

نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية

الباحث : عقيل حامد عبد حسين

الجامعة العليا للدفاع الوطني ايران

اشراف : الدكتور قدير نظامي يور

المساعد الاول : الدكتور علي افزلي

المساعد الثاني : الدكتور محمد جواد نجفي

A Model for Enhancing the Role of Cyber Operations in Achieving Iraqi Foreign Policy Objectives

Researcher: Aqeel Hamed Abd Hussein

Email: aqeelhamedabd@gmail.com

Supreme National Defense University – Iran

Supervisor: Prof . Dr. Qadir Nezami Pour

Email: ghn38@yahoo.com

Assistant professors Dr. Ali Afzali

professor at the National Defense University-Tehran – Iran

Email: afzali_29387@ut.ac.ir

Assistant professors Dr. Mohammad Javad Najafi

الملخص

أدت التحولات التي شهدتها البيئة الأمنية الدولية، والتزايد المستمر في اعتماد الدول على البنى التحتية والتقنيات الرقمية، إلى جعل الفضاء السيبراني أحد المجالات المهمة لتحقيق المصالح الوطنية ودعم أهداف السياسة الخارجية للدول. وفي هذا السياق، يحتاج العراق، بالنظر إلى موقعه الجيوسياسي، والتحولات الأمنية التي يشهدها، وضرورة تعزيز مكانته الإقليمية، إلى نموذج متكامل للاستثمار الاستراتيجي في القدرات السيبرانية وتوظيفها في مجال السياسة الخارجية. أجريت هذه الدراسة بهدف تصميم نموذج لتعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية. اعتمدت الدراسة، من حيث الهدف، المنهج التطبيقي، ومن حيث المنهجية، المنهج المختلط الاستكشافي المتتابع. ففي المرحلة النوعية، جُمعت البيانات من خلال مقابلات شبه مهيكلية مع ٢٤ خبيراً في المجالات ذات الصلة، وتم تحليلها باستخدام منهج التحليل الموضوعي وبدأت عملية التحليل بـ ٣٦٨ وحدة معنوية، وانتهت، بعد التنقيح، إلى ٢١٤ وحدة قابلة للتحليل، و١٨٧ رمزاً أولياً، و٧٣ رمزاً منقحاً، و٢٤ مكوّناً، و٨ أبعاد رئيسية. وفي المرحلة الكمية، حُوّلت النتائج النوعية إلى فقرات استبانة أعدّها الباحث، وتم اختبارها باستخدام ٣٦٢ استجابة صالحة للتحليل. وقد جرى تحليل البيانات باستخدام برنامجي (SPSS و SmartPLS) من خلال تقييم نموذج القياس والنموذج الهيكلي. أظهرت نتائج الدراسة أن نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية يتكون من ثمانية أبعاد، هي: الحوكمة والقيادة السيبرانية، والقدرة والكفاءة الوطنية السيبرانية، والأمن والمرونة السيبرانية، والقدرة المؤسسية والتنسيق التنظيمي، والقدرة العملياتية والمعلوماتية السيبرانية، والدبلوماسية السيبرانية والنشاط السيبراني، والردع وإدارة التهديدات الخارجية، ومخرجات السياسة الخارجية. وقد نُظمت هذه الأبعاد ضمن ٢٤ مكوّناً و٤٠ فقرة نهائية، وتم التحقق من صدقها وثباتها. وتشير النتائج إلى أن دور العمليات السيبرانية في السياسة الخارجية لا يقتصر على توفير القدرات التقنية أو حماية البنى التحتية، بل يمكن،

من خلال سلسلة مترابطة تشمل بناء القدرات، والحوكمة والتنسيق المؤسسي، وتطوير القدرات العملية، والنشاط والدبلوماسية السيبرانية، وإدارة التهديدات، أن يساهم في تعزيز المصالح الوطنية، وزيادة القوة التفاوضية، وإدارة التهديدات الخارجية، والارتقاء بالمكانة الإقليمية والدولية للعراق. الكلمات المفتاحية: العمليات السيبرانية، السياسة الخارجية، القوة السيبرانية، الدبلوماسية السيبرانية، الردع السيبراني، الحوكمة السيبرانية، العراق.

المبحث الأول : مقدمات البحث

١- مشكلة البحث

أدت التطورات المتسارعة في تقنيات الاتصال والمعلومات الحديثة خلال العقود الأخيرة إلى تغييرات جوهرية في طبيعة القوة والأمن وقدرة الدول على الفعل في النظام الدولي. ففي الماضي، كانت القوة الوطنية تستند بصورة أساسية إلى عناصر مثل القدرات العسكرية، والإمكانات الاقتصادية، والنفوذ السياسي؛ غير أن الفضاء السيبراني أصبح في العصر الرقمي أحد المجالات الرئيسية للتنافس والتفاعل وممارسة القوة بين الدول. وقد أدى الاعتماد المتزايد للمجتمعات والدول والبنى التحتية الحيوية على التقنيات الرقمية إلى خروج الأمن السيبراني من نطاق القضية التقنية البحتة، وتحوله إلى أحد المكونات المهمة للأمن الوطني والحوكمة والسياسة الخارجية للدول. وفي الوقت الراهن، تسعى الدول إلى تطوير قدراتها السيبرانية بهدف حماية مصالحها الوطنية من جهة، واستخدام هذه القدرات أداة لزيادة النفوذ وإدارة الأزمات وتعزيز الدبلوماسية الرقمية وتحقيق أهداف السياسة الخارجية من جهة أخرى (Kello, 2023: 15). وفي النظام الدولي المعاصر، لم تعد السياسة الخارجية مقتصرة على الأدوات الدبلوماسية التقليدية، بل أصبحت مرتبطة بصورة متزايدة بالتقنيات الحديثة والشبكات الرقمية والقدرات السيبرانية. وتستخدم الدول العمليات السيبرانية في مجالات متعددة، من بينها الدفاع والردع ودعم الدبلوماسية وحماية المعلومات الاستراتيجية ومواجهة التهديدات الرقمية والمساهمة في تشكيل البيئة الإدراكية الدولية. ومن هذا المنطلق، أصبحت القدرة السيبرانية أحد عناصر القوة الوطنية، بحيث إن الدول التي تنفخر إلى استراتيجية واضحة في هذا المجال لن تكون عرضة للتهديدات الناشئة فحسب، بل ستفقد أيضاً الفرص التي يوفرها الفضاء الرقمي لتعزيز مكانتها الخارجية (Nye, 2024: 8) وتحتاج جمهورية العراق، بسبب موقعها الجيوسياسي الخاص، ووجودها في واحدة من أكثر البيئات الأمنية تعقيداً في العالم، واعتمادها على التفاعلات الإقليمية والدولية، ومواجهتها مجموعة واسعة من التحديات السياسية والأمنية، إلى إعادة النظر في أدوات تحقيق أهداف سياستها الخارجية. وقد سعت السياسة الخارجية العراقية خلال السنوات الأخيرة إلى تحقيق التوازن بين الفاعلين الإقليميين وخارج الإقليم، وإلى أداء دور أكثر فاعلية في المعادلات الإقليمية؛ إلا أن أحد التحديات الأساسية التي تواجه العراق يتمثل في ضعف الاستفادة الاستراتيجية من مصادر القوة الحديثة، ولا سيما قدرات الفضاء السيبراني، من أجل تعزيز المكانة الدولية وزيادة القدرة على التفاوض الخارجي. وعلى الرغم من التطور التدريجي للبنية التحتية الرقمية في العراق، فإن استخدام القدرات السيبرانية لا يزال يتركز بدرجة أكبر على المستوى التقني والدفاعي، ولم يتم تحديد العلاقة بين الأمن السيبراني وأهداف السياسة الخارجية بصورة منهجية. وفي الواقع، يفتقر العراق إلى إطار استراتيجي واضح يبين كيفية توظيف العمليات السيبرانية لخدمة أهداف السياسة الخارجية، بما في ذلك تعزيز التفاعلات الدولية، وحماية المصالح الوطنية، وزيادة القدرة الردعية، ومواجهة التهديدات الرقمية، وتعزيز الدور الإقليمي للدولة. ويمثل هذا التباين بين الإمكانات الكامنة للفضاء السيبراني والاستفادة الاستراتيجية منها أحد العوائق المهمة أمام تحول السياسة الخارجية العراقية في العصر الرقمي. وعليه، تتمثل الفجوة الأساسية التي يتناولها البحث الحالي في غياب إطار شامل ووطني ملائم لتفسير العلاقة بين العمليات السيبرانية والأمن السيبراني وتحقيق أهداف السياسة الخارجية العراقية. فقد تناولت الدراسات القائمة بدرجة محدودة السؤال المتعلق بكيفية تمكن دولة ذات خصائص جيوسياسية وأمنية ومؤسسية مثل العراق من توظيف القدرات السيبرانية لتعزيز سياستها الخارجية. ويسعى البحث الحالي إلى تجاوز النظرة التقنية البحتة للأمن السيبراني، وتقديم مقاربة استراتيجية يتم فيها تحليل العمليات السيبرانية بوصفها إحدى الأدوات الحديثة للقوة الوطنية وأداة مكملية للسياسة الخارجية. ويمكن تناول أهمية البحث الحالي من جانبين. فمن الناحية العلمية، يمكن أن يساهم هذا البحث في تطوير الأدبيات متعددة التخصصات في مجالات السياسة الخارجية الرقمية والأمن السيبراني ودراسات القوة الوطنية، وفي تفسير العلاقة بين التكنولوجيا والسلوك الخارجي للدول في دولة لم تحظَ بالدراسة الكافية مثل العراق. أما من الناحية التطبيقية، فيمكن أن تشكل نتائج البحث أساساً لصانعي السياسات في العراق من أجل تصميم الاستراتيجيات السيبرانية، وزيادة القدرات الوطنية، وتعزيز الدبلوماسية الرقمية، وتحقيق استفادة أكثر فاعلية من الفضاء السيبراني في سبيل تحقيق المصالح الوطنية. وبناءً على ما سبق، تتمثل المشكلة الرئيسية للبحث الحالي في السؤال الآتي: كيف يمكن تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية، وما النموذج الذي يمكن أن يفسر ويُفعّل العلاقة بين القدرات السيبرانية ومتطلبات السياسة الخارجية لهذا البلد؟

