereuse menace, s'inspirant des enseignements tirés de la manière de mener une guerre différente. La guerre contre le terrorisme, qui a suivi le 11 Septembre, a présenté une feuille de route pour les organisations, publiques et privées, sur la manière de répondre à un autre type de bataille, la bataille de l'information.

Dans le contexte d'une pleine conscience des menaces terroristes, le gouvernement américain et les sociétés du secteur privé ont livré bataille à l'autre dans l'espace virtuel et sur le terrain. Le degré d'engagement du gouvernement américain est apparu entre 2002 et 2017, alors que la guerre mondiale contre le terrorisme lui coûtait environ 2,8 trillions de dollars de dépenses connexes, et environ 16% de dépenses discrétionnaires pour la même période. C'est le prix de la stratégie pour conjurer le danger et contenir le terrorisme avant qu'il ne frappe à domicile, l'armée américaine s'attaquant alors au terrorisme dans ses tanières en dehors des États-Unis.

Compagnies de médias sociaux affectées

Les nouvelles compagnies de médias et les plateformes de médias sociaux ont formé un groupe solidaire pour organiser la lutte contre le terrorisme, en particulier après que Daech a revendiqué la publication d'un clip vidéo sur le meurtre du journaliste américain James Foley sur YouTube et Twitter en 2014, ouvrant un nouveau front pour ces sociétés. En 2015, Facebook, opposé à la législation antiterroriste défaillante, a tenu plusieurs réunions avec d'autres sociétés technologiques, pour discuter de l'idée d'une plate-forme de lutte contre le terrorisme. Début 2016, des responsables de la Maison Blanche et des officiels de l'État se sont rendus à la Silicon Valley pour rencontrer de hauts responsables technologiques, avec à leur tête le PDG d'Apple, Tim Cook et des représentants de Google, Facebook, Yahoo et Twitter, pour discuter de solutions susceptibles de freiner la propagation du contenu terroriste sur l'Internet.

La même année, l'Incubateur Jigsaw, relevant de la Société Alphabet, a participé à faire face aux tactiques de Daech sur Internet et à épurer le contenu sur YouTube, sachant que l'idée de créer l'incubateur appartient à Google. En 2018, Facebook a embauché 7500 employés, en tant que gestionnaires de contenu, et l'une de leurs principales tâches consistait à garder la plateforme sociale exempte de contenu terroriste. Au cours des trois années qui se sont écoulées depuis ces discussions initiales en 2015, Twitter a suspendu 1,2 million de comptes d'abonnés qui ont violé les politiques antiterroristes.

Avec le début de la guerre contre le terrorisme, les entreprises technologiques ont commencé à intensifier la guerre de leurs plateformes contre les représentants terroristes, et ont eu recours à des personnes douées pour combler les lacunes et accroître l'expertise dans la lutte contre le terrorisme, créant de nouveaux postes pour coordonner et superviser la réglementation antiterroriste mondiale. Elles ont passé des contrats avec les parties prenantes concernées dans les forums internes et établi des mesures techniques et des procédures fiables pour éliminer les contenus et les utilisateurs abusifs. Les grandes et les petites sociétés technologiques ont coopéré par la force de la loi pour échanger toute information relative aux menaces à la sécurité et ont élaboré des règlements pour empêcher le terrorisme d'abuser de leurs plateformes numériques en particulier, et ce en mettant à jour les instructions internes à leurs sociétés, et en soutenant les initiatives intellectuelles pour réfuter la propagande terroriste.

Moyens de campagnes d'impact externe

1) La désinformation

Les campagnes d'impact qui reposent sur la promotion préméditée de la désinformation peuvent être définies comme étant: L'utilisation systématique d'informations fausses ou trompeuses, dans le but de semer le trouble et d'induire en erreur délibérément, ou de transformer l'opinion publique en personnes ciblées, pour atteindre des objectifs stratégiques. Afin de résister à l'impact de ce type d'informations, nous devons prêter une attention particulière aux agents «influenceurs», et aux facilitateurs «outils et mécanismes» des campagnes de désinformation numérique et d'impact étranger.

Quant aux agents ou influenceurs, les chercheurs, les médias et le public continuent d'attirer l'attention sur les campagnes d'influence, parrainées par certains pays, sous la direction des forces autoritaires de premier plan intellectuellement opposées aux démocraties. Ainsi, l'utilisation par la Russie d'opérations d'influence pour saper la solidarité transatlantique est bien documentée.

