LE PRÉSIDENT
COMITÉ CONSULTATIF DES
TÉLÉCOMMUNICATIONS POUR LA SÉCURITÉ
NATIONALE

Rapport du NSTAC au Président sur un coup de projecteur sur la cybersécurité

14 novembre 2018

TABLE DES MATIÈRES

RÉSUMÉ EXÉCUTIF

"Rendre l'Internet sûr et sécurisé pour le fonctionnement du gouvernement et des services essentiels pour le peuple américain d'ici 2028".

Les États-Unis se trouvent à un point d'inflexion : ils sont simultanément confrontés à un environnement de menaces de cybersécurité qui s'aggrave progressivement et à une dépendance toujours plus grande à l'égard des technologies de l'internet qui sont fondamentales pour la sécurité publique, la prospérité économique et le mode de vie en général. Notre sécurité nationale est désormais inexorablement liée à la cybersécurité. Par conséquent, la nation doit s'appuyer sur les efforts passés et les stratégies actuelles pour saisir l'opportunité de réorienter stratégiquement sa posture de cybersécurité largement réactive et progressive vers une approche proactive qui assure avec audace la confiance, la sécurité et la résilience numériques de tous les Américains. Pour parvenir à ce résultat audacieux, il faudra un leadership national fort, une volonté politique et un investissement soutenu de l'ensemble de la nation sur une longue période.
Le gouvernement américain peut prendre des mesures immédiates qui jettent les bases de cette vision partagée à long terme de la cybersécurité pour la nation, tout en produisant simultanément des avantages à court terme qui assurent un leadership technologique mondial continu.

Le leadership doit commencer par une déclaration d'intention stratégique audacieuse et ambitieuse, comme l'ont fait les États-Unis à quelques reprises dans l'histoire lorsqu'ils ont dû faire face à des défis existentiels. Le Comité consultatif présidentiel sur la sécurité nationale et les télécommunications (NSTAC) estime que la cybersécurité représente l'un des plus grands défis du XXIe siècle, que les États-Unis doivent tout simplement relever durablement en tant qu'impératif stratégique national. Pour communiquer cela, le
*L'*administration, à ses niveaux les plus élevés, doit fournir une vision claire et inspirée en tant que catalyseur des activités nationales. Elle doit déclarer une intention stratégique nationale : *Rendre l'internet sûr et sécurisé pour le fonctionnement du gouvernement et les services essentiels au peuple américain d'ici 2028.* Une telle poursuite garantirait la confiance de la société dans l'infrastructure numérique, favoriserait la vitalité économique et renforcerait le leadership américain en matière d'innovation.

Le NSTAC a adopté le terme "Cybersécurité Moonshot" pour décrire cette approche, du nom de la National Aeronautics and Space
L'effort du programme Apollo de la NASA pour envoyer un homme sur la Lune, suite au discours du président John F. Kennedy en mai 1961, lors d'une session conjointe du Congrès. Le premier tir lunaire a orienté l'action nationale collective vers un objectif ambitieux : envoyer un homme sur la Lune et le ramener sain et sauf sur Terre avant la fin de la décennie. Il est important de noter que le président Kennedy a clairement a articulé cet objectif final sans être prescriptif des nombreuses innovations et actions individuelles nécessaires pour atteindre ce résultat.

> "Je crois que nous possédons toutes les ressources et tous les talents nécessaires. Mais le fait est que nous n'avons jamais pris les décisions nationales ou mobilisé les ressources nationales nécessaires à un tel leadership. Nous n'avons jamais fixé d'objectifs à long terme dans un calendrier urgent ni géré nos ressources et notre temps de manière à assurer leur réalisation".
>
> - Le président John F. Kennedy dans son discours à une session conjointe du Congrès le 25 mai 1961

Les différences entre les caractéristiques de la vision du président Kennedy et celles prévues d'un "moonshot" pour la cybersécurité sont cependant nombreuses. Principalement, les critères de succès d'une initiative "Moonshot" pour la cybersécurité seront moins précis et moins mesurables, car sa réalisation sera une transformation sociétale plutôt qu'un triomphe visuel singulier. Le NSTAC reconnaît les limites de l'analogie mais croit fermement que l'initiative Moonshot représente un

un modèle puissant et très applicable pour l'établissement des priorités nationales, l'action collective et l'innovation accélérée nécessaires à la cybersécurité.

Pour atteindre son objectif, l'initiative Cybersécurité Moonshot doit chercher des réponses à plusieurs questions complexes. Pour commencer : Que signifie "sûr et sécurisé" dans la société numérique moderne ?
Quels sont les "services essentiels" les plus fondamentaux pour la sécurité nationale et la sécurité publique et qui doivent être considérés comme prioritaires au niveau national afin de réaliser un Internet sûr et sécurisé de manière mesurable ? Commencer à affronter publiquement ces questions complexes sur une base nationale et avec une communauté de parties prenantes beaucoup plus inclusive est fondamental pour réaliser cet avenir plus audacieux et durable. Dans certains cas, le NSTAC cherche à répondre à ce type de questions dans le cadre du présent rapport. Dans d'autres cas, ces réponses devraient s'inscrire dans le cadre de l'initiative nationale à plus long terme "Cybersécurité Moonshot" dont le lancement est proposé dans ce rapport.

Il ne suffit pas, bien sûr, de faire une déclaration d'intention ambitieuse. L'initiative "Cybersécurité Moonshot" doit être profondément ancrée dans un cadre stratégique clair et des principes partagés qui transcendent les stratégies individuelles et mettent l'accent sur un véritable changement générationnel. Elle doit être dotée d'une structure de gouvernance qui permette à des groupes répartis de parties prenantes au sein du gouvernement, du secteur privé, du monde universitaire et de la société civile de concentrer leurs énergies et leurs activités collectives sur les objectifs nationaux définis et d'ordre supérieur de l'initiative "Cybersécurité Moonshot".

Tout au long de ce rapport, le NSTAC s'efforce de répondre à plusieurs questions fondamentales, notamment sur ce qu'est une initiative "Moonshot" en matière de cybersécurité, pourquoi elle est nécessaire et comment la nation peut la mettre en œuvre efficacement. La section 1.0, *Introduction*, et la section 2.0, *Pourquoi la cybersécurité nécessite-t-elle une* initiative "Moonshot" *?* se concentrent sur les raisons pour lesquelles une initiative "Moonshot" de cybersécurité est nécessaire, pourquoi la trajectoire actuelle d'amélioration progressive de la cybersécurité est inadéquate et pourquoi ce défi est digne d'être relevé par une génération.

La section 3.0, *Plan d'action de l'Initiative Moonshot sur la cybersécurité,* fournit des recommandations stratégiques et des mesures concrètes que le gouvernement américain peut prendre pour diriger cette initiative et utiliser ses pouvoirs uniques pour défendre, organiser, diriger, financer et habiliter stratégiquement des activités nationales alignées sur ses objectifs. La section 3.0 définit les éléments de départ d'un guide de l'initiative Cybersécurité Moonshot, en présentant des recommandations relatives à l'organisation pratique et à l'opérationnalisation de l'initiative. Cela comprend des considérations clés liées à la gouvernance, aux objectifs, aux étapes, au financement et à un cadre d'organisation appelé "piliers stratégiques". Un résumé des principales recommandations contenues dans ce rapport est présenté ci-après :

Recommandations clés : Gouvernance de l'initiative "Moonshot" en matière de cybersécurité

(section 3.1-3.3)

Le président ou le vice-président devrait présenter et défendre stratégiquement une initiative "Moonshot" en matière de cybersécurité afin de signaler clairement que le fait de relever les défis de la cybersécurité de manière durable est un impératif stratégique fondamental pour l'avenir de la nation. Cette proclamation devrait être faite dans un forum d'importance historique, tel que l'État de l'Union ou une allocution spéciale lors d'une session conjointe du

- Congrès, pour souligner ce niveau de priorité nationale.

- L'initiative "Cybersécurité Moonshot" doit englober une approche nationale globale, y compris un modèle de gouvernance à plusieurs niveaux couvrant le gouvernement, l'industrie et les universités, qui alignent leurs capacités et activités inhérentes à la réalisation d'un Internet sûr et sécurisé. Ce modèle pourrait inclure une structure commerciale de type consortium qui facilite la coopération, la gestion des ressources, la gestion des risques et la gestion des risques.

et le partage des récompenses lorsque cela est approprié et ne nuit pas à la dynamique du marché concurrentiel qui promet le chemin le plus efficace vers les objectifs. Il devrait également y avoir des mécanismes formels de collaboration avec les partenaires gouvernementaux et universitaires pour atteindre des objectifs communs.

- Au sein du gouvernement américain, un Conseil de la cybersécurité (Cybersecurity Moonshot Council) dirigé par l'administration devrait diriger et gérer l'initiative. Le Conseil devrait être responsable et habilité à : accroître la visibilité nationale, plaider pour un financement durable, développer des stratégies au niveau national, et créer des politiques et des processus qui habilitent et incitent les parties prenantes non gouvernementales à accélérer l'innovation dans des domaines définis de l'Initiative Moonshot sur la cybersécurité. Le mandat du Conseil devrait être exclusivement orienté vers l'obtention de résultats à long terme, distincts mais complémentaires de la direction actuelle du gouvernement en matière de cybersécurité, souvent naturellement orientée vers des exigences à court terme et d'actualité.

- Le président ou le vice-président devrait officiellement présider le Conseil, qui devrait être composé de fonctionnaires de niveau ministériel issus des ministères et organismes concernés. Le Conseil Moonshot sur la cybersécurité devrait disposer de mécanismes formels permettant à des entités non gouvernementales désignées de contribuer directement à la stratégie et au processus d'élaboration des politiques de l'Initiative Moonshot sur la cybersécurité. Un directeur exécutif nommé par le président devrait diriger l'initiative sur le plan opérationnel et être responsable et habilité à maintenir la visibilité de toutes les activités nationales de l'Initiative Moonshot sur la cybersécurité et à promouvoir les activités qui ont le plus grand impact stratégique sur la réalisation d'un environnement Internet sûr et sécurisé.

- Le Cybersecurity Moonshot Council devrait élaborer publiquement un cadre stratégique, après une période de consultation interne et externe, afin de fournir une structure commune qui aide à organiser les activités réparties de l'Initiative Moonshot de cybersécurité dans l'ensemble du pays. Comme point de départ recommandé, le NSTAC propose six piliers stratégiques, reconnaissant que la réalisation d'un Internet plus durablement sûr et sécurisé au cours des dix prochaines années nécessitera une approche holistique et multidisciplinaire.

Recommandations clés : Piliers stratégiques de l'initiative "Moonshot" en matière de cybersécurité (*section 3.4*)

La réalisation de progrès significatifs vers un Internet plus durablement sûr et sécurisé au cours des dix prochaines années ne sera pas le résultat d'une solution singulièrement transformatrice. La complexité du défi de la cybersécurité exigera une attention stratégique et un rythme d'innovation accéléré dans les domaines de la technologie, des personnes, des processus et des politiques, comme le montre le programme stratégique
Piliers. Pour réaliser des progrès significatifs, il faudra encourager les solutions existantes et connues et poursuivre la réalisation de nouvelles solutions transformationnelles.

Le NSTAC recommande six piliers stratégiques pour guider cette activité répartie sur l'ensemble du territoire national :
(1) *Technologie* ; (2) *Comportement humain ; (*3) *Éducation ; (*4) *Écosystème ; (*5) *Vie privée* ; et (6) *Politique*. Ces piliers ne doivent pas être considérés comme des axes de travail indépendants. Ils doivent être considérés comme des éléments interdépendants essentiels de l'initiative globale Cybersécurité Moonshot, y compris les activités qui sont toutes complémentaires et qui renforcent le résultat souhaité d'un Internet sûr et sécurisé.

1. Technologie

Les progrès technologiques spectaculaires continuent d'élargir le paysage numérique et créent de nouveaux risques en matière de cybersécurité que les acteurs malveillants cherchent activement à exploiter. Toutefois, ces mêmes nouvelles technologies qui émergent rapidement, si elles sont exploitées de manière stratégique, peuvent permettre des capacités de sécurité défensive plus automatisées et plus efficaces. Bon nombre de ces fondements technologiques existent ou sont en cours de développement, mais ils nécessiteront une stratégie nationale concertée de recherche et de développement de produits pour les mettre à profit face au défi national de la cybersécurité. Les principaux résultats souhaités dans le cadre du pilier stratégique technologique sont les suivants

- Les technologies stratégiques jugées critiques pour la sûreté et la sécurité globales de l'environnement Internet sont identifiées, classées par ordre de priorité et font l'objet d'investissements pour accélérer leur disponibilité. Voici quelques exemples de domaines technologiques jugés critiques sur la base des conclusions du NSTAC

    - Un renseignement amélioré qui aide les humains plutôt que de les remplacer, pour une prévention automatisée des menaces qui peut devancer le rythme des agresseurs ;

    - Les communications quantiques et la cryptographie résistante aux quanta qui peuvent protéger les méthodes cryptographiques actuelles utilisées pour la défense de la cybersécurité ;

    - la biométrie comportementale pour fournir des scores d'identité qui réduisent la dépendance à l'égard des mots de passe traditionnels et l'identification personnelle souvent compromise pour l'authentification ; et

    - Les communications 5G et les autres réseaux de prochaine génération ont été conçus et architecturés dès le départ avec une sécurité, une connectivité et une disponibilité accrues.

- Des plans stratégiques nationaux visant à accélérer la croissance dans ces domaines technologiques essentiels, notamment par le biais de grands défis ciblés en matière de cybersécurité, le cas échéant, sont mis en œuvre pour devancer les efforts internationaux concurrentiels.

- Un cadre politique est élaboré et les obstacles réglementaires sont rationalisés afin d'encourager et de récompenser l'investissement et l'innovation du secteur privé dans les technologies qui sous-tendent l'initiative "Cybersécurité Moonshot".

2. Comportement humain

La technologie ne peut à elle seule répondre aux principaux défis de la nation en matière de cybersécurité. Ces défis exigeront l'ingéniosité d'une communauté d'innovation beaucoup plus large, composée d'experts pluridisciplinaires inspirés à consacrer leur expertise à des objectifs de transformation de la cybersécurité. Les citoyens et les entreprises doivent également comprendre leur responsabilité dans la prévention des cyberattaques réussies et être dotés d'informations et d'outils qui les incitent à prendre les bonnes décisions en matière de sécurité, par défaut. Des campagnes efficaces de changement de comportement, comme "Smokey the Bear" et

les initiatives de lutte contre l'alcool au volant visant à accroître la pression sociale contre les comportements à risque et préjudiciables à la société, sont l'un de ces outils.

1. Éducation

L'initiative "Cybersécurité Moonshot" doit remédier à l'importante pénurie de compétences et de financement dans les principales disciplines de recherche stratégique, y compris les technologies critiques déjà identifiées. L'initiative doit promouvoir des outils éducatifs hautement distribués et exponentiellement évolutifs et développer l'utilisation du mentorat et de l'apprentissage en tant que multiplicateurs de force dans des domaines critiques. La planification stratégique de l'enseignement de la cybersécurité doit également tenir compte de la manière dont les technologies émergentes, telles que l'intelligence augmentée, modifieront les besoins traditionnels en main-d'œuvre dans le domaine de la cybersécurité.

2. Rôles et responsabilités des écosystèmes

Aucune entité gouvernementale, entreprise ou groupe industriel n'est individuellement capable de concevoir, d'élaborer, de construire ou de mettre en œuvre les fondements d'un environnement Internet sûr. L'effort doit être le résultat d'une approche coordonnée où les parties prenantes ont une compréhension commune de leurs rôles et responsabilités respectifs et prennent des mesures qui favorisent l'intégration des capacités complémentaires des écosystèmes. L'internet est composé de milliards d'appareils, de logiciels, de services et d'utilisateurs. Permettre un environnement Internet fondamentalement sûr pour les gouvernements et les services essentiels, tout en maintenant l'omniprésence de l'accès Internet, nécessitera un effort conscient et coordonné pour travailler avec une grande variété de participants à différents niveaux de confiance.

3. Vie privée

Le respect de la vie privée est un principe fondamental qui doit imprégner tous les aspects du projet "Cybersécurité Moonshot
Le développement de l'initiative et sera primordial pour susciter la confiance du peuple américain. Les citoyens américains doivent pouvoir faire confiance aux systèmes d'information qui fournissent des services essentiels et avoir la certitude pratique que l'initiative "Cybersécurité Moonshot" ne créera pas de problèmes de protection de la vie privée
mais plutôt de renforcer l'assurance de la protection de la vie privée et de garantir que leurs données personnelles et leurs transactions restent protégées et sous leur contrôle.

4. Politique

Le gouvernement doit soigneusement évaluer et mettre en œuvre des politiques qui donnent des moyens d'action et des incitations aux principaux acteurs responsables de l'initiative "Moonshot" en matière de cybersécurité, permettant des innovations et une mise en œuvre. Des politiques devront être créées, réformées ou supprimées pour favoriser la création d'un environnement Internet fondamentalement sûr. Par exemple, l'exigence d'une identité fiable et d'interactions pleinement authentifiées pour assurer un environnement internet sûr nécessitera une infrastructure politique de sécurité, d'attribution et de responsabilité renforcées. Une coordination étroite avec les législateurs, la communauté nationale et internationale et les partenaires privés sur les normes mondiales de comportement dans le cyberespace sera également essentielle pour réussir.

Recommandations clés : Initiative "Moonshot" en matière de cybersécurité - Grands défis (*section 3.5*)

Lorsqu'il propose une initiative aussi complexe et à long terme que l'Initiative Moonshot sur la cybersécurité, le NSTAC estime qu'il est essentiel d'identifier un certain nombre de domaines d'action spécifiques à court terme qui serviront de modèles représentatifs des principes généraux de la vision globale de l'Initiative Moonshot sur la cybersécurité. Les principes représentés par les "grands défis" bien établis - réflexion attentive à la communauté, incitation basée sur les résultats, innovation ouverte, solution

Le crowdsourcing correspond à ce modèle. Cette approche du "grand défi" doit être plus fermement adoptée par la communauté de la cybersécurité. Le gouvernement américain peut mener cette transformation en lançant une série de "grands défis" en matière de cybersécurité qui produisent des avancées plus immédiates et plus dynamiques vers la réalisation d'un environnement Internet sûr et sécurisé.

- En tant que catalyseur de l'initiative globale Cybersécurité Moonshot, le Cybersecurity Moonshot Council devrait diriger l'identification et le lancement d'un ou plusieurs grands défis en menant un processus de collaboration de six mois qui engage officiellement les parties prenantes dans tout le pays. Ces grands défis devraient être organisés autour de domaines critiques du développement technologique dans lesquels l'intransigeance systémique et la défaillance du marché ont précédemment entravé les progrès. Le gouvernement américain peut utiliser divers outils pour encourager et accélérer l'adhésion de l'ensemble du pays à ces activités alignées sur les six piliers stratégiques.

- Lors de l'évaluation des candidats potentiels au Grand Challenge, le gouvernement doit tenir compte de plusieurs considérations et questions clés, notamment (1) Le gouvernement a-t-il un rôle clair à jouer pour catalyser des activités alignées sur le Grand Défi lorsque les précédents moteurs basés sur le marché se sont avérés insuffisants ? (2) Le Grand Défi nécessite-t-il des activités dépassant le champ d'action des autorités et/ou des forces gouvernementales et bénéficierait-il d'une collaboration plus large ?
  (3) La société, en particulier les experts non spécialisés dans la sécurité, comprendrait-elle largement la valeur et l'importance stratégiques du Grand défi ? (4) Le Grand défi est-il à la fois mesurable et réalisable ? (5) La réalisation des objectifs du Grand défi produirait-elle un résultat hautement évolutif ? et (6) Le Grand défi a-t-il une portée suffisamment large pour inclure des activités relevant de plusieurs piliers stratégiques ?

L'administration a une opportunité unique dans l'histoire. Des décennies d'activités bien intentionnées mais disjointes ont rendu l'internet progressivement moins sûr pour les services essentiels qui en dépendent. Le NSTAC estime que nous devons être plus audacieux et proclamer, comme un impératif stratégique national, que notre objectif à dix ans est de rendre l'internet sûr pour les interactions des Américains avec le gouvernement et les services essentiels. Le NSTAC est clairvoyant quant à l'énormité de cet objectif et fait cette recommandation en saisissant pleinement à la fois l'urgence du succès et les problèmes critiques qui ont fait échouer les efforts antérieurs bien intentionnés.