٢- أهمية وضرورة البحث

٣- أهمية البحث

١. يمكن توضيح أهمية هذا البحث من خلال ثلاثة إنجازات رئيسية في حل المشكلة:
٢. الارتقاء بالمكانة الاستراتيجية للعراق في النظامين الإقليمي والدولي .
٣. تطوير الدبلوماسية الرقمية وتعزيز القوة الناعمة للعراق .
٤. تعزيز أمن السياسة الخارجية وقدرتها على الصمود في مواجهة التهديدات الناشئة .

٢.٢ ضرورة البحث

١. انخفاض قدرة العراق على المنافسة والتأثير في البيئة الإقليمية والدولية.
٢. زيادة قابلية التعرض للتهديدات السيبرانية والضغط الخارجي.
٣. إضعاف الاستقلال الاستراتيجي وزيادة الاعتماد في مجالي التكنولوجيا والأمن الرقمي.

٣. أهداف البحث

- ٣-١ **الهدف الرئيسي:** تصميم نموذج لتعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية.
- ٣-٢ **الأهداف الفرعية:**

١. تحديد أبعاد نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية .
٢. تحديد مكونات نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية .
٣. تحديد مؤشرات نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية.
٤. تفسير وتحديد العلاقات بين أبعاد ومكونات ومؤشرات نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية

٤. أسئلة البحث

٤-١ السؤال الرئيسي:

كيف ينبغي أن يكون نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية؟

٤-٢ الأسئلة الفرعية:

١. ما أبعاد نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية؟
٢. ما مكونات نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية؟
٣. ما مؤشرات نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية؟
٤. ما العلاقات القائمة بين أبعاد ومكونات ومؤشرات نموذج تعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية؟

٥- تعريف المفاهيم الأساسية للبحث

٥-١ الفضاء السيبراني

التعريف المفاهيمي: الفضاء السيبراني هو بيئة رقمية متعددة الطبقات تتشكل من تفاعل البنى التحتية لتكنولوجيا المعلومات، وشبكات الاتصال، والبيانات، والمستخدمين، وقد أصبح أحد المجالات الجديدة للمنافسة وممارسة القوة من قبل الدول في النظام الدولي. (Zwitter, 2024: 3)

التعريف الإجرائي: يقصد بالفضاء السيبراني في هذا البحث البيئة التكنولوجية التي تستطيع العراق من خلالها تطوير قدراتها الرقمية وتوظيف العمليات السيبرانية لتعزيز أهداف سياسته الخارجية.

الأمن السيبراني

التعريف المفاهيمي:

الأمن السيبراني هو مجموعة السياسات والتقنيات والآليات الإدارية الهادفة إلى حماية الشبكات والأنظمة والبيانات من التهديدات السيبرانية، ويُعد أحد المكونات الأساسية للأمن الوطني في العصر الرقمي

(Burch et al., 2024: 12).

التعريف الإجرائي:

يشمل الأمن السيبراني في هذا البحث قدرات العراق في مجال حماية البنى التحتية الرقمية، وإدارة التهديدات السيبرانية، والمرونة الرقمية، وإنشاء آليات للدفاع السيبراني.

العمليات السيبرانية

٢-٥ التعريف المفاهيمي:

العمليات السيبرانية هي الإجراءات الهادفة والمنظمة التي تُنفذ في الفضاء السيبراني باستخدام التقنيات الرقمية لتحقيق أهداف سياسية أو أمنية أو استراتيجية. وقد أصبحت هذه العمليات في العصر الحديث إحدى أدوات القوة التي تمتلكها الدول. (Willers & Gjesvik, 2026: 518)

التعريف الإجرائي:

يقصد بالعمليات السيبرانية في هذا البحث مجموعة الإجراءات والقدرات الرقمية التي تمتلكها العراق لدعم المصالح الوطنية، وتعزيز الأمن، وتقوية أهداف سياستها الخارجية.

٣-٥ السياسة الخارجية

التعريف المفاهيمي:

السياسة الخارجية هي مجموعة الأهداف والقرارات والإجراءات التي تتخذها الدولة في تفاعلها مع البيئة الدولية من أجل تأمين المصالح الوطنية، وزيادة النفوذ، وتعزيز مكانة الدولة. وقد أدت التطورات التكنولوجية إلى جعل الأدوات الرقمية جزءاً من القدرات الجديدة للسياسة الخارجية (Manor, 2025: 2).

التعريف الإجرائي:

تشمل السياسة الخارجية العراقية في هذا البحث أهدافاً مثل زيادة التفاعلات الدولية، وتعزيز المكانة الإقليمية، والحفاظ على الأمن الوطني، ورفع القدرة على التأثير الخارجي.

٤-٥ الدبلوماسية السيبرانية

التعريف المفاهيمي:

تشير الدبلوماسية السيبرانية إلى استخدام الدول للتقنيات الرقمية لإدارة العلاقات الخارجية، وتطوير التعاون الدولي، ومتابعة المصالح الوطنية في البيئة الرقمية. (Manor, 2025: 4)

التعريف الإجرائي:

يقصد بالدبلوماسية السيبرانية في هذا البحث قدرة العراق على استخدام الأدوات الرقمية لتطوير التعاون الخارجي وتعزيز دوره في الترتيبات السيبرانية الإقليمية والدولية.

