

# AMERICAN STRATEGY FOR INTERNATIONAL CYBERSPACE

مركز سمث للدراسات  
SMT Studies Center

## قراءة في "الاستراتيجية الأميركية للفضاء السيبراني الدولي والسياسة الرقمية"





## المحتويات

٣	تمهيد
٥	التضامن الرقمي
٦	الجهود الأميركية لتحقيق التضامن الرقمي
٧	مواجهة التهديدات العالمية
٩	تعزيز الدفاع السيبراني
١٠	نقاط القوة
١١	نقاط الضعف المحتملة
١٢	في الختام



## تمهيد

في ٦ مايو ٢٠٢٤، خلال مؤتمر RSA في سان فرانسيسكو، أصدر وزير الخارجية الأمريكي "أنتوني بلينكين"، استراتيجية دولية للفضاء السيبراني والسياسة الرقمية (USICDPS). الاستراتيجية التي أُطلقت خلال أكبر تجمع سنوي لمحترفي الأمن السيبراني في وادي السيليكون، حملت عنوان "استراتيجية الولايات المتحدة الأميركية للفضاء السيبراني الدولي والسياسة الرقمية: نحو مستقبل رقمي مبتكر وآمن ويحترم الحقوق".

تركز استراتيجية وزارة الخارجية بشكل كبير على التهديد المتمثل في الهجمات الإلكترونية العدائية، لكنها ليست الوثيقة الأولى لإدارة "بايدن" التي تفعل ذلك. أصدر البيت الأبيض استراتيجيته الوطنية للأمن السيبراني في مارس ٢٠٢٣. وأعقبها خطة تنفيذ في يونيو، وأصدرت وزارة الدفاع وثيقة استراتيجية الأمن السيبراني الخاصة بها في سبتمبر.



# الاستراتيجية الأميركية للفضاء السيبراني الدولي والسياسة الرقمية

تاريخ إعلان الاستراتيجية | ٦ مايو ٢٠٢٤ م  
جهة الإعلان | وزارة الخارجية الأميركية  
الحدث | مؤتمر RSA  
المكان | سان فرانسيسكو

لبناء تضامن رقمي واسع، تحدد الاستراتيجية ثلاثة مبادئ توجيهية وأربعة مجالات عمل:

**المبادئ التوجيهية**  
رؤية إيجابية لفضاء إلكتروني آمن وشامل يرتكز على القانون الدولي، بما في ذلك قانون حقوق الإنسان الدولي. نهج سياسي شامل يستخدم الأدوات المناسبة للدبلوماسية وفن الحكم الدولي عبر النظام البيئي الرقمي كالم. دمج الأمن السيبراني والتنمية المستدامة والابتكار التكنولوجي.

## مجالات العمل

- تعزيز وبناء وصيانة نظام بيئي رقمي مفتوح وشامل وآمن ومرن.
- مواصلة النهج التي تحترم الحقوق في حوكمة البيانات والتكنولوجيا الرقمية مع الشركاء الدوليين.
- تعزيز السلوك الدولي المسؤول في الفضاء الإلكتروني ومواجهة التهديدات للفضاء الإلكتروني والبنية التحتية الحيوية من خلال بناء التحالفات وإشراك الشركاء.
- تعزيز وبناء سياسة الشركاء الدوليين الرقمية وقدراتهم السيبرانية.

عدم وجود بنود محددة قابلة للتنفيذ



الرؤية الشاملة





## التضامن الرقمي

اللافت في هذه الاستراتيجية هو اهتمامها الواضح بمفهوم "التضامن الرقمي"، وهو الرغبة في العمل معًا لتحقيق أهداف مشتركة، والوقوف معًا، ومساعدة الشركاء على بناء القدرات، وتقديم الدعم المتبادل. ومن خلال التعاون مع الوكالات الفيدرالية الأخرى، تهدف وزارة الخارجية إلى توجيه المشاركة الدولية في دبلوماسية التكنولوجيا، والمواءمة مع استراتيجية الأمن القومي والاستراتيجية الوطنية للأمن السيبراني.

ولبناء تضامن رقمي واسع النطاق، تحدد الاستراتيجية ثلاثة مبادئ توجيهية وأربعة مجالات عمل. وتشمل المبادئ التوجيهية ما يلي:

- رؤية إيجابية لفضاء إلكتروني آمن وشامل يركز على القانون الدولي، بما

في ذلك القانون الدولي لحقوق الإنسان.

- تكامل الأمن السيبراني والتنمية المستدامة والابتكار التكنولوجي.