L'histoire constitue un véritable précédent pour la nation qui doit relever des défis apparemment impossibles. Dans ces cas historiques, les dirigeants ont déclaré une intention stratégique sans avoir une compréhension claire des moyens pour atteindre la fin. Dans ces exemples historiques, comme maintenant, il y avait un objectif clair, des premiers pas tangibles et une approche globale de la nation que les dirigeants du gouvernement américain ont utilisés pour diriger l'effort et inspirer le succès. Une opportunité tout aussi impérative existe pour le 21e siècle. Notre prospérité et notre succès futurs en tant que nation dépendent désormais intrinsèquement de notre réussite dans le domaine de la cybersécurité, et un effort inspirant de type "Moonshot" est nécessaire pour y faire face.

1.0 INTRODUCTION

L'internet, et l'ère numérique qu'il a inaugurée, a été la source d'avantages économiques et sociétaux incommensurables. La capacité d'utiliser l'internet ouvert et la liberté d'utiliser les technologies connectées à l'internet sont tout simplement devenues un droit fondamental. Les États-Unis doivent préserver cette liberté en veillant à ce que les Américains puissent utiliser ces technologies en toute sécurité, en tant qu'impératif stratégique national, tout en montrant l'exemple au niveau international.

Peut-être plus que tout autre défi économique et de sécurité nationale du 21e siècle, la cybersécurité exige un plus grand sens de la responsabilité partagée et de l'action collective.

Sur leur trajectoire actuelle, les États-Unis sont confrontés à des risques sans équivoque pour la réalisation de cet impératif national et international. Les menaces de cybersécurité sont de plus en plus fréquentes et sophistiquées, et plus destructeur - érodant progressivement la confiance de la société dans les infrastructures numériques. Alors que la technologie continue de progresser et que chaque facette de la vie quotidienne est de plus en plus interconnectée, tant la
La probabilité et le coût de l'échec augmentent considérablement. Les technologues et les experts en cybersécurité du monde entier reconnaissent cette tendance inquiétante, mais elle n'est pas encore largement comprise par de nombreux dirigeants gouvernementaux, cadres d'entreprises ou le grand public. Peut-être plus que tout autre défi économique et de sécurité nationale du XXIe siècle, la cybersécurité exige un plus grand sens de la responsabilité partagée et de l'action collective. Notre époque d'hyperconnectivité signifie aujourd'hui que votre risque est le mien, car les attaques contre les maillons les plus faibles peuvent désormais avoir des conséquences sur l'environnement numérique au sens large. *1*

La nature complexe de la cybersécurité a créé une multitude de défis qui touchent à la fois à la technologie, aux personnes et aux processus. Cette complexité a conduit à une tendance à compartimenter le défi en ses composantes individuelles, plus faciles à comprendre. Le fait que les capacités, les autorités et les responsabilités en matière de cybersécurité soient fortement réparties dans l'écosystème complique encore l'identification de solutions durables. Aucune partie prenante ne peut relever le défi unilatéralement. Souvent, les principaux coûts d'une attaque de cybersécurité ne sont pas
supportée par la victime initiale, ce qui entraîne des externalités négatives et des incitations mal adaptées pour améliorer les comportements à risque en matière de cybersécurité. Ces caractéristiques nous ont trop souvent amenés à conceptualiser les solutions de manière trop fragmentée, réactive ou progressive. En conséquence, les défis discrets en matière de cybersécurité ont tendance à être traités au détriment de la prévention proactive des cyberattaques et de la réduction du risque systémique de cybersécurité sur une base holistique.

L'ampleur, la gravité et la complexité de la menace de la cybersécurité représentent aujourd'hui un risque existentiel pour l'avenir de la nation - ce qui exige l'exploration d'une approche fondamentalement nouvelle afin d'identifier des solutions plus audacieuses pour un Internet plus durablement défendable et sûr. Le Comité consultatif présidentiel sur les télécommunications pour la sécurité nationale (NSTAC) reconnaît qu'il existe de nombreuses bonnes pratiques et politiques connues qui, si elles étaient appliquées plus judicieusement, amélioreraient de manière mesurable la sécurité et la sûreté de l'internet. Toutefois, le présent rapport est axé sur la poursuite d'efforts de transformation plus importants qui modifieront fondamentalement le niveau par défaut de la sécurité et de la sûreté de l'internet. Cette poursuite constituera un défi

déterminant pour la génération et, comme la course à l'espace qui l'a précédée, elle peut servir d'inspiration et constituer le fondement du maintien du leadership technologique mondial des États-Unis dans les décennies à venir. Bien que les États-Unis n'aient pas encore vécu un événement galvanisant unique, à la manière de Spoutnik, pour cybersécurité, la nation doit faire preuve de la force d'âme et de la prévoyance nécessaires pour prendre des mesures audacieuses et proactives avant qu'un tel événement catastrophique ne se produise.

[1] Kirstjen M. Nielsen, "Remarks by Secretary Kirstjen M. Nielsen at the RSA Conference" (remarques, San Francisco, CA, 17 avril 2018) Discours, https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference.

2.0POURQUOI LA CYBERSÉCURITÉ NÉCESSITE-T-ELLE UN "MOONSHOT" ?

La première phase de recherche du NSTAC pour cette étude s'est intentionnellement concentrée sur des disciplines autres que la cybersécurité où la nation, et dans certains cas le monde, a organisé des activités contre la réalisation d'un résultat très ambitieux. L'examen de ces efforts historiques de type "moonshot" a permis de dégager un consensus commun : Les efforts de type "moonshot" ont un temps et un lieu distincts dans l'histoire. Ils nécessitent une convergence unique de forces politiques, sociétales, technologiques et autres pour créer l'environnement favorable nécessaire à leur réussite. [2] En fin de compte, ces forces se rassemblent de manière à aboutir à un consensus sociétal autour de deux grands principes : (1) le défi est d'une telle importance que l'échec n'est pas un résultat acceptable ; et (2) la conviction que l'échec est une fatalité sur la trajectoire actuelle, en l'absence d'une approche fondamentalement nouvelle. Ces principes s'appliquent directement et complètement à l'environnement de cybersécurité actuel et futur.

Mais un travail important reste à faire pour favoriser une compréhension nationale commune de la nature et de la gravité du défi de la cybersécurité. Cela commence par l'élaboration d'une réponse claire et convaincante à la question "Pourquoi" afin de justifier les investissements nationaux importants, les réalignements de priorités et même les sacrifices personnels qui seront nécessaires pour réaliser des progrès réels et durables face à ce défi particulièrement complexe. L'un des objectifs fondamentaux de ce rapport est de contribuer à catalyser un plan d'action national qui recadre et élève la cybersécurité au rang de défi économique et de sécurité nationale presque unique.

En tant que nation, les États-Unis ont fondamentalement échoué à articuler le défi de la cybersécurité d'une manière qui incite et assure ce niveau d'action collective. En raison de la complexité de la cybersécurité, la nation a trop souvent cloisonné l'ensemble du défi et l'a caractérisé en termes essentiellement techniques. Cette approche a souvent exclu les principales parties prenantes de la discussion, les laissant mal informées et estimant qu'elles n'ont aucune responsabilité ou capacité à contribuer à relever le défi. Le gouvernement américain doit définir le défi de la cybersécurité de manière plus large, en précisant que les facteurs politiques, éducatifs et de comportement humain sont aussi importants que l'innovation technologique pour une solution à long terme et qu'un plus large éventail d'experts doit être mis à contribution.

La cybersécurité en tant que défi national apporte également une réponse claire et convaincante à la question "Pourquoi maintenant ? Le peuple américain semble avoir accepté les atteintes à la protection des données qui compromettent ses informations personnelles comme le prix à payer pour la commodité de la technologie. Cependant, il est peu probable qu'ils tolèrent à l'avenir des cyberattaques ayant un impact direct et physique sur leur vie. Dans un environnement numérique où l'information n'existe de plus en plus que sous forme de bits et d'octets, il existe une ligne de démarcation de plus en plus étroite entre une société numérique fonctionnant sans heurts et reposant sur des bases numériques fiables et l'effondrement chaotique de la société qui résulterait de l'érosion de cette confiance.

Sur la trajectoire actuelle, il est très probable que dans les dix prochaines années, les États-Unis subiront des cyberattaques plus graves et physiquement destructrices que celles qui ont été subies jusqu'à présent. Pour les prévenir, il faudra adopter une approche proactive, stratégique et systématique de la défense qui galvanise l'action collective du peuple américain. Cette approche doit commencer par une déclaration des dirigeants nationaux, soutenue au plus haut niveau du gouvernement américain, de l'industrie et du monde universitaire, qui présente le défi de la cybersécurité non plus comme un risque acceptable, mais comme une menace existentielle pour le mode de vie fondamental du peuple américain.

Les dirigeants de la nation doivent articuler ce "pourquoi et maintenant" d'une manière ambitieuse et optimiste. S'il est important d'être franc sur les conséquences négatives de l'inaction, les dirigeants nationaux doivent également épouser les effets positifs et en cascade d'une action ciblée, accélérée et globale de la nation en faveur d'un Internet fondamentalement sûr et sécurisé. Ces effets positifs et en cascade pourraient être similaires aux résultats de la mobilisation nationale autour du programme spatial. Au cours du premier tir de lune, des investissements massifs dans la recherche et le développement (R&D) répartis entre le gouvernement américain, le secteur privé et le système universitaire ont conduit à des percées techniques spectaculaires et à des innovations inattendues en médecine, en science des matériaux et en technologies GPS qui ont constitué le fondement du leadership technologique mondial des États-Unis dans les décennies qui ont suivi.

Les États-Unis possèdent une grande partie des bases technologiques en matière de cybersécurité, ce qui fait que cette recherche est plus qu'un simple exercice académique. Les percées technologiques récentes et à court terme (explorées en profondeur dans le *rapport* du NSTAC *au président sur la vision stratégique des technologies émergentes3)* dans des domaines tels que l'informatique quantique, l'intelligence artificielle (IA) et l'apprentissage machine, l'informatique en nuage et les communications 5G créent le potentiel pour des défenses de cybersécurité plus simplifiées et automatisées, en transférant davantage de moyens de pression et l'équilibre général du pouvoir aux défenseurs de la cybersécurité.

Les gouvernements et l'industrie doivent prendre en compte ces questions technologiques et les questions interdépendantes de politique, de processus et de comportement, afin d'évaluer, de hiérarchiser et d'encourager efficacement les actions en faveur des innovations qui offrent le plus grand effet de levier et, en fin de compte, un avantage contre les cyberacteurs malveillants. Cela commence par une déclaration d'intention stratégique axée sur les résultats, ambitieuse et stimulante.

---

[2] Lisa Goldman et Kate Purmal, "How to Launch a Successful Moonshot," (Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 20 février 2018).

3.0 PLAN D'ACTION DE L'INITIATIVE "MOONSHOT" EN MATIÈRE DE CYBERSÉCURITÉ

Les États-Unis sont sur la voie de l'incrémentalisme dans leur approche de la cybersécurité. Il est difficile de conceptualiser une trajectoire de progrès fondamentalement nouvelle, mais le pays doit tout simplement abandonner sa mentalité insoutenable et coûteuse en matière de cybersécurité. Cela exigera un leadership national au plus haut niveau pour galvaniser les ressources et les énergies en vue d'une poursuite plus audacieuse. Pour réussir, l'initiative doit devenir véritablement "nationale", sous l'impulsion d'une direction charismatique, d'un plan d'exécution complet et d'une coalition d'experts gouvernementaux, industriels et universitaires.

Cette section, le *plan d'action de l'Initiative Moonshot sur la cybersécurité*, détaille les recommandations stratégiques liées à l'exécution pratique et à l'opérationnalisation de l'Initiative Moonshot sur la cybersécurité. Elle détaille les mesures concrètes que le gouvernement américain peut prendre pour mener à bien cette

en utilisant ses pouvoirs et ses capacités uniques pour défendre et organiser stratégiquement, de diriger, de financer et de responsabiliser les activités de l'ensemble du pays en fonction des objectifs définis. Le message général est ici simple : Bien qu'il puisse être difficile de visualiser et impossible de prévoir toutes les actions à long terme nécessaires pour réaliser un environnement Internet fondamentalement "sûr et sécurisé" au cours des dix prochaines années, cette administration peut faire preuve de leadership en prenant des mesures spécifiques à court terme qui produisent des gains immédiats et jettent les bases d'une vision à long terme plus audacieuse de la cybersécurité.

Le NSTAC ayant pour mission de conseiller le président, les autres recommandations contenues dans ce rapport sont orientées vers des actions spécifiques que le gouvernement américain peut prendre pour faire avancer cette initiative. Le NSTAC reconnaît et célèbre la nature mondialement interconnectée de l'Internet. Il sera essentiel d'établir un partenariat étroit avec des partenaires de même sensibilité. Toutefois, étant donné la portée de la charte du NSTAC, nos recommandations sont axées sur les mesures que le gouvernement américain peut prendre pour servir de modèle aux nations partageant les mêmes idées. Toutefois, ces recommandations ne doivent pas être interprétées comme des actions que le gouvernement américain devrait prendre unilatéralement, mais plutôt comme des actions que le NSTAC recommande au gouvernement américain de prendre pour renforcer l'écosystème au sens large. Souvent, cela nécessitera une consultation étroite et directe avec les parties prenantes non gouvernementales au cours du processus d'élaboration des politiques et des initiatives. En conséquence, de nombreuses recommandations de cette section font directement référence à l'exercice par le gouvernement américain de ses capacités de rassemblement et de mobilisation pour diriger ce processus de collaboration.

[3] NSTAC. *Rapport du NSTAC au Président sur la vision stratégique des technologies émergentes*. (Washington, DC : NSTAC, 14 juillet 2017) 2017 NSTAC Publications, https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

Initiative "Moonshot" en matière de cybersécurité
Actions recommandées : Calendrier

- Annoncer l'initiative "Moonshot" en matière de cybersécurité/remettre la déclaration d'aspiration (*section 3.1*) lors du lancement
- Établir un Conseil de la cybersécurité (*section 3.2.1*) au moment du lancement
- Établir la composante non gouvernementale du Conseil (*section 3.2.2*). Lancement + 60 jours
- Définir le cadre stratégique et les priorités nationales en matière de R&D pour la cybersécurité (*Section 3.4) Lancement* + 120 jours
- Lancement d'un processus multipartite pour définir les grands défis (*Section 3.5*) Lancement +180 jours
- Lancement du premier grand défi de la cybersécurité (*section 3.5*) Lancement +1 an

3.1 Faire une déclaration d'intention

Recommandation clé : Le président ou le vice-président devrait présenter et défendre stratégiquement une initiative "Moonshot" en matière de cybersécurité afin de signaler clairement que la résolution durable des problèmes de cybersécurité de la nation est un impératif stratégique unique. Cette proclamation devrait être faite dans un forum d'importance historique, tel que l'État de l'Union ou une allocution conjointe spéciale au Congrès, afin de souligner cette priorité nationale.

En examinant les messages historiques relatifs aux initiatives à grande échelle, y compris le discours original du président Kennedy, le NSTAC a identifié plusieurs caractéristiques communes qui doivent être intégrées dans une proclamation sur la cybersécurité au niveau présidentiel ou vice-présidentiel. Parmi les principales caractéristiques, citons

- **Un objectif clair et convaincant : la** déclaration comportait un objectif succinct, basé sur les résultats, articulé de manière à réduire la complexité à quelque chose qui peut être largement compris par l'ensemble de la société.

- **Une tonalité d'aspiration : la** déclaration a formulé le défi et sa solution attendue en termes optimistes qui favorisent les objectifs nationaux, par opposition à "vendre la peur" ou les conséquences négatives de l'inaction.

- **Une chronologie comprimée :** La déclaration présentait un calendrier clairement articulé et établi, soulignant l'urgence de la résolution.

- **Une approche audacieuse et non prescriptive :** La déclaration était intentionnellement de nature audacieuse pour susciter le scepticisme et un dialogue productif sur sa faisabilité. [4]

Recommandation clé : Compte tenu de ces caractéristiques, le NSTAC recommande que le président ou le vice-président fasse une déclaration d'intention d'aspiration : *"Rendre l'Internet sûr et sécurisé pour le fonctionnement du gouvernement et des services essentiels pour le peuple américain d'ici 2028".*

Le NSTAC a trouvé cette déclaration d'aspiration efficace dans la mesure où elle est considérée comme spécifique dans son intention mais souple dans son interprétation. Le terme "sûr" a été spécifiquement choisi parce que les conceptions sociétales de la sécurité ont été déterminées comme étant plus universellement comprises, instinctives et
identifiable - surtout si on le compare aux termes techniques plus ambigus communément associés à la cybersécurité. Le terme "sûr" a également été jugé instructif dans la mesure où il reconnaît à juste titre que les menaces de cybersécurité transcendent désormais le domaine numérique et constituent de véritables menaces physiques pour la sécurité publique, alors que la société adopte de plus en plus un monde de voitures connectées et de systèmes d'infrastructures critiques dépendant d'Internet.

Le terme "sûr" a également été déterminé à porter un degré d'ambiguïté productif, essentiel pour catalyser une conversation nationale plus solide. Par exemple, pour réaliser un Internet "sûr", quelles technologies de base la nation doit-elle privilégier pour les investissements de R&D à long terme ? Comment les États-Unis doivent-ils réformer leur système éducatif pour former des experts en cybersécurité bien formés et encourager les citoyens à adopter de meilleures pratiques en matière de cybersécurité ? Comment les politiques relatives à la chaîne d'approvisionnement des technologies de l'information doivent-elles s'adapter pour assurer plus fondamentalement la sécurité ?

Le NSTAC ne prétend pas avoir toutes les réponses à ces questions difficiles, dont beaucoup seront des compromis en matière de gestion des risques et ne seront pas de nature binaire. Par ses conclusions, le NSTAC espère catalyser un dialogue national plus large qui englobe ces conversations complexes et, parfois, difficiles, car il s'agit de défis qui doivent simplement être surmontés pour l'avenir de la nation. La section 3.4, *Définir le cadre et les piliers stratégiques,* explore plus en profondeur ce type de questions.

Peut-être plus important encore que le contenu de la déclaration d'aspiration, il s'agit de savoir qui délivre le premier message et où l'individu le délivre. Cet individu doit être un homme fort et

[4] Lisa Goldman et Kate Purmal *L'effet Moonshot : Disrupting Business as Usual* (San Carlos, CA : Wynnefield Business Press, 2016).

un leader charismatique, une personne considérée avec légitimité par de multiples parties prenantes et motivée par l'intérêt national au sens large. Cette personne doit articuler la vision pour mettre l'accent sur un engagement de continuité et d'investissement soutenu dans l'Initiative Cybersécurité Moonshot sur le long terme - imperméable aux transitions de l'administration et à la partisanerie politique. Cela nécessitera un niveau d'aspiration et d'unité d'effort entre et au sein des pouvoirs exécutif et législatif qui n'a pas été observé depuis un certain temps.

L'évaluation du NSTAC est que seul un niveau d'importance présidentielle ou vice-présidentielle peut générer la mobilisation nationale appropriée autour de ce défi avec une urgence semblable à celle du temps de guerre. Lorsque le président ou le vice-président commence à articuler l'initiative, il doit le faire en étroite coordination avec les responsables du cabinet, les dirigeants du Congrès, les chefs d'entreprise et les universitaires concernés afin de démontrer une unité d'effort réelle et symbolique qui s'étend à des éléments de la société bien au-delà de la communauté traditionnelle de cybersécurité. Le lieu et le forum de présentation doivent également être d'une grande importance historique ; le Capitole américain pour un discours sur l'état de l'Union ou un discours conjoint spécial au Congrès sont des exemples représentatifs appropriés qui permettraient de faire comprendre l'importance stratégique et historique de cette initiative nationale.

3.2 Établir une gouvernance pour une approche globale de la nation

Toutefois, il ne suffit pas de faire une déclaration d'intention ambitieuse. La déclaration doit être profondément ancrée dans un cadre stratégique clair et des principes partagés. Elle doit être soutenue par une structure de gouvernance claire qui permette à des groupes de parties prenantes répartis au sein du gouvernement, du secteur privé, des universités et de la société civile de contribuer et de concentrer leurs énergies et activités collectives vers les objectifs nationaux définis et de plus haut niveau de l'initiative "Cybersécurité".

