رقمنة النزاع في العراق: من الحرب التقليدية إلى التهديدات الرقمية المُركبة

م.م. نورا رياض الدباغ

مركز الدراسات الاستراتيجية والدولية/ جامعة بغداد

يتناول البحث رقمنة النزاع في العراق بوصفها تحولًا بنيويًا في طبيعة الصراعات الإقليمية من ساحة القتال التقليدية إلى فضاءات رقمية تتداخل فيها الهجمات السيبرانية، والتضليل الإعلامي، وتطبيقات الذكاء الاصطناعي، ويوضح البحث أن ثورة الويب (2.0) أسهمت في تفكيك احتكار تدفق المعلومات، ودفعت نحو أنماط نزاع رقمي هجين يعتمد على مشاركة جماهيرية واسعة، وعمليات تأثير نفسي ومعلوماتي، كما يناقش البحث محطات مفصلية رسخت المجال السيبراني بوصفها حيزًا عملياتيًا رسميًا مثل: حرب جورجيا عام (2008)، وإقرارات الناتو اللاحقة، ويبين أن حرمان الدول من تدفق المعلومات أو تعطيل البنى التحتية الرقمية يمثل مساسًا مباشرًا بالسيادة، كما يركز البحث على هشاشة الوضع العراقي نتيجة ضعف البنية التحتية التقنية، ونقص التشريعات، ومحدودية خطط الطوارئ، وتعرض مؤسسات حكومية لمحاولات اختراق وتجسس، ويعرض البحث انعكاسات النزاع الرقمي على العراق عبر استهداف البنى الحيوية والبيانات السيادية، وزعزعة الثقة بالمؤسسات، ويختتم برؤية عراقية لمواجهة التهديدات عبر بناء قدرات وطنية، وتطوير التشريعات، وتفعيل الدبلوماسية الرقمية، وتوسيع التراكات الإقليمية والدولية، بما يعزز السيادة السيبرانية، ويحول التهديدات إلى فرص تحديث.

الكلمات المفتاحية: رقمنة النزاع، النزاع الرقمي، الأمن السيبراني، السيادة السيبرانية، الذكاء الاصطناعي.

Digitization of Conflict in Iraq: From Conventional Warfare to Compound Digital Threats

Asst. Inst. Noura Riyadh Al-Dabbagh

Researcher at the Center for Strategic and International Studies University of Baghdad

The study addresses the digitization of conflict in Iraq as a structural shift in the nature of regional contention from conventional battlefields to digital arenas where cyberattacks, disinformation, and artificial intelligence applications. It argues that the Web (2.0) transformation dismantled traditional monopolies over information flows and led to the emergence of hybrid digital conflict that relies on mass participation, psychological and information influence operations. The study also highlights pivotal developments that consolidated cyberspace as an operational domain, notably the (2008) Georgia war and subsequent NATO determinations, underscoring that denying states access to critical information or disrupting digital infrastructure constitutes a direct infringement on sovereignty.The research focuses on the vulnerability of the Iraqi condition resulting from weakness of technical infrastructure, lack of legislation, limited cyber contingency planning, and the exposure of Government institutions to incidents of intrusion and espionage. The research

presents the repercussions of digital conflict affects Iraq targeting critical infrastructure, sovereign data, and erosion of public trust in state authority. The study concludes with an Iraqi vision to encounter threats by building national capabilities, strengthening legislation, institutionalizing cyber diplomacy, and expanding regional and international partnerships to enhance cyber sovereignty and convert digital threats into opportunities for modernization.

Keywords ::Digitization of Conflict, digital conflict, cybersecurity, cyber sovereignty, Artificial Intelligence.

الاستلام	الإرجاع	القبول
2026/2/12	2026/2/22	2026/3/4

المقدمة

شهدت الصراعات الإقليمية تحولات نوعية لم تقتصر على ميادين القتال التقليدية، بل امتدت إلى الفضاءات الرقمية، حيث بات النزاع يدار عبر أدوات رقمية، وصيغ التضليل الإعلامي، والهجمات السيبرانية، وبرمجيات الذكاء الاصطناعي، ولم تعد القوة المسلحة وحدها هي الفاعل الحاسم، بل صارت البيانات والمعلومات والقدرة على اختراق الشبكات وتوجيه الرأي العام عناصر مركزية في بنية النزاع، ففي الشرق الأوسط، برزت هذه التحولات بشكل مكثف، حيث تحولت بعض النزاعات إلى أنماط نزاع رقمي هجين، فالنزاع هنا لا يختزل بالحرب المسلحة، بل يشمل أنماطًا رقمية وإعلامية وسيبرانية تستخدم دون الوصول إلى صدام عسكري مباشر، بل بات الفضاء السيبراني امتدادا للمعارك الجيوسياسية التقليدية، وأداة لتقويض استقرار الدول، والتأثير على القرار السياسي، وتوجيه الوعي المجتمعي، وبينما كثّفت بعض الدول الإقليمية من قدراتها في هذا الميدان، وقعت دول أخرى ضحية لهذه التحولات دون بنى مؤسسية أو تشريعية أو تقنية كافية.

العراق، بوصفه ساحة تنافس إقليمي ودولي، يجد نفسه في مواجهة تهديدات رقمية تتجاوز قدراته الحالية، وليس العراق هنا مجرد متلقٍ للتهديدات الرقمية، بل ساحة تتقاطع فيها أجندات إقليمية ودولية تسعى إلى توجيه الإدراك العام، واختراق مؤسسات الدولة، والتحكم بالبيئة المعلوماتية بوصفها مدخلًا للنفوذ السياسي، ما يجعل الرقمنة جزءا من معادلة الأمن الوطني لا هامشًا تقنيا، ورغم تنامي الإدراك الحكومي بخطورة النزاع الرقمي، ما زالت الاستجابات متقطعة وغير متكاملة، وسط بيئة سياسية هشة، ونقص في التشريعات، وضعف في البنى التحتية السيبرانية، تأتي هذه

الورقة لفهم هذا التحول في طبيعة النزاع من منظور دولي، وتحديد موقع العراق ضمنه، وتقديم رؤية استراتيجية لمواجهة هذا التحدي وتحويله إلى فرصة وطنية لتعزيز السيادة الرقمية.