- نهج سياسي شامل يستخدم الأدوات المناسبة للدبلوماسية وفن الحكم الدولي عبر النظام البيئي الرقمي كله.

وتشمل مجالات العمل، التي سلطت وزارة الخارجية الضوء عليها، تعزيز وبناء وصيانة نظام بيئي رقمي مفتوح وشامل وآمن ومرن، ومواءمة النهج التي تحترم الحقوق في الإدارة الرقمية وإدارة البيانات مع الشركاء الدوليين، وتعزيز سلوك الدولة المسؤول في الفضاء الإلكتروني، ومواجهة التهديدات التي يتعرض لها الفضاء الإلكتروني والبنية التحتية الحيوية من خلال بناء التحالفات وإشراك الشركاء، وتعزيز وبناء القدرات الرقمية والسيبرانية للشركاء الدوليين، بما في ذلك القدرة على مكافحة الجرائم السيبرانية.



على تعزيز الجهود الرامية إلى تشكيل التضامن الرقمي من خلال مشاركتها النشطة في الهيئات الدولية والمتعددة الأطراف ومتعددة أصحاب المصلحة، حيث يتم تطوير الالتزامات والقواعد والمعايير والمبادئ التي تؤثر في قضايا الفضاء الإلكتروني والرقمي والإنترنت والتكنولوجيا. وفي حين أن التقدم في هذه المجالات يمكن أن يكون بطيئاً وتدرجياً - في كثير من الأحيان نتيجة لأهدافها - فإن الافتقار إلى القيادة الأميركية في المحافل الدولية قد يسمح للخصوم بملء الفراغ وتشكيل مستقبل التكنولوجيا على حساب مصالح الولايات المتحدة وقيمها.

وتركز الاستراتيجية على بناء التحالفات، وإشراك الشركاء لتعزيز سلوك الدولة المسؤول في الفضاء الإلكتروني ومواجهة التهديدات التي يتعرض لها الفضاء الإلكتروني والبنية التحتية الحيوية.

ويعكس كل مجال من مجالات العمل الأربعة للاستراتيجية، جوانب من رؤية وزارة الخارجية للتضامن الرقمي. وللمضي قدماً، ستعمل وزارة الخارجية على جلب مجموعة واسعة من الشركاء في جميع أنحاء العالم إلى عملية بناء وتوسيع التضامن الرقمي.

في تقديمه لها، قال وزير الخارجية "أنتوني بلينكن"، إن قلب الاستراتيجية يتمحور حول جهود بناء التضامن الرقمي، والعمل معاً لتقديم المساعدة المتبادلة لضحايا الأنشطة السيبرانية الخبيثة والأضرار الرقمية الأخرى، ومساعدة الشركاء - خاصة الاقتصادات الناشئة - في نشر تقنيات آمنة ومأمونة ومرنة ومستدامة لتعزيز أهداف تطويرهم، وبناء اقتصادات ابتكارية قوية وشاملة يمكنها تشكيل مستقبلنا الاقتصادي والتكنولوجي. نحن نجمع التحالفات من الحكومات، والأعمال التجارية، والمجتمع المدني لتشكيل ثورة رقمية على كل مستوى من مستويات "المكس" التكنولوجي، من بناء الكابلات البحرية وشبكات الاتصالات، إلى نشر خدمات السحابة والذكاء الاصطناعي الموثوق، إلى تعزيز حوكمة البيانات التي تحترم الحقوق ومعايير السلوك المسؤول للدول.

## الجهود الأميركية لتحقيق التضامن الرقمي

ومن المفترض أن تعمل وزارة الخارجية



الوثيق مع الشركاء المشتركين بين الوكالات والدوليين، تنظيم وتنفيذ حملات ضغط دبلوماسية مستمرة لرفع مستوى الوعي الدولي والعام بالتهديدات السيبرانية الكبيرة ولزيادة التكاليف والمخاطر التي تتعرض لها الجهات الفاعلة السيبرانية الخبيثة. على سبيل المثال، عملت الولايات المتحدة مع الحلفاء والشركاء والقطاع الخاص، لتعطيل جهود توليد الإيرادات في كوريا الشمالية من خلال الجرائم الإلكترونية، وسرقة العملات المشفرة، والعاملين في مجال تكنولوجيا المعلومات.