Avant que l'initiative ne soit officiellement présentée au public par le président ou le vice-président, la Maison Blanche devrait mener un processus interne visant à établir une structure de gouvernance pour l'initiative "Cybersécurité Moonshot". De manière générale, le NSTAC définit la gouvernance comme la manière dont l'Initiative Moonshot sur la cybersécurité organise les participants, autorise les autorités décisionnelles, fixe les objectifs et impose des mesures de responsabilité pour garantir les progrès. Une évaluation solide et complète des modèles de gouvernance et d'organisation appropriés sera fondamentale pour la viabilité et l'efficacité à long terme d'une initiative nationale distribuée de cybersécurité.

Recherche de clés : L'initiative "Cybersécurité Moonshot" ne sera couronnée de succès que si elle s'appuie sur une unité d'action qui tire parti à la fois des autorités et des capacités uniques de l'ensemble du gouvernement et des efforts harmonisés de l'ensemble du secteur industriel et universitaire.

La cybersécurité est un défi intrinsèquement réparti, avec des autorités, des rôles et des responsabilités uniques qui sont partagés dans l'ensemble de l'écosystème public, privé et universitaire. Toutes ces capacités doivent être exploitées efficacement dans un modèle de sécurité collective pour faire
des progrès significatifs. La mise en œuvre et le succès de l'initiative "Cybersécurité Moonshot" dépendront d'un système très distribué de groupes de parties prenantes qui sont effectivement habilités, dotés de ressources et mobilisés.

Sur la base d'une compilation des résultats de plusieurs réunions d'information, le NSTAC a

élaboré le graphique ci-dessous pour visualiser conceptuellement comment une compréhension commune des rôles et responsabilités distribués, et une vision stratégique peuvent aider à concentrer, et non à limiter ou à étouffer, l'innovation ciblée sur des domaines définis qui peuvent conduire à un internet plus fondamentalement sûr et sécurisé. Conceptuellement, cela inclut la pression descendante exercée par les plus hauts niveaux du gouvernement américain pour définir l'intention stratégique, et la pression ascendante exercée par les moteurs opérationnels du secteur privé et du monde universitaire qui définissent activement les priorités en matière d'innovation et dirigent le progrès.

Figure 1 : *Modèle conceptuel de l'orientation de l'ensemble de la nation vers les objectifs définis de l'initiative "Cybersécurité Moonshot".*

3.2.1 Ensemble du gouvernement

Recommandation clé : Au sein du gouvernement américain, la Maison Blanche devrait mettre en place un Conseil de la cybersécurité ("Conseil") pour diriger et superviser stratégiquement l'initiative. Le Conseil sera responsable et habilité à : établir une intention stratégique, augmenter la visibilité nationale, plaider pour un financement durable, développer en collaboration des stratégies au niveau national, réunir les parties prenantes et créer des politiques et des processus qui habilitent et incitent les entités non gouvernementales à accélérer l'innovation dans des domaines définis de la cybersécurité.

Le Conseil doit être officiellement présidé par le président ou le vice-président et composé de fonctionnaires de niveau ministériel issus des ministères et organismes concernés. De nouveaux bureaux devraient être créés au sein des ministères et organismes existants, avec la responsabilité et l'autorité de mettre en œuvre et d'exécuter les directives politiques interinstitutionnelles du Conseil. Ces bureaux doivent comprendre les départements des entités de haut niveau ayant la responsabilité et l'autorité de diriger l'engagement du secteur privé et des universités dans les initiatives de cybersécurité, comme indiqué dans les recommandations du rapport. Sur la base de la capacité démontrée et de l'autorité du Congrès à diriger la collaboration avec la communauté des infrastructures critiques, le NSTAC recommande que le Département de la sécurité intérieure (DHS) soit habilité à assumer les responsabilités principales pour ce type d'engagement des parties prenantes.

En outre, le Conseil devrait disposer de mécanismes formels pour désigner des entités non gouvernementales qui contribueront directement à la stratégie de l'Initiative et au processus d'élaboration des politiques dans le cadre de la structure officielle du Conseil. Le Conseil devrait avoir une composante non gouvernementale officielle, composée de représentants d'entités essentielles du secteur privé et du monde universitaire. Le président devrait déterminer la structure et les pouvoirs qui régissent la participation des entités non gouvernementales et le niveau d'autorité de ces représentants en ce qui concerne la prise de décision globale du Conseil. Toutefois, le NSTAC est fermement convaincu que les responsabilités et les pouvoirs des participants non gouvernementaux au sein de la structure de direction du Conseil doivent dépasser les responsabilités traditionnellement accordées aux participants non gouvernementaux dans les organes consultatifs gouvernementaux.

Modèle illustratif : Conseil national de l'espace pangouvernemental

En juin 2017, le président Trump a signé le décret 13803, *Reviving the National Space* Council, qui rétablit le Conseil national de l'*espace en* tant que forum multipartite dirigé par le gouvernement américain et chargé de coordonner l'élaboration et la mise en œuvre des politiques spatiales nationales. Le Conseil national de l'espace offre un modèle de gouvernance utile, avec de nombreux attributs organisationnels que le NSTAC recommande au Conseil de la cybersécurité sur l'espace, notamment

- Présidé par le vice-président, le Conseil est composé de représentants du niveau du cabinet.
- Les entités non gouvernementales officiellement impliquées dans le processus de prise de décision par le biais du groupe consultatif des utilisateurs du Conseil national de l'espace, composé d'experts de haut niveau issus du secteur privé et du monde universitaire.
- Bureaux correspondants au niveau des départements/agences chargés de la mise en œuvre des politiques du Conseil national de l'espace (y compris le ministère de la défense, le ministère du commerce et la NASA)
- Capacité à élaborer et à publier efficacement des politiques du pouvoir exécutif conçues pour abaisser les barrières et renforcer l'écosystème de l'industrie spatiale nationale au sens large. Le Conseil national de l'espace a publié trois directives sur la politique spatiale nationale au cours de sa première année d'existence.

Un directeur exécutif nommé par le président devrait diriger l'initiative sur le plan opérationnel et être responsable et habilité à maintenir la visibilité de toutes les activités nationales de l'initiative "Moonshot" en matière de cybersécurité. Le directeur exécutif devrait être responsable de :

- Des activités d'élévation déterminées à fournir le plus grand levier stratégique vers le résultat d'un environnement Internet sûr ;
- Communiquer les objectifs stratégiques à long terme de l'initiative, décomposer l'effort en ses composantes essentielles, communiquer aux parties prenantes la manière dont chaque composante s'intègre dans l'initiative globale et diriger sa mise en œuvre ;
- Reconnaître et coordonner la valeur que chaque groupe de parties prenantes peut apporter à l'objectif global et la manière dont les groupes peuvent créer des synergies pour optimiser davantage la valeur
- Identifier les parties prenantes et faire des recommandations sur la manière d'inciter les parties prenantes à agir en faveur des objectifs communs de l'initiative "Cybersécurité Moonshot".

3.2.2 Industrie et universités

Le rôle de leader du secteur privé et du monde universitaire dans l'Initiative Moonshot sur la cybersécurité au sens large ne peut se limiter aux personnes officiellement nommées pour servir au sein du Conseil officiel
construire. Les entités gouvernementales ne peuvent pas seules lancer, gérer ou soutenir l'Initiative Moonshot sur la cybersécurité. La structure de l'initiative doit refléter la nature hautement distribuée de l'Internet et susciter activement l'engagement enthousiaste et la participation soutenue au Conseil d'un groupe diversifié de parties prenantes ayant des rôles, des responsabilités et des pouvoirs complémentaires en matière de cybersécurité.

Ce faisant, la gouvernance de l'Initiative Moonshot sur la cybersécurité doit reconnaître que le centre de gravité de l'innovation dans ce pays a évolué, passant d'une R&D principalement financée par le gouvernement américain à une R&D financée par le secteur privé. Dans le premier "Moonshot", le président Kennedy a présenté son aspiration comme un mandat national, en invoquant la lutte entre la liberté et la tyrannie et, ce faisant, a obtenu une participation notable des entrepreneurs et des entreprises privées. L'initiative "Cybersécurité Moonshot" doit dépendre encore plus fortement de divers groupes d'acteurs du secteur privé et du monde universitaire.

Recommandation clé : L'initiative "Cybersécurité Moonshot" doit engendrer une approche nationale, y compris un modèle de gouvernance coopérative reliant le gouvernement, l'industrie et les universités afin d'aligner leurs capacités et activités inhérentes à la réalisation des objectifs de sécurité et de sûreté de l'internet. Cette approche devrait inclure une structure commerciale de type consortium qui facilite la coopération, partage les ressources et les récompenses et travaille en étroite collaboration avec les partenaires gouvernementaux et universitaires pour atteindre des objectifs communs.

Le leadership de la Cybersecurity Moonshot Initiative va émerger, par nécessité, dans de nombreux forums distribués. Si elle est efficacement galvanisée au niveau présidentiel ou vice-présidentiel, l'idéal serait de mettre en place volontairement une myriade de consortiums indépendants à but non lucratif, d'associations éducatives et d'autres efforts communs pour atteindre les objectifs définis par l'initiative. Le rôle du gouvernement américain, par l'intermédiaire du Cybersecurity Moonshot Council, serait d'encourager, de faire connaître, voire de financer sélectivement les réalisations de ces entités indépendantes si elles sont alignées sur les objectifs stratégiques de l'Initiative Moonshot sur la cybersécurité.

Un certain nombre d'exemples historiques illustrent ce modèle. Par exemple, à la fin des années 1990, le gouvernement américain - par l'intermédiaire de la Maison Blanche, de l'Institut national de la santé et du Congrès - a fourni un financement important et a soutenu stratégiquement de grandes parties du projet du génome humain. Toutefois, la réalisation finale du projet a été le produit d'activités largement indépendantes d'entités comme la Celera Corporation et de plus de 20 universités et entités de recherche du monde entier qui composaient le Consortium international de séquençage du génome humain. [5]

Dans les années 1980 et 1990, un certain nombre d'efforts ont été déployés par plusieurs parties prenantes pour défendre l'avance technologique des États-Unis contre les entreprises étrangères fortement subventionnées par leur

[5] "L'achèvement du projet sur le génome humain : Frequently Asked Questions", 30 octobre 2010, Institut national de recherche sur le génome humain, https://www.genome.gov/11006943/.

gouvernements. Le résultat a été la création de consortiums d'entreprises tels que le Semiconductor Manufacturing Technology Consortium (SEMATECH)[6] et la Microelectronics and Computer Technology Corporation (MCC). Ces consortiums étaient des sociétés privées à but non lucratif, à charte du Congrès, conçues spécifiquement pour aider la nation dans des domaines spécifiques de recherche et de développement commercial. En fin de compte, plus de 100 entreprises ont travaillé ensemble pour résoudre les problèmes technologiques de l'époque à grande échelle, ce qui a permis de réaliser des percées importantes dans des domaines tels que les puces électroniques et l'infrastructure Internet.

Modèle illustratif : Ensemble de l'industrie et du monde universitaire
La société de microélectronique et de technologie informatique

Confrontée à la perte de la supériorité technologique américaine au profit des entreprises japonaises en raison du niveau accru de l'aide gouvernementale, la Microelectronics and Computer Technology Corporation (MCC) a été fondée en 1982. Parrainée par l'administration Reagan, conçue par d'anciens membres de la communauté du renseignement américaine, promulguée par le Congrès et dirigée par de récentes personnalités du gouvernement, la MCC a fait appel à de grands fabricants d'ordinateurs et de semi-conducteurs, à des représentants d'écoles technologiques d'élite et à des groupes connexes pour favoriser la croissance technologique.

En vertu de la *loi nationale sur la recherche coopérative de 1984, le* MCC a joué un rôle essentiel dans le développement des technologies d'IA, des tactiques d'ingénierie inverse et de la création de fonctions de recherche fondamentales sur Internet. Elle a été l'une des premières entreprises à enregistrer une adresse électronique ".com". Le MCC a rassemblé des organisations disparates pour partager le personnel de recherche et les fonds d'investissement rares, collaborer sur des objectifs communs et développer des solutions qui bénéficieront à l'ensemble de la nation.

* Source : The Microelectronics and Computer Technology Corporation[7]

3.3 Autres considérations clés de l'initiative "Moonshot" en matière de cybersécurité

Le lancement d'une initiative officielle de cybersécurité "Moonshot" nécessite des décisions sur des considérations complexes liées à la gouvernance, à la politique, au budget et à de nombreux autres facteurs afin de rendre l'effort inclusif, durable et réalisable. Cette section s'attache à présenter quelques considérations initiales, ainsi que des recommandations spécifiques pour éclairer les décisions organisationnelles clés que le directeur exécutif doit prendre avant le lancement de l'initiative "Cybersécurité Moonshot".

3.3.1 Considérations budgétaires

L'histoire fournit d'innombrables exemples de commissions et de comités consultatifs qui ont *conseillé* le président sur l'allocation des ressources mais n'ont contrôlé aucune ressource budgétaire. Dans ce cas, il est essentiel que le directeur exécutif ait un rôle officiel dans la planification et l'exécution du budget pour soutenir le processus et les recommandations de l'initiative "Cybersécurité Moonshot", y compris les activités relatives aux entités non gouvernementales. Le président et le directeur exécutif doivent articuler les besoins en ressources budgétaires fédérales, faire correspondre les ressources aux objectifs spécifiques de l'Initiative Moonshot sur la cybersécurité et s'assurer que les résultats justifient les investissements. Le niveau de financement et d'investissement du gouvernement américain dans la cybersécurité doit dépasser de plusieurs ordres de grandeur les niveaux actuels et doit être maintenu à des niveaux

comparables à ceux de la guerre pendant les dix ans que durera l'initiative.

6 Robert Hof, "Lessons from Sematech", *MIT Technology Review*, 25 juillet 2011, https://www.technologyreview.com/s/424786/lessons-from-sematech/.

7 David V. Gibson et Everett M. Rogers, *R&D Collaborations on Trial (*Boston : Harvard Business School Press, 1994), , Introduction, 15.

Recommandation clé : Le directeur exécutif de l'Initiative Moonshot sur la cybersécurité devrait se voir confier un rôle important dans la planification, la formulation et l'exécution du budget. Le président devrait envisager de désigner le directeur exécutif comme co-responsable, avec le directeur de l'Office de gestion et du budget, de l'élaboration de la proposition de budget annuel de l'administration. Le président devrait également envisager de demander au directeur exécutif de certifier que le budget annuel soutient pleinement les objectifs de l'initiative "Moonshot" en matière de cybersécurité. Enfin, le directeur exécutif doit disposer d'une ligne de communication régulière et directe avec les commissions des crédits et les commissions d'autorisation pertinentes du Sénat et de la Chambre des représentants des États-Unis

3.3.2 Mesurer le succès, définir les étapes du progrès et créer une dynamique

Recherche de clés : Le succès global de l'initiative "Moonshot" en matière de cybersécurité dépendra de la capacité du Conseil à articuler clairement l'objectif final stratégique, à identifier les étapes importantes des progrès et à élaborer des mesures pour démontrer la réussite. La manière dont le gouvernement articule et mesure le succès de l'Initiative Moonshot sur la cybersécurité est primordiale pour son impact éventuel et pour la manière dont les Américains se souviennent et se sentent par rapport à l'Initiative.

Comme pour le premier tir de lune dans l'espace, le gouvernement doit identifier des jalons concrets que le public peut facilement saisir, même si les détails sous-jacents sont complexes. Le discours du président Kennedy, diffusé publiquement en mai 1961, a implicitement tracé une voie régulière et visible pour l'avenir : Le vol suborbital, les vols multiorbitaux du programme Mercury, les manœuvres d'amarrage et les activités extra-véhiculaires du programme Gemini, le développement de la capsule Apollo à trois hommes, les vols orbitaux habités plus longs, les vols lunaires non habités et, enfin, l'alunissage de juillet 1969.

Sous ces événements importants, diffusés publiquement, les ingénieurs ont accompli un flot continu de triomphes en matière de développement : des boosters plus grands, plus de puissance, le développement de nouveaux carburants, des
fiabilité, et de meilleurs systèmes de nutrition et d'élimination des déchets. De même, il est essentiel de communiquer les progrès de l'initiative "Cybersécurité Moonshot" pour que le public reste concentré sur l'effort et pour lui rappeler de manière intermittente, voire continue, son importance nationale.

La difficulté et la complexité de l'objectif global ainsi que l'intensité et le rythme de l'action exigent que le gouvernement observe, mesure et, dans une certaine mesure, fasse respecter les progrès et l'achèvement de l'initiative "Cybersécurité Moonshot". Le Conseil Moonshot sur la cybersécurité, en coordination avec les parties prenantes identifiées, devrait être chargé de définir les étapes et les paramètres de l'Initiative Moonshot sur la cybersécurité. Il existe plusieurs mesures théoriques qui illustrent la manière dont l'Initiative Moonshot sur la cybersécurité pourrait mesurer la réalisation de sous-objectifs sur un horizon de 10 ans, notamment

- La cybersécurité ne figure plus en tête des menaces du Bureau du directeur du renseignement national pour l'évaluation de la menace mondiale ;

- Démonstration répétée et mesurable par les opérateurs d'infrastructures critiques, grandes et petites, de la capacité à maintenir la continuité du service pendant les cyberattaques ;

- Les mesures prises par le ministère du travail ou les associations industrielles concernant les postes vacants et les déficits de la cyberactivité diminuent ;

- Amélioration des sondages d'opinion concernant la perception de la sécurité et de la confiance dans l'infrastructure de l'internet et les technologies connectées à l'internet ;

- une diminution marquée du nombre d'incidents matériels de cybersécurité signalés aux organismes de réglementation étatiques et fédéraux, y compris la Securities and Exchange Commission ; et

- Une diminution du temps nécessaire pour remédier aux vulnérabilités connues ("time to patch") par les fournisseurs d'infrastructures critiques qui sont tenus de communiquer ces données.

3.4 Définir le cadre stratégique et les piliers

Recommandation clé : Après une période de consultation interne et externe, le Conseil Moonshot sur la cybersécurité devrait, dans un premier temps, élaborer publiquement un cadre stratégique afin de fournir une structure commune pour aider à organiser les activités de l'Initiative Moonshot sur la cybersécurité dans l'ensemble du pays. Comme point de départ recommandé, le Le NSTAC propose six piliers stratégiques : *Technologie, Comportement humain, Éducation, Écosystème, Vie privée et Politique* ; reconnaissant que la réalisation d'un Internet plus durablement sûr et sécurisé dans les 10 prochaines années nécessite une approche holistique et multidisciplinaire.