إشكالية البحث

يقوم البحث على إشكالية مركزية تتمثل في كيفية تأثير رقمنة النزاع على الأمن والسيادة السيبرانية في العراق، في ظل التحول المتسارع نحو أنماط نزاع رقمي مركّب، وتنامي استخدام الهجمات السيبرانية، والتضليل الإعلامي، والذكاء الإصطناعي مثل: أدوات الصراع، مقابل محدودية القدرات المؤسسية والتشريعية والتقنية العراقية على الاستجابة الفاعلة لهذه التحديات.

أهمية البحث

تأتي أهمية البحث من معالجته لتحول نوعي في طبيعة النزاعات الإقليمية، حيث لم تعد تقتصر على المواجهات العسكرية المباشرة، بل امتدت إلى الفضاء السيبراني بوصفه ساحة صراع مركزية، كما يكتسب البحث أهميته من تركيزه على الحالة العراقية بوصفها بيئة هشّة رقميا، ما يجعله مساهمة علمية في فهم العلاقة بين رقمنة النزاع والسيادة الوطنية في سياق شرق أوسطي مضطرب.

أهداف البحث

يهدف البحث إلى:

1. تحليل مفهوم رقمنة النزاع وأبعاده النظرية والعملية.
2. توضيح أدوات النزاع الرقمي، لا سيما الهجمات السيبرانية، والتضليل الإعلامي، والذكاء الإصطناعي.
3. تشخيص انعكاسات النزاع الرقمي على الأمن والسيادة السيبرانية في العراق.
4. تقييم مستوى الجاهزية العراقية في مواجهة التهديدات الرقمية.
5. تقديم رؤية استراتيجية لتعزيز السيادة السيبرانية العراقية.

فرضية البحث

يفترض البحث أن رقمنة النزاع في الإقليم أسهمت في تصاعد التهديدات الرقمية المركبة ضد العراق، وأضعفت سيادته السيبرانية، وأن مواجهة ذلك تتطلب تبني إستراتيجية وطنية متكاملة تقوم على بناء القدرات والتشريع والتنسيق المؤسسي والدبلوماسية الرقمية.

حدود البحث

1. **الحدود الموضوعية:** يركز البحث على النزاع الرقمي وأدواته السيبرانية والإعلامية والذكية.
2. **الحدود المكانية:** العراق ضمن سياقه الإقليمي والدولي.
3. **الحدود الزمانية:** يغطي المدة من عام (2008) حتى عام (2025)، بوصفها مرحلة ترسخ النزاع الرقمي.

مصطلحات الدراسة وتعريفاتها الإجرائية

- **رقمنة النزاع:** انتقال أدوات ووسائل إدارة النزاع إلى الفضاء الرقمي، بما يشمل: الهجمات السيبرانية والتأثير المعلوماتي والذكاء الإصطناعي.
- **النزاع الرقمي:** نمط صراع غير تقليدي يدار عبر الفضاء السيبراني من دون اشتراط الصدام العسكري المباشر.
- **السيادة السيبرانية:** قدرة الدولة على التحكم في فضائها الرقمي وحماية بنيتها التحتية وبياناتها الوطنية من التدخل الخارجي.
- **الحرب الرقمية:** استخدام الوسائل الرقمية بوصفها أداة داخل النزاع لتحقيق أهداف سياسية أو أمنية.

الدراسات السابقة

تناولت الأدبيات الحديثة موضوع النزاع الرقمي من زوايا متعددة، ركزت في معظمها على تطور الفضاء السيبراني بوصفه مجالاً عملياتيا جديدا، وعلى دور الهجمات السيبرانية والتضليل الإعلامي في إعادة تشكيل طبيعة الصراع، وفي هذا السياق، تناولت دراسة Mareš and Netolická (2020) ديناميكيات الصراع السيبراني في حرب جورجيا 2008، وبينت كيف تم توظيف الهجمات الرقمية بالتوازي مع العمليات العسكرية، مما رسخ الفضاء السيبراني بوصفه ساحة حرب فعلية، كما ركزت دراسة Sarah Cherry (2024) على دور حملات التضليل الإعلامي في النزاعات الحديثة، موضحةً تأثيرها في تشكيل البيئة المعلوماتية والتأثير على الرأي العام وصناعة القرار السياسي، من جهة أخرى، ناقشت تقارير The Asia Foundation

(2020) دور شركات التكنولوجيا ووسائل التواصل الاجتماعي في النزاعات العنيفة، مؤكدة تحول هذه الشركات إلى فاعلين مؤثرين في إدارة الصراع الرقمي.

أما على المستوى العربي، فقد تناولت دراسة حسين إسماعيل حداد (2024) التحول الرقمي في الخطاب الإعلامي العراقي، وأشارت إلى تأثير البيئة الرقمية في تشكيل السلوك السياسي والإعلامي داخل العراق، ورغم أهمية هذه الدراسات، إلا أنها ركزت في الغالب على أطر نظرية أو حالات دولية، ولم تتناول بشكل مباشر حالة العراق ضمن مفهوم النزاع الرقمي المركب، وهو ما يسعى هذا البحث إلى معالجته.

منهج البحث

يعتمد البحث المنهج التحليلي – الاستشرافي، من خلال تحليل تطور النزاع الرقمي وأدواته، وربطها بالواقع العراقي، واستشراف المسارات المستقبلية لتعزيز الأمن والسيادة السيبرانية في العراق.

المحور الأول: التحول من النزاع التقليدي إلى أنماط الحرب الرقمية

تعود جذور الحرب الرقمية الحديثة بوصفها أداة للنزاع المعاصر إلى حرب الخليج عام (1991)، التي استعرضت التطورات التكنولوجية، وأسست لأنموذجٍ جديد يجمع بين الإدارة العسكرية والإعلامية الوثيقة، وهذا الأنموذج، الذي تم تطبيقه لاحقًا في أفغانستان (2001)، والعراق (2003)، كان يعتمد على سيطرة مركزية في تدفق المعلومات، إلا أن (ثورة الويب 2.0) المتمثلة بظهور في إحدى جوانبها بظهور وسائل التواصل الاجتماعي من فيسبوك، ومنصة إكس، وأنستغرام، ويوتيوب، وغيرها، قلبت هذه المعادلة، حيث مكنت التقنيات الرقمية الجديدة أي فرد من أن يصبح منتجا وموزعا للمعلومات، مما أدى إلى انهيار السيطرة المعلوماتية التقليدية وظهور ما يعرف بـ (الحرب التشاركية)، وقد لوحظ هذا النمط الجديد من الصراع في مناطق مثل: غزة، والعراق، وسوريا، حيث أصبحت المشاركة الجماهيرية عبر المنصات الرقمية جزءا من ديناميكيات النزاع[1].