## مواجهة التهديدات العالمية

تقع وثيقة الاستراتيجية عند تقاطع ثلاث سمات مميزة للولاية الأولى لإدارة بايدن: صراع متصاعد مع خصوم مثل روسيا والصين، ويدور بشكل متكرر في عالم الإنترنت، والتركيز على "التعددية" من خلال بناء تحالفات وشراكات دولية بين مجموعات أصغر ومستهدفة، والتصميم على الحفاظ على التفوق التكنولوجي العالمي للولايات المتحدة. ووفقاً للاستراتيجية، تمثل جمهورية الصين الشعبية أكبر تهديد إلكتروني نشط ومستمر لشبكات الحكومات والقطاع الخاص في الولايات المتحدة. قامت بكين بتنفيذ عمليات تجسس إلكتروني ضد الفاعلين الحكوميين والتجاربيين وممثلي المجتمع المدني، وقد زادت من

وسوف تتابع الخارجية الأميركية المزيد من المناقشات ذات التوجه العملي في الأمم المتحدة، والتي تركز على كيفية عمل الدول الأعضاء والمؤسسات معاً لتنفيذ العناصر الأساسية للإطار وبناء قدرات جميع الدول على إدارة التهديدات المتعلقة بالإنترنت.

ولاستيعاب هذه المحادثة المتطورة، اقترحت الولايات المتحدة وشركاؤها منتدى أكثر توجهاً نحو العمل، وهو برنامج عمل (POA)، كأية مستقبلية دائمة للحوار حول القضايا السيبرانية المتعلقة بالأمن الدولي في الأمم المتحدة. وصممت خطة العمل لتكون مرنة بما فيه الكفاية لمعالجة التهديدات المستقبلية، مع تحديد الدول الأعضاء اتجاهاً مع مرور الوقت. وسوف تتضمن خطة العمل أيضاً وجهات نظر المجتمع المدني والقطاع الخاص وأصحاب المصلحة الآخرين من غير الدول.

كما ستواصل وزارة الخارجية، بالتنسيق





ووكالة الأمن القومي (NSA)، ووزارة الأمن الداخلي (DHS)، ووزارة العدل (DOJ)، ومكتب التحقيقات الفيدرالي (FBI)، عن برامج ضارة لكوريا الشمالية، واستولت على بنية تحتية إلكترونية ضارة، وصادرت عملات مشفرة وعملة ورقية، وتبادل المعلومات الاستخبارية المتعلقة بالتهديدات القابلة للتنفيذ مع القطاع الخاص. علاوة على ذلك، تقوم وزارة الخارجية بتنسيق العمل مع جمهورية كوريا من خلال مجموعة العمل السيبرانية الثنائية لكوريا الديمقراطية، بما في ذلك تبادل المعلومات وتنسيق السياسات.

كما تقوم الولايات المتحدة واليابان وجمهورية كوريا بتنسيق الجهود لمواجهة التهديدات السيبرانية لكوريا الديمقراطية من خلال مجموعة عمل ثلاثية تم الإعلان عنها خلال قمة "كامب ديفيد" في أغسطس ٢٠٢٣. كما

قدرتها على تنفيذ هجمات إلكترونية مدمرة ومعطلة. ويمكن للصين إطلاق هجمات إلكترونية قد تعطل خطوط أنابيب النفط والغاز، وأنظمة السكك الحديدية، وغيرها من خدمات البنية التحتية الحيوية داخل الولايات المتحدة أو حلفائها وشركائها. تهدف محاولات اختراق البنية التحتية الحيوية من قبل الفاعلين الصينيين جزئياً، إلى تمكين أنفسهم من تعطيل أو تدمير البنية التحتية الحيوية في حالة وقوع نزاع؛ مما يمنع الولايات المتحدة من قدرتها على إسقاط القوة في آسيا، أو للتأثير على قراراتنا خلال أزمة من خلال إثارة الفوضى في المجتمع داخل الولايات المتحدة. يشكّل النشاط المدعوم من الدولة وذلك الذي يرتبط بالفاعلين الصينيين، جزءاً من النهج الإلكتروني للصين.

وكشفت القيادة الإلكترونية الأميركية،



برزت برامج الفدية بشكل خاص في السنوات الأخيرة كتهديد واضح للأمن القومي والسلامة العامة والازدهار الاقتصادي. "من خلال ممارسة أنشطتهم من ملاذات آمنة مثل جمهورية الصين الشعبية وكوريا الديمقراطية وإيران وروسيا وبلدان أخرى، تسبب مشغلو برامج الفدية في تعطيل الخدمات الحكومية والمستشفيات والمدارس وعمليات خطوط الأنابيب وكيانات المجتمع المدني. ووفقاً لوثيقة الاستراتيجية، فمع استخدام بعض الدول لممثلي برامج الفدية كوكلاء أو تغاضيها عن أنشطتهم، وتأثير هجماتهم الإلكترونية على البنية التحتية الحيوية، فإن نشاط برامج الفدية يُشكل تهديداً متزايداً للسلامة والأمن الدوليين".