Quant aux éléments d'autonomisation, les influenceurs peuvent combiner les tactiques d'amplification et de micro-ciblage pour renforcer leur impact au maximum. En évaluant l'activité des robots via Internet en 2016, la cybersécurité américaine a constaté que les robots représentent plus de 50% de l'activité motrice sur Internet. Les robots politiques ciblent l'opinion publique en amplifiant des histoires destructrices ou distrayantes à travers les «champs de nains», qui sont des groupes d'Internautes coordonnant leurs publications avec d'autres utilisateurs, dans l'intention de harceler et d'induire en erreur, de diffuser des informations incorrectes et d'utiliser des robots de médias sociaux, qui sont des réseaux automatisés de faux comptes. Les acteurs influents cachent leurs effets numériques en utilisant un réseau (protocole) plagié. De même, les métadonnées dont les publicités profitent peuvent également être utilisées, par les utilisateurs de plateformes Internet, pour brosser un tableau du comportement des consommateurs, également à des fins de désinformation.

2) L'amplification

Parmi les moyens auxquels les campagnes étrangères influentes ont recours l'amplification de la polarisation politique; car la polarisation politique permet aux entités étrangères de diviser le public américain. À titre d'exemple: au lendemain de la fusillade du Parkland High School, en 2018, la Russie a cherché à alimenter le débat aux États-Unis, sur l'absence de lois relatives au contrôle des armes, en inondant Twitter de commentaires controversés sous la balise, appelant au contrôle immédiat sur les armes #gun_control_now, et en ouvrant d'autres balises pour susciter des réactions émotionnelles.

Les faibles barrières de protection sur les médias sociaux et les nouveaux médias permettent aux parties malveillantes d'y accéder facilement pour diffuser des contenus faux ou biaisés et propager des propagandes systématiques, qui désorientent l'environnement de l'information. Une étude menée par des chercheurs du Massachusetts Institute of Technology, en 2018, a révélé que la propagation de fausses nouvelles sur Twitter est plus rapide et plus tangible que la diffusion de la vérité, en particulier

en ce qui concerne les informations politiques. Les chercheurs ont attribué ce résultat en partie à l'excitation des émotions des gens.

3) Le phishing

Le phishing électronique essaie de tromper des personnes spécifiques, et se charge d'installer des logiciels malveillants, en envoyant des requêtes par e-mail, qui semblent être valides. Parmi les exemples de phishing numérique: l'attaque par courrier électronique qui a porté atteinte à la candidate à la présidentielle américaine Hillary Clinton, en nuisant à son Chef de campagne John Podesta et à la Convention Nationale Démocratique en 2016, et ce par le biais du système d'autonomisation de l'information, fourni par l'intelligence artificielle. Il est de plus en plus difficile de faire la différence entre les attaques malveillantes et les messages fiables, outre que la possibilité de mener des campagnes de phishing électroniques de manière automatisée, à grande échelle, augmente les chances de succès des assaillants.

Les campagnes d'influence étrangère utilisent un autre type de désinformation: l'implantation de fausses informations dans des paquets d'information piratées véridiques et authentiques, ce qui entache la confiance aux candidats aux élections eux-mêmes. Par exemple: Lors de la campagne électorale française du Président Emmanuel Macron, en 2017, un incident a été considéré comme un exemple réaliste de ce mécanisme. Les Russes ont infiltré le réseau de la campagne, divulgué des informations sur un employé de la campagne, achetant des drogues tout en simulant un tissu élaboré de désinformation mélangé à des informations fiables, dans le but de dérouter les masses françaises et de renverser leurs positions à propos de Macron.

4) L'infiltration

Les campagnes d'influence étrangère frappent les infrastructures des processus électoraux traditionnels, en particulier avant 2016, lorsque le «Brennan Center» de l'Université de New York a annoncé que plus de 43 États utilisaient d'anciennes machines à voter et des appareils mobiles reliés à des réseaux électroniques facilement accessibles et peu sûrs, ce qui pourrait exposer les opérations de vote et le comptage des voix à des vulnérabilités. Dans un rapport publié par l'American Center for Progress, en 2018, il a été noté que chaque État a pris de nouvelles mesures de cybersécurité depuis 2016, afin d'améliorer la gestion des élections semi-finales, mais il existe encore de nombreuses lacunes et une nette disparité dans les niveaux de progrès.