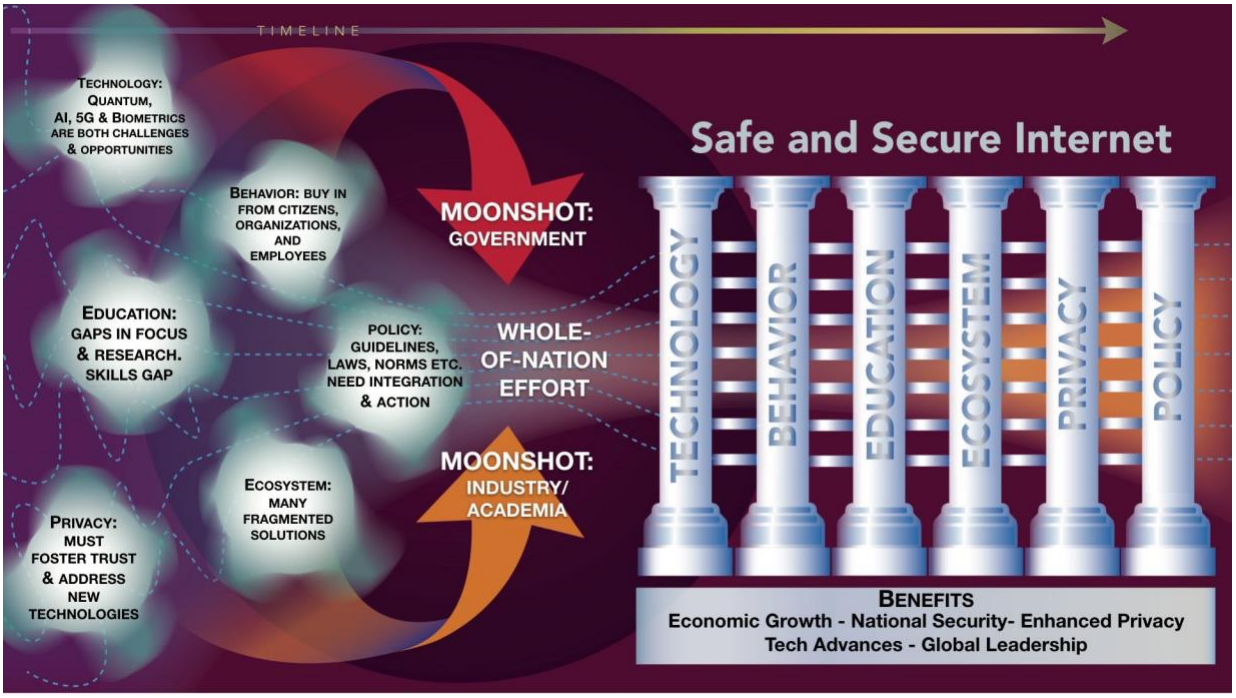

Figure 2 : La *recommandation du NSTAC concernant les piliers stratégiques de l'initiative "Cybersécurité Moonshot" - une proposition de structure organisationnelle pour les catégories d'activités requises, vastes mais interdépendantes.*

Le NSTAC a utilisé le concept de piliers stratégiques pour décrire les grandes catégories d'activités dans lesquelles une action nationale et multidisciplinaire doit être organisée afin de réaliser un environnement Internet fondamentalement sûr et sécurisé qui assure la confiance et la résilience des services gouvernementaux et essentiels connectés numériquement à un niveau fondamentalement supérieur à celui du statu quo. Les piliers stratégiques doivent être interprétés comme des flux de travail renforcés et interdépendants plutôt que séparés et indépendants. En effet, certains piliers stratégiques
Les piliers, tels que le pilier politique, sont principalement axés sur la réalisation directe des objectifs des autres piliers. Ces relations interdépendantes et habilitantes sont étudiées dans la section sur les dépendances entre piliers.

Le NSTAC recommande la poursuite d'un environnement Internet sûr et sécurisé sur l'actuel réseau ouvert
Internet afin d'assurer une interaction sûre avec les services essentiels d'une manière plus résistante et plus résiliente. Les principales caractéristiques permettant d'atteindre ce résultat sont les suivantes

- Les résultats et les actions seront attribuables ;
- Un comportement malveillant aura des conséquences ;
- Les identités iront au-delà des mots de passe et des IIP ;
- Le respect de la vie privée et la confiance seront renforcés et appliqués
- Un processus volontaire, avec option de participation, pour bénéficier de tout l'éventail des avantages.

Le NSTAC estime que cela doit être accompli d'ici 2028, dans le cadre d'un effort national, avant que les défis ne deviennent plus difficiles et complexes.

C'est le moment idéal pour amener le pays à exploiter plus efficacement les capacités technologiques émergentes afin de parvenir à un environnement Internet fondamentalement sûr - avec les progrès à venir de la technologie de communication de cinquième génération (5G) pour une connectivité considérablement accrue et un des infrastructures défendables, des percées en matière d'intelligence artificielle et augmentée pour une prévention plus automatisée des cyber-menaces, la biométrie comportementale qui peut offrir une toute nouvelle façon d'identifier les personnes, et de nouvelles capacités en matière de cryptage quantique qui peuvent résister à des attaques avancées dans un avenir lointain. Alors que tous ces progrès sont réalisés - tant par les États-Unis que par nos adversaires - sans cadre national pour orienter leur recherche, leur développement et leur déploiement vers le bien commun, nous risquons de perdre cette opportunité générationnelle.

Pour être clair, le NSTAC ne préconise pas la balkanisation de l'Internet, la création d'une infrastructure Internet entièrement séparée, ni ne prescrit un type spécifique d'architecture technique. Le NSTAC préconise un Internet fondamentalement sûr et sécurisé pour les services essentiels, caractérisé par l'exploitation d'avancées technologiques significatives, des incitations et des conséquences plus fortement alignées sur les comportements des utilisateurs qui favorisent des choix sûrs, des réformes de la politique de cybersécurité et de l'éducation, et une compréhension plus claire des rôles et responsabilités des écosystèmes dans la construction et le fonctionnement de cet environnement fondamentalement sûr pour des services essentiels spécifiques. Parmi les autres éléments souhaités qui ont été identifiés, on peut citer

- Résistance aux attaques ;
- Garantie de disponibilité des services ;
- Actions entièrement imputables aux utilisateurs, pour des fonctions de services critiques spécifiques ;

- Conséquences pour les actions malveillantes ;
- Protection assurée des informations privées ;
- La confiance des consommateurs et des entreprises dans les systèmes ;
- le principal canal de prestation des services de sauvetage
- Accessible à tous ceux qui en ont besoin.

Dans le présent rapport, le NSTAC utilise une définition des services "essentiels" et "vitaux" qui s'inspire de la politique bien établie du gouvernement américain. Grâce à une série de politiques couvrant les trois administrations actuelles et précédentes, le gouvernement américain s'est regroupé autour d'une stratégie de gestion des risques de cybersécurité qui donne la priorité à la protection des infrastructures critiques connectées à Internet. En application du décret 13636, *Amélioration de la cybersécurité des infrastructures critiques,* le DHS et les agences sectorielles concernées identifient et tiennent à jour chaque année une liste d'entités de la "Section 9", qui sont définies comme "des *infrastructures critiques où un incident de cybersécurité pourrait raisonnablement avoir des effets catastrophiques au niveau régional ou national sur la santé ou la sécurité publique, la sécurité économique ou la sécurité nationale"*."[8] Dans la *stratégie nationale de cybersécurité* publiée en septembre 2018, l'administration a défini plus précisément sept domaines prioritaires pour identifier les fonctions critiques et axer les activités de réduction des risques autour de : la sécurité nationale, l'énergie et l'électricité, la banque et la finance, la santé et la sécurité, les communications, les technologies de l'information et les transports. Mais la conception du NSTAC en matière de services vitaux n'est pas définie sur une base purement sur une base sectorielle. Le NSTAC soutient pleinement les nouveaux efforts de hiérarchisation de la gestion des risques liés aux infrastructures critiques, notamment ceux préconisés par le Centre national de gestion des risques du DHS, qui cherchent à identifier et à hiérarchiser la protection des fonctions intersectorielles jugées les plus essentielles à un Internet sûr et sécurisé.

Cadre de réalisation

Le NSTAC a jugé utile d'examiner et de classer les initiatives en fonction de leur probabilité de réalisation dans le cadre du calendrier de dix ans de l'initiative "Moonshot" de cybersécurité. Certaines initiatives ont été classées dans ce rapport à titre d'exemple. Ces catégories sont basées sur des informations et des recherches directes d'experts, sont subjectives et ne sont utilisées qu'à titre d'orientation générale. Un tel cadre serait utile au Cybersecurity Moonshot Council pour évaluer les initiatives proposées. Ces catégories sont les suivantes :

R : Il est prévu d'aborder la question en fonction de la trajectoire actuelle, y compris le rythme prévu de l'innovation et du développement technologiques.

B : Il est prévu d'y répondre par des investissements accrus, une concentration au niveau national et une collaboration en vue de développements technologiques clés et d'applications innovantes des cinq autres piliers stratégiques.

C : Il ne devrait pas être possible de relever ce défi sans un grand défi ciblé qui utilise divers outils d'incitation pour accélérer considérablement l'innovation dans l'ensemble du pays.

D : Pas d'approche raisonnable connue (Note : Le NSTAC n'a pas inclus d'initiatives "D", de sorte que ce qui

8 Exéc. Ordre. No. 13800, 82 FR 22391 (11 mai 2017), https://www.dhs.gov/sites/default/files/publications/EO-13800-Section- 9-Rapport - Résumé-20180508-508.pdf.

3.4.1 Pilier technologique

Objectif du pilier stratégique : exploiter stratégiquement les développements des technologies émergentes pour offrir un environnement Internet sûr et sécurisé, accessible aux citoyens moyens, aux entreprises et aux entités gouvernementales fédérales, étatiques et locales, afin d'effectuer des transactions de services critiques sans crainte de compromis.

Introduction et contexte

Les États-Unis dépendent de plus en plus d'Internet et des technologies numériques pour leur sécurité nationale, leur sécurité publique et leur prospérité économique. L'initiative "Cybersécurité Moonshot" vise à identifier, hiérarchiser, coordonner et accélérer le développement de technologies qui permettront de créer un environnement Internet plus fiable et capable de répondre aux besoins de sûreté, de sécurité et de respect de la vie privée d'un environnement moderne d'infrastructures critiques hyper-connectées.

Parmi les exemples représentatifs de ces technologies, citons l'intelligence augmentée, les communications quantiques et la cryptographie quantique résistante, la biométrie, les communications 5G et les technologies d'authentification. Ces technologies fourniront la base technologique nécessaire à la réalisation d'un internet plus sûr et plus sécurisé.
Le NSTAC comprend que les adversaires poursuivent ces mêmes technologies vers leurs propres objectifs. Par conséquent, l'initiative "Cybersécurité Moonshot" doit inclure de fortes mises en œuvre défensives de ces nouvelles technologies, notamment
la protection contre l'empoisonnement des données par l'entraînement au renseignement renforcé, basé sur le matériel
les vulnérabilités introduites dans les chaînes d'approvisionnement des écosystèmes, et les ordinateurs quantiques à usage général capables de décrypter les données existantes.

Changement de paradigme de l'identité

Pour les identités en ligne, nous devons aller au-delà des identités, des mots de passe et des informations personnelles identifiables - qui peuvent tous être compromis - pour trouver un moyen plus sûr et plus sécurisé d'identifier les utilisateurs. Le NSTAC recommande de tirer parti des avancées technologiques en matière de biométrie comportementale, d'intelligence augmentée et de nouvelles données de capteurs disponibles avec le déploiement des communications 5G, afin de fournir un score d'identité en temps réel (de 1 à 99 %) lorsqu'un justificatif d'identité est requis. Cette méthode assure la transparence pour des transactions sans friction, une assurance d'identité beaucoup plus grande basée sur
de nombreux points de données, et réduit considérablement le risque d'identité en ligne.

L'histoire de NSTAC : Études antérieures et futures relatives aux technologies émergentes

Le *rapport* 2017 du *NSTAC au Président sur la résilience de l'internet et des communications s'est* principalement concentré sur des recommandations à court terme liées aux meilleures pratiques et technologies existantes et connues qui, si elles sont mises en œuvre plus largement, pourraient avoir un impact immédiatement tangible sur la réduction de la menace de cyberattaques automatisées et distribuées. Le rapport a également renforcé les conclusions et les recommandations du *rapport du NSTAC au président sur la vision stratégique des technologies émergentes* (2017) et a conclu que le paysage technologique émergent, y compris les avancées significatives en matière d'IA, d'informatique dématérialisée, d'informatique quantique, de biométrie et d'authentification, constitue la base nécessaire pour réaliser une transformation radicale de la cybersécurité. Le NSTAC élabore actuellement un rapport sur l'amélioration de la résilience et la promotion de l'innovation dans l'écosystème des technologies de l'information et de la communication (TIC), qui examinera les capacités technologiques qui sont essentielles à la sécurité nationale et à la préparation aux situations d'urgence (NS/EP) des États-Unis et la manière dont le gouvernement peut gérer les risques à court terme, soutenir l'innovation et accroître la diversité des fournisseurs pour les capacités critiques NS/EP. Le NSTAC a l'intention d'achever ce rapport au printemps 2019.

Dans le cadre de ce rapport, le rôle du NSTAC n'est pas de prescrire des technologies spécifiques liées
comme des solutions singulières pour atteindre les résultats souhaités de l'initiative "Cybersécurité Moonshot". L'identification des domaines d'intervention prioritaires, ceux qui offrent le plus grand levier stratégique pour la mise en place d'un environnement de cybersécurité sûr et sécurisé pour les services essentiels, devra être le fruit d'un processus plus distribué. Toutefois, il existe de grandes catégories de technologies qui sont fondamentales pour la réalisation d'un environnement de cybersécurité sûr à l'avenir. Les exemples suivants ne sont qu'indicatifs. Avec le lancement de l'initiative "Cybersécurité Moonshot", les dirigeants du gouvernement américain peuvent utiliser divers leviers politiques pour inciter le secteur privé et le monde universitaire à accélérer la recherche et le développement de ces technologies essentielles qui changent de paradigme et leur donner les moyens de le faire :

- **Communications 5G et réseaux de prochaine génération :** Fournir un réseau de communication 5G (sans fil et câblé) conçu avec une sécurité, une interconnectivité, une confidentialité et une disponibilité accrues. Cela permettra d'obtenir une infrastructure beaucoup plus résiliente, d'étendre la connectivité sécurisée pour l'internet des objets (IoT), les systèmes de contrôle industriel, la téléphonie mobile, les soins de santé, et bien plus encore, avec une bande passante considérablement plus large et une latence en temps quasi réel. [9]

- **Intelligence artificielle** : Assurer le développement de l'apprentissage machine et de l'IA pour augmenter (plutôt que remplacer) les humains, tout en minimisant les risques tels que l'empoisonnement des données des systèmes d'IA. Permettre une réponse quasi autonome aux cyber-menaces à la vitesse de la machine afin d'obtenir des environnements informatiques auto-guéris qui identifient les défauts, empêchent l'exploitation de ces défauts et atténuent les impacts des défaillances.

- **Biométrie comportementale pour l'identité : La** biométrie comportementale combinée aux capacités d'IA peut réduire la dépendance à l'égard d'une identification personnelle facilement compromise, permettant la création de scores d'identité qui rendent les mots de passe obsolètes et donnent une plus grande transparence et confiance dans l'identification des utilisateurs. [10]

- **Communications quantiques et cryptographie quantique résistante :** Fournir une plate-forme de cryptage et de communication fiable, tirant parti des technologies quantiques, qui soit résistante aux ordinateurs quantiques à usage général (QGP), inviolable et disponible pour tous les services. Cette plateforme doit être mise en place avant l'arrivée des ordinateurs QGP qui peuvent décrypter les données sensibles existantes.

- **Résilience commune :** Assurer l'accès et la disponibilité des fonctionnalités requises pour les services critiques en automatisant et en simplifiant le modèle de consommation des outils et des capacités de cybersécurité axés sur la prévention des menaces. [11]

- **Micro-segmentation : La** mise en œuvre de microsegments cryptographiquement assurés au sein de réseaux distribués peut réduire les surfaces d'attaque, limiter la reconnaissance latérale et réduire considérablement les impacts des logiciels malveillants, afin de favoriser à la fois la résilience opérationnelle et les méthodologies de confiance zéro.

9 William O'Hern, "AT&T NSTAC Moonshot Briefing," (Briefing au sous-comité de cybersécurité du NSTAC Moonshot, Arlington, VA, 18 septembre 2018).

10 John M. Poindexter, "Internet Accountability", (Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 22 mars 2018).

11 Samuel Visner, "Cybersecurity Moonshots," (Briefing au sous-comité de la cybersécurité du NSTAC, Arlington, VA, 29 mars 2018).

Résultats escomptés

Bien que le NSTAC ne cherche pas à prescrire des solutions technologiques spécifiques, il définit les états finaux souhaités comme un défi organisationnel pour les innovateurs qui exploiteront les technologies précédemment décrites. La nation doit développer un modèle de confiance plus important qui permette une authentification plus forte et d'autres mécanismes de sécurité et assure une réaction rapide aux nouveaux défis en matière de sécurité et de protection de la vie privée. Les résultats escomptés sont les suivants :

- Renforcer la confiance des propriétaires et des exploitants d'infrastructures critiques ;
- Assurer la résilience des systèmes d'infrastructures critiques ; [12]
- Garantir le respect de la vie privée des utilisateurs grâce à des contrôles de données qui renforcent la confiance par la transparence, tout en reconnaissant les complexités de la propriété des informations partagées et des informations dérivées ;
- garantir que les utilisateurs puissent compter sur des appareils et des infrastructures qui fonctionnent correctement
- Veiller à ce que les informations et les dispositifs soient raisonnablement protégés contre les menaces en évolution.

Des exigences plus spécifiques seront nécessaires pour tirer pleinement parti des progrès technologiques potentiels afin d'assurer la sûreté et la sécurité fondamentales. Ces exigences sont notamment les suivantes

- Promouvoir les scores d'identité basés sur la biométrie comportementale (catégorie B) ;
- Développement de réseaux et de moyens de défense informatiques basés sur l'IA (catégorie B) ;
- Fournir la gestion des données de l'IdO avec 5G (catégorie C) ;
- Encourager la recherche et le développement en matière de cryptage et de gestion des clés résistants aux quanta, qui sont améliorés pour correspondre aux développements de l'informatique quantique (catégorie C) ;
- Promouvoir des opérations en ligne sûres et centrées sur le citoyen, comme le vote et la déclaration d'impôts, suivies d'autres fonctions d'infrastructures essentielles (catégorie C) ;
- Permettre la réalisation d'une ou plusieurs transactions entre deux entités avec confidentialité, intégrité et résilience (catégorie B) ;
- Gestion des relations des dispositifs physiques et virtuels connectés à l'internet (catégorie B) ;
- Permettre la capacité de prévenir, de se défendre, de fonctionner avec succès malgré l'incursion et de supprimer le code malveillant de manière autonome (catégorie B)

- Prévenir, identifier, suivre et remédier à la corruption des données et aux compromis dans tous les aspects d'une infrastructure critique (catégorie C).

[12] Ibid.

Dépendances interpiliers

Cette section comprend des références aux résultats, initiatives et activités d'autres piliers stratégiques ayant un impact sur la technologie, y compris ceux où le rythme du développement technologique peut être accéléré avec un soutien approprié. Par exemple :

- Si l'enseignement était plus accessible et stratégiquement axé sur les domaines informatiques essentiels, les progrès dans les technologies habilitantes essentielles pourraient être accélérés ;
- La formation des pouvoirs exécutif, législatif et judiciaire du gouvernement en matière de technologie pourrait contribuer à garantir que le gouvernement fournit le cadre politique adéquat pour permettre des avancées rapides et assurer le leadership des États-Unis dans les avancées technologiques nécessaires ;

- Garantir un cadre politique et rationaliser les obstacles réglementaires afin d'encourager et de récompenser les investissements et l'innovation du secteur privé dans les technologies qui sous-tendent l'initiative "Cybersécurité" ;

- élaborer un cadre qui incite les acteurs de l'écosystème à travailler ensemble pour atteindre les objectifs technologiques

- Développer des technologies qui abstractionnent la complexité de la sécurité de l'utilisateur final et permettent aux humains d'agir de manière plus sûre, par défaut.

3.4.2 Pilier du comportement humain

Objectif du pilier stratégique : la réalisation et le maintien d'un internet sûr et sécurisé nécessiteront des changements de comportement importants dans toutes les composantes de l'écosystème de la cybersécurité, y compris les utilisateurs, les fournisseurs et leurs employés. Toutes les parties devront comprendre leurs rôles spécifiques et leur relation au succès, ainsi que le lien étroit entre la cybersécurité et notre sécurité nationale. Pour progresser vers ce résultat, il faudra agir sur plusieurs fronts :

- Tirer parti de la communauté intrinsèque de l'innovation américaine en dynamisant et en élargissant l'intérêt pour la cybersécurité en tant que recherche socialement admirable, au-delà des technologues de niche, vers le grand public ;

- Fournir des incitations tangibles aux utilisateurs de l'internet pour qu'ils prennent des décisions plus sûres grâce à l'ensemble des outils qui renforcent le choix approprié de la sécurité et de l'authentification au lieu du choix le moins cher ; [13]

- démontrer aux citoyens que les bonnes pratiques en matière de cybersécurité font partie de la sécurité nationale en leur offrant des messages clairs, convaincants et peu techniques

- Veiller à ce qu'un ensemble adéquat d'outils, d'options et de technologies de sécurité soit accessible à un large éventail de citoyens américains, quel que soit leur niveau de connaissances techniques.