يتم التعبير عن التضامن الرقمي بوضوح من خلال الجهود التي تبذلها وزارة الخارجية للاستفادة من قدراتها الدبلوماسية؛ لدعم مكافحة الحكومة

أطلعت وزارة الخارجية المسؤولين في جميع أنحاء العالم على التهديدات التي تشكلها كوريا الشمالية. وتم استثمار أموال المساعدة الأجنبية في تعزيز قدرة عمال تكنولوجيا المعلومات والجهات الفاعلة السيبرانية على اكتشاف ومكافحة التهديدات الإلكترونية والتشفيرية لكوريا الديمقراطية والدفاع عنها.

ستواصل وزارة الخارجية العمل مع الحلفاء والشركاء، من خلال سفاراتنا على الأرض وخبرائنا في مجال الإنترنت في واشنطن، لتنسيق الدعم المناسب أثناء التحقيق والتخفيف والتعافي من مثل هذه الحوادث السيبرانية. يمكن أن يشمل هذا الدعم، حسب الاقتضاء، تقديم المشورة من قبل خبراء الإنترنت في السفارات، وتسهيل أنشطة التحقيق والمطاردة وتحليل البرامج الضارة عن بعد أو على الأرض. كما يشمل ذلك مشاريع المساعدة الخارجية وتنسيق جهود المساعدة السيبرانية مع الدول الشريكة.

## تعزيز الدفاع السيبراني

علاوة على ذلك، ترى وزارة الخارجية أن مثل هذه الأنشطة ضرورية لتعزيز الدفاع السيبراني الجماعي، والقدرة على الصمود، ومساعدة البلدان على مقاومة الهجمات السيبرانية التي تهدف إلى إكراهها أو التدخل في سيادتها بطريقة أو أخرى.



يضم ما يقرب من ٦٠ دولة، بالإضافة إلى مؤسسات متعددة الأطراف مثل: الاتحاد الأوروبي والإنتربول ومنظمة الدول الأميركية، ملتزمة ببناء مرونة جماعية في مواجهة برامج الفدية، وملاحقة الجهات الفاعلة المسؤولة ومكافحتها، والتمويل غير المشروع الذي يدعم النظام البيئي لبرامج الفدية، والعمل مع القطاع الخاص للدفاع ضد هجمات برامج الفدية.

للمضي قدمًا، ستواصل حكومة الولايات المتحدة العمل على تثبيط سوء الاستخدام وإعادة تشكيل سوق برامج التجسس التجارية بشكل إيجابي، من خلال استبعاد أو تشجيع الإصلاح من قبل الشركات المرتبطة بإساءة استخدام هذه الأدوات. ستواصل وزارة الخارجية جهودها الدبلوماسية لحث الدول التي انضمت بالفعل إلى البيان المشترك، على اتخاذ خطوات ملموسة لمواجهة سوء استخدام وانتشار برامج التجسس التجارية، وحث دول إضافية على الانضمام، وإقناع الدول التي تسيء استخدام أو تمكن من إساءة استخدام برامج التجسس لتنفيذ ضمانات للانحراف بشكل أقل عن سياسة الولايات المتحدة.

## نقاط القوة

لدى الاستراتيجية أكثر من نقطة قوة، يأتي على رأسها الرؤية الشاملة، إذ تؤكد على اتباع نهج شمولي، مع التركيز



برمتها ضد برامج الفدية وغيرها من أشكال الجرائم السيبرانية، وذلك من خلال بناء قدرات الشركاء، وتطوير تحالفات لمنع السلوك الإجرامي وتعطيله ومعاقبته، وتعزيز التعاون مع القطاع الخاص.

ستواصل وزارات الخارجية والأمن الداخلي والعدل، المشاركة في فرقة العمل المشتركة الأميركية المعنية ببرامج الفدية والشراكة مع الصناعة الخاصة والحلفاء الدوليين؛ لتعطيل البنية التحتية والموارد الإجرامية عبر الإنترنت، وإزالة شبكات الروبوت، والاستيلاء على العملات المشفرة التي تم الحصول عليها من حملات برامج الفدية.