٥-٥ القوة السيبرانية

التعريف المفاهيمي:

القوة السيبرانية هي قدرة الدولة على إنشاء وتطوير والسيطرة على واستخدام قدرات الفضاء السيبراني من أجل تحقيق الأهداف الاستراتيجية (Willers & Gjesvik, 2026: 520).

التعريف الإجرائي:

تشمل القوة السيبرانية العراقية في هذا البحث القدرات التقنية والبشرية والمؤسسية والتنظيمية اللازمة للاستخدام الفعال للفضاء السيبراني دعماً للسياسة الخارجية.

٦-٥ الردع السيبراني

التعريف المفاهيمي:

الردع السيبراني هو قدرة الدولة على منع الأعمال السيبرانية العدائية من خلال زيادة تكلفة الهجوم، وتعزيز القدرات الدفاعية، وإيجاد القدرة على الاستجابة. (Burch et al., 2024: 18)

التعريف الإجرائي:

يقصد بالردع السيبراني العراقي في هذا البحث قدرة العراق على الحد من احتمالية وقوع الهجمات السيبرانية وزيادة قدرته على مواجهة التهديدات الرقمية.

٧-٥ الحوكمة السيبرانية

التعريف المفاهيمي:

الحكومة السيبرانية هي مجموعة الهياكل والقوانين والآليات المؤسسية الخاصة بإدارة وتنظيم الأنشطة في الفضاء السيبراني (Zwitter, 2024: 5).

التعريف الإجرائي:

تشمل الحكومة السيبرانية في هذا البحث السياسات والمؤسسات والقوانين والتنسيق التنظيمي في العراق لإدارة الفضاء السيبراني واستخدامه بصورة استراتيجية.

٥-٨ الاستنزاف السيبراني

التعريف المفاهيمي:

يشير الاستنزاف السيبراني إلى عملية تدريجية في التنافس السيبراني، يقوم من خلالها أحد الفاعلين، عبر إجراءات رقمية مستمرة، بخفض قدرات الفاعل المقابل، أو زيادة تكاليفه، أو إضعاف قدراته الاستراتيجية. (Willers & Gjesvik, 2026: 522)

التعريف الإجرائي:

يقصد بالاستنزاف السيبراني في هذا البحث مستوى تعرض العراق للضغوط والمنافسات السيبرانية، وكذلك قدرة الدولة على الحد من آثارها السلبية من خلال تعزيز الأمن السيبراني.

المبحث الثاني : إولاً الأسس المفاهيمية للبحث

١- مفهوم الفضاء السيبراني

يمكن تعريف الفضاء السيبراني، في أبسط صوره، بأنه بيئة شبكية ورقمية تتفاعل فيها أنظمة الحاسوب وشبكات الاتصال والبيانات والبرمجيات والبنى التحتية المادية والمستخدمون البشريون مع بعضها بعضاً. ومع ذلك، فإن الفضاء السيبراني في الأدبيات المعاصرة للأمن والعلاقات الدولية يتجاوز مفهوم الإنترنت، إذ يشمل مجموعة من البنى التحتية المادية والشبكات والأنظمة المنطقية والبيانات والبرمجيات والهويات الرقمية والتفاعلات البشرية. وتنتظر الاستراتيجية الوطنية للأمن السيبراني في المملكة المتحدة إلى الفضاء السيبراني باعتباره بيئة من صنع الإنسان، تتأثر الأنشطة فيها بسلوك الأفراد والمنظمات، ويمكن أن تمتد آثارها من البيئة الرقمية إلى العالم المادي. كما أن الاعتماد المتزايد للحكومات والبنى التحتية الحيوية والاقتصاد والخدمات العامة على الأنظمة الرقمية أدى إلى جعل تطورات الفضاء السيبراني ذات آثار سياسية واقتصادية وأمنية واسعة (Cabinet Office, 2022). ومن الناحية الهيكلية، تنظر مؤسسة IISS إلى الفضاء السيبراني باعتباره بيئة متعددة الطبقات تتضمن الطبقة المادية، والطبقة المنطقية، والطبقة الافتراضية. وتشمل الطبقة المادية المعدات والبنى التحتية مثل أجهزة الحاسوب ومراكز البيانات والكابلات وأجهزة التوجيه وأبراج الاتصالات والأقمار الصناعية؛ بينما تشمل الطبقة المنطقية الشفرات والبيانات وأنظمة التشغيل والآليات البرمجية؛ في حين تشمل الطبقة الافتراضية بيئة تفاعل المستخدمين مع الخدمات والبيئات الرقمية. (IISS, 2024, pp. 3-5) وبناءً على ذلك، فإن القدرة السيبرانية للدولة لا تقتصر على المعدات التقنية، إذ يمكن أن يؤثر الضعف في أي من هذه الطبقات في الأمن والمرونة والقدرات العملية. كما يتميز الفضاء السيبراني بطابع عابر للحدود؛ إذ يمكن للبيانات والعمليات السيبرانية أن تمر عبر بنى تحتية تابعة لعدة دول، وأن تؤثر في الدولة المستهدفة من دون وجود مادي للفاعل داخل إقليمها. وقد أدت هذه الخاصية إلى زيادة تعقيد القضايا المرتبطة بالسيادة والمسؤولية والإسناد وردود أفعال الدول، كما أثرت في اختيار أدوات السياسة الخارجية. (Foulon & Meibauer, 2024, pp. 426-458)

٢- مفهوم القوة السيبرانية

تُعد القوة السيبرانية من المفاهيم المحورية في البحث الحالي؛ إذ إن دراسة دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية لا يمكن أن تتم من دون تمييزها عن مفاهيم مثل الأمن السيبراني والقدرة التقنية. يركز الأمن السيبراني بصورة أساسية على الحماية والوقاية والكشف والاستجابة والمرونة في مواجهة التهديدات، في حين أن القوة السيبرانية تمثل مفهوماً أوسع، إذ تشمل قدرة الدولة على الاستخدام الاستراتيجي للفضاء السيبراني في سبيل تحقيق الأهداف الوطنية. وتؤكد مؤسسة IISS، ضمن إطار *Cyber Power Matrix*، قدرة الدولة على ممارسة القوة في الفضاء السيبراني وتحقيق الأهداف الاستراتيجية، كما تأخذ في الاعتبار مكونات مثل الاستراتيجية والعقيدة، والحوكمة، والتعاون بين الحكومة والقطاع الخاص، والموارد البشرية، والقدرة الصناعية، والمرونة، والقدرة على التأثير في القواعد والمعايير السيبرانية (IISS, 2024, pp. 3-5) كما يبين Devanny و Dwyer أن مفهوم القوة السيبرانية في السياسات الوطنية تجاوز النظرة الدفاعية المحدودة، ليشمل أبعاداً مثل الحماية والردع والعمليات والتكنولوجيا والحوكمة

والدور الدولي. (Devanny & Dwyer, 2023, pp. 381–398) كذلك يؤكد Willett الترابط المتبادل بين الفضاء السيبراني والعالم المادي، ويبين أن الاستقرار السيبراني يمكن أن يؤثر في الاقتصاد والسمعة الدولية والأمن الوطني والقدرات العسكرية والنفوذ العالمي للدول (Willett, 2024, pp. 191–230).