مثلت حرب جورجيا عام (2008) نقطة تحول محورية في هذا الجانب، حيث شهدت أول استخدام منسق للهجمات السيبرانية بالتزامن مع العمليات العسكرية التقليدية، مما رسخ مكانة الفضاء السيبراني بوصفها ساحة عملياتية خامسة إلى جانب البر والبحر والجو والفضاء، وتكرس لاحقًا بقرار حلف شمال الأطلسي (الناتو) في عام (2014) بمساواة الهجمات السيبرانية بالهجمات

الحركية، وتأكيد قمة وارسو عام (2016) على أن المجال السيبراني هو مجال عملياتي رسمي، لقد أدى هذا التطور إلى إدراك أن حرمان أي بلد من الوصول إلى المعلومات التي يحتاجها ليعمل (خاصة في سياق تبادل المعلومات) يعد انتهاكا واضحا لسيادته.

في العراق تبرز هذه النقطة بصورة أكثر حساسية لأن تعطيل الخدمة الرقمية أو التلاعب بتدفق المعلومات لا يضرب البنية التقنية فقط، يضغط أيضا على شرعية الدولة وثقة المجتمع، ويحول السيادة السيبرانية إلى ملف سيادي مرتبط بالاستقرار السياسي ووحدة القرار العام[2].

يمثل هذا التحول، المعروف بـ (رقمنة النزاع)، تطورا نوعيا في أدوات وإستراتيجيات الحرب[3]، فرقمنة النزاع لا تمثل حالة ثابتة، بل هي عملية ديناميكية تشمل: الاستخدام المتزايد للوسائل والأساليب الرقمية المدعومة بتطورات تكنولوجية سريعة في الإنترنت، والذكاء الإصطناعي، والتعلم الآلي، والروبوتات، التي تعيد تشكيل النزاع من خلال خلق (جغرافيات الكترونية) جديدة تتفاعل مع الظروف الواقعية مثل: مستويات التعليم، وسرعة الاتصال بالإنترنت، والسياسات المحلية، فهو يشمل مجموعة معقدة من الأدوات والتكتيكات التي تستهدف البيئة الرقمية بأكملها[4]، يمكن تقسيم أبعاد الحرب الرقمية الرئيسة على:

1. **الهجمات السيبرانية:** التي تمثل مكونا أساسيا في الصراعات الحديثة، حيث تؤثر بشكل مباشر في الأمن القومي والاستقرار العالمي يمكن تصنيف هذه الهجمات إلى فئات متعددة، لكل منها أهداف وتأثيرات مختلفة، كما يوضح الجدول رقم (1) في أدناه لتحليل النزاعات الحديثة مثل: الصراع الروسي الأوكراني ونزاع جورجيا[5].

جدول رقم (1): تحليل النزاعات الحديثة

ت	نوع الهجوم السيبراني	وصف الهجوم	أمثلة
1	هجمات حجب الخدمة الموزعة (DDoS)	تهدف إلى إغراق الأنظمة المستهدفة (مواقع حكومية، بنوك) بحركة مرور زائفة لجعلها غير متاحة للمستخدمين الشرعيين.	استخدام شبكات الروبوتات (Botnets) لتوليد كميات هائلة من حركة المرور، وتطوير أدوات (DDoS) تكيفية تستفيد من الذكاء الاصطناعي؛ لتغيير أساليب الهجوم.
2	برمجيات المسح (Wiper Malware)	برمجيات خبيثة مصممة لتدمير البيانات بشكل دائم وجعل الأنظمة والشبكات غير قابلة للتشغيل.	استخدام برمجيات مثل: WhisperGate، HermeticWiper، CaddyWiper، و AcidRain في أوكرانيا لتدمير سجلات الإقلاع الرئيسة والبيانات الحساسة.

ت	نوع الهجوم السيبراني	وصف الهجوم	أمثلة
3	تشويه المواقع (Defacement)	تغيير المظهر المرئي للمواقع الإلكترونية البارزة ونشر رسائل دعائية أو صور مهينة.	استهداف مواقع البنك الوطني الجورجي ووزارة الخارجية بصور تقارن الرئيس الجورجي بأدولف هتلر، بهدف التأثير المعنوي السلبي.
4	التصيد الاحتيالي والتجسس الإلكتروني (Phishing & E-espionage)	هجمات تستهدف سرقة بيانات حساسة أو استراتيجية من خلال خداع المستخدمين أو اختراق الأنظمة.	هجمات التصيد الاحتيالي الموجه (Spear-phishing) التي تستهدف أفرادًا أو مؤسسات معينة للحصول على معلومات استراتيجية خلال النزاعات.
5	هجمات سلسلة التوريد (Supply Chain Attacks)	اختراق طرف ثالث موثوق مثل: مزود برمجيات؛ للوصول إلى شبكات الهدف النهائي.	أصبحت هذه الهجمات أكثر قدرة وتشابكًا مع حملات برامج الفدية، مما يسمح بتوسيع نطاق العمليات من خلال اختراق أولي واحد.

الجدول من عمل الباحثة بالاعتماد على المصدر:

Miroslav Mareš and Veronika Netolická. "Georgia 2008: Conflict Dynamics in the Cyber Domain." Strategic Analysis 44, no. 3 (2020).
https://doi.org/10.1080/09700161.2020.1778278

العراق، مثله مثل دول أخرى في المنطقة، يفتقر حاليا إلى القدرات الكافية لإدارة حرب سيبرانية واسعة النطاق؛ بسبب ضعف البنية التحتية التقنية، وغياب خطط طوارئ سيبرانية واضحة، وتتفاقم هذه المشكلة بسبب التركيز على الحرب التقليدية، وإهمال الفضاء السيبراني، بوصفه ساحة عمليات متكاملة، وهذا القصور لا ينعكس على مستوى الحماية فقط، بل يخلق فجوة ردع، ويجعل الفضاء العراقي مجالاً مناسبا للابتزاز السياسي والتجسس والتأثير، بما يسمح لخصوم الدولة أو منافسيها بتحقيق مكاسب دون مواجهة عسكرية أو مسؤولية معلنة[6].