ستواصل وزارة الخارجية استخدام التزاماتها الدبلوماسية، وبناء القدرات لتوسيع وتعزيز المشاركة في المبادرة الدولية لمكافحة برامج الفدية (CRI). يعد CRI تحالفًا فريدًا ومتنوعًا جغرافيًا

## نقاط الضعف المحتملة

رغم كون الاستراتيجية تحظى بدعم وتفؤل كبيرين بين الأوساط الدولية المختصة، فإن هناك نقاط ضعف محتملة تهدد تنفيذها على الوجه الأمثل.

فمع أن الاستراتيجية تحدد أهدافاً واسعة النطاق، إلا أنها قد تفتقر إلى تفاصيل ملموسة حول التنفيذ. تعد خطط العمل الواضحة وتخصيص الموارد أمراً بالغ الأهمية للتنفيذ الفعال.

كذلك، لا يزال تحقيق التوازن بين الأمن السيبراني والحريات عبر الإنترنت يمثل تحدياً. ويجب أن تضمن الاستراتيجية اتخاذ تدابير أمنية قوية دون المساس بالقيم الديمقراطية والابتكار.

كما أن الاستراتيجية لا تقدم معالجة واضحة ودقيقة للفجوة الرقمية العالمية، وضمان الوصول العادل إلى التكنولوجيا وسد الفجوة بين الدول المتقدمة والنامية.

أيضاً، غاب عن الاستراتيجية مراعاة

على الأمن والازدهار الاقتصادي وحقوق الإنسان والابتكار التكنولوجي. وتتعرف هذه الرؤية المترابطة بالطبيعة المتعددة الأوجه للفضاء السيبراني.

كما تركز على التعاون الدولي، وتعطي الأولوية للتعاون مع الحلفاء والشركاء لوضع معايير دولية ومواجهة التحديات العابرة للحدود الوطنية. ويدرك هذا النهج التعاوني أن الفضاء الإلكتروني يتجاوز الحدود الوطنية.

وراعت الاستراتيجية كذلك التوافق مع القانون الدولي، بحرصها على تأكيد أهمية القانون الدولي كأساس لإدارة الفضاء الإلكتروني. وهذا الالتزام بالأطر القانونية يعزز الاستقرار والقدرة على التنبؤ في المجال الرقمي.

أيضاً، تعترف الاستراتيجية بالترابط بين الفضاء الإلكتروني ومجالات السياسة الأخرى، مثل التنمية المستدامة والنمو الاقتصادي. ويضمن هذا النهج المتكامل استراتيجية وطنية أكثر شمولاً.







شركات التكنولوجيا وأصحاب المصلحة الآخرين، أمراً ضرورياً للتنفيذ الناجح للاستراتيجية.

وكذلك يعد استمرار الوعي العام والتعليم فيما يتعلق بأفضل ممارسات الأمن السيبراني، أمراً ضرورياً لبناء نظام بيئي رقمي أكثر مرونة.

وتدرك الاستراتيجية أن الاستثمارات في الفضاء الإلكتروني ودبلوماسية التكنولوجيا الرقمية، ستشكل مختلف قضايا السياسة الخارجية، مثل: الأمن الدولي، والديمقراطية، وحقوق الإنسان، والصحة العالمية، وتغير المناخ.

بشكل عام، يمكن القول إن الاستراتيجية خطوة إيجابية نحو نهج أكثر شمولية لسياسة الفضاء السيبراني. ومن خلال معالجة نقاط الضعف المحتملة والاستفادة من نقاط قوتها، يمكن لهذه الاستراتيجية أن تعزز مستقبلاً رقمياً أكثر أمناً وازدهاراً وإنصافاً للجميع.

التكيف مع التهديدات المتطورة، فالمشهد الرقمي يتغير باستمرار. ويجب أن تكون الاستراتيجية مرنة وقابلة للتكيف لمواجهة التهديدات السيبرانية الناشئة والتقدم التكنولوجي.

## في الختام

تتمتع الاستراتيجية بالقدرة على تشكيل مستقبل رقمي أكثر أمناً وشمولاً وازدهاراً للولايات المتحدة والمجتمع العالمي. ومع ذلك، فإن نجاحها سوف يعتمد على التنفيذ الفعال، وتعزيز التعاون الدولي، والتكيف مع بيئة سريعة التغير.

ستعتمد فعالية الاستراتيجية على توافقها مع استراتيجيات الحلفاء والشركاء الرئيسيين. إن بناء الإجماع العالمي حول إدارة الفضاء الإلكتروني أمر بالغ الأهمية لنجاحه.

ويؤدي القطاع الخاص دوراً حيويًا في الفضاء السيبراني. ويعد التعامل مع

# للاطلاع على الأعداد السابقة





مركز سمث للدراسات  
SMT Studies Center