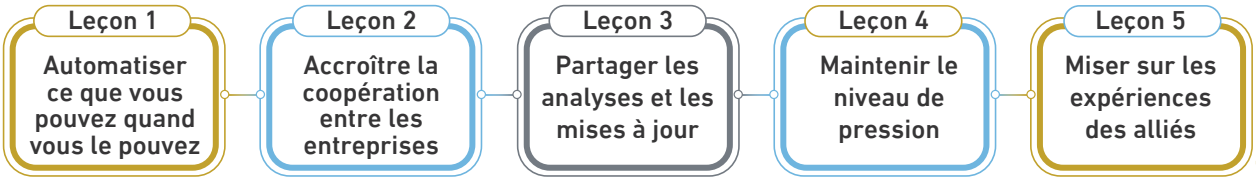
Leçons de la mémoire musculaire

Les technologies numériques modernes accusent de nouvelles vulnérabilités et subissent de moyens de sabotage modernes aux niveaux cognitif et numérique, mais les entreprises technologiques et le secteur public possèdent la mémoire musculaire pour connaître l'identité de ces agresseurs et pour assiéger l'espace à partir duquel les parties malveillantes agissent, avant de répondre avec force à leurs initiatives. L'expérience antiterroriste a créé cette mémoire musculaire, qui peut se résumer en cinq leçons:

Leçon 1: Automatiser ce que vous pouvez quand vous le pouvez:

Dans un premier temps, les nouveaux médias et les sociétés de médias sociaux doivent assaillir l'espace dans lequel les acteurs étrangers se livrent à des actions malveillantes, en améliorant la disposition de leurs plateformes à être «hostiles» au contenu terroriste, puis en appliquant des méthodes défensives dans le cadre de campagnes efficaces parrainées par l'État. Pour limiter les actions menées par les campagnes d'influence étrangère, telles que les conditions dans lesquelles Facebook fonctionne en guise de «comportement coordonné», les sociétés peuvent adopter des mesures spécifiques dans ce contexte, notamment en réduisant l'utilisation des pseudonymes et en s'appuyant sur des étapes strictes pour vérifier l'identité, telles que de vérifier les comptes qui montrent des indicateurs plus automatisés que humains et d'évaluer l'intégrité des comptes.

Leçons de la mémoire musculaire



Recourir à ces méthodes précédemment testées dans la lutte contre le terrorisme pour réduire les capacités des réseaux malveillants, peut être appliqué pour réduire le nombre de faux comptes qui publient des informations fausses et trompeuses. Google et Facebook mettent en œuvre des mesures similaires pour avorter les tentatives de diffuser les informations abusives.

Quant à Twitter, il a suspendu définitivement 70 millions de comptes, entre mai et juin 2018. Plus la quantité et la variété des données sont importantes dans l'environnement d'information, et plus l'automatisation est de rigueur pour modifier automatiquement le contenu, avec une moindre inflation et un référentiel plus rigoureux, moins les attaquants ont de chances d'accéder à l'espace de l'Internet.

Leçon 2: Accroître la coopération entre les entreprises:

Les défis auxquels sont confrontées les entreprises concernées sont souvent des défis communs dans cette nouvelle bataille mondiale, ce qui nécessite l'union dans la prise des mesures. Ainsi, Facebook a imposé de nouvelles réglementations et des technologies de pointe, dont l'application dépasse les États-Unis et le Canada à des millions d'utilisateurs dans le monde.

En Septembre 2018, Sherrill Sandberg, Chef des Opérations de Facebook, a déclaré à la Commission Sénatoriale du Renseignement que Facebook travaille, en étroite collaboration avec ses pairs de l'industrie, pour progresser dans la lutte contre le problème des campagnes d'impact étrangères. Au cours du même mois, Google, Facebook et Twitter se sont engagés à travailler ensemble pour lutter contre les fakenews (infox) en Europe, ce qui est un test pour généraliser l'expérience et étendre cette coopération à l'échelle mondiale. Il est nécessaire de réaliser que la coopération des entreprises entre elles est cruciale et inévitable, et que certaines d'entre elles ont lancé des prototypes accrédités prêts à l'emploi parmi les tenants de l'industrie eux-mêmes. C'est le résultat des efforts de lutte contre le terrorisme, dont il faudrait profiter et le développer si nécessaire.