2. **التضليل الإعلامي:** يعرف التضليل الإعلامي بأنه النشر المتعمد لمعلومات كاذبة بهدف إلحاق الضرر أو تحقيق مكاسب سياسية، وهو يختلف عن (المعلومات المضللة) التي قد تنشر عن غير قصد، وقد تطور التضليل الإعلامي إلى سلاح رقمي متطور في العصر الحديث، حيث تستخدم اليوم وسائل الإعلام الجماهيرية، ومنصات التواصل الإجتماعي، ومحركات البحث، والذكاء الإصطناعي لنشر روايات كاذبة وتشكيل المشهد المعلوماتي، وتهدف حرب المعلومات إلى ممارسة تأثير نفسي على السكان أو الضغط على دولة، لاتخاذ قرارات تصب في مصلحة الخصم[7]، ففي أثناء الضربات العسكرية المتبادلة في حزيران (2025)، شنت إيران حملات

مكثفة من الأخبار الكاذبة والتضليل بهدف التأثير على الرأي العام الصهيوني وحتى الدولي، استخدمت وسائل الإعلام الإيرانية تقنيات الذكاء الاصطناعي لإنتاج محتوى مثل: صور أو مقاطع مفبركة لنشر رسائل إنهزامية بين الصهاينة تهدف إلى تقويض الروح المعنوية، علاوة على ذلك، تضمنت الحملة نشر محتوى مضلل بالعبرية، مع رسائل تختفي خلفها دعوات للاستسلام أو تراجع الدعم الداخلي[8].

3. **استخدام الذكاء الإصطناعي:** وفّر التقدم في تقنيات الذكاء الإصطناعي أدوات جديدة للحرب الرقمية، تستغل فيها خوارزميات التعلم الآلي، لتحليل كميات هائلة من البيانات، واستهداف الفئات المحددة من الجمهور برسائل مصممة خصيصا للتأثير عليهم، كما أصبحت تقنيات التزييف العميق (Deepfake) قادرة على إنتاج مقاطع فيديو أو تسجيلات صوتية مزيفة تبدو حقيقية تماما، مما يفتح الباب أمام حملات خداع غير مسبوقة قد تستخدم لتأجيج النزاعات أو تبريرها، فضلاً عن ذلك، دخل الذكاء الاصطناعي في تطوير أسلحة وأنظمة ذاتية التشغيل مثل: الطائرات المسيرة المسلحة بأنظمة توجيه ذكية، وكذلك في عمليات المراقبة الجماعية، وتحليل المعلومات الاستخبارية بوتيرة تفوق القدرات البشرية[9]، أشار خبراء دوليون إلى أن النزاعات الحديثة مثل الحرب على غزة (2023) باتت تشهد تحويل السكان إلى بيانات قابلة للاستهداف عبر أساليب رقمية استغلت لارتكاب انتهاكات وتبريرها، وعليه فإن إدماج الذكاء الاصطناعي في ميدان الصراع يطرح تحديات أخلاقية وأمنية كبيرة، من أبرزها: صعوبة التمييز بين الحقيقة والتضليل، وتصاعد وتيرة الصراع وسرعته، نتيجة الأتمتة[10].

هذه التحولات مجتمعة تعني أن طبيعة النزاعات الإقليمية لم تعد كما كانت، وأصبحت الدول تسعى لبناء قدرات سيبرانية هجومية ودفاعية بوصفها جزءا أساسا من منظوماتها الأمنية، ففي الشرق الأوسط على وجه الخصوص، تداخلت ساحات الحرب التقليدية والرقمية، فكل صراع عسكري يصاحبه اليوم بعد إلكتروني من اختراق البنى التحتية، وقطع الإنترنت عن العدو، إلى حملات التأثير عبر وسائل الإعلام، وبذلك دخلت المنطقة عصرا يمكن وصفه بعصر (عسكرة الفضاء السيبراني)، الذي يستخدم الشيفرات والبرمجيات الخبيثة جنبا إلى جنب مع الصواريخ والمدافع لتحقيق أهداف الصراع، وهذا الواقع الجديد يفرض فهما

أعمق لأبعاد رقمنة النزاع، وتأثيراتها بعيدة المدى على أمن الدول واستقرارها، عراقيا فإن رقمنة النزاع تعني انتقال الضغط من خطوط التماس إلى شبكات الدولة، من الجبهة العسكرية إلى البنى الخدمية والبيانات والوعي العام، وبذلك يصبح النزاع الرقمي وسيلة لتعديل ميزان القوة داخل الدولة عبر استنزافها إداريا وإرباكها سياسيا[11].

بالنسبة للعراق، فعلى الرغم من غياب دراسات مفصلة عن استخدام هذه الأدوات في سياق النزاع، فإن التحليل الإعلامي يشير إلى أن الخطاب الإعلامي يتأثر بشدة بالتحولات الرقمية والسياسية، وأن المشهد السياسي المضطرب يخلق تعددية في الخطابات المتضاربة التي تغذيها مصالح الصراع السياسي، كما إن العراق كان ساحة للحرب التشاركية التي نتجت عن انتشار وسائل الإعلام الرقمية، مما يؤكد تأثره بهذه التحولات[12]، يزعم أن أداة الذكاء الاصطناعي (Eleven Labs) استخدمت لإنشاء هذه المقاطع، التي تم تفنيدها من مجموعة التحقق من الحقائق (التقنية من أجل السلام)[13].

المحور الثاني: انعكاسات النزاع الرقمي على العراق

يقع العراق في قلب منطقة تشهد سباق تسلح رقمي متصاعد، لا يشمل فقط الهجمات المباشرة ، بل تتضمن أيضا التجسس وحملات التأثير التي يمكن أن تمتد لتشمل دول الجوار ، بما فيها العراق، وتكمن خصوصيته في أن تعرضه للهجمات لا يأتي فقط من ضعف البنية، بل من موقعه بوصفه حلقة وصل في صراع إقليمي متوتر؛ ما يجعله هدفا للتجسس وجمع البيانات، وميدانا لحروب الوكالة الرقمية التي تسعى لتصفير كلفة التصعيد على الفاعل الخارجي[14].

فطبيعة الفضاء السيبراني، الذي لا يعترف بالحدود الجغرافية، تجعل من السهل شن الهجمات من أي مكان، مع صعوبة بالغة في تحديد المسؤولين عنها بدقة، مما يجعل العراق عرضة للاستغلال بوصفه ساحة للحرب بالوكالة في المجال الرقمي، علاوة على ذلك، فإن السياسات الرقمية التي تتبناها القوى الكبرى مثل: الولايات المتحدة والإتحاد الأوروبي والصين، والتي تتضمن قيودا على سلاسل توريد التكنولوجيا وتدابير حماية شبكات الجيل الخامس، مما يؤثر بشكل غير مباشر في الخيارات المتاحة أمام العراق لتطوير بنيته التحتية الرقمية، وتؤثر في سيادته الرقمية، وهنا تظهر معضلة سياسية عراقية واضحة، فاختيارات التكنولوجيا ليست قرارا فنيا

محايدا، بل يمثل قرارا سياديا يحدد تبعية سلاسل التوريد ومدى إنكشاف الشبكات، وقدرة الدولة على فرض التحكم بالبيانات داخل حدودها[15].