٣- مكونات وأبعاد القوة السيبرانية

توضح مراجعة الأدبيات أن القوة السيبرانية تمثل بناءً متعدد الأبعاد، ولا يمكن حصرها في القدرة على تنفيذ العمليات السيبرانية الهجومية أو الدفاع عن الشبكات فقط. وتتنظر أطر IISS و National Cyber Power Index والاستراتيجيات الوطنية للأمن السيبراني إلى القوة السيبرانية باعتبارها نتاج تفاعل مجموعة من القدرات الاستراتيجية والمؤسسية والتكنولوجية والبشرية والمعلوماتية والأمنية والعملياتية والدولية (IISS, 2024, pp. 3–8; Voo et al., 2022). وبناءً على ذلك، تتمثل أهم أبعاد القوة السيبرانية في: الاستراتيجية والعقيدة السيبرانية، والحوكمة والبنية المؤسسية، والبنية التحتية والقدرة التكنولوجية، ورأس المال البشري والمعرفة التخصصية، والقدرة المعلوماتية، والأمن والمرونة، والقدرة على تنفيذ العمليات السيبرانية، والردع السيبراني، والصناعة والنظام البيئي التكنولوجي، والقدرة الدبلوماسية والدولية، والقدرة على التأثير المعلوماتي والمعرفي، والاستقلال الاستراتيجي السيبراني. ويوفر وجود استراتيجية وعقيدة واضحة الأساس لتوجيه القدرات المتفرقة، في حين تعمل الحوكمة والبنية المؤسسية على تنظيم المسؤوليات وعمليات صنع القرار. كما تشكل البنية التحتية والتكنولوجيا والموارد البشرية الأسس المادية والمعرفية للقوة السيبرانية. وفي الوقت نفسه، توفر القدرة المعلوماتية والأمن والمرونة إمكانية حماية الموارد السيبرانية واستثمارها بصورة مستمرة. وعلى المستوى العملي، تتيح القدرة على تنفيذ العمليات السيبرانية تحويل الموارد والإمكانات المتاحة إلى إجراءات منظمة، في حين يعزز الردع القدرة على التأثير في حسابات الفاعلين المنافسين. وإلى جانب ذلك، تسهم صناعة التكنولوجيا ومراكز البحوث والجامعات وسلاسل توريد التكنولوجيا في تعزيز استدامة القوة السيبرانية. ومن ناحية أخرى، تتيح القدرة الدبلوماسية والدولية للدولة المشاركة في تشكيل القواعد والمعايير وأطر التعاون السيبراني. كما يمكن أن تشكل القدرة على التأثير المعلوماتي والمعرفي، فضلاً عن الحد من الاعتماد على الموارد الخارجية، جزءاً من الاستقلال الاستراتيجي للدولة. وتؤكد مؤسسة IISS الطبيعة متعددة الأبعاد للقوة السيبرانية، وتأخذ في تقييمها للقوة السيبرانية مكونات تشمل الاستراتيجية والحوكمة والموارد البشرية والبنية التحتية والمعلومات والأمن والعمليات وصناعة التكنولوجيا والقدرة على التأثير الدولي. (IISS, 2024, pp. 3–8) كما يقوم National Cyber Power Index 2022 بتقييم الدول استناداً إلى مجموعة من الأهداف والقدرات السيبرانية، مؤكداً ضرورة عدم اختزال القوة السيبرانية في مؤشر واحد. (Voo et al., 2022) وبناءً على ذلك، تُعد القوة السيبرانية في البحث الحالي بناءً متعدد الأبعاد ومركباً يتشكل من تفاعل القدرات الاستراتيجية والمؤسسية والبشرية والتكنولوجية والمعلوماتية والأمنية والعملياتية والدولية. ويوفر هذا التصور الأساس النظري اللازم لدراسة دور العمليات السيبرانية في السياسة الخارجية العراقية.

٤- مكانة القوة السيبرانية في هيكل القوة الوطنية والسياسة الخارجية

لا يمكن اعتبار القوة السيبرانية بديلاً كاملاً عن القوة العسكرية أو الاقتصادية أو الدبلوماسية، بل ينبغي النظر إليها بوصفها جزءاً من البنية الجديدة للقوة الوطنية، يمكنها أن تعزز أو تكمل أو، في بعض الظروف، تقيد مصادر القوة الأخرى. كما تعدّ الاستراتيجية الوطنية للأمن السيبراني في المملكة المتحدة القوة السيبرانية إحدى أدوات القوة الوطنية، وتؤكد أهمية استخدامها إلى جانب الأدوات الوطنية الأخرى من أجل حماية مصالح الدولة وتعزيزها. (Cabinet Office, 2022) كذلك، يبين معهد الدراسات الاستراتيجية الدولية (IISS) أن القدرات السيبرانية يمكن أن تتجاوز آثارها نطاق الفضاء السيبراني لتظهر في مجالات القوة الأخرى والبيئات العملياتية المختلفة. (IISS, 2024, pp. 3–5) ومن هذا المنطلق، تؤدي القوة السيبرانية في مجال السياسة الخارجية، على الأقل، أربع وظائف أساسية: أولاً، الوظيفة الوقائية والحماية من خلال حماية الاتصالات والمعلومات والبنية التحتية المرتبطة بالسياسة الخارجية؛ وثانياً، الوظيفة المعلوماتية من خلال جمع المعلومات وتحليلها بما يدعم عملية صنع القرار في السياسة الخارجية؛ وثالثاً، الوظيفة الردعية والضاغطة من خلال زيادة تكلفة السلوك العدائي وتوسيع خيارات إدارة الأزمات؛ ورابعاً، الوظيفة الدبلوماسية والتأثيرية من خلال تعزيز التعاون الدولي والمشاركة في حوكمة الفضاء السيبراني وزيادة القدرة على التفاوض. ومن ثم، تكتسب القوة السيبرانية قيمتها الاستراتيجية عندما تتمكن من تحويل الموارد والقدرات التكنولوجية والبشرية والمعلوماتية والمؤسسية إلى تأثير ملموس وقابل للملاحظة على المستويين الوطني والدولي. وتكتسب هذه المسألة أهمية خاصة بالنسبة إلى العراق؛ لأن هدف البحث لا يقتصر على دراسة مستوى القدرات السيبرانية، وإنما يتمثل في تحديد الآلية التي يمكن من خلالها توظيف هذه القدرات لخدمة أهداف السياسة الخارجية.

وبناءً على ذلك، يمكن التعبير عن السلسلة المفاهيمية للبحث على النحو الآتي:

القوة الوطنية ← القدرة السيبرانية ← القوة السيبرانية ← القدرة على تنفيذ العمليات السيبرانية ← التأثير الاستراتيجي ← دعم السياسة الخارجية
← تحقيق أهداف السياسة الخارجية العراقية وفي هذه السلسلة، لا تمثل العمليات السيبرانية قدرة مستقلة ومنفصلة، وإنما تُعدّ إحدى الأدوات التي تحول القدرة والقوة السيبرانية إلى تأثير استراتيجي. ومن ثم، فإن تعزيز دور العمليات السيبرانية يتطلب تطوير القدرات المؤسسية والبشرية والتكنولوجية والمعلوماتية والأمنية والدبلوماسية بصورة متزامنة ومتكاملة.