---

13 New York Cyber Task Force, *Building a Defensible Cyberspace* (New York : Columbia University School of International and Public Affairs, 28 septembre 2017), https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

Introduction et contexte

Les efforts nationaux précédents en matière de cybersécurité n'ont pas réussi à obtenir un succès généralisé, en partie parce qu'ils ne comportaient pas de composante comportementale humaine intégrée. Ces efforts antérieurs, bien qu'ils aient apporté des avantages considérables au pays, étaient souvent trop cloisonnés ou compartimentés pour offrir l'approche globale qu'exige le défi de la cybersécurité.

Comme pour l'initiative initiale, le "collectif de citoyens" doit être reconnu comme un acteur clé de l'initiative "Moonshot" de cybersécurité. Le grand public est souvent isolé des graves menaces de cybersécurité qui pèsent sur la nation et ne voit pas le problème comme affectant le bien-être national, et encore moins la sécurité nationale. [14,15] Il sera essentiel d'exploiter l'énergie et la concentration du "collectif de citoyens" pour faire face aux défis techniques et les résoudre, mais aussi pour naviguer dans le paysage politique, ce qui est primordial pour le succès de l'initiative "Cybersécurité".

En outre, cette initiative, comme le premier "moonshot", peut susciter des innovations dans d'autres domaines et laisser un héritage durable bien au-delà d'un environnement fiable et résistant pour les services essentiels. La stabilité, la sûreté et la sécurité de l'internet sont des facteurs clés pour l'innovation dans d'autres secteurs vitaux, tels que les soins de santé, l'énergie et les transports. Il s'est avéré impossible de trouver une solution aux problèmes auxquels nous sommes confrontés sur l'internet aujourd'hui. Il n'existe pas de solution technologique miracle pour résoudre nos principaux problèmes de cybersécurité. En outre, aucun progrès significatif n'a été réalisé pour faire les choix difficiles qui permettent de simplifier, de sécuriser et de sécuriser l'environnement. Les changements globaux dans les comportements des citoyens, des développeurs et des opérateurs technologiques, des fonctionnaires et des utilisateurs de l'internet ont été manifestement et frustramment insaisissables.

Résultats escomptés

Les activités de l'ensemble de la nation liées au pilier du comportement humain devraient se concentrer sur les résultats idéaux suivants :

- **Faire appel à l'imagination et à l'énergie du public américain :** La mise en place d'une base technologique sûre et sécurisée pour la fourniture de services essentiels nécessitera l'engagement de plus que les fournisseurs de technologie, les opérateurs de réseau et les professionnels de la sécurité qui se sont traditionnellement concentrés sur ces défis. Des changements fondamentaux dans le fonctionnement de l'environnement, la manière dont les utilisateurs s'engagent, l'idée d'identité en ligne et les rôles de chacun seront nécessaires pour soutenir la réalisation de cette ambitieuse avancée. Ces changements ne peuvent être couronnés de succès que si nous disposons d'une population dévouée, informée et engagée.
- **Dynamiser la communauté de l'innovation : L**'innovation doit être reconnue comme une composante culturelle essentielle de la vie américaine. Le montant du financement global de la recherche avancée continue à représenter un pourcentage décroissant du produit intérieur brut global, ce qui fait que chaque

14 Michael Daniel, Necessary Policy Foundations for a Cyber Moonshot," (Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 27 mars 2018).

15 Dov S. Zakheim, "Structuring Government to Address the Cyber Challenge," (Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 27 septembre 2018).

L'application du dollar de la recherche est encore plus critique. [16] Les universités ont plus à offrir dans ce domaine car elles sont traditionnellement un acteur clé de la communauté de l'innovation. L'établissement et le maintien d'une communauté alignée sur des objectifs de recherche communs ont permis de faire des découvertes importantes dans les domaines de la physique et des matériaux ; ce modèle doit être adapté et accéléré dans le domaine de la cybersécurité.

- La **décision la plus sûre est le choix par défaut :** Tous les utilisateurs, y compris les employés, les étudiants, les consommateurs et les citoyens, doivent prendre conscience de l'importance de la cybersécurité pour le bien de la société et comprendre leur rôle dans l'aide apportée à l'Amérique par des pratiques de cybersécurité améliorées. Dans le même temps, les choix en matière de sécurité doivent être aussi transparents que possible afin de ne pas ajouter de charges importantes ou d'exiger des connaissances techniques avancées ou une certaine sophistication, de sorte que les utilisateurs finaux prennent les bonnes décisions en matière de sécurité. Par exemple, des études ont montré que certains des changements les plus importants en matière de sécurité se sont produits lorsque les fonctions de sécurité sont activées par défaut et ne nécessitent aucune action de la part de l'utilisateur. [17, 18]

- Les **incitations renforcent le choix approprié des exigences de sécurité et d'authentification au lieu de se limiter à la sélection la moins chère :** Le gouvernement américain, par l'intermédiaire du DHS, du ministère du commerce et d'agences sectorielles, soutient et fournit depuis longtemps des recommandations et des directives volontaires dans le domaine de l'encouragement des résultats sécuritaires. Un élément nécessaire au succès de l'initiative "Cybersécurité Moonshot" sera l'influence directionnelle sur les acteurs privés qui incitent à l'action. Le gouvernement peut encourager les comportements par des incitations financières telles que des directives d'achat axées sur les résultats, l'organisation de grands défis ou de concours. [19] Dans le même temps, des campagnes de relations publiques, avec un fort rayonnement organisationnel, peuvent aider les consommateurs à prendre les bonnes décisions en matière de sécurité. Enfin, le gouvernement peut promouvoir la sécurité en établissant des exigences de sécurité pour les interactions entre le public et le gouvernement sur Internet.

Afin de transformer l'engagement en action, les utilisateurs doivent disposer de méthodes simples et peu coûteuses pour accroître leur sécurité. Ces mécanismes doivent être facilement compris et accessibles à un large éventail de citoyens américains. L'exploitation des innovations en matière d'apprentissage machine, d'autonomie et d'informatique permettra d'établir et de renforcer le choix de voies sécurisées pour les transactions critiques, ainsi que de gérer l'hyperconnectivité que la 5G aidera
établir. [20,21]

---

16 Jeffrey Mervis, "Data Check : La part du gouvernement américain dans le financement de la recherche fondamentale est inférieure à 50 %". *Science Magazine*, 9 mars 2017, http://www.sciencemag.org/news/2017/03/data-check-us-government-share-basic-research-funding-falls- below-50.

17 New York Cyber Task Force, Building a Defensible Cyberspace, https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

18 Randy Sabett, "The Role of Incentive-Based Policies in a Whole-Of-Nation Cybersecurity Strategy," (Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 26 septembre 2018).

19 Paul Afonso, "Utility Regulation and Coordination with State-Level Agencies as it Relates to a Cybersecurity Moonshot Initiative," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 26 septembre 2018).

20 Bruce McConnell, "Make the [Global] Internet Safe and Secure ... by 2028," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 22 août 2018).

21 O'Hern, "AT&T NSTAC Moonshot Briefing."

Dépendances interpiliers

L'ingéniosité et la volonté du peuple américain seront un élément déterminant du succès de l'initiative "Cybersécurité Moonshot". La mise en place, le maintien et l'application de cette ingéniosité et de cette volonté humaine se mesurent à l'aune de l'attention, de l'action et des ressources et auront un impact significatif sur les autres piliers stratégiques. Par exemple, les réformes éducatives, la protection des droits à la vie privée, l'évolution et l'adoption des technologies, et les politiques qui incitent les comportements à améliorer de façon exponentielle la sécurité sur Internet nécessiteront toutes une coordination et un développement conjoint entre les piliers stratégiques.

3.4.3 Pilier de l'éducation

Objectif du pilier stratégique : la nation doit accroître de façon spectaculaire la disponibilité, la qualité et la diversité des talents en matière de cybersécurité dans les domaines d'intervention stratégiques de l'initiative "Cybersécurité Moonshot", tout en sensibilisant tous les citoyens à leurs responsabilités communes dans la création d'un environnement Internet sûr et sécurisé. Cela implique une compréhension fondamentale des risques et des incitations positives à s'acquitter de leurs responsabilités en toute sécurité.

Introduction et contexte

Le développement et la mise en œuvre de technologies permettant un environnement sûr entraîneront une demande accrue de praticiens qualifiés pour développer et exploiter l'infrastructure de cybersécurité sous-jacente. Pour répondre à ce besoin, il faudra accroître l'étendue et la profondeur des programmes de sciences, de technologies, d'ingénierie et de mathématiques (STEM) de la maternelle à la 12e année qui alimentent les domaines d'intervention stratégiques alignés de l'initiative Moonshot sur la cybersécurité. La nation doit élaborer une stratégie nationale concertée pour augmenter rapidement le nombre de chercheurs et de professionnels qualifiés dans le domaine de la cybersécurité. Ces professionnels de la cybersécurité doivent être capables de favoriser les percées technologiques transformatrices les plus essentielles au développement et au maintien d'un environnement Internet sûr. Ces avancées doivent être réalisées en temps utile pour soutenir le développement, le déploiement et la mise en œuvre de la cybersécurité.
la culture des meilleures pratiques, en particulier dans les domaines clés identifiés comme l'informatique quantique, l'IA et les 5G.

De nouvelles incitations doivent être nécessaires pour augmenter les mécanismes normaux de l'offre et de la demande du marché afin de retenir les diplômés des STEM dans le milieu universitaire et dans les rôles de sécurité nationale et d'infrastructure du gouvernement. Ces incitations peuvent contribuer à attirer et à retenir dans la main-d'œuvre du secteur public de la cybersécurité des personnes qui, autrement, pourraient entrer dans le secteur privé. [22] Cela nécessitera un financement supplémentaire et des collaborations innovantes entre le gouvernement, les organisations à but non lucratif et le secteur privé pour développer de nouvelles initiatives d'éducation à la cybersécurité. [23]

Un solide enseignement des STIM à tous les âges sera également un élément fondamental de l'éducation à la cybersécurité et des initiatives de développement de la main-d'œuvre. Il faut tirer parti des technologies innovantes basées sur les nuages pour améliorer la rapidité et la qualité de l'enseignement des STIM. Par exemple, l'intelligence artificielle, les données de grande taille et la

réalité augmentée peuvent contribuer à lever les obstacles dans l'enseignement primaire et secondaire et dans l'enseignement supérieur. Ces programmes peuvent tirer parti de la gammification, des médias et des plateformes distribuées pour l'apprentissage. Efforts

22 Richard Heimann, "State of the Discipline : Artificial Intelligence," (Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 6 septembre 2018).

23 Maughan, "Briefing to the NSTAC Cybersecurity Moonshot Subcommittee."

doit également être fait pour retenir les meilleurs et les plus brillants diplômés des collèges et universités américains, dont beaucoup ne sont pas résidents américains, afin qu'ils restent aux États-Unis et rejoignent la population active américaine. En outre, les membres de l'écosystème devraient envisager un système de rotation ou d'échange, dans le cadre duquel les employés du gouvernement sont affectés, sur une base volontaire, à des fournisseurs commerciaux clés et vice-versa. [24] Bien que plusieurs initiatives d'éducation à la cybersécurité et de développement de la main-d'œuvre soient en cours, la nation est confrontée à une pénurie de main-d'œuvre critique et bien documentée. [25,26] Les études varient mais indiquent que d'ici 2021, il y aura au moins 350 000 postes de cybersécurité non pourvus aux États-Unis et jusqu'à 3,5 millions de postes vacants liés à la cybersécurité dans le monde. [27,28] Ce déficit massif persiste encore dans un environnement où les salaires dans le domaine de la cybersécurité sont en moyenne trois fois supérieurs au revenu national médian, les salaires du secteur privé étant nettement supérieurs à ceux du gouvernement. [29]

Enfin, travailler dans un environnement de cybersécurité fondamentalement sûr peut entraîner un certain niveau de désagrément personnel : un changement de paradigme pour l'utilisateur moyen. Les utilisateurs finaux sont souvent le maillon de sécurité le plus faible d'un système, que ce soit en raison d'une intention malveillante, d'un manque de formation ou d'une négligence. [30] Les gouvernements, les universités et le secteur privé doivent s'engager à contribuer à l'éducation sur cette transformation culturelle. [31]

Résultats escomptés

Les activités nationales liées au pilier de l'éducation devraient se concentrer sur les résultats idéaux suivants :

- L'accent mis au niveau national sur les impératifs de l'éducation peut être divisé en deux grandes catégories : (1) pour les carrières professionnelles dans les sciences et technologies liées à la cybersécurité ; et (2) pour la population générale des utilisateurs d'infrastructures de cybersécurité sûres et sécurisées ;

- Davantage de financement de la communauté de recherche universitaire - tant pour la recherche pure que pour la recherche appliquée - pour créer et développer des programmes de cybersécurité alignés sur le développement à court terme des domaines habilitants identifiés dans le pilier technologique ;

- Création de structures de consortiums pour l'éducation, avec rotation des emplois et pollinisation croisée entre le gouvernement, l'industrie et les universités ; [32]

- Développement spectaculaire des bourses et des subventions pour rendre l'enseignement des STEM plus accessible ; stages, apprentissages et placements de troisième cycle pour aider à combler les postes de travail critiques besoins ; un mentorat précoce et soutenu, en particulier pour les populations traditionnellement sous-représentées dans les STEM ;

- A fait évoluer les programmes d'enseignement des STEM pour introduire des sujets informatiques dans l'éducation de la petite enfance jusqu'au lycée (y compris par des cours de cybersécurité Advanced Placement), de sorte que la cybersécurité est considérée comme un parcours professionnel clairement défini et socialement admirable ;

- D'ici 2028, chaque élève de la maternelle à la 12e année devrait avoir une connaissance de base des meilleures pratiques d'hygiène cybernétique et connaître les principes fondamentaux des systèmes informatiques tels que définis par le National Institute of Standards and Technology (NIST)

- Des possibilités de citoyenneté grâce à des quotas de visas ciblés et des incitations financières à rester dans le
  La main d'œuvre américaine fait sortir du système éducatif américain les talents nés à l'étranger dans le domaine de la cybersécurité.

---

[24] Zakheim "Structurer le gouvernement pour relever le défi du cybernétique".

[25] "Meet the Millennials", 2017, Center for Cyber Safety and Education, https://iamcybersafe.org/research_millennials/.

[26] Center for Strategic and International Studies, *Hacking the Skills Shortage*, (Washington, DC : McAfee, 2016), https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf.

[27] Ibid.

[28] Douglas Maughan, "Briefing to the NSTAC Cybersecurity Moonshot Subcommittee," Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 28 août 2018.

[29] Kenneth Corbin, "Cybersecurity Pros in High Demand, Highly Paid, and Highly Selective", 8 août 2013, CIO, https://www.cio.com/article/2383451/careers-staffing/cybersecurity-pros-in-high-demand--highly-paid-and-highly-selective.html.

[30] Robert Hinden et Russell Housley, "Challenges to Deploying Security on the Internet," (Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 25 septembre 2018).

[31] Sabett, "The Role of Incentive-Based Policies in a Whole-Of-Nation Cybersecurity Strategy".[32] *Ibid*.

Dépendances interpiliers

Les résultats de l'éducation ont des interdépendances importantes avec les autres piliers stratégiques. En voici quelques exemples représentatifs :

- **Comportement humain :** Des incitations de type "carotte" et "bâton" seront nécessaires pour obtenir des résultats éducatifs clés, notamment des campagnes de sensibilisation du public pour (1) amener les étudiants à s'engager dans des domaines universitaires alignés sur l'initiative "Cybersécurité Moonshot" et (2) améliorer de manière significative les comportements de la population en général en matière de cybersécurité.

- **Ecosystème : D**'innombrables autres professionnels de la cybersécurité des secteurs public et privé devront être formés pour construire et exploiter l'infrastructure sous-jacente d'un environnement Internet fondamentalement sûr.

- **La vie privée :** Informer les Américains sur le rôle de la protection des données, sur leurs responsabilités connexes nécessaires au maintien de cette protection et sur les répercussions des politiques nationales sur leurs actions est un résultat essentiel de l'éducation.

3.4.4 Pilier de l'écosystème

Objectif du pilier stratégique : d'ici 2028, les États-Unis ont besoin d'un écosystème intégré de parties prenantes volontaires travaillant en collaboration pour concevoir, développer et exploiter un environnement sûr pour les services essentiels et vitaux. Un tel écosystème n'est pas quelque chose qu'une seule entité, même le gouvernement fédéral seul, peut simplement mandater. Il nécessite plutôt un ensemble d'organisations représentatives qui ont une motivation à la fois commerciale et de sécurité nationale, qui sont ouvertes à toutes les parties à différents niveaux de confiance et qui fonctionnent avec une approche nationale, qui adoptent une mentalité de "sécurité du marché" plutôt que de "premier arrivé sur le marché".

[33] Craig Fields, "A National Cyber Initiative". (Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 21 août 2018).

Introduction et contexte

Aujourd'hui, les entreprises technologiques proposent en grande partie des produits et services compétitifs disponibles sur le marché, généralement fiables, résistants, accessibles et susceptibles d'évoluer en permanence. Individuellement, ces entités peuvent apporter peu de changements, mais en travaillant dans le cadre d'un écosystème cohésif, le collectif peut fournir les solutions de sécurité plus intégrées requises. Cet écosystème de cybersécurité comprend des composantes des gouvernements (fédéral, étatique et local), des universités et du secteur privé, avec des tendances inhérentes à la fois à la concurrence et à la coopération. [34]

Les participants à l'écosystème comprennent tous ceux qui fournissent ou utilisent des infrastructures de services essentiels. Outre les chercheurs, les fabricants, les opérateurs et les utilisateurs, cela comprend également les chaînes d'approvisionnement des fabricants et des opérateurs. L'écosystème comprend les acteurs des entités du secteur privé, tous les niveaux de gouvernement, les citoyens, les organismes de normalisation, les entités étrangères, les organisations à but non lucratif, la communauté des logiciels libres et d'autres encore. Les composantes physiques et logiques de l'écosystème englobent les dispositifs, les composants, les réseaux, les services et les technologies appliquées qui fonctionnent ensemble pour créer l'Internet, les systèmes d'infrastructure essentiels et les services gouvernementaux.

Dans le contexte de l'initiative "Cybersécurité Moonshot", les services gouvernementaux et les infrastructures critiques ont besoin de garanties plus élevées en matière d'authentification, d'intégrité, de sécurité, de respect de la vie privée, d'accessibilité, de résilience et d'attribution. Alors que l'Initiative Moonshot sur la cybersécurité confie au gouvernement le leadership stratégique ultime, le secteur privé commercialisera la technologie et envisagera, construira et activera des capacités qui assureront un environnement Internet sûr en permanence. Alors que l'Initiative Moonshot sur la cybersécurité est proposée comme une initiative américaine, l Le gouvernement américain devrait continuer à coordonner étroitement son action avec les alliés de "Five Eyes" et d'autres nations partageant les mêmes idées.

L'écosystème actuel fournit des produits et des services très pratiques, qui permettent une utilisation accrue des ressources et offrent d'innombrables autres avantages. Ces solutions présentent des niveaux de sécurité, de résilience et de durabilité variables dans une base installée en constante expansion. Le marché américain des produits TIC s'efforce en permanence de trouver un équilibre entre le coût, la convivialité et les caractéristiques visibles pour le client, d'une part, et la sécurité et les capacités de résilience (souvent) invisibles, d'autre part. Les entreprises qui tentent d'offrir une sécurité supérieure à la moyenne sont remplacées par celles qui mettent les produits sur le marché en premier ou qui offrent des fonctionnalités équivalentes à un coût inférieur à celui des produits existants.

Les solutions commerciales prêtes à l'emploi et largement adoptées permettent de réaliser des économies d'échelle qui rendent toute tentative de créer des solutions personnalisées plus sûres irréalisable. Dans le meilleur des cas, les entreprises ayant des marques fortes tentent de réduire les risques en allouant des ressources à la gestion des risques, à la sécurité, à la résilience ou à la réponse aux incidents. Les normes ou les technologies qui nécessitent un déploiement à grande échelle pour améliorer la sécurité mais qui ne sont pas intrinsèquement liées à une valeur localisée, sont souvent sous-utilisées. [35]

Dans tous les secteurs, les briefers du NSTAC ont anticipé une application transformatrice sans précédent des nouvelles technologies. On s'attend à ce que les solutions deviennent sans cesse plus intégrées, interconnectées et

34 Ibid.

35 Hinden et Housely, "Challenges to Deploying Security on the Internet".

complexe. Parmi les exemples cités par les experts, citons les applications 5G pour les infrastructures de transport36 et l'ajout de ressources énergétiques distribuées37 au réseau, les menaces accrues que fait peser l'informatique quantique sur les protocoles de cryptage existants et la double nature de l'IA, qui peut être utilisée comme outil de sécurité préventive ou comme cyber-arme.