Leçon 3: Partager les analyses et les mises à jour:

Un élément fondamental dans la lutte contre les réseaux malveillants et leurs représentants, réside dans la capacité d'organiser les lignes de bataille et leurs outils. Comme le secteur de la technologie est un facteur majeur dans les guerres futures, s'appuyer sur les réalisations passées peut combler le fossé entre les secteurs public et privé, grâce aux experts qui partagent des objectifs communs. Ces cadres et ces systèmes d'intégration existent et peuvent être mesurés. Il en est ainsi du Centre National de Lutte Contre le Terrorisme, fondé en Virginie du Nord en 2004, pour améliorer le système de partage d'informations et pour améliorer les capacités de prévision et de réponse rapide aux menaces terroristes. Les experts suggèrent donc de simuler l'idée et de créer une institution similaire, avec la même fonction, pour contrer les processus d'influence étrangère.

Les recommandations indiquent la nécessité de nommer un organisme composé de membres de l'agence de renseignement pour lutter contre le terrorisme, en coordination avec le secteur privé, afin de créer des cellules plus petites, plus susceptibles de se déplacer et de s'intégrer facilement, sous sa supervision et son financement,

et de traiter numériquement les campagnes d'influence étrangère malveillantes. Les sociétés de médias sociaux devraient accorder à ce stade une attention particulière à ces efforts et fournir à ces petites cellules l'expertise de leurs analystes spécialisés dans la lutte contre le terrorisme.

Leçon 4: Maintenir le niveau de pression:

Il existe toujours un besoin urgent pour plus de pression, malgré les bonnes performances du gouvernement et des entreprises technologiques; mais les terroristes continueront de trouver des moyens innovants pour porter atteinte à la société, par le biais des plateformes de médias sociaux et des nouveaux médias. Les entreprises de médias sociaux continueront d'employer des analystes et des auditeurs spécialisés dans le terrorisme pour les accompagner. Si la possibilité de transférer ces outils et ces technologies de lutte contre le terrorisme constitue un bon départ, le problème de la désinformation et des (infox), et leurs vastes implications, pour les institutions démocratiques, imposent, toujours de prendre, systématiquement, une position proactive.

Les mensonges et les nouvelles fallacieuses nourrissent les régimes dictatoriaux qui gouvernent par la force et la peur, alors que la vérité constitue le point de contact et l'antidote de la corruption et de la tyrannie dans les sociétés libres. Certains régimes usent de mensonges, pour se maintenir au pouvoir, comme c'est le cas en Corée du Nord ou en Chine qui gouvernent avec une main de fer. De l'autre côté, les démocraties donnent aux gens l'accès à la vérité. Si les régimes autoritaires se basent sur les mensonges pour assurer leur emprise, cela fait de la vérité une arme face à la répression, et les États-Unis ne doivent pas abandonner cet avantage. Lorsque la vérité prévaut, la démocratie triomphe.

Leçon 5: Miser sur les expériences des alliés:

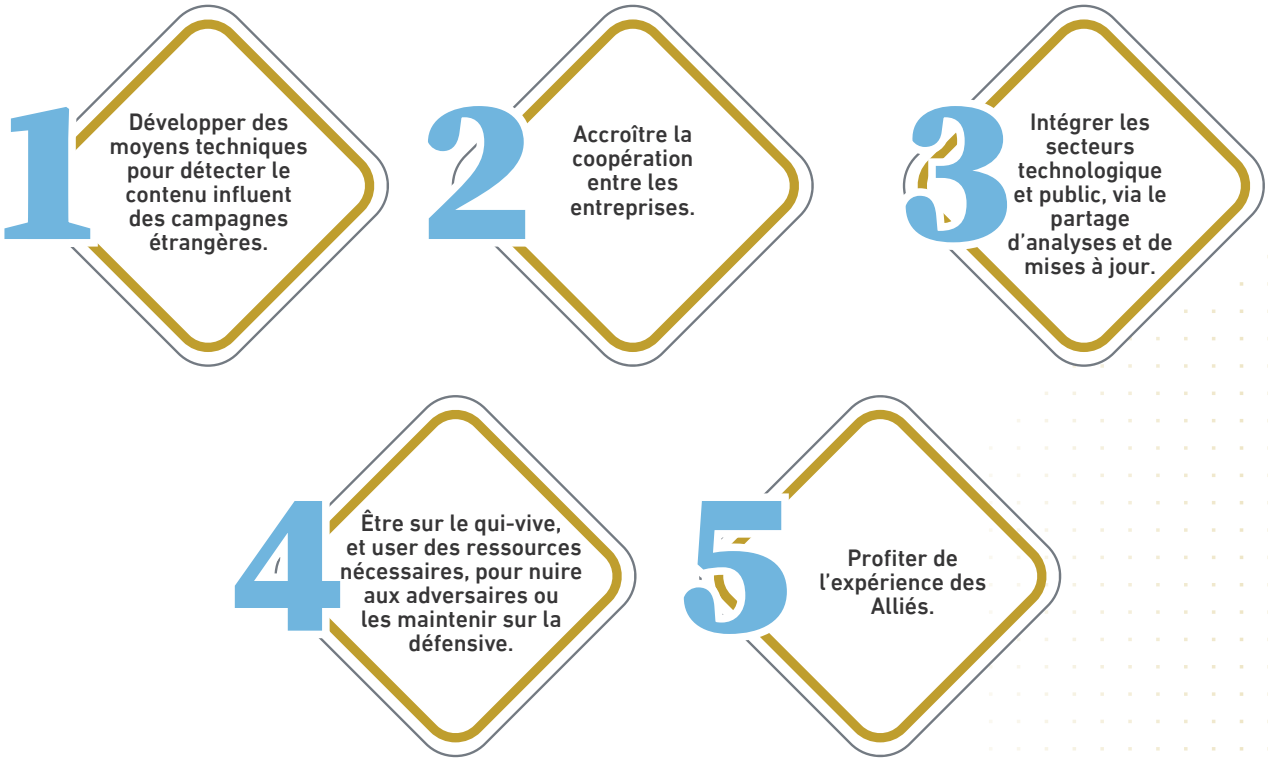
Tous les efforts et plans reposent sur un avantage important, non exploité comme il se doit, qui est les alliés démocratiques des États-Unis. La contribution de l'OTAN à la guerre contre le terrorisme a renforcé la collecte de renseignements et les opérations opérationnelles dans le cadre de «l'Opération Enduring Freedom», en Afghanistan. L'OTAN est devenue un membre officiel de la coalition mondiale pour vaincre Daech, en Mai 2017, et un membre de la Cellule de Renseignement sur le Terrorisme, basée à Bruxelles, siège de son bureau principal. Face aux menaces à la sécurité en Afghanistan, 38 pays, ainsi que les États-Unis, unissent leurs forces pour financer les forces soutenant les opérations de lutte contre le terrorisme.

Les États-Unis devraient inviter des alliés démocratiques à partager les meilleures pratiques, sur la base de leurs propres expériences dans la lutte contre les campagnes d'influence étrangère, pour assouplir les restrictions sur les cyber-mesures offensives. Les États-Unis devraient également recourir à un procédé fiable pour fournir au cyber-leadership les résultats de l'échange d'informations et lui donner des directives concrètes.

Résumé

Après le 11 Septembre, le champ de bataille contre le terrorisme a changé. Nous sommes entrés dans une nouvelle étape appelée l'ère de la lutte contre le terrorisme, et ce changement a affecté les couloirs des entreprises technologiques américaines. L'écrivain dit: «Aujourd'hui, les États-Unis participent à une lutte expansionniste qui nécessite l'intervention des principaux influenceurs eux-mêmes, les entreprises technologiques du secteur privé et le gouvernement américain. Ils ne peuvent plus se permettre de répéter l'erreur et manquer de nombreuses leçons apprises au cours des deux dernières décennies dans la lutte contre le terrorisme, sur les plans stratégique, technique et organisationnel». S'appuyant sur des expériences réussies dans le secteur de la technologie et sur les efforts antiterroristes du gouvernement américain, les États-Unis sont mieux à même de relever les défis de la désinformation numérique à l'avenir.

Il y a cinq leçons dont les secteurs privé et public devraient tirer parti avec soin et diligence pour lutter contre le terrorisme:



- Développer des moyens techniques pour détecter le contenu influent des campagnes étrangères.
- Accroître la coopération entre les entreprises.
- Intégrer les secteurs technologique et public, via le partage d'analyses et de mises à jour.
- Être sur le qui-vive, et user des ressources nécessaires, pour nuire aux adversaires ou les maintenir sur la défensive.
- Profiter de l'expérience des Alliés.