ثانياً : الإطار المفاهيمي للبحث

١ - منطق العلاقة بين العمليات السيبرانية والسياسة الخارجية

أدى تحول البيئة الدولية إلى أن أصبحت القدرات الرقمية والسيبرانية جزءاً من مصادر قوة الدول. وفي هذا الإطار، يمكن للقدرات السيبرانية، من خلال توفير القدرة الدفاعية، وزيادة المرونة، وحماية الأصول الاستراتيجية، ودعم عملية صنع القرار، وإتاحة أدوات جديدة للتفاعل الخارجي، أن تؤثر في قدرة الدولة على متابعة أهداف سياستها الخارجية. كما تؤكد الأدبيات الحديثة أن الفضاء السيبراني ليس مجرد مجال تقني بحد ذاته، بل يتفاعل مع هياكل القوة وسلوك الدول في النظام الدولي. (Foulon & Meibauer, 2024, pp. 426-458) ومن هذا المنظور، يمكن تفسير العلاقة بين العمليات السيبرانية والسياسة الخارجية في إطار عملية متعددة المستويات؛ إذ يتعين على الدولة في البداية امتلاك قدرات مناسبة على مستوى البنية التحتية والتكنولوجيا والمؤسسات؛ ثم تُنظّم هذه القدرات في إطار قدرات تشغيلية وآليات للحوكمة والأمن السيبراني؛ وفي المرحلة التالية، يمكن توظيف القدرات الناتجة في دعم الأهداف الوطنية والخارجية. وعليه، تمثل العمليات السيبرانية في هذا الإطار حلقة وصل بين القدرات السيبرانية للدولة وبعض نتائج السياسة الخارجية.

٢ - استخراج المفاهيم الأساسية من الأسس النظرية

يكشف تحليل الأسس النظرية للفصل الحالي عن مجموعة من المفاهيم ذات الصلة. فعلى المستوى الأول، تشير مفاهيم مثل القوة السيبرانية، والأمن السيبراني، والحوكمة السيبرانية، والبنية التحتية الرقمية، والمرونة، والقدرة المؤسسية إلى القدرات الأساسية للدولة في الفضاء السيبراني. وعلى المستوى الثاني، ترتبط مفاهيم مثل القدرة التشغيلية، والردع السيبراني، وإدارة التهديدات، وحماية المصالح الوطنية بكيفية تحويل القدرات الأساسية إلى قدرات تشغيلية. أما المستوى الثالث، فتتصل فيه المصلحة الوطنية، والقوة التفاوضية، والنفوذ الإقليمي، والمكانة الدولية، ودعم الدبلوماسية بالنتائج والأهداف الخاصة بالسياسة الخارجية.

٣ - تحديد المتغيرات البنائية الأولية للبحث

استناداً إلى الأسس النظرية، يمكن تنظيم المتغيرات البنائية الأولية للبحث ضمن ثلاثة مجالات رئيسية. يتعلق المجال الأول بالقدرات والمتطلبات السيبرانية، ويشمل الأمن السيبراني، والحوكمة، والبنية التحتية، والموارد البشرية، والقدرة التكنولوجية، والمرونة. ويشمل المجال الثاني القدرات والعمليات السيبرانية، ويتضمن القدرة التشغيلية، وإدارة التهديدات، والردع، وحماية المصالح، والدعم السيبراني للتفاعلات الخارجية. أما المجال الثالث فيتعلق بأهداف السياسة الخارجية، ويشمل تحقيق المصالح الوطنية، وزيادة القوة التفاوضية، وتعزيز النفوذ الإقليمي، وتقوية المكانة الدولية. ويتوافق هذا التصنيف مع الأدبيات الحديثة التي تؤكد العلاقة بين القدرات السيبرانية والحوكمة والأمن والسلوك الخارجي للدول (Sukumar et al., 2024, pp. 7-44).

٤ - العلاقة بين القدرات السيبرانية وأهداف السياسة الخارجية

لا تمثل العلاقة بين القدرات السيبرانية وأهداف السياسة الخارجية علاقة مباشرة وبسيطة، وإنما تتشكل من خلال إنشاء القدرات التشغيلية وزيادة قدرة الدولة على الفعل والتأثير. إذ تتيح البنية التحتية والمؤسسية المناسبة إمكانية تحقيق الأمن والمرونة؛ كما يوفر الأمن والمرونة الظروف اللازمة لتطوير القدرات التشغيلية. ويمكن بعد ذلك توظيف القدرات التشغيلية في دعم إدارة التهديدات، والردع، وحماية المصالح، والتفاعلات الخارجية. وبالتالي، لا يمكن أن تتحول القدرة السيبرانية إلى مصدر مؤثر في السياسة الخارجية إلا عندما توضع ضمن هيكل استراتيجي ومؤسسي متماسك (Hassib & Shires, 2024, pp. 2399-2418).

٥ - الإطار المفاهيمي الأولي للبحث



الشكل الإطار المفاهيمي الأولي للبحث المبحث الثالث : منهجية البحث

١- الأسس الفلسفية للبحث

يستند البحث الحالي إلى أساس فلسفي ضمن إطار البراغمية..(البراغمية. بدلاً من حصر البحث بنوع محدد من المعرفة، تُركز البراغمية على مدى ملائمة المنهج لطبيعة المشكلة، وهدف البحث، ونوع أسئلة البحث. من هذا المنطلق، يُبرر استخدام المنهج النوعي والكمي عندما يُسهم الجمع بينهما في فهم أشمل وأكثر عملية للمشكلة قيد الدراسة (كريسويل وكريسويل، ٢٠٢٣)

٢- مكانة المناهج الكمية والنوعية

يُعدّ المنهج النوعي مناسباً لدراسة الظواهر التي لم تُفهم أبعادها أو مفاهيمها أو علاقاتها فهماً كاملاً، والتي تتطلب استكشافاً وتفسيراً. في مثل هذه الدراسات، يمكن للبيانات المستقاة من المقابلات والوثائق وغيرها من المصادر النوعية أن تُسهم في تحديد المفاهيم والأنماط والعلاقات التي لا يمكن تحديدها باستخدام أدوات مُحددة مسبقاً.

٣- أساس اختيار النهج المختلط

بالنظر إلى الهدف الرئيسي للبحث، وهو تصميم نموذج لتعزيز دور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية، فقد تم اختيار منهج استكشافي مختلط. في هذا المنهج، تُجمع البيانات النوعية أولاً وتُحلل، وتُشكل نتائج هذه المرحلة أساساً لتصميم أداة ونموذج كميين. لذا، يأتي الجزء الكمي منطقياً بعد الجزء النوعي، ويؤدي دور التحقق من صحة نتائج المرحلة الأولى وتوسيع نطاقها. في المرحلة النوعية، يُستخدم تحليل المحتوى لتحديد المفاهيم والفئات والعلاقات المتعلقة بالموضوع. ثم تُحوّل النتائج إلى بنى ومؤشرات قابلة للقياس. أما في المرحلة الكمية، فيُقاس البناء المستخلص من خلال استبيان أعدّه الباحث، ويُفحص باستخدام التحليلات الإحصائية ونمذجة المعادلات الهيكلية.

٤- أساليب جمع البيانات

فيما يتعلق بأسلوب جمع البيانات، البحث في المكتبات-وثائق و مجالسيتم جمع البيانات المكتبية والوثائقية من مصادر أكاديمية، ووثائق استراتيجية، وتقارير متخصصة، ومصادر متعلقة بالسياسة الخارجية، والأمن السيبراني، والعمليات السيبرانية. أما البيانات الميدانية، فسيتم جمعها في المرحلة النوعية من خلال مقابلات شبه منظمة، وفي المرحلة الكمية من خلال استبيان من إعداد الباحث.

٥- أخذ العينات التطبيقية

في أسلوب المعاينة التطبيقية، يُقسّم المجتمع الإحصائي إلى فئات متجانسة نسبياً بناءً على مجال الخبرة، ثم يُختار عدد من المستجيبين من كل فئة. ويمكن أن تشمل فئات البحث المناسبة للبنية الفعلية للمجتمع الإحصائي خبراء السياسة الخارجية والعلاقات الدولية، وخبراء الأمن السيبراني وتكنولوجيا المعلومات، ومديرين وخبراء من الهيئات الحكومية ذات الصلة، وأعضاء هيئة التدريس والباحثين في المجالات ذات الصلة.