مع تحول الفضاء السيبراني إلى ساحة خامسة للعمليات العسكرية والسياسية، أصبح العراق، بموقعه الاستراتيجي، عرضة لأن يكون ميدانا لتنافس القوى الإقليمية والدولية، عبر سباق التسلح السيبراني والانتقام الرقمي، مما أدى إلى تصعيد الاحتكاكات الجيوسياسية، وهذا يعني أن العراق قد يجد نفسه هدفا أو ممرا لهجمات سيبرانية تسعى من خلالها القوى المتنافسة إلى تحقيق نفوذ سياسي أو اقتصادي[16] ، خصوصا أن العراق يعاني من موقع سيبراني هش نسبيا فدول الخليج مثلاً: استثمرت مبالغ طائلة في تعزيز أمنها السيبراني وباتت ضمن أفضل (20) دولة عالميا في بعض المؤشرات، كما طورت إيران قدرات سيبرانية هجومية ودفاعية متقدمة بوصفها جزءا من استراتيجيتها[17].

إذ تعد البنية التحتية الحيوية في أي دولة، بما في ذلك شبكات الطاقة والمياه، والأنظمة المصرفية، وخدمات الاتصالات، والإدارة العامة، التي تمثل (الجبهة الجديدة) في الحروب الرقمية في العراق، التي بالإمكان أن تكون ذات نتائج مدمرة لأنها تؤدي إلى[18]:

1. تعطيل الخدمات الأساسية وشل الاقتصاد؛ مما يؤثر في حياة المواطنين اليومية واستقرار الدولة[19].
2. تهديد البيانات الوطنية السيادية، حيث يواجه مركز البيانات الوطني العراقي (INDC) صعوبات في تلبية متطلبات تخزين البيانات وأمنها، مما يجعل البيانات الحكومية والمواطنين عرضة للاختراق والسرقة من الجهات الخارجية[20].
3. التأثير في الأمن القومي إذ لا تقتصر آثار الهجمات على الأضرار المادية، بل تمتد لتشمل الأمن القومي من خلال التجسس وسرقة البيانات الحساسة عن طريق التهديدات المتقدمة المستمرة مثل: ونشر التضليل الإعلامي؛ لزعزعة الاستقرار الاجتماعي والسياسي، وتقويض ثقة المواطنين في مؤسسات الدولة[21].

فمن جهة يمكن أن تستغل جماعات إرهابية دولية أو محلية الثغرات لضرب أهداف عراقية أو استخدام الأراضي العراقية لبث رسائلها، ومن جهة أخرى قد تجد دول الجوار في العراق هدفا لاختبار أسلحتها الرقمية، وقد حذّر خبراء من أن العراق إذا لم يعزز دفاعاته السيبرانية سريعا

فسيصبح ساحة تجارب للهجمات دون قدرة حقيقية على الردع، ومما يثبت واقعية هذا التحذير تعرض مؤسسات حكومية عراقية لهجمات سيبرانية متطورة خلال السنوات الأخيرة، مثلاً: تعرض العراق في عام (2024) إلى حملة اختراق وتجسس رقمي استهدفت شبكات حكومية عراقية باستخدام برمجيات خبيثة مخصصة عالية التعقيد سميت (Veaty و Spearal) ترجح وقوف جهات إقليمية متقدمة وراء الهجوم، مثل هذه الحوادث تظهر أن العراق فعليا في مرمى نيران الحروب الرقمية الدائرة حوله، سواء أكان ذلك نتيجة تنافس القوى الكبرى أم نشاط جماعات عابرة للحدود[22].

إذ أظهرت النزاعات الحديثة، مثل الصراع الروسي – الأوكراني، أن شركات التكنولوجيا العالمية بدأت تتخذ أدوارا كانت حكرا على الدول، متحولة إلى دول رقمية وقوى عظمى يمكنها التأثير على المشهد الجيوسياسي الرقمي من خلال فرض (حصار رقمي) على دول معينة أو دعم أخرى، وهذا الواقع يجعل الدول التي تعتمد على التكنولوجيا الأجنبية، مثل العراق، عرضة لهذه الديناميكيات، مما يهدد سيادته الرقمية، ويفرض عليها ضرورة تطوير استقلاله الرقمي لمواجهة الضغوط الخارجية[23]، فالقوى الدولية والإقليمية المتصارعة تسعى أحيانا لاستخدام الأراضي العراقية أو فضائه الإلكتروني لتحقيق مكاسب في صراعها الأوسع، على سبيل المثال: خلال التصعيد الإقليمي في أعقاب حرب غزة أواخر عام (2023) [24]، وهذا يعني أن البنية التحتية الرقمية العراقية قد تستغل بوصفها نقطة انطلاق لهجمات بين خصوم إقليميين، مما يجر العراق إلى معركة إلكترونية بالوكالة[25]، وبالمثل، تسعى دول كبرى لتعزيز نفوذها في الفضاء الإلكتروني العراقي، سواء عبر تقديم الدعم التقني والتدريب؛ لكسب الجانب العراقي إلى صفها، أو عبر أنشطة استخبارية رقمية؛ لمراقبة الساحة العراقية، والاستفادة منها في صراعاتها مع خصومها[26]، وهكذا أصبح العراق جزءا من رقعة الشطرنج السيبرانية التي تتحرك عليها القوى المختلفة في المنطقة[27].

المحور الثالث: الرؤية العراقية في سياق النزاع الرقمي المُركب

في ظل المشهد الرقمي المعقد والمتغير، يتطلب الأمر من العراق تبني استراتيجية متعددة الأوجه لا تقتصر على الدفاع فحسب، بل تهدف لتحويل التهديدات إلى فرص للنمو والتحديث، عبر بناء قدرات وطنية قوية، ووضع سياسات شاملة، وتطوير شراكات استراتيجية على المستويين الإقليمي والدولي لأن ملف الأمن السيبراني في العراق لم يعد ملفا قطاعيا، بل أداة لحماية القرار

السياسي، ومنع اختراق المؤسسات، وضبط المجال المعلوماتي الذي تدار عبره المنافسة على السلطة وتوجيه الرأي العام[28].