En somme, les recommandations suivantes devront contribuer à lutter contre les campagnes étrangères influentes à la lumière de ces cinq enseignements tirés, les deux premières cibleront le secteur privé de l'industrie technologique, tandis que la troisième concernera le secteur de l'industrie et le gouvernement américains, et les deux dernières seront dirigées vers les agences gouvernementales américaines.

Recommandations

- À long terme, les entreprises technologiques doivent consacrer une partie permanente de leur capacité d'ingénierie à automatiser les opérations pour la recherche de l'identité des campagnes influentes et malveillantes. Ainsi, les entreprises peuvent obtenir un effet de levier important en exploitant les pratiques et les traditions en usage dans les logiciels, telles que: Le (Backathon) sur Facebook, en réunissant les programmeurs informatiques pour leur permettre d'échanger des expériences et des missions d'ingénierie, construire des prototypes et rechercher des réformes techniques au problème de la désinformation.
- Les entreprises technologiques devraient créer une association spécialisée dans la désinformation, et la financer, et à laquelle peuvent se joindre les entreprises créées après le Forum Internet Mondial de Lutte Contre le Terrorisme (GIFCT). L'Association se charge de mettre au point les normes de l'industrie et traque les sociétés malveillantes de désinformation.
- En coordination avec le secteur privé, le Bureau du Directeur du Renseignement National (ODNI), devra désigner un comité, regroupant les représentants des agences

chargé de créer des cellules plus petites et plus actives rassemblant les analystes des secteurs public et privé, et les financer. Les nouveaux médias sont tenus de tirer parti de leurs employés travaillent sur l'analyse des menaces de renseignement, avec les agences de renseignement pour fournir des inductions à cet organisme et ouvrir un dialogue continu, tout en respectant les normes de confidentialité pour chaque contact. Et si la commission montre certains signes de succès, le gouvernement américain devra envisager d'affecter une force indépendante, au plus haut niveau commun, en vue d'assurer l'harmonie entre ces cellules, et d'assumer toutes les responsabilités pour contrer toute opération numérique étrangère influente.

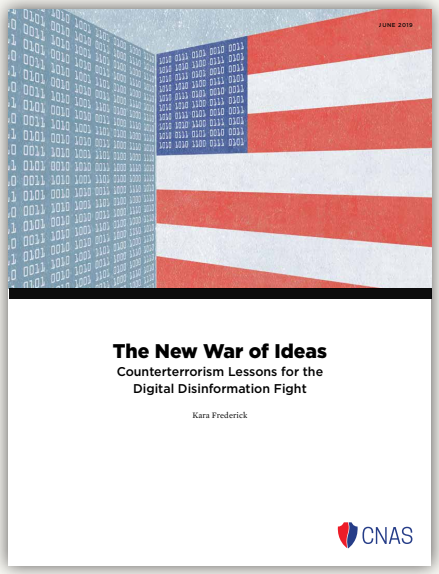
- Le pouvoir exécutif devra étendre la stratégie de cyber-sécurité et les prérogatives de la cyber-direction américaine en menant des opérations offensives qui causent des pertes aux adversaires.
- Le gouvernement américain devra travailler avec ses alliés démocratiques pour échanger les pratiques et les expériences concernant l'influence étrangère des campagnes offensives, tout en s'appuyant sur leur expertise pour prendre des cyber-mesures offensives. Le processus de fondation, lui-même, devra être utilisé comme moyen formel pour le partage des résultats de ces informations, en plus des recommandations d'action.

Auteur

Kara Frederick a passé six ans en tant qu'analyste de lutte contre le terrorisme, au département américain de la Défense. Elle a exercé en tant qu'analyste en Chef du Renseignement Militaire, de la marine américaine, et contribué à la formation de la première équipe mondiale de cybersécurité sur Facebook. Elle a été Chef de l'équipe régionale d'enquête au siège de Facebook en Californie. Elle est, actuellement, adjointe au programme de sécurité nationale et technique du New American Security Center (CNAS). Elle détient une License en Histoire et Affaires Étrangères de l'Université de Virginie et une Maîtrise du King's College de Londres, en Études de Guerre.

La Nouvelle Guerre des Idées

Leçons pour la Lutte Contre la Désinformation Numérique




التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION


التحالف الإسلامي العسكري لمحاربة الإرهاب
ISLAMIC MILITARY COUNTER TERRORISM COALITION