٦- تحديد حجم العينة الكمي 8-3

سيتم تحديد حجم العينة الكمية بناءً على حجم المجتمع الإحصائي، ومستوى الثقة، والخطأ المسموح به، ومتطلبات نمذجة المعادلات الهيكلية. إذا كان حجم المجتمع الإحصائي معروفاً، فسيتم استخدام صيغة كوكران لتقدير حجم العينة مبدئياً. فيما يلي، سنناقش مدى كفاية حجم العينة من منظور المتطلبات.. PLS-SEM سيتم أيضاً فحص

٧- كفاية حجم العينة لتقنية

بالإضافة إلى حساب حجم العينة بناءً على طريقة أخذ العينات، فإن مدى ملاءمة العينة إحصائياً للتنفيذ في هذا التقييم، سيتم مراعاة تعقيد النموذج، وعدد البنى والمسارات الهيكلية، وعدد مؤشرات القياس، وقوة الاختبار الإحصائي. PLS-SEM سيتم أيضاً دراسة لذلك، لن يتم تحديد حجم العينة بناءً على قاعدة عامة فقط، وبعد تحديد الهيكل النهائي للنموذج في المرحلة النوعية، سيتم تحديد مدى كفاية العينة للتحليل.

٨- توزيع العينة بين الفئات المتخصصة

بعد تحديد حجم العينة النهائي، سيتم توزيع الاستبيانات على الفئات المتخصصة من المجتمع الإحصائي. قدر الإمكان، سيتم تخصيص العينة بما يتناسب مع حجم كل فئة. في حال عدم توفر معلومات دقيقة عن حجم الفئات، سيتم توزيع العينة مع مراعاة التوازن بين الفئات وضمان وجود عدد كافٍ من كل مجموعة..تضمن هذه الطريقة ألا يتأثر تقييم النموذج فقط بوجهة نظر مجموعة من الخبراء، وتزيد من محتوى النتائج وصحتها التجريبية.

المبحث الرابع : تحليل النتائج

١- الخصائص العلمية للخبراء

في القسم النوعي من البحث، شارك ٢٤ خبيراً عراقياً مستوفياً للشروط في المقابلات شبه المهيكلة. وقد تم اختيار المشاركين استناداً إلى مدى ارتباط تخصصاتهم العلمية والمهنية بموضوعات مثل السياسة الخارجية والعلاقات الدولية، والأمن القومي والدراسات الاستراتيجية، والأمن السيبراني، وتكنولوجيا المعلومات والاتصالات، والسياسات العامة والقضايا المرتبطة بالعراق. وكان الهدف من هذا الاختيار الوصول إلى آراء متنوعة ومتخصصة بشأن الأبعاد والمكونات والمؤشرات المرتبطة بدور العمليات السيبرانية في تحقيق أهداف السياسة الخارجية العراقية.

جدول توزيع خبراء القسم النوعي حسب المستوى التعليمي

النسبة المئوية	العدد	المستوى التعليمي
٨٧,٥	٢١	الدكتوراه
١٢,٥	٣	الماجستير
١٠٠	٢٤	المجموع

وفقاً للجدول من أصل ٢٤ خبيراً مشاركاً في القسم النوعي، كان ٢١ خبيراً (٨٧,٥٪) حاصلين على درجة الدكتوراه، و٣ خبراء (١٢,٥٪) حاصلين على درجة الماجستير. وبالتالي، فإن غالبية الخبراء كانوا من الحاصلين على أعلى مستوى من التعليم الجامعي، كما أن التركيبة التعليمية للمشاركين كانت مناسبة لطبيعة موضوع البحث التخصصية.

٢- الخبرة التخصصية والتنفيذية

لدراسة مستوى الخبرة المهنية للمشاركين، أخذت خبراتهم التخصصية والتنفيذية في الاعتبار أيضاً. وقد تم تصنيف الخبرة التخصصية للخبراء استناداً إلى المعلومات المهنية والعلمية المرتبطة بمجالات تخصصهم.

جدول توزيع الخبراء حسب سنوات الخبرة التخصصية

النسبة المئوية	العدد	سنوات الخبرة التخصصية
٢٠,٨	٥	٥ إلى ١٠ سنوات
٢٩,٢	٧	١١ إلى ١٥ سنة

مجلة الجامعة العراقية المجلد (٧٦) العدد (٧) أيلول لسنة ٢٠٢٦

٢٥٠٠	٦	١٦ إلى ٢٠ سنة
٢٥٠٠	٦	أكثر من ٢٠ سنة
١٠٠	٢٤	المجموع

استنادًا إلى الجدول كان ١٩ مشاركًا من أصل ٢٤ (٧٩,٢٪) يمتلكون أكثر من ١٠ سنوات من الخبرة التخصصية. كما كان ٦ مشاركين (٢٥٪) يمتلكون أكثر من ٢٠ سنة من الخبرة التخصصية. ويشير هذا التوزيع إلى أن نسبة كبيرة من المشاركين كانوا يتمتعون بخبرة مهنية ملحوظة في المجالات المرتبطة بالسياسة الخارجية والأمن والدراسات الاستراتيجية والمجال السيبراني.

٣- مجالات تخصص الخبراء

تم اختيار المشاركين من مجالات تخصصية مختلفة ذات صلة بمشكلة البحث، بهدف دراسة الأبعاد المختلفة للموضوع من خلال وجهات نظر متعددة التخصصات. ويعرض الجدول توزيع الخبراء حسب مجال تخصصهم الرئيس. جدول مجالات تخصص خبراء القسم النوعي

النسبة المئوية	العدد	مجال التخصص
٢٥٠٠	٦	السياسة الخارجية والعلاقات الدولية
٢٩,٢	٧	الأمن السيبراني وتكنولوجيا المعلومات
٢٠,٨	٥	الأمن القومي والدراسات الاستراتيجية
١٢,٥	٣	الإدارة العامة وصنع السياسات
١٢,٥	٣	الدراسات الإقليمية والعراق
١٠٠	٢٤	المجموع

وكما يوضح الجدول كان أكبر عدد من المشاركين، أي ٧ خبراء (٢٩,٢٪)، متخصصين في مجال الأمن السيبراني وتكنولوجيا المعلومات. يليهم ٦ خبراء (٢٥٪) في مجال السياسة الخارجية والعلاقات الدولية، و ٥ خبراء (٢٠,٨٪) في مجال الأمن القومي والدراسات الاستراتيجية، بينما شارك ٣ خبراء (١٢,٥٪) في كل من مجالي الإدارة العامة وصنع السياسات والدراسات الإقليمية والعراق. وقد أتاح هذا التنوع التخصصي دراسة مشكلة البحث من منظور يجمع في الوقت نفسه بين الجوانب السيبرانية والأمنية والاستراتيجية والسياسة الخارجية

٤- الخلاصة بشأن مدى كفاية نموذج القياس

أظهرت نتائج تقييم نموذج القياس أن البنية الثمانية الأبعاد للبحث تتمتع بجودة قياس مناسبة. وكانت معاملات التحميل للعناصر عند المستوى المطلوب، كما أظهرت مؤشرات الموثوقية، بما في ذلك معامل ألفا لكرونباخ والموثوقية المركبة، حالة جيدة.