سياسيا يبذل العراق جهودا حثيثة لبناء قدراته الوطنية في مجال الأمن السيبراني والذكاء الإصطناعي، لمواكبة تصاعد التهديدات الرقمية[29]، حيث شهدت السنوات الأخيرة خطوات مؤسسية وتعليمية مهمة في هذا الصدد، فعلى المستوى المؤسسي، تم تأسيس أول مركز للأمن السيبراني ضمن وزارة الداخلية بداية العام (2025)؛ لدمج الدفاع السيبراني ضمن المنظومة الأمنية الوطنية، ويتولى هذا المركز سبع مهام رئيسة تشمل: مكافحة الإبتزاز الإلكتروني، والتصدي للإرهاب الإلكتروني والمنصات المتطرفة، ومعالجة حملات التشهير الرقمية، وحماية المواقع والمنصات الحكومية، وكشف الهجمات السيبرانية، فضلاً عن تنمية الملاكات الوطنية القادرة على توسيع التجربة، وإنشاء مراكز إضافية في المحافظات، وهذه المهام تعكس الفهم الرسمي بأن الفضاء الرقمي أصبح جبهة موازية للصراع ينبغي تأمينها أسوة بالجبهات التقليدية[30]، حيث يسعى العراق إلى صياغة دبلوماسية رقمية تحفظ مصالحه السيبرانية، فعلى سبيل المثال: تتبنى الحكومة خطابا يحذّر من إساءة استخدام الفضاء الإلكتروني لنشر المعلومات المضللة أو تهديد السلم المجتمعي، عبر مبادرات تعاون رقمي إقليمية ودولية بوصفها جزءا من دبلوماسيتها الحديثة، إيمانا منها بأن الأمن السيبراني لا يتحقق داخل الحدود فقط، بل عبر التعاون العابر للحدود[31].

هذا التوجه نحو الدبلوماسية الرقمية يظهر أيضا في انفتاح العراق على المنظمات الدولية المتخصصة في الاقتصاد الرقمي والتحول التكنولوجي، حيث ناقشت الحكومة مؤخرا مع (منظمة التعاون الرقمي) في مقرها الرياض، سبل دعم خطة التحول الرقمي الوطنية، واستعداد العراق للاستفادة من المبادرات الدولية في مجالات مثل: الذكاء الاصطناعي، وبناء القدرات الشبابية[32]، مما يدل على أن العراق بين عامي (2024-2025) بدأ صياغة سياسة وطنية رقمية أكثر وضوحا، تجمع بين تعزيز البنية التحتية والقانونية داخليا، وبين الانخراط المسؤول في المجتمع الرقمي الدولي خارجيا[33].

من جهة أخرى، قامت هيئة الإعلام والاتصالات في (2024) بتنظيم دورات وورش توعية بالأمن السيبراني والاستخدام الأمثل للتكنولوجيا بهدف بناء مجتمع رقمي واعٍ وقادر على مواجهة التحديات السيبرانية، وفي الإطار ذاته، شرعت الهيئة بعقد اتفاقيات استراتيجية مع شركات تقنية

عالمية لتدريب موظفي الدولة ومنحهم شهادات احترافية معتمدة، كما في شراكتها مع شركة (Fortinet) الأميركية[34]، التي تندرج ضمن استراتيجيتها لبناء شراكات تعزز نقل المعرفة، وتطوير القدرات المحلية في الأمن السيبراني، ومن الجدير بالذكر أيضا أن الجامعات العراقية بدأت باستحداث كليات وأقسام أكاديمية متخصصة بهندسة الأمن السيبراني والذكاء الاصطناعي، لرفد سوق العمل بفرق عمل وطنية مؤهلة تقنيا، وهذه الجهود مجتمعة تشير إلى تحول نوعي في بناء رأس المال البَشري السيبراني في العراق (وإن كان التقدم بطيئًا)، واستثمار التهديدات الرقمية بوصفها فرصة لتأهيل جيل جديد من المختصين[35].

إقليميا، يسعى العراق إلى تحالفات رقمية مع دول الجوار لمواجهة التحديات المشتركة، مثال بارز على ذلك هو مذكرة التفاهم العراقية–السورية الموقعة في أوائل العام (2024) لتعزيز التعاون في الاتصالات والأمن السيبراني[36]، وتهدف هذه المذكرة إلى مد كابل ضوئي دولي عبر حدود البلدين لتحسين البنية التحتية للإنترنت وخدمات الاتصال، والأهم أنها تنص على تنسيق مشترك للسيطرة على المحتوى الرقمي، وصد الهجمات السيبرانية العابرة للحدود، كما تم الاتفاق على تشكيل لجان فنية مشتركة لوضع برامج تنفيذية، وتحقيق التعاون العملي في هذا المجال، وهذه الخطوة تعكس تحول التعاون الإقليمي التقليدي ليشمل الأمن الرقمي، بحيث تستثمر التهديدات الإلكترونية بوصفها فرصة لتكاتف الدول في حماية فضائها السيبراني المشترك، وبجانب سوريا، تمكن الإشارة إلى جهود عراقية لتعزيز التعاون السيبراني مع دول عربية أخرى تمتلك خبرات متقدمة[37]، فقد أشار خبراء إلى أن الدول العربية ذات القدرات السيبرانية العالية يمكن أن تكون شركاء طبيعيين للعراق في بناء دفاعاته الرقمية على سبيل المثال، الانفتاح على دول الخليج منها السعودية (تم ذكرها سابقًا) التي تصنّف ضمن أعلى (20) دولة عالميا في جاهزية الأمن السيبراني، وهذا ما يتيح للعراق الاستفادة من خبراتها ونقل التكنولوجيا وبناء برامج تدريب إقليمية مشتركة[38].