Résultats escomptés

En fin de compte, le gouvernement doit s'engager avec tous les participants de l'écosystème pour donner la priorité à la réduction des risques liés à la cybersécurité et parvenir à un environnement sûr et sécurisé pour les services essentiels d'ici 2028. Il existe trois résultats idéaux fondamentaux que le gouvernement américain doit atteindre pour permettre à l'ensemble de la nation de mener des activités liées au pilier de l'écosystème :

- Diriger et organiser l'écosystème à travers les secteurs qui unit les parties prenantes volontaires pour atteindre les objectifs communs nécessaires à un environnement sûr et sécurisé, sur la base d'une atténuation des risques importants, de normes, de technologies défensives, d'infrastructures et de services partagés. Une organisation d'intérêt public, suivant les traces réussies de SEMATECH et de MCC des années 1980 (explorées plus en détail dans la section 3.2.2, *Ensemble du secteur industriel et universitaire*) est un modèle utile pour ce type de structure de consortiums volontaires.

- Participer à la transition entre les phases de conception et d'exécution afin de permettre un environnement sûr et sécurisé, dédié à l'ensemble des services gouvernementaux et critiques, dans un délai de 10 ans. Les éléments fondamentaux de sécurité, de résilience et d'accessibilité nécessaires à la mise en place d'une infrastructure d'environnement sûre et sécurisée doivent être définis pour l'ensemble des services gouvernementaux, des infrastructures critiques et des autres secteurs qui participent volontairement. Les obstacles à la mise en œuvre - qu'ils soient financiers, techniques, réglementaires ou liés à la transparence - doivent être traités collectivement par le gouvernement américain. *38*

- Mettre à la disposition d'autres applications et solutions commerciales tous les éléments nécessaires à la fourniture sûre et sécurisée des services gouvernementaux et des services essentiels. Ces éléments comprennent une infrastructure de base résiliente, des services partagés, l'authentification des utilisateurs par la biométrie, des fournisseurs d'identité de confiance qui pourraient remplacer les mots de passe traditionnels, une identité forte pour les dispositifs et les services, l'attribution, la réponse aux incidents des fabricants et l'application de correctifs, les meilleures pratiques en matière de cybersécurité, les mécanismes de récupération à distance, l'assurance logicielle, les organismes de réponse aux cyberattaques et les autorités chargées d'enquêter sur les activités illégales et d'y remédier.

Dépendances interpiliers

Par définition, le pilier "Écosystème" comprendra des activités dont les interdépendances s'étendent à tous les autres piliers, car il représente la collecte, l'agrégation, l'intégration et l'exécution de l'initiative "Cybersécurité". Cette approche fondamentale, selon laquelle chaque pilier est vital pour la réussite du projet, ne peut être surestimée.

36 Terry Halvorsen, "5G Network Technology and Capabilities," (Briefing au NSTAC Cybersecurity Moonshot

Subcommittee, Arlington, VA, 5 septembre 2018).

[37] Afonso, "Réglementation des services publics et coordination avec les agences de l'État en ce qui concerne l'initiative "Moonshot" en matière de cybersécurité". [38] Jennifer Gustetic, "Designing and Implementing Grand Challenges : Learning from NASA's Experience", (Briefing à l

NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 23 août 2018).

3.4.5 Pilier de la vie privée

Objectif du pilier stratégique : la protection de la vie privée est un élément clé de la confiance nécessaire pour fournir des services essentiels à la nation. [39] D'ici 2028, les citoyens américains doivent pouvoir faire confiance aux systèmes d'information qui fournissent des services essentiels et exigeront avec une certitude pratique que les activités de l'initiative "Cybersécurité Moonshot" ne créent pas de vulnérabilités en matière de vie privée mais renforcent au contraire l'assurance de la protection de la vie privée et garantissent que les données et les transactions personnelles sont sécurisées, resteront protégées et sous leur contrôle. Le respect de la vie privée est un principe fondamental, fondamentalement lié aux objectifs de sûreté et de sécurité, qui doit imprégner tous les aspects de l'initiative "Cybersécurité Moonshot".

Introduction et contexte

Le respect de la vie privée dans un environnement Internet sûr devrait être un droit, faisant écho aux droits du [4e] amendement selon lequel les Américains seront "en *sécurité dans leurs personnes, leurs maisons, leurs papiers et leurs effets, contre les fouilles et les saisies abusives". "*La définition pionnière d'Alan Westin selon laquelle *"la vie privée est la revendication des individus, des groupes ou des institutions à déterminer eux-mêmes quand, comment et dans quelle mesure les informations les concernant sont communiquées à d'autres*", fournit un autre fondement. [40] La conception et les directives de la Cybersecurity Moonshot Initiative doivent intégrer les principes de la vie privée, qui s'étendent à toutes les interactions dans un environnement sûr. Un élément fondamental du pilier de la protection de la vie privée est que les individus, les groupes et les institutions détermineront comment et quand les informations personnelles seront communiquées. [41,] Enfin, l'architecture d'un environnement Internet sûr doit tenir compte de l'exposition importante des données personnelles due à l'augmentation de l'IdO et de la connectivité des capteurs entraînée par la mise en œuvre de la 5G. [42]

Dans le monde numérique, la protection de la vie privée s'est détériorée en partie à cause de la compromission constante des informations et de la prolifération de pratiques commerciales basées sur l'information qui, dans certains cas, n'ont pas été accompagnées de pratiques de sécurité appropriées. Presque tous les Américains ont été touchés par une atteinte à la protection des données qui porte atteinte à leur vie privée. Dans l'état actuel des choses, alors que le nombre d'appareils connectés et d'échanges de données augmente, la probabilité et l'impact de futures violations de la vie privée augmentent de manière exponentielle. Face à ces défis, l'initiative "Cybersécurité Moonshot" doit établir un niveau de confiance, de transparence et de respect de la vie privée pour garantir une adoption optimale dans des environnements Internet sûrs.

En ce qui concerne la vie privée, il est important de comprendre l'interaction entre l'anonymat et l'attribution. Tous les utilisateurs, quel que soit leur niveau d'attribution ou d'anonymat dans les activités en ligne, ont une attente valable en matière de respect de la vie privée et des choix quant à la manière dont leurs données seront utilisées. Si l'anonymat protège la vie privée, cela ne signifie pas que chaque communication sur l'internet, y compris l'accès à une infrastructure critique, doit être anonyme ; en effet, cet anonymat a souvent entraîné un manque de dissuasion à l'égard des activités préjudiciables. Dans le même temps, l'anonymat doit être protégé, en particulier dans les domaines où la peur ou l'incapacité d'exercer les droits fondamentaux de l'homme sont menacées. Dans l'environnement en ligne actuel, on ne craint guère les conséquences d'une activité malveillante ; l'environnement sûr doit tenir compte de cette réalité et s'efforcer de garantir que l'attribution est absolue pour des services critiques spécifiques et que les conséquences pour un individu sont non seulement possibles mais probables.

39 Poindexter, "Internet Accountability".

40 Westin, Alan, *Privacy and Freedom*, New York : IG Publishing, 1967.

41 "Revue de livres" : Privacy and Freedom", 24 novembre 2004, Privacilla.org, http://www.privacilla.org/fundamentals/privacyandfreedom.html.

42 O'Hern, "AT&T NSTAC Moonshot Briefing."

Résultats escomptés

Le pilier de la vie privée préconise des solutions pour aider à résoudre les problèmes dans de nombreux domaines fondamentaux de la vie privée. Parmi les domaines spécifiques qui doivent être abordés, citons : l'attribution et la responsabilité, la transparence, l'identité, le cryptage, les données des capteurs et l'intelligence augmentée. Le succès sera démontré avec transparence et sera basé sur des résultats objectifs et subjectifs, tels que :

- Toutes les transactions effectuées dans des environnements Internet sûrs seront pleinement responsables, avec une identité positive et une attribution complète ; [43]

- Une solide gouvernance de la protection de la vie privée, comprenant la contribution et la surveillance des principaux groupes de défense de la vie privée ainsi que des parties prenantes du gouvernement et de l'industrie, est intégrée dans l'ensemble de l'initiative Cybersécurité Moonshot ;

- La perception mesurée du grand public sera que les transactions de services essentiels sont sûres, sécurisées et fiables.

L'attribution et la responsabilité doivent pouvoir être appliquées dans des environnements sûrs, ce qui est presque impossible à réaliser aujourd'hui. En dehors de l'environnement sûr, l'absence d'attribution et de responsabilité est un impératif moral (par exemple, soutenir la liberté d'expression sans crainte de représailles) ; cependant, ce même environnement a de plus en plus permis des activités et des comportements qui constituent une menace pour notre société. L'asymétrie des risques et des récompenses favorise l'utilisateur malveillant.

Pour garantir le respect de la vie privée, il faut modifier la gestion de l'identité, le cryptage, l'utilisation des données des capteurs et le déploiement de l'intelligence augmentée. Par exemple, l'identité doit être sensible au contexte, en tirant les attributs nécessaires pour confirmer positivement l'identité d'une entité en fonction du besoin spécifique de savoir ; les protocoles de cryptage doivent être résistants aux quanta ; des protections doivent être mises en place pour éviter que la vie privée ne soit violée par l'utilisation de l'intelligence artificielle ; et les données des dispositifs et des capteurs de l'IdO doivent être gérées et protégées. L'établissement et la fourniture de notes d'identité, au lieu de mots de passe, dérivées
Les données biométriques et les capteurs en temps réel dévalueront les informations personnelles identifiables tout en augmentant la confidentialité dans un environnement sûr et en s'étendant à d'autres aspects de l'utilisation en ligne.

Dépendances interpiliers

Si la protection de la vie privée dépend de l'interaction réussie des cinq autres piliers, trois d'entre eux ont une codépendance particulièrement forte : une compréhension approfondie du *comportement humain* est essentielle pour mettre en œuvre avec succès les protections de la vie privée, l'élaboration de *politiques* qui soutiennent et encouragent les innovations en matière de protection de la vie privée doit être mise en œuvre et la *technologie, en* particulier avec l'émergence de la 5G et la maturation de l'IA pour les applications de cybersécurité.

43 Poindexter, "Internet Accountability".

3.4.6 Pilier politique

Objectif des piliers stratégiques : la nation doit apporter des changements ciblés et significatifs à sa politique, notamment aux lois, règlements, normes, règles et standards, afin de permettre des avancées majeures dans les autres piliers stratégiques. Ces changements peuvent être motivés par des mesures d'incitation, l'élaboration de normes nationales et internationales, les nouvelles menaces et les nouvelles technologies, tous ayant pour objectif commun de faciliter l'avènement d'un Internet plus durablement sûr et sécurisé. Les politiques devront reconnaître, encourager et récompenser les acteurs de cet espace pour leur comportement positif, ainsi que renforcer la responsabilité, l'attribution et les conséquences des comportements négatifs. [44] *Les* politiques devront évoluer, selon les besoins, pour assurer le succès de l'initiative "Cybersécurité" et tenir compte de l'ampleur internationale du défi.

Introduction et contexte

Aujourd'hui, la nation lutte pour suivre le rythme des cyber-menaces sophistiquées et croissantes, qui mettent fondamentalement en danger le mode de vie américain. La ferme résolution de la nation à préserver et à respecter l'ouverture de la société et la liberté de tous les citoyens crée des opportunités pour les criminels et les adversaires de nous exploiter et de nous nuire par le biais de cyber-attaques. Tout comme les services répressifs doivent relever le défi de mettre un terme au terrorisme visant des cibles vulnérables, les politiques relatives à l'internet ont rendu les systèmes essentiels vulnérables au vol de données privées et sensibles et à leur éventuelle perturbation ou destruction. Peut-être plus que toute autre transformation dans l'histoire de la nation, la politique de cybersécurité doit être adaptée pour dépasser les défis actuels et futurs posés par notre monde numériquement connecté.

Étude de cas : Politique et sécurité automobile

Les leçons du passé concernant l'utilisation d'une vaste réforme politique pour susciter le changement devraient être prises en compte dans cet effort. À la fin des années 1960, le gouvernement s'est associé à l'industrie automobile pour relever le défi de la création de conditions plus sûres pour le nombre croissant de personnes et de véhicules sur les routes. Le gouvernement a instauré des règles de sécurité strictes, à commencer par l'obligation de porter la ceinture de sécurité en 1968. En 1989, de simples airbags pour le conducteur sont devenus obligatoires, mais aujourd'hui, le marché exige de multiples systèmes d'airbags avant, latéraux et arrière pour augmenter la probabilité de survie des passagers en cas d'accident. Le gouvernement a également abordé le problème par le biais de réglementations sur la conception des routes, les contrôles de circulation et les limitations de vitesse obligatoires, ainsi que par des directives strictes pour les conducteurs, telles que des permis spécifiques à la catégorie de véhicule et de fortes conséquences pour les infractions au code de la route. Aujourd'hui, l'industrie introduit de nouvelles technologies comme le freinage automatique pour réduire encore plus la probabilité d'un accident. Tous ces changements ont été apportés pour le plus grand bien d'une société qui devient de plus en plus dépendante de l'automobile. Bien que le nombre d'accidents de la route, de blessures et de décès reste beaucoup trop élevé, les véhicules et les infrastructures utilisés par les conducteurs aujourd'hui sont nettement plus sûrs qu'il y a 20 ans.

Résultats escomptés

Ni le gouvernement, ni l'industrie, ni le monde universitaire ne peuvent résoudre les problèmes de cybersécurité de manière globale sans une réforme des politiques. Comme le montre l'approche pluridisciplinaire adoptée pour rendre les déplacements en voiture plus sûrs pour tous les Américains, trouver le bon équilibre entre la promotion d'un environnement de cybersécurité sûr pour les entreprises, les consommateurs et le gouvernement - sans pour autant étouffer l'innovation et la concurrence - nécessitera une application délicate de divers outils politiques.

[44] Visner, "Cybersécurité Moonshots".

Les politiques nationales et internationales, qui comprendront des lois, des normes et des orientations émanant de divers organismes, notamment le Congrès, les normes gouvernementales, les normes industrielles et technologiques, ainsi que les normes internationales de l'Internet, pourraient comprendre les éléments suivants

- Définir et investir dans l'infrastructure nécessaire pour concevoir et exploiter l'internet d'une manière fondamentalement plus sûre et plus sécurisée ;

- Définir les responsabilités et les pouvoirs des acteurs de l'écosystème de la cybersécurité qui incitent à des actions proactives et volontaires en fonction de leurs rôles spécifiques et responsabilités ; [45]

- Définir les limites des normes de cybersécurité au sein de l'environnement sécurisé et promouvoir la compréhension, par le public et le privé, du rôle que leurs décisions jouent dans notre sécurité nationale ;

- Définir des voies de décision pour les parties prenantes (notamment encourager les moteurs du marché ou développer de nouvelles ressources non technologiques) afin d'encourager les incitations positives et d'éviter les conséquences en cas de violation des normes comportementales établies pour les activités dans l'environnement sûr. Par exemple, définir des certifications de type "Underwriters Laboratory" pour les produits et services de cybersécurité ;

- élaborer des politiques qui encouragent la définition de la résilience des infrastructures critiques par l'utilisation de technologies à haute disponibilité et redondantes ainsi que par la responsabilisation des fournisseurs de services à fournir les services promis

- Définir des récompenses pour les partenariats de recherche et d'innovation en matière de cybersécurité entre l'industrie, le gouvernement et les universités afin d'orienter le développement des technologies de cybersécurité vers les exigences définies dans l'initiative "Cybersécurité Moonshot" et d'augmenter le volume et la qualité de la cybertechnologie américaine et des cyberprofessionnels de notre future main-d'œuvre.

Dépendances interpiliers

La politique est le catalyseur et le principal outil du gouvernement américain pour assurer le succès de l'initiative Cybersécurité Moonshot. À cette fin, le pilier *politique* soutient le pilier *technologique,* notamment par la définition de feuilles de route technologiques qui traitent de la sécurité ; du *comportement,* dans lequel
Les politiques de l'UE en matière de protection de la *vie privée, qui* garantissent le droit du public à déterminer l'utilisation de ses informations personnelles, et l'*éducation, dans laquelle les* efforts gouvernementaux visant à accroître le nombre de cyberprofessionnels ont des répercussions sur les politiques éducatives de la maternelle à la 12e année. Ces piliers aident à déterminer l'orientation générale de la gouvernance de l'initiative afin de créer un environnement sûr, fiable, résilient et accessible. Pour soutenir l'initiative globale "Cybersécurité Moonshot", la réforme des politiques devrait être

- Basé sur des incitations positives et l'évitement des conséquences négatives ;
- être pris en compte dès le début et tout au long des initiatives dans les autres piliers

stratégiques de l'initiative Moonshot sur la cybersécurité, et non à la fin comme une réflexion après coup ou une conséquence

- Juste et équitable pour le bien commun américain, tout en étant l'exemple pour le monde et en promouvant si possible des résultats internationaux positifs et la liberté de l'internet.

---

45 Par exemple, tant les entreprises utilisatrices que les fournisseurs d'infrastructures critiques devraient s'attendre à mettre en œuvre un cadre de cybersécurité accepté, tel que le NIST ou le SANS Institute, applicable par le biais des canaux de responsabilité sectoriels existants.

3.5 Les grands défis de l'initiative "Moonshot" en matière de cybersécurité

Recommandation clé : Après avoir défini le cadre stratégique de l'Initiative Moonshot sur la cybersécurité et les priorités nationales de R&D en matière de cybersécurité, le Conseil Moonshot sur la cybersécurité et les entités associées au niveau des départements devraient mener un processus national multipartite pour définir, identifier et lancer un ou plusieurs grands défis en matière de cybersécurité. Le Cybersecurity Moonshot Council peut également jouer un rôle essentiel pour accroître la visibilité et la
en encourageant les actions distribuées et alignées sur ses objectifs.

Tout au long de l'étude, les experts ont souligné à plusieurs reprises l'importance d'identifier un ou deux domaines initiaux spécifiques dans lesquels l'accélération de la concentration sur l'ensemble du territoire national pourrait produire des progrès démontrables sur un horizon de trois à cinq ans. Ces experts ont souligné l'importance de cette approche pour produire des percées plus immédiates, pour aider à créer une dynamique et pour établir un modèle de base pour la vision à plus long terme (10 ans) de l'initiative globale "Cybersécurité Moonshot". Le NSTAC a adopté le modèle bien établi des "grands défis" pour décrire cette approche en vue d'un ciblage spécifique. Les participants ont présenté diverses définitions de ce qui constitue un grand défi, notamment les suivantes

- Des objectifs scientifiques, technologiques et d'innovation audacieux mais réalisables qui exigent un grand nombre d'activités dans des disciplines techniques et non techniques ;

- Une "étoile polaire" pour les collaborations multidisciplinaires à fort impact entre le gouvernement, l'industrie, les universités, les organisations à but non lucratif et l'élite des scientifiques, des ingénieurs et des citoyens du pays ;

- un mécanisme permettant aux organisations de tirer parti de leurs compétences et capacités uniques pour résoudre des problèmes plus importants que ceux qu'elles peuvent résoudre seules avec succès ; et

- Un moyen de s'attaquer à bon nombre des problèmes les plus difficiles du siècle, en particulier ceux qui captent l'imagination de la société, et donc le soutien politique.

Le NSTAC a entendu des experts ayant une expérience directe dans la gestion d'initiatives "Grand Challenge" au sein du gouvernement, du secteur privé et de la communauté à but non lucratif. Ces activités ont couvert de nombreuses disciplines, et ont surtout été menées dans des domaines tels que l'espace, la biomédecine et la santé publique. Notre recherche a également révélé une importante communauté d'intérêt pour les grands défis au sein du gouvernement fédéral, avec des ressources importantes sur les meilleures pratiques agnostiques aux disciplines, fournies de manière centralisée par des ressources comme Innovation.gov et Challenge.gov, gérées administrativement par l'administration des services généraux. [46,47] Cependant, la cybersécurité en tant que discipline n'a pas

46 "Challenges of Challenge", 2018, Challenge.gov, https://challenge.gov/list.