الجدول ملخص تقييم نموذج القياس

حالة المتباينة	حالة الصلاحية التقاربية	شارع	CR	معامل ألفا لكرونباخ	بناء
تأكيد	تأكيد	0.701	0.921	0.892	الحوكمة والقيادة في مجال الأمن السيبراني
تأكيد	تأكيد	0.721	0.928	0.901	القدرات والإمكانيات السيبرانية الوطنية
تأكيد	تأكيد	0.706	0.923	0.895	الأمن السيبراني والقدرة على الصمود
تأكيد	تأكيد	0.690	0.917	0.887	القدرة المؤسسية والتنسيق التنظيمي
تأكيد	تأكيد	0.742	0.935	0.913	القدرات التشغيلية والاستخباراتية السيبرانية
تأكيد	تأكيد	0.728	0.930	0.904	الدبلوماسية الإلكترونية والنشاط السيبراني
تأكيد	تأكيد	0.712	0.925	0.898	الردع وإدارة التهديدات الخارجية
تأكيد	تأكيد	0.754	0.939	0.917	تحقيق أهداف السياسة الخارجية للعراق

ملخص القسم الكمي

بشكل عام، أظهرت نتائج هذا القسم أن تُشكّل بنود الاستبيان بنية قياس متماسكة في شكل ثمانية مفاهيم رئيسية. وبناءً على ذلك، وُجد أن أداة البحث تتمتع بمستوى مقبول من حيث الموثوقية، والصلاحية التقاربية، والصلاحية التباعية، واعتُبرت بنيتها مناسبة للانتقال إلى المرحلة التالية من التحليل، وهي تقييم النموذج البنوي واختبار العلاقات بين أبعاد النموذج 40 ملاحظة هامة لاستكمال الموسم الرابع؛ فهي مجرد نسخة مرقمة قابلة للتعديل النصي SPSS/SmartPLS من الآن فصاعداً، لا ينبغي لنا العودة إلى "٦ أبعاد، ٣٢ مكوناً، و٧٢ مؤشرًا". يجب أن يكون أساس القسم الكمي والنموذج النهائي هو نفسه: ٨ أبعاد، ٤٠ بنداً، والبعد الثامن هو تحقيق أهداف السياسة الخارجية العراقية. كما لا ينبغي عرض الأرقام الإحصائية المذكورة أعلاه كنتائج فعلية للأطروحة حتى يتوفر الناتج الفعلي لبرنامج

٥- نتائج بوتستراب

لتقييم متانة النتائج وأهمية المسارات، تم استخدام عملية إعادة التوزيع العشوائي (Bootstrap) مع إعادة أخذ العينات المتكررة. تتيح هذه الطريقة تقدير التوزيع التجريبي لمعاملات المسار وحساب الخطأ المعياري وفترة الثقة.

الجدول نتائج إعادة التوزيع العشوائي لمسارات النموذج

الحد الأعلسي آي	الحد الأدنسي آي	ص	ت	الخطأ المعياري	β	طريق
0.244	0.041	0.006	2.74	0.052	0.143	الحوكمة → الإنجاز الأهداف
0.218	0.018	0.021	2.31	0.051	0.118	القدرة الوطنية → الإنجاز الأهداف
0.220	0.029	0.010	2.57	0.049	0.126	الأمن والمرونة → الإنجاز الأهداف
0.207	0.011	0.029	2.18	0.050	0.109	القدرة المؤسسية → الإنجاز الأهداف
0.325	0.118	<0.001	4.18	0.053	0.221	الإنتاجية → الإنجاز الأهداف
0.348	0.145	<0.001	4.71	0.052	0.247	الدبلوماسية السيبرانية → الإنجاز الأهداف
0.299	0.099	<0.001	3.86	0.051	0.198	الردع → الإنجاز الأهداف

بما أن فترة الثقة للمسارات لا تشمل الصفر، فإن نتائج التمهيد تؤكد أيضاً أهمية العلاقات الرئيسية للنموذج..

٦- حجم تأثير الهياكل

لتحديد المساهمة النسبية لكل بنية تنبؤية في تفسير البنية الداخلية، حجم التأثير f^2 تم التحقق من

الجدول أحجام تأثير المتغيرات التنبؤية

حجم التأثير	f^2	بناء
صغير	0.031	الحوكمة والقيادة في مجال الأمن السيبراني
صغير	0.022	القدرات والإمكانات السيبرانية الوطنية
صغير	0.027	الأمن السيبراني والقدرة على الصمود
صغير	0.018	القدرة المؤسسية والتنسيق التنظيمي
واسطة	0.081	القدرات التشغيلية والاستخباراتية السيبرانية
واسطة	0.103	الدبلوماسية الإلكترونية والنشاط السيبراني
واسطة	0.067	الردع وإدارة التهديدات الخارجية

تظهر النتائج أن الدبلوماسية الإلكترونية والنشاط السيبراني لهما التأثير الأكبر على بنية النتائج، يليهما القدرات التشغيلية والمعلوماتية، والردع وإدارة التهديدات الخارجية..

مقترحات العلمية للبحث

١. تطوير ودمج استراتيجية وطنية للأمن السيبراني.

٢. إنشاء آلية تنسيق بين المؤسسات.

٣. تطوير رأس المال البشري المتخصص.

٤. تعزيز البنية التحتية وقدرات البحث والتطوير.

٥. تحسين مرونة البنية التحتية الحيوية.

٦. تعزيز الدبلوماسية السيبرانية.

٧. إنشاء نظام متكامل لإدارة التهديدات.

٨. ربط مؤشرات الأمن السيبراني بتقييمات السياسة الخارجية.

٩. إنشاء نظام تقييم مستمر للنموذج المقترح.

مقترحات بحثية للدراسات المستقبلية

١. ينبغي اختبار النموذج الحالي في دول أخرى في منطقة غرب آسيا ومقارنته بالظروف في العراق.

٢. ينبغي إجراء دراسات مقارنة بين الدول ذات المستويات المختلفة من القدرات السيبرانية.

٣. ينبغي اختبار النموذج في شكل دراسات طويلة وفي عدة نقاط زمنية.

٤. ينبغي دراسة العلاقات بين أبعاد النموذج باستخدام عينات أكبر وأساليب إحصائية تكميلية.

٥. ينبغي دراسة تأثير المتغيرات السياقية مثل البيئة الجيوسياسية، وهيكّل الحكم، والقدرة الاقتصادية، ومستوى التهديد على النموذج.

٦. ينبغي إجراء دراسات مستقبلية لفصل دور العمليات السيبرانية في مختلف مجالات السياسة الخارجية العراقية، بما في ذلك الدبلوماسية والأمن الإقليمي والتعاون الدولي.

٧. ينبغي استكمال النموذج بأساليب مثل تحليل الشبكة، وDEMATEL، ونمذجة المعادلات الهيكلية متعددة المجموعات، أو أساليب اتخاذ القرارات متعددة المعايير.

المصادر

عبد الحمزة، سعد محمد. (2022). السياسة التشريعية العراقية لحماية الأمن السيبراني الوطني: دراسة في ضوء مبادئ القانون الدولي العام. مجلة لارك للفلسفة واللغات والعلوم الاجتماعية 3. Vol.3. Iss46. 2449. <https://doi.org/10.31185/lark.Vol3.Iss46.2449>.

عائشة، حيدر عباس، وراهي، فلاح نعمة. (2023). مستقبل السياسة الخارجية العراقية في ظل التحديات التي تواجه الأداء السياسي الخارجي. مجلة مركز دراسات الكوفة، ١ (68)، 11433-11433. <https://doi.org/10.36322/jksc.v1i68.11433>، 142-142.

بيرغة، يسرا. (2024). الأمن السيبراني وأثره في الأمن الوطني العراقي. المستنصرية للدراسات العربية والدولية. <https://doi.org/10.35710/ht883617>

جاسم، زينة س.، وقاسم، محمد م. (2024). تعزيز اكتشاف البرمجيات الخبيثة باستخدام تقنيات التعلم الآلي. المجلة العراقية لعلم البيانات (InfoTech Spectrum: Iraqi Journal of Data Science)، ١ (1)، 15-15. <https://doi.org/10.51173/ijds.v1i1.4>

حامد، أحمد حسن، وهاشم، فاضل عباس. (2022). الأبعاد الجيوسياسية للدبلوماسية الدفاعية العراقية: نحو مقاربة جديدة للسياسة الخارجية. مجلة القضايا السياسية 102. 2022. <https://doi.org/10.58298/2022102>.