أما على الصعيد الدولي، تربط العراق شراكة متنامية مع حلف شمال الأطلسي (الناتو) في مجال الأمن السيبراني ضمن إطار تحديث قدرات القوات المسلحة، وقد جدد الناتو في العام (2025) التزامه طويل الأمد بدعم العراق في بناء جيش قوي خاصة في مجالي الأمن السيبراني وإدارة الأزمات[39]، من جانب آخر، برزت شراكات مع القطاع الخاص العالمي بوصفها وسيلة

لتحويل التهديدات إلى فرص تطوير، فقد وقّع فريق الاستجابة الوطني العراقي (IQ-CERT) في منتصف العام (2025) مذكرة تفاهم استراتيجية مع شركة (Resecurity) الأمريكية المتخصصة في استخبارات التهديدات السيبرانية، تهدف هذه الشراكة إلى تعزيز الدفاعات السيبرانية الوطنية، عبر تسريع تبني تقنيات استخبارات تهديد متقدمة تعتمد على الذكاء الاصطناعي، معدة للبيئة الرقمية العراقية، وأكد الجانب العراقي أن هذا التعاون يتوافق مع استراتيجية العراق لتحديث دفاعاته السيبرانية، واعتماد حلول عالمية المستوى، حيث سيسهم في رفع جاهزية الأمن السيبراني، وحماية المستقبل الرقمي للبلاد[40].

الخاتمة

إن رقمنة النزاع لم تعد مجرد تطور تقني عابر، بل أصبحت تحولاً بنيويا يعيد تشكيل طبيعة الصراعات الإقليمية وأدواتها وفاعليها، فقد انتقل النزاع من ساحات القتال التقليدية إلى فضاءات رقمية تتقاطع فيها الهجمات السيبرانية، والتضليل الإعلامي، وتطبيقات الذكاء الإصطناعي، بما جعل الفضاء السيبراني ساحة عمليات مركزية تؤثر مباشرة في الأمن القومي والسيادة الوطنية، وأظهر البحث أن هذا التحول أسهم في تآكل الحدود بين الحرب والسلم، وبين الفعل العسكري والفعل المعلوماتي، وأعاد تعريف مفاهيم الردع والسيطرة والتأثير.

في هذا السياق، تبرز الحالة العراقية بوصفها أنموذجا لدولة تواجه تهديدات رقمية مركبة في بيئة إقليمية شديدة التنافس، وسط هشاشة بنيوية في البنى التحتية الرقمية، وضعف تشريعي ومؤسسي، واعتماد واسع على التكنولوجيا الأجنبية، ومع أن العراق بدأ مؤخرا باتخاذ خطوات مؤسسية ودبلوماسية لتعزيز أمنه السيبراني، إلا أن حجم التهديدات وتسارعها يفوق مستوى الجاهزية الحالية، وهنا تكشف الحالة العراقية أن الخطر الرقمي لا يظهر فقط بوصفه تعطيلاً تقنيا، بل بوصفه آلية لإضعاف الدولة من الداخل عبر التشكيك بالمؤسسات، وتفكيك الإجماع العام، مما يعني أن تعزيز السيادة السيبرانية يجب أن يعامل بوصفه أولوية سيادية تمس وحدة الدولة واستقرارها.

وعليه، فإن التعامل مع رقمنة النزاع يتطلب انتقالاً من الاستجابات الجزئية إلى رؤية استراتيجية شاملة تدمج الأمن السيبراني ضمن منظومة الأمن الوطني، وتحول التهديد الرقمي إلى أداة لتعزيز السيادة الرقمية وبناء الدولة الحديثة.

الاستنتاجات

1. أثبت البحث أن رقمنة النزاع أصبحت سمة مركزية للصراعات الإقليمية المعاصرة، ولم تعد مكملة للحرب التقليدية بل تمثل بديلاً جزئيا عنها في كثير من الحالات.
2. يشكّل الفضاء السيبراني اليوم ساحة عمليات رسمية تستخدم لتحقيق أهداف سياسية وأمنية من دون اللجوء إلى الصدام العسكري المباشر.
3. يعاني العراق من هشاشة رقمية واضحة ناتجة عن ضعف البنية التحتية التقنية، وتشتت الإطار التشريعي، ومحدودية خطط الطوارئ السيبرانية.
4. تؤثر النزاعات الرقمية على العراق بشكل مباشر عبر استهداف البنى التحتية الحيوية، وتهديد البيانات السيادية، وزعزعة الثقة بالمؤسسات الحكومية.
5. أظهرت التطورات الإقليمية والدولية أن الشركات التكنولوجية والقوى غير الحكومية باتت فواعل مؤثرة في النزاع الرقمي، ما يقيد سيادة الدول الضعيفة رقميا.
6. تمثل الخطوات العراقية الأخيرة في مجال الأمن السيبراني والذكاء الاصطناعي بداية مهمة، لكنها ما تزال غير كافية لمواجهة نزاع رقمي مركب ومتسارع.

التوصيات

1. إعداد استراتيجية وطنية شاملة للأمن السيبراني تدمج ضمن منظومة الأمن القومي، وتحدد بوضوح أدوار المؤسسات المدنية والعسكرية.
2. تطوير إطار تشريعي متكامل لحماية البيانات السيادية وتنظيم الفضاء الرقمي وتجريم الاعتداءات السيبرانية وفق معايير دولية واضحة.
3. إدماج الأمن السيبراني ضمن هيكل الأمن الوطني، من خلال توزيع الوظائف السيبرانية على الأجهزة الأمنية والعسكرية القائمة، وربطها بمركز تنسيق وطني موحد، بما يحقق وحدة القرار ويمنع تشتت الصلاحيات.
4. تعزيز الاستثمار في البنية التحتية الرقمية الوطنية وتقليل الاعتماد على التكنولوجيا الأجنبية الحساسة.
5. دعم الجامعات ومراكز البحث لإنشاء برامج متخصصة في الأمن السيبراني والذكاء الاصطناعي وبناء رأس مال بشري وطني مؤهل.

6. تفعيل الدبلوماسية الرقمية العراقية وتوسيع الشراكات الإقليمية والدولية لتبادل الخبرات وبناء منظومات دفاع سيبراني مشتركة.
7. اعتماد مقاربة استباقية في إدارة النزاع الرقمي تقوم على الرصد المبكر والردع السيبراني، بدل الاكتفاء بردود الفعل بعد وقوع الهجمات.

المصادر

(1) عبد الغني، أمين سعيد. "الحرب الرقمية." مجلة بحوث الإعلام الرقمي 3، العدد 3 (كانون الثاني 2024): 3. https://doi.org/10.21608/jsmd.2024.357424.

(2) Mareš, Miroslav, and Veronika Netolická. "Georgia 2008: Conflict Dynamics in the Cyber Domain." *Strategic Analysis* 44, no. 3 (2020): 43. https://doi.org/10.1080/09700161.2020.1778278 .