47 "The Better Government Toolkit provides resources to build a better government through innovation", 2018, Innovation.gov, https://innovation.gov/toolkit/.

a développé une culture tout aussi solide d'innovation ouverte et de réflexion "au clair de lune", représentée par la communauté Grand Challenges. Le NSTAC estime que cela doit changer.

À cette fin, le NSTAC recommande que le Cybersecurity Moonshot Council dirige l'identification et le lancement d'un ou plusieurs grands défis ciblés en matière de cybersécurité. Pour identifier les candidats appropriés aux Grands Défis, le Conseil et les entités ministérielles associées devraient mener un processus de collaboration de six mois qui engage formellement les acteurs du secteur privé et du monde universitaire dans tout le pays. Il est essentiel que ce processus inclue des citoyens sans association professionnelle ou expertise en matière de cybersécurité afin d'insuffler une nouvelle réflexion dans ce dialogue.

3.5.1 Critères d'identification et d'évaluation

Une désignation "Grand défi" est appropriée pour un domaine de développement prioritaire spécifique dans lequel les progrès de l'ensemble du pays sont insuffisants et qui bénéficierait d'une attention nationale ciblée et d'une orientation stratégique (catégorie "C" dans la rubrique "Cadre de réalisation" introduite au début de la section 3.4, *Définir le* cadre *stratégique et les piliers*). Lors de l'évaluation des candidats potentiels au Grand Défi dans le cadre de ce processus multipartite, le Conseil doit proposer et pondérer plusieurs critères d'évaluation et questions clés, notamment

- **Rôle clair du gouvernement :** Le gouvernement a-t-il un rôle clair à jouer pour catalyser les activités de l'ensemble de la nation qui s'alignent sur l'initiative ? L'attention stratégique du gouvernement, la réduction des obstacles, les ressources ou les exigences peuvent-elles inciter à agir là où les précédents moteurs basés sur le marché se sont révélés insuffisants ?

- **Avantages de la collaboration : L**'initiative nécessite-t-elle des activités qui dépassent le cadre des autorités ou des forces du gouvernement ? L'initiative bénéficierait-elle d'un effort plus réparti, à plus grande échelle, qui tirerait parti de diverses sources de partenariat et de collaboration ?

- **Résonance sociale : L**'initiative peut-elle être articulée de manière à être largement comprise par l'ensemble de la société, en particulier par les experts non spécialistes de la cybersécurité, comme étant fondamentalement importante et stratégique sur une base nationale ?

- **Mesurable et réalisable :** Y a-t-il des étapes et des objectifs démontrables qui sont réalisables dans les dix ans de l'initiative globale "Cybersécurité" ?

- **Hautement évolutif : La** réalisation des objectifs de l'initiative produirait-elle un résultat susceptible d'être facilement, voire automatiquement, exploité dans les environnements de défense de la cybersécurité ?

- **Multidimensionnel : L**'initiative a-t-elle une portée large, suffisamment complète pour inclure des activités relevant de plusieurs piliers stratégiques ?

Un examen minutieux de ces critères et d'autres, bien que les contributions du processus multipartite de six mois, devrait aboutir à l'identification d'une déclaration spécifique basée sur les résultats, ainsi que des activités alignées sur la réalisation de ce résultat dans les six piliers stratégiques.

- La Maison Blanche a annoncé un prix pour réaliser le "Saint Graal" de la technologie de la cyber-IA dans les 5 ans
- Concours à grand renfort de public pour le développement d'algorithmes de prévention automatisée des menaces
- Innovations politiques/Campagnes de communication visant à rendre la discipline "AI pour le cybernétique" aussi prestigieuse que celle de "l'AI pour les véhicules autonomes".
- Modèles de consortiums éducatifs reliant le monde universitaire et l'industrie privée afin d'encourager, de développer et de conserver l'expertise en matière d'IA pour les applications de cybersécurité

3.5.2 Le rôle du gouvernement américain dans l'incitation à l'action par le biais des grands défis de la cybersécurité

Une fois la phase d'identification terminée, le gouvernement américain peut jouer un rôle essentiel pour accroître et maintenir la visibilité des grands défis de la cybersécurité tout au long de son cycle de vie.
Parmi les exemples représentatifs, on peut citer l'annonce du lancement du Grand Challenge au niveau présidentiel ou vice-présidentiel ou les célébrations de haut niveau des grandes avancées liées au Grand Challenge. Le gouvernement américain peut également susciter et maintenir un intérêt permanent en utilisant divers outils pour encourager et accélérer les activités nationales visant à réaliser le grand défi. Il s'agit notamment d'outils qui récompensent principalement la démonstration et l'obtention de résultats, conformément aux principes de l'approche "moonshot".

Pour être clair, le NSTAC ne propose pas que le gouvernement américain dirige unilatéralement le développement et le lancement de ces Grands Défis de la Cybersécurité et dirige toutes les activités associées. De nombreuses entités non gouvernementales, telles que XPrize et la Fondation Gates, ont une solide expérience dans l'exécution réussie des Grands Défis et des concours de prix associés pour atteindre des objectifs ambitieux et axés sur les résultats. Mais le gouvernement américain peut jouer un rôle essentiel en suscitant l'intérêt, en définissant la portée du défi et en créant une voie qui permette une démocratisation potentielle et de futures opportunités commerciales. En associant une vision inspirante et percutante à des technologies organiquement émergentes, telles que la fabrication d'additifs à faible coût, les applications en nuage et l'IA, ces grands défis de la cybersécurité peuvent être naturellement soutenus par les entreprises, les universités et les organisations à but non lucratif qui servent leurs propres priorités.

Category	Types
1. Pay-for-Performance	A. **Incentive Prizes**: Results-based market incentives that are designed to overcome market failures and catalyze innovation. Unlike "recognition" prizes that honor past achievements, "inducement" or "incentive" prizes encourage participants in the competition to achieve a particular goal.
	B. **Pay-for-Success Bonds**: Also known as a social impact bonds. The financing organization and the Federal, state, or local government enter into a contract that specifies the population to be served, the outcomes to be achieved, the measurement methodology to be used, and the schedule of payments to be made. The financing organization works with philanthropic and other investors to invest in innovative, data-driven service providers that can achieve results.
	C. Mi**lestone-Based Payments**: Terms in a contract in which the payment for each performance milestone established in the statement of work is not made until the prior milestone is proven to have been achieved. Risk is placed on the performer or vendor, unlike other contracts in which payment is either guaranteed with limited protections for quality of performance or in which payments are designed to support in advance the performer's effort to complete the next milestone.
	D. **Challenge Based Acquisitions**: A Federal Acquisition Regulation (FAR)-based acquisition approach that uses challenges to communicate the needed capability, encourage innovation in a minimally prescriptive environment, assess candidate offerings, and, ultimately, purchase the proven solution(s).
2. Purchase Commitments	A. **Advance Market Commitments (AMCs)**: Binding commitments to purchase, or to subsidize purchase, of a certain volume of a product at a fixed prize, if the product meets pre-defined performance characteristics
	B. **Non-Binding Purchase Commitments**: Non-binding commitments to purchase products can provide market pull, if there is both a clearly defined performance specification and a strong expression of interest from potential buyers.
	C. **Buyer's Consortia**: Cooperative agreements between purchasers of products that leverage the combined buying power of those purchasers to drive down the price of products
3. Accelerated Review or Exclusive Access	A. **Priority Review Vouchers**: An accelerated regulatory review offered to products that meet certain performance or cost criteria
	B. **Exclusive Access**: Unique or accelerated access to training, partnership, or procurement opportunities
	C. **Pilot and Third-Party Evaluation Opportunities**: Dedicated opportunities to deploy a pilot implementation a solution/intervention, potentially with resources for third-party evaluation 8

Figure 3 : Le *gouvernement américain dispose d'un large éventail de "mécanismes d'attraction" comme outils pour inciter à une action axée sur les résultats et alignée sur les grands défis définis.* [48]

4.0 CONCLUSION

Ce rapport du NSTAC a présenté le cas de la mise en place d'une initiative nationale de cybersécurité "Moonshot" dont l'objectif fondamental est de rendre l'internet sûr et sécurisé d'ici 2028. Cette initiative s'appuie sur un solide précédent historique de réussite collective face à un défi comportant des risques nationaux importants.

Ce rapport trace la voie d'un futur état de l'internet qui soit résistant et résilient, qui valorise la vie privée et la responsabilité personnelle, qui soit disponible et accessible, et qui exploite pour de bon les nouvelles capacités technologiques. Cette voie nécessitera des changements radicaux dans l'éducation et la politique, la mise en place de grands défis que les Américains peuvent relever, des incitations plus fortement alignées pour les comportements sûrs et des conséquences pour les comportements malveillants, et une compréhension fondamentale de la nature mondiale et interconnectée de l'internet. Le rapport présente une voie dans laquelle l'Amérique peut montrer l'exemple au monde et devrait servir à la fois de guide et d'avertissement, qu'en ce qui concerne la préservation de la confiance et de la sécurité de l'internet et de notre manière numérique de
la vie qui en dépend, l'échec n'est pas une option.

[48] Jennifer Gustetic, "Conception et mise en œuvre de grands défis : Learning from NASA's Experience", (Briefing au sous-comité du NSTAC sur la cybersécurité, Arlington, VA, 23 août 2018).

ANNEXE A : MÉTHODOLOGIE DE L'ÉTUDE DU SOUS-COMITÉ

Le sous-comité de la cybersécurité du Comité consultatif sur les télécommunications pour la sécurité nationale (NSTAC) du président était composé de représentants de plus de 20 entités gouvernementales, universitaires et du secteur privé de tout l'écosystème des technologies de l'information, des télécommunications et de la cybersécurité. En plus de la représentation des entreprises membres du NSTAC, le sous-comité a nommé des membres issus du monde universitaire pour s'assurer que le groupe représentait des perspectives importantes de l'approche globale de l'initiative Cybersécurité Moonshot. Le NSTAC a utilisé plusieurs méthodes pour recueillir des informations, notamment des briefings d'experts en la matière, l'examen de nombreux rapports et articles sur la cybersécurité, et la conduite d'examens politiques. Plus précisément, le NSTAC :

- a reçu 27 briefings officiels d'experts de l'industrie, des universités et du secteur public (annexe E), ainsi que de nombreux autres entretiens non officiels avec des experts externes

- A procédé à un examen des politiques, réglementations, rapports et documents de meilleures pratiques du secteur privé et du gouvernement fédéral en matière de cybersécurité.

> "Chaque fois que je rencontre un problème que je ne peux pas résoudre, je l'aggrave toujours. Je ne peux jamais le résoudre en essayant de le rendre plus petit, mais si je le rends assez grand, je peux commencer à voir les contours d'une solution".
>
> - Président Dwight D. Eisenhower

Au cours de la période d'étude qui a débuté en février 2018, le sous-comité "Cybersécurité" a tenu environ 50 réunions. Dans la première phase de l'étude, le sous-comité s'est délibérément concentré sur la réception de briefings d'experts ayant une expérience directe ou une expertise dans les efforts de type "moonshot" en dehors du domaine de la cybersécurité. L'objectif de cette approche était d'identifier les meilleurs diagnostics du domaine des modèles de pratique et des méthodologies permettant de déterminer comment les ressources de l'ensemble du pays ont été efficacement exploitées dans le passé en vue de la réalisation de résultats ambitieux. Le NSTAC a estimé que cela était essentiel pour libérer la réflexion au-delà des limites normales qui, selon nous, ont souvent limité notre dialogue national sur la cybersécurité. Parmi les exemples représentatifs, on peut citer les réunions d'information sur le projet du génome humain, la création du réseau de l'Agence des projets de recherche avancée /Internet, les grands défis de l'Agence américaine pour le développement international en matière de santé publique mondiale et le programme Apollo.

Dans la deuxième phase de l'étude, le sous-comité a entendu les principaux experts de la cybersécurité pour commencer à identifier les principes d'organisation communs et les résultats souhaités pour parvenir à un environnement de cybersécurité fondamentalement sûr et sécurisé. Parmi les exemples représentatifs, on peut citer les exposés d'experts sur les technologies critiques, l'éducation, la recherche et le développement, les grands défis et la politique d'innovation, ainsi que les modèles de gouvernance destinés à éclairer la structure de l'initiative "Cybersécurité Moonshot".

ANNEXE B : COMPOSITION DES SOUS-COMMISSIONS

MEMBRES DES SOUS-COMMISSIONS

M. Peter Altabef, Unisys Corporation et coprésident du sous-comité M. Mark McLaughlin, Palo Alto Networks et coprésident du sous-comité

M. Sean Morgan, co-chef du groupe de travail sur les réseaux Palo Alto et la cybersécurité
M. Thomas Patterson, co-responsable du groupe de travail "Moonshot" d'Unisys Corporation et de Cybersécurité

Nom	Société
M. Mark Bentley	Unisys Corp.
M. Christopher BoyerAT&T	, Inc.
Mme Cherilyn Caddy	Agence de sécurité nationale
M. John Campbell	Iridium Communications, Inc.
M. James Carnes	Ciena Corp.
Mme Terri Claffey	Neustar, Inc.
M. Mark Cohn	Unisys Corp.
Mme Kathryn Condello	CenturyLink, Inc.
Mme Amanda Craig-DeckardMicrosoft Corp.	
M. Michael Daly	Raytheon Co.
M. Darrell Durst	Lockheed Martin Corp.
M. Victor EinfeldtIridium Communications, Inc.	
M. Patrick Flynn	McAfee, Inc.
Dr. Boaz Gelbord	Dun & Bradstreet, Inc.
M. William Gravell	Groupe Diogène, LLC
Mme Katherine GronbergForeScout	Technologies, Inc.
M. Dean Hullings	ForeScout Technologies, Inc.
M. Rodney JoffeNeustar	, Inc.
Mme Ilana JohnsonNeustar	, Inc.
M. Kent LandfieldMcAfee	, Inc.
M. Gregory Lebovitz	Equinix, Inc.
M. William RyanDépartement de la sécurité intérieure	

M. Jerry Scarborough	Raytheon Co.
M. John Scimone	Dell, Inc.
M. Robert Spiger	Microsoft Corp.
Mme Roberta Stempfley	Institut de génie logiciel
M. Kent Varney	Lockheed Martin Corp.
M. Milan Vlajnic	Communication Technologies, Inc.
Dr. Prescott Winter	Oracle Corp.

GESTION DES SOUS-COMITÉS

Mme Helen Jackson	Comité consultatif présidentiel sur les télécommunications pour la sécurité nationale (NSTAC) Fonctionnaire fédéral désigné (DFO)
Mme Sandra Benevides	Remplaçant NSTAC MPO
Mme DeShelle Cleghorn	Remplaçant NSTAC MPO
Mme Kayla Lord	Département de la sécurité intérieure Soutien NSTAC
Mme Stephanie Curry	Booz Allen Hamilton, Inc.
Mme Laura Karnas	Booz Allen Hamilton, Inc.
M. Barry Skidmore	Total Systems Technologies Corp.

ANNEXE C : ACRONYMES

AI Intelligence artificielle

DHSDdépartement de la sécurité intérieure

Ministère de la Justice

DSB Conseil scientifique de la défense

FDA Administration des denrées alimentaires et des médicaments

GPS Système de positionnement global

TIC Technologies de l'information et de la

communication IoT Internet des objets

MCC Société de microélectronique et de technologie

informatique NASA Administration nationale de l'aéronautique et de

l'espace

NIST Institut national des normes et de la technologie

NS/EP Sécurité nationale / Préparation aux situations

d'urgence

NSTAC Comité consultatif des télécommunications pour la sécurité

nationale NTIA Administration nationale des télécommunications et de

l'information QGP Objectif général de Quantum

R&D Recherche et développement

SEMATECH Semiconductor Manufacturing Technology Consortium

STEMScience , Technology, Engineering, and Math

ANNEXE D : GLOSSAIRE

5G - Un futur réseau mobile de cinquième génération, dont l'Union internationale des télécommunications (UIT) n'a pas encore entièrement défini les spécifications. Il devrait permettre des débits de données de 10 gigabits par seconde et plus. Les déploiements commerciaux de la 5G ne sont pas attendus avant 2020 environ. (Newton's Telecom Dictionary)

Fabrication additive - Se définit comme le processus d'assemblage de matériaux pour fabriquer des objets à partir de données de modèles tridimensionnels (3D), généralement couche après couche, par opposition aux méthodes de fabrication soustractives telles que l'usinage. (An Additive Manufacturing Test Artifact, Shawn Moylan, John Slotwinski, April Cooke, Kevin Jurrens et M. Alkan Donmez, Journal of Research of the National Institute of Standards and Technology, Volume 119 (2014) http://dx.doi.org/10.6028/jres.119.017)

Intelligence artificielle - L'intelligence manifestée par des machines ou des logiciels. Terme popularisé par Alan Turing, il décrit historiquement une machine qui pouvait tromper les gens en leur faisant croire qu'elle était un être humain via le test de Turing. Récemment, les scientifiques dans ce domaine ont largement abandonné cet objectif pour se concentrer sur le caractère unique de l'intelligence des machines et apprendre à travailler avec elle de manière intelligente et utile. (Dictionnaire des télécommunications de Newton)

Intelligence Augmentée - Une conceptualisation alternative de l'intelligence artificielle qui se concentre sur le rôle d'assistance de l'IA, en soulignant le fait qu'elle est conçue pour améliorer l'intelligence humaine plutôt que de la remplacer. (whatis.techtarget.com/definition/augmented-intelligence)

Authentification - Processus par lequel un utilisateur, une source d'information ou simplement une information prouve qu'il est bien celui qu'il prétend être ; processus de détermination de l'identité d'un utilisateur qui tente d'accéder à un réseau et/ou à un système informatique. (Newton's Telecom Dictionary)

Biométrie comportementale - Traits comportementaux appris ou acquis, tels que la vérification dynamique des signatures et la dynamique de la frappe. (Programme et centre de ressources sur les normes biométriques du NIST)

Biométrie - Utilisation de caractéristiques biologiques mesurables, telles que la reconnaissance d'empreintes digitales, la reconnaissance vocale et les scanners de la rétine et de l'iris pour fournir une authentification. (Dictionnaire Newton's Telecom)

Cloud Computing - Modèle permettant un accès réseau à la demande à un ensemble partagé de capacités/ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services), qui peuvent être rapidement approvisionnées et libérées avec un minimum d'effort de gestion ou d'interaction avec le fournisseur de services. Il permet aux utilisateurs d'accéder à des services technologiques à partir du nuage de réseaux sans avoir connaissance, expertise ou contrôle de l'infrastructure technologique qui les soutient. Tant les données de l'utilisateur que les services de sécurité essentiels peuvent résider et être gérés dans le nuage de réseau. (Comité sur l'instruction relative aux systèmes de sécurité nationale (CNSSI) 4009, adaptée) (Rapport NSTAC 2016)

Infrastructures critiques - Systèmes et actifs, physiques ou virtuels, si vitaux pour les États-

Unis que leur incapacité ou leur destruction aurait un effet débilitant sur la sécurité, la sécurité économique nationale, la santé ou la sécurité publique nationale, ou tout

combinaison de ces questions. Les infrastructures critiques peuvent être détenues et exploitées par le secteur public et le secteur privé. [*Loi sur la protection des infrastructures critiques de 2001,* 42 U.S.C.519c(e)] (CNSSI 4009, adapté)

Cyber-attaque - Attaque, via le cyberespace, visant l'utilisation du cyberespace par une entreprise dans le but de perturber, désactiver, détruire ou contrôler malicieusement un environnement ou une infrastructure informatique ; ou de détruire l'intégrité des données ou de voler des informations contrôlées. (CNSSI 4009)

Cybersécurité - Capacité à protéger ou à défendre l'utilisation du cyberespace contre les cyberattaques. (CNSSI 4009)

Systèmes de contrôle industriel - Système d'information utilisé pour contrôler les processus industriels tels que la fabrication, la manipulation des produits, la production et la distribution. Les systèmes de contrôle industriel comprennent des systèmes de contrôle de surveillance et d'acquisition de données utilisés pour contrôler des actifs géographiquement dispersés, ainsi que des systèmes de contrôle répartis et des systèmes de contrôle plus petits utilisant des automates programmables pour contrôler des processus localisés. (NIST SP 800-53A, Révision 4)

Technologie de l'information - Équipement, processus, procédures et systèmes utilisés pour fournir et soutenir les systèmes d'information (informatisés et manuels) au sein d'une organisation et ceux qui s'adressent aux clients et aux fournisseurs. (Dictionnaire Newton's Telecom)

Internet des objets - L'ensemble des réseaux d'appareils interconnectés. (Dictionnaire des télécommunications de Newton)

Apprentissage automatique - Type d'intelligence artificielle dans lequel les ordinateurs utilisent d'énormes quantités de données pour apprendre à faire des tâches plutôt que d'être programmés pour les faire. (Oxford Learner's Dictionary)

Incident matériel de cybersécurité - un événement qui entraîne effectivement ou potentiellement des conséquences négatives pour les systèmes d'information ou les données d'une entreprise, dont on pourrait raisonnablement s'attendre à ce qu'il affecte la valeur des titres (de l'entreprise) ou influence les décisions des investisseurs. (ART. 33-10459).