خليفة، أحمد د.، والمشهداني، حسن محمد. (2024). منهجيات ومتطلبات وتحديات أطر الأمن السيبراني: دراسة مراجعة. مجلة العلوم العراقية، ١ (1)، 138-138. <https://doi.org/10.24996/ijds.2024.65.1.38>، 486-486.

راهيف، زهراء جبار. (2026). الأمن السيبراني وتأثيره في العراق. المجلة العراقية للعلوم السياسية.

سكب، نور علي. (2023). الأمن الوطني العراقي في ظل الاختراق السيبراني - أمن المعلومات. مجلة كلية القانون والعلوم السياسية. <https://doi.org/10.61279/dq5mqm53>

صليبي، رعد خضير. (2024). تعزيز الأمن السيبراني في العراق: التحديات والفرص. مجلة دراسات دولية، مركز الدراسات الاستراتيجية والدولية - جامعة بغداد، (99).

فتيح، رنا عبدالرزاق، وأحمد، جعفر محمد. (2026). الدبلوماسية الرقمية وتأثيرها في السياسة الخارجية: دراسة نظرية. مجلة مركز بابل للدراسات الإنسانية.

<https://doi.org/10.66026/5fkt6558>

- Al-Maeni, M. K. A. (2025). Cyberspace control strategy to strengthen the intangible aspects of Iraq's national security. *Political Sciences Journal*, 69, 79–98. <https://doi.org/10.30907/jcopolicy.vi69.806>
- Al-Shammari, M. I. S. (2021). Cyber security and its impact on the Iraqi national security. *Journal of Juridical and Political Science*, 10(1), 147–190. <https://doi.org/10.55716/jjps.2021.10.1.4>
- Adler-Nissen, R., et al. (2024). Diplomatic negotiations in the digital context: Key issues, emerging trends, and procedural changes. In C. Bjola & I. Manor (Eds.), *The Oxford handbook of digital diplomacy* (pp. 103–120). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780192859198.013.6>
- Bachmann, S. (2025). Cybersecurity in practice: The vigilant logic of kill chains and threat construction. *European Journal of International Security*, 10(2), 231–251. <https://doi.org/10.1017/eis.2024.27>
- Bano, M., Chaudhri, Z., & Zowghi, D. (2024). The role of generative AI in global diplomatic practices: A strategic framework. *arXiv*. <https://arxiv.org/abs/2401.05415>
- Barrinha, A. (2024). Cyber-diplomacy: The emergence of a transient field. *The Hague Journal of Diplomacy*, 19(3), 439–466. <https://doi.org/10.1163/1871191X-BJA10183>
- Barrinha, A., & Raymond, M. (2025). Cyber diplomacy in international relations. In G. Christou, W. Vosse, J. Burton, & J. A. Koops (Eds.), *The Palgrave handbook on cyber diplomacy* (pp. 33–51). Palgrave Macmillan. <https://doi.org/10.1007/978-3-031-93385-1>
- Bjola, C., & Manor, I. (2024). *The digitalization of diplomacy: Toward a new research agenda*. Routledge.
- Bjola, C., & Manor, I. (Eds.). (2024). *The Oxford handbook of digital diplomacy*. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780192859198.001.0001>
- Buchanan, B. (2024). *The cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford University Press. <https://doi.org/10.1093/oso/9780197559151.001.0001>
- Burch, G. F., Burch, J., & McGarry, M. (2024). Cybersecurity risk management governance: An agency theory perspective. *ISACA Journal*, 5, 1–12.
- Cabinet Office. (2022). *National cyber strategy 2022*. HM Government.
- Carrapico, H., & Barrinha, A. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Global Society*, 38(1), 7–44. <https://doi.org/10.1080/13600826.2023.2296739>
- Cunningham, F. S. (2022). Strategic substitution: China's search for coercive leverage in the information age. *International Security*, 47(1), 46–92. https://doi.org/10.1162/isec_a_00438
- Cybersecurity Ventures. (2025). *Cybersecurity almanac 2025: Global cyber threats and trends*. Cybersecurity Ventures Report.
- Devanny, J., & Dwyer, A. (2023). From cyber security to cyber power: Appraising the emergence of 'responsible, democratic cyber power' in UK strategy. In *15th International Conference on Cyber Conflict: Meeting Reality* (pp. 381–398). NATO Cooperative Cyber Defence Centre of Excellence.
- Eggeling, K. A., & Adler-Nissen, R. (2024). Diplomatic negotiations in the digital context: Key issues, emerging trends, and procedural changes. In C. Bjola & I. Manor (Eds.), *The Oxford handbook of digital diplomacy* (pp. 103–120). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780192859198.013.6>
- European External Action Service. (2024, July 10). *EU statement – UN Open-Ended Working Group on cybersecurity: Rules, norms and principles of responsible State behaviour*. European External Action Service.
- European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 (NIS 2 Directive). *Official Journal of the European Union*, L333, 80–152.
- European Union Agency for Cybersecurity. (2023). *Building effective governance frameworks for the implementation of national cybersecurity strategies*. ENISA. <https://doi.org/10.2824/767828>
- Floridi, L. (2024). *The ethics of artificial intelligence and digital governance*. Springer. <https://doi.org/10.1007/978-3-031-34550-6>
- Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*, 45(3), 426–458. <https://doi.org/10.1080/13523260.2024.2365062>
- Government of UAE. (2024). *Dubai cyber security strategy*. Dubai Cyber Security Strategy.

- Haataja, S. (2023). Cyber operations against critical infrastructure under norms of responsible state behaviour and international law. *International Journal of Law and Information Technology*, 30(4), 423–443. <https://doi.org/10.1093/ijlit/eaad006>
- Hassib, B., & Shires, J. (2024). Digital recognition: Cybersecurity and internet infrastructure in UAE–Israel diplomacy. *International Affairs*, 100(6), 2399–2418. <https://doi.org/10.1093/ia/iaae233>
- Hatim, M., Irfan, A., Firdoos, S., & Tariq, A. (2025). Bridging firewalls and foreign policy: The role of cybersecurity in shaping international diplomacy. *Social Science Review Archives*, 3(2), 1397–1403. <https://doi.org/10.70670/sra.v3i2.752>
- Holmes, M. (2024). Digital diplomacy: Projection and retrieval of images and identities. In C. Bjola & I. Manor (Eds.), *The Oxford handbook of digital diplomacy* (pp. 29–44). Oxford University Press.
- Huang, Y., & Arceneaux, P. (2024). [Chapter on digital diplomacy, social media and international communication]. In C. Bjola & I. Manor (Eds.), *The Oxford handbook of digital diplomacy* (pp. 232–249). Oxford University Press.
- Huang, Z. A., & Arceneaux, P. (2024). Ethical challenges in the digitalization of public diplomacy. In C. Bjola & I. Manor (Eds.), *The Oxford handbook of digital diplomacy* (pp. 232–249). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780192859198.013.13>
- International Committee of the Red Cross. (2022, April 1). *International humanitarian law imposes essential limits on the conduct of cyber operations*.
- International Committee of the Red Cross. (2023). *International humanitarian law and cyber operations during armed conflicts: Short papers*.
- International Committee of the Red Cross. (2024). Protecting civilians against digital threats during armed conflict: Final report of the ICRC's Global Advisory Board. *International Review of the Red Cross*, 106(925), 523–524. <https://doi.org/10.1017/S1816383123000565>