(3) الشيخلي، تحسين. "دور الحرب السيبرانية في تشكيل ملامح الصراع في الشرق الأوسط." وكالة الحدث الإخبارية. نُشر في 27 تشرين الأول 2024. تم الوصول إليه في تشرين الأول 2025. https://www.alhadathcenter.net/index.php/views/132356-2024-10-27-11-33-27.

(4) "The Asia Foundation. Violent Conflict, Tech Companies, and Social Media in Southeast Asia: Key Dynamics and Responses." San Francisco: *The Asia Foundation*, October 28, 2020. Accessed September 2025. https://asiafoundation.org/wp-content/uploads/2024/08/Violent-Conflict-Tech-Companies-and-Social-Media-in-Southeast-Asia.pdf

(5) Mareš and Netolická, "Georgia 2008".

(6) شفق نيوز. "الحرب الصامتة: العراق والمنطقة تحت تهديد الهجمات السيبرانية." نُشر في 21 أيلول 2025. تم الوصول إليه في 18 تشرين الأول 2025. www.shafaq.com.

(7) Cherry, Sarah. "Modern Armed Conflicts: Disinformation Campaigns Shaping the Digital Information Landscape." *The Serials Librarian* 85, no. 1–4 (2024): 25. https://doi.org/10.1080/0361526x.2024.2348140.

(8) Khorrami, Nima. "Digital Frontlines: What the 12-Day War Revealed about the Evolution of Iran's Cyber Strategy." *Middle East Institute*. August 4, 2025. Accessed September 2025. https://mei.edu/publication/digital-frontlines-what-12-day-war-revealed-about-evolution-irans-cyber-strategy ./

(9) Arab Center Washington DC. "The Threats of AI and Disinformation in Times of Global Crises." May 29, 2024. Accessed September 2025. https://arabcenterdc.org/event/the-threats-of-ai-and-disinformation-in-times-of-global-crises ./

(10) Ibid.

(11) Haddad, Hussein Ismail. "Digital and Political Transformation: A Perspective on the Discourse of Iraqi Media System." *European Journal of Communication and Media Studies* 3, no. 2 (2024): 4. https://doi.org/10.24018/ejmedia.2024.3.2.33.

(12) Ibid.

(13) Amwaj Media. "'Weaponized' AI-Generated Audio Riles Iraq Ahead of Elections." *Amwaj Media*. September 22, 2025. Accessed October 10, 2025.

https://www.amwaj.media/media-monitor/weaponized-ai-generated-audio-riles-iraq-ahead-of-elections .

(14) "Cyber Attacks and Its Implication to National Security: The Need for International Law Enforcement." *Pakistan Journal of Criminology* 16, no. 3 (May 2024): 862. https://doi.org/10.62271/pjc.16.3.851.864.

(15) Ibid.

(16) Peng, Shin-yi. "Digital Economy and National Security: Contextualizing Cybersecurity-Related Exceptions." *AJIL Unbound* 117 (2023): 123. https://doi.org/10.1017/aju.2023.18.

(17) Shafaq News. "Iraq: A Soft Target in the Middle East's Cyber Battlefield." *Shafaq News*. September 15, 2025. Accessed September 2025. https://www.shafaq.com/en/Report/Iraq-A-soft-target-in-the-Middle-East-s-cyber-battlefield.

(18) Al Barazanchi, Israa Ibraheem, and Dima Haider Rasheed. "The Role of the Iraqi National Data Center in Advancing Digital Transformation and Data Sovereignty." *SHIFRA 2024* (June 2024): 90. https://doi.org/10.70470/SHIFRA/2024/010.

(19) Ibid, 90.

(20) Ibid, 91.

(21) Ibid, 91.

(22) Fernández Provecho, Ernesto, Pham Duy Phuc, and John Fokker. "The Iranian Cyber Capability." *Trellix*. September 19, 2024. Accessed September 2025. https://www.trellix.com/blogs/research/the-iranian-cyber-capability/

(23) Aviv, Itzhak, and Uri Ferri. "Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem." *International Journal of Critical Infrastructure Protection* 43 (December 2023): 100637. https://doi.org/10.1016/j.ijcip.2023.100637.

(24) Mako, Gerald. "Firewalls and Fault Lines: Cyber War in the Middle East." *Lieber Institute, U.S. Military Academy, West Point*. August 6, 2025. Accessed September 2025. https://lieber.westpoint.edu/firewalls-fault-lines-cyber-war-middle-east/.

(25) Ibid.

(26) Ibid.

(27) Ibid.

(28) Radanliev, Petar. "Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing." *Journal of Cyber Security Technology* 9, no. 1 (2024): 43. https://doi.org/10.1080/23742917.2024.2312671.

(29) وكالة بغداد اليوم. "إنشاء أول مركز للأمن السيبراني في العراق: 7 مهام رئيسية لمواجهة التحديات الحديثة." بغداد اليوم، 23 كانون الثاني 2025. تم الوصول إليه في أيلول 2025. https://baghdadtoday.news/266479.

(30) المصدر نفسه.

(31) Shafaq News, "Iraq: A Soft Target in the Middle East's Cyber Battlefield".

(32) DCO (Digital Cooperation Organization). "Iraq's Prime Minister Meets with Secretary-General of the Digital Cooperation Organization to Discuss Opportunities for Mutual Cooperation." *Digital Cooperation Organization (DCO)*. November 25, 2024. Accessed September 2025. https://dco.org/media/iraqs-prime-minister-meets-with-secretary-general-of-the-digital-cooperation-organization-to-discuss-opportunities-for-mutual-cooperation./

(33) Ibid.

(34) Channel 8. "Iraq Boosts Cybersecurity and Digital Culture with New International Partnerships." Channel 8. July 25, 2024. Accessed September 2025. https://channel8.com/english/news/17533.

(35) Ibid.

(36) بغداد اليوم، "إنشاء أول مركز للأمن السيبراني في العراق،" 23 كانون الثاني 2025.

(37) المصدر نفسه.

(38) المصدر نفسه.

(39) Rudaw. "NATO, Iraq Set Long-Term Goals to Build Stronger Army." *Rudaw*. September 19, 2025. Accessed September 2025. https://www.rudaw.net/english/middleeast/iraq/190920254 .

(40) Resecurity. "Resecurity Partners with Iraq Cyber Events Response Team (IQ-CERT) to Advance National Cybersecurity and Threat Intelligence." *Business Wire*. July 23, 2025. Accessed September 2025. https://www.businesswire.