Science des matériaux - Étude scientifique des propriétés et des applications des matériaux de construction ou de fabrication (comme les céramiques, les métaux, les polymères et les composites). (Merriam - Dictionnaire Webster)

Communications de **sécurité nationale/protection civile (NS/EP)** - Services de télécommunications utilisés pour maintenir un état de préparation ou pour répondre et gérer tout événement ou crise (locale, nationale ou internationale) qui cause ou pourrait causer des blessures ou des dommages à la population, des dommages ou des pertes de biens, ou qui dégrade ou menace la posture NS/EP des États-Unis (47 Code of Federal Regulations Chapitre II, § 201.2(g)). Les communications NS/EP comprennent principalement les capacités techniques soutenues par les politiques et les programmes qui permettent au pouvoir exécutif de communiquer à tout moment et en toutes circonstances pour remplir les fonctions essentielles de sa mission et pour répondre à tout événement ou crise (locale, nationale ou internationale), ce qui inclut la communication avec lui-même, les pouvoirs législatif et judiciaire, les

gouvernements des États, des territoires, des tribus et des collectivités locales, les entités du secteur privé, ainsi que le public, les alliés et les autres nations. Les communications NS/EP comprennent en outre les systèmes suivants

et les capacités à tous les niveaux du gouvernement et du secteur privé qui sont nécessaires pour assurer la sécurité nationale et pour gérer efficacement les incidents et les situations d'urgence. (Comité exécutif des communications NS/EP basé sur le décret (EO) 13618, *Assignation des fonctions de communication en matière de sécurité nationale et de préparation aux situations d'urgence* [2012])

Réseaux - Système(s) d'information mis en œuvre avec un ensemble de composants interconnectés, qui peuvent comprendre des routeurs, des concentrateurs, des câblages, des contrôleurs de télécommunications, des centres de distribution de clés et des dispositifs de contrôle technique. (Glossaire NIST des termes de sécurité de l'information - NIST IR 7298 - Révision 2)

Protocole - Ensemble de règles et de formats, sémantiques et syntaxiques, permettant aux systèmes d'information d'échanger des informations. (Glossaire des termes de sécurité de l'information du NIST - NISTIR 7298 - Révision 2)

Communications quantiques - Un domaine de la physique quantique appliquée étroitement lié au traitement de l'information quantique et à la téléportation quantique. Son application la plus intéressante est la protection des canaux d'information contre les écoutes au moyen de la cryptographie quantique. (www.picoquant.com/applications/category/quantum-optics/quantum-communication)

Informatique quantique - Une technologie informatique en développement qui exploite les propriétés des atomes pour créer un type d'architecture informatique radicalement différent grâce à la physique quantique. L'informatique quantique repose sur les caractéristiques de base d'un atome, comme la direction de son spin (de gauche à droite, de droite à gauche) pour créer un état, tel que "1" ou "0", autant que les ordinateurs classiques utilisent les variations de l'énergie électrique (polarité positive et négative). (Newton's Telecom Dictionary)

Cryptographie résistante aux quanta - Le cryptage résistant aux quanta est un ensemble d'algorithmes de cryptage à clé publique déployés qui résistent à être cassés par un ordinateur quantique pleinement fonctionnel (Rapport du NSTAC au Président sur la vision stratégique des technologies émergentes, 2017)

Assurance logicielle - Niveau de confiance dans le fait qu'un logiciel est exempt de vulnérabilités, qu'il ait été conçu intentionnellement ou accidentellement inséré à tout moment de son cycle de vie et qu'il fonctionne de la manière prévue. (NIST SP 800-163)

Menace - Toute circonstance ou tout événement susceptible d'avoir un impact négatif sur les opérations de l'agence (y compris sa mission, ses fonctions, son image ou sa réputation), sur les actifs de l'agence ou sur les personnes par le biais d'un système d'information, en raison d'un accès non autorisé, de la destruction, de la divulgation, de la modification des informations et/ou d'un refus de service. (NIST SP 800-53, CNSSI 4009, adapté)

ANNEXE E : BIBLIOGRAPHIE

Afonso, Paul. "Réglementation des services publics et coordination avec les agences de l'État dans le cadre d'une initiative de cybersécurité. Briefing au sous-comité de cybersécurité du Comité consultatif sur les télécommunications de sécurité nationale (NSTAC) du Président, Arlington, VA, 13 septembre 2018.

"Le programme Apollo (1963-1972)". 16 septembre 2013. National Aeronautics and Space Administration (NASA). https://nssdc.gsfc.nasa.gov/planetary/lunar/apollo.html.

Bade, Gavin. "'Darknet' et les communications quantiques pourraient améliorer la cybersécurité du réseau, disent les scientifiques au Sénat." *Utility Dive*. 27 octobre 2017. https://www.utilitydive.com/news/darknet-and-quantum-communications-could-enhance-grid-cybersecurity-scie/508357/.

Bauer, Lujo. "Cybersécurité, IA et ML : opportunités et défis". Briefing au NSTAC Cybersecurity Moonshot Subcommittee Arlington, VA, 18 septembre 2018.

"The Better Government Toolkit" fournit des ressources pour construire un meilleur gouvernement grâce à l'innovation. 2018. Innovation.gov. https://innovation.gov/toolkit/.

"Revue de livres" : Vie privée et liberté". 24 novembre 2004. Privacilla.org. http://www.privacilla.org/fundamentals/privacyandfreedom.html.

Braga, Matthew. "Dans le futur, nous laisserons la chasse aux bugs logiciels aux machines." *Carte mère.* 16 juin 2016. https://motherboard.vice.com/en_us/article/mg73a8/cyber-grand-challenge.

Calvert, Kenneth et Gianchandani, Erwin. "NSF/CISE : Une vue d'ensemble et des "photos de lune"". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 15 mars 2018.

Centre d'études stratégiques et internationales. Hacking the Skills Shortage. (Washington, DC : sponsorisé par McAfee, 2016). https://www.mcafee.com/us/resources/reports/rp-hacking- skills-shortage.pdf.

Cerf, Vinton. "L'avenir de l'Internet des objets". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 5 avril 2018.

"Les défis du défi". 2018. Challenge.gov. https://challenge.gov/list.

Le Conseil de coordination du secteur des communications. *Livre blanc technique de l'industrie*. Washington, DC : NTIA, 17 juillet 2017. https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.

Le Conseil pour la sécurité, la fiabilité et l'interopérabilité des communications. *Groupe de travail 2A : Rapport final sur les meilleures pratiques en matière de cybersécurité*. Washington, DC :

Communications fédérales

Commission, mars 2011. https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

Corbin, Kenneth. "Les pros de la cybersécurité sont très demandés, très payés et très sélectifs". 8 août 2013. CIO. https://www.cio.com/article/2383451/careers-staffing/cybersecurity- pros-in-high-demand-highly-paid-and-highly-selective.html.

"Secteurs des infrastructures critiques". 22 août 2018. Département de la sécurité intérieure (DHS). https://www.dhs.gov/critical-infrastructure-sectors.

Daniel, Michael. "Les bases politiques nécessaires pour un cyber Moonshot". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 27 mars 2018.

Diamandis, Peter. "L'informatique quantique entraîne des perturbations massives." 10 octobre 2016. SingularityHub. https://singularityhub.com/2016/10/10/massive-disruption-quantum- computing/.

DHS. *Charte du conseil consultatif du Partenariat pour les infrastructures critiques.* Washington, DC : DHS, 30 novembre 2016. https://www.dhs.gov/sites/default/files/publications/cipac-charter-11- 30-16-508.pdf.

"Initiatives du DHS en matière de cybersécurité". 6 février 2013. Équipe de préparation aux urgences informatiques des États-Unis. https://www.us-cert.gov/security-publications/dhs-cyber-security-initiatives.

Ministère de la Justice (DoJ). "Le ministère de la justice accueille une table ronde sur l'industrie de la cybersécurité". 28 septembre 2018. https://www.justice.gov/opa/pr/justice-department-hosts-cybersecurity- industry-roundtable.

DOJ. "Les sessions du procureur général annoncent la publication du rapport du groupe de travail sur le cyber-numérique". 19 juillet 2018. https://www.justice.gov/opa/pr/attorney-general-sessions-announces- publication-cyber-digital-task-force-report.

Defense Science Board (DSB). *La cybernétique en tant que capacité stratégique - Résumé.* Washington, DC : Bureau du sous-secrétaire à la défense pour la recherche et l'ingénierie (USD-R&E), juin 2018. https://www.acq.osd.mil/dsb/reports/2010s/DSB_CSC_Report_ExecSumm_Final_Web.pdf.

DSB. *Cyber dissuasion.* Washington, DC : USD-R&E, février 2017. https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

DSB. *Cyber Supply Chain - Résumé exécutif.* Washington, DC : USD-R&E, avril 2017. https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf.

The Economist. "La grande brèche de données subie par Equifax a des implications alarmantes." 16 septembre 2017. https://www.economist.com/finance-and-economics/2017/09/16/the- big-data-breach-suffered-by-equifax-has-alarming-implications.

"Activer la sécurité distribuée dans le cyberespace". 4 octobre 2016. DHS. https://www.dhs.gov/enabling-distributed-security-cyberspace.

Ferguson, David et Kavanaugh-Ulku, Lorin. "Les grands défis de l'USAID pour le développement". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 1er mars 2018.

Fields, Craig. "Une initiative cybernétique nationale". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 21 août 2018.

La Food and Drug Administration (FDA). *Gestion de la cybersécurité des dispositifs médicaux après la mise sur le marché : Guidance for Industry and Food and Drug Administration Staff.* Washington, DC : FDA, 28 décembre 2016. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

Frontain, Michael. "Microelectronics and Computer Technology Corporation." *État du Texas Association historique.* 15 juin 2010. https://tshaonline.org/handbook/online/articles/dnm01.

Gallagher, Patrick. "Programmes d'éducation et de recherche liés au développement de technologies critiques de cybersécurité". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 11 septembre 2018.

Gibson, David V., et Everett M. Rogers. *Collaborations de R&D à l'essai.* Boston : Harvard Business School Press, 1994.

"Étude mondiale sur la main-d'œuvre dans le domaine de la sécurité de l'information". 2017. Centre pour la sécurité et l'éducation en ligne. https://iamcybersafe.org/GISWS.

Goldman, Lisa et Purmal, Kate. "How to Launch a Successful Moonshot", Briefing au sous-comité de cybersécurité du NSTAC, Arlington, VA, 20 février 2018.

Goldman, Lisa et Kate Purmal. *L'effet Moonshot : Perturbation des activités habituelles*. San Carlos, CA : Wynnefield Business Press, 2017.

Greatwood, Duncan. "Faciliter le respect de la réglementation en matière de cybersécurité pour les infrastructures critiques". *CPO Magazine*. 3 octobre 2018. https://www.cpomagazine.com/2018/10/03/making-compliance-with-cybersecurity-regulations-easy-for-critical-infrastructure/.

Greenburg, Andrew. "L'histoire inédite de NOTPETYA, la cyberattaque la plus dévastatrice de l'histoire". *Câblé.* 22 août 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russie-code-crashed-the-world.

Gustetic, Jennifer. "Concevoir et mettre en œuvre de grands défis : Apprendre de l'expérience de la NASA". Briefing au sous-comité de la cybersécurité du NSTAC, Arlington, VA, 23 août 2018.

Gustetic, Jennifer, et al. "NASA's Asteroid Grand Challenge : Strategy, Results and Lessons Learned". Politique spatiale (2018). 10.1016/j.spacepol.2018.02.003.

Halvorsen, Terry. "5G Network Technology and Capabilities." Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 5 septembre 2018.

Halvorsen, Terry. "Entrant : Nous devons anticiper les conséquences 5G maintenant." *Signal.* 1er mars 2018. https://www.afcea.org/content/incoming-we-must-anticipate-5g-consequences-now.

Hawkins, Derek. "The Cybersecurity 202" : Le Congrès s'apprête à permettre au DHS de prendre la tête de la cybersécurité fédérale." *Le Washington Post*. 25 septembre 2018. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/25/the-cybersecurity-202-congress-poised-to-allow-dhs-to-take-the-lead-on-federal-cybersecurity/5ba915ba1b326b7c8a8d162c/?utm_term=.706f4fe7dca5.
.

Heimann, Richard. "État de la discipline : Intelligence artificielle." Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 6 septembre 2018.

Hinden, Robert et Russell Housley. "Les défis du déploiement de la sécurité sur Internet". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 25 septembre 2018.

Hof, Robert. "Leçons de Sematech." *MIT Technology Review.* 25 juillet 2011. https://www.technologyreview.com/s/424786/lessons-from-sematech/.

"L'achèvement du projet sur le génome humain : Foire aux questions". 30 octobre 2010. Institut national de recherche sur le génome humain. https://www.genome.gov/11006943/.

Isaacson, Walter. "Construire le prochain Internet : A Moonshot to Make a Secure and Verified Identification System for Online Communications" Briefing au sous-comité de cybersécurité du NSTAC, Arlington, VA, 6 mars 2018.

Kalil, Thomas. "Leçons tirées des tirs de lune de la Maison Blanche et du secteur privé". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 27 février 2018.

Lewis, James. "Cybersecurity Moonshot Issues." Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 30 août 2018.

Markoff, John. "Tuer l'ordinateur pour le sauver". *The New York Times.* 29 octobre 2012. https://nyti.ms/S91QbY.

Maughan, Douglas. "Accélération des efforts liés au développement des technologies critiques de cybersécurité". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 28 août 2018.

McConnell, Bruce. "Rendre l'Internet [mondial] sûr et sécurisé ... d'ici 2028." Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 22 août 2018.

Mervis, Jeffrey. "Vérification des données : La part du gouvernement américain dans le financement de la recherche fondamentale est inférieure à 50 %". *Science*. 9 mars 2017. http://www.sciencemag.org/news/2017/03/data-check-us- government-share-basic-research-funding-falls-bow-bow-50.

LA NASA. *Faits sur la NASA : Avantages d'Apollo : Des avancées technologiques majeures.* Houston, TX : NASA. Juillet 2004. https://www.nasa.gov/sites/default/files/80660main_ApolloFS.pdf.

"Objectifs du plan national de communication d'urgence". 17 mai 2018. DHS. https://www.dhs.gov/national-emergency-communications-plan-necp-goals.

NSTAC. *Rapport du NSTAC au Président sur la vision stratégique des technologies émergentes.* Washington, DC : NSTAC, 14 juillet 2017. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

NSTAC. *Rapport du NSTAC au Président sur la mobilisation des technologies de l'information et des communications.* Washington, DC : NSTAC, 19 novembre 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20-Information%20et%20Communications%20Technologie%20Mobilisation%20Rapport%2011-19-2014.pdf.

NSTAC. *Rapport du NSTAC au Président sur la résilience de l'Internet et des communications.* Washington, DC : NSTAC, 16 novembre 2017. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

NSTAC. *Rapport du NSTAC au Président sur l'Internet des choses.* Washington, DC : NSTAC, 19 novembre 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

Administration nationale des télécommunications et de l'information (NTIA). *Catalog of Existing IoT Security Standards Draft Version 0.01*, Washington, DC : NTIA, juillet 2017. https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.

NTIA. *Favoriser l'avancement de l'Internet des objets*. Washington, DC : NTIA, janvier 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

NTIA. *Processus multipartite : Vulnérabilités de la cybersécurité*. Washington, DC : NTIA, 15 décembre 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder- process-cybersecurity-vulnerabilities.

New York Cyber Task Force. *Construire un cyberespace défendable.* New York : Ecole des affaires internationales et publiques de l'Université de Columbia, 28 septembre 2017.

https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

Nielsen, Kirstjen M. "Remarques de la secrétaire Kirstjen M. Nielsen à la conférence RSA". Remarques, San Francisco, CA, 17 avril 2018. Discours. https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference.

O'Hern, William. "Briefing au NSTAC Cybersecurity Moonshot Subcommittee on 5G Networks and Standards." Briefing au NSTAC Cybersecurity Moonshot Subcommittee. Arlington, VA, 18 septembre 2018.

Office of Management and Budget (OMB). Guide sur l'utilisation des défis et des prix pour promouvoir l'ouverture gouvernementale. Mars 2010. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-11.pdf.

Pence, Michael. Remarques du vice-président Pence au sommet sur la cybersécurité du DHS. 31 juillet 2018. https://www.whitehouse.gov/briefings-statements/remarks-vice-president- pence-dhs-cybersecurity-summit/.

Perullo, Jerry. Briefing "Intercontinental Exchange/ NYSE" devant le sous-comité de cybersécurité du NSTAC. Arlington, VA, 27 septembre 2018.

Poindexter, John M. "Internet Accountability". Briefing au NSTAC Cybersecurity Moonshot Subcommittee. Arlington, VA, 22 mars 2018.

Rosenblum, Todd. "Cybersécurité : A Whole-of-National Power Approach". *The Cipher Brief.* 11 janvier 2017. https://www.thecipherbrief.com/column_article/cybersecurity-a-whole-of-national-power-approach.

Rung, Anne E. et Tony Scott. "Acquisition Innovation Labs & Pilot for Digital Acquisition Innovation Lab". Note de Anne E. Rung et Tony Scott aux directeurs des acquisitions, aux cadres supérieurs des acquisitions et aux directeurs de l'information. 9 mars 2016. https://www.dhs.gov/sites/default/files/publications/March%202016%20Memo.pdf.

Rutkowski, Kenneth. "Session facilitée". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 10 avril 2018.

Sabett, Randy. "Le rôle des politiques d'incitation dans une stratégie nationale de cybersécurité". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 26 septembre 2018.

"Formation à la sécurité de l'information du SANS". 2018. Institut de la SANS. https://www.sans.org/.

Seffers, George. "AFCEA : une approche globale de la cybersécurité est nécessaire." *Signal.* https://www.afcea.org/content/afcea-whole-nation-cybersecurity-approach-needed.

Serbu, Jared. Les cyberarmes étrangères "dépassent de loin" la capacité des États-Unis à défendre les infrastructures critiques, selon le groupe d'experts sur la défense. *Réseau d'information fédéral*. 17 mars 2017. https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2017/03/foreign-cyber- weaps-far-exceed-u-s-ability-defend-critical-infrastructure-defense-panel-says/.

L'étincelle. "Comment notre gouvernement peut s'adapter à l'évolution des besoins en matière de cybersécurité et d'infrastructure informatique". Juillet 2017. https://www.icf.com/blog/cybersecurity/how-government-can-adapt-to- evolving-cybersecurity-needs.

"Engagement des parties prenantes et résilience de la cyberinfrastructure". 22 août 2018. DHS. https://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience.

Étalon, William. "Dialogue avec le NSTAC Cybersecurity Moonshot Subcommittee." Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 22 mars 2018.

Commission américaine d'assistance électorale (EAC). *POINT DE DÉPART : Les systèmes électoraux américains en tant qu'infrastructures critiques.* Silver Spring, MD : EAC https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

Visner, Samuel. "Cybersécurité Moonshots". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 29 mars 2018.

Waldrop, M. Mitchell. "La Grande Transition". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 8 mars 2017.

Westin, Alan. *Vie privée et liberté.* New York : IG Publishing, 1967.

Zakheim, Dov S. "Structurer le gouvernement pour relever le défi du cybernétique". Briefing au NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, 27 septembre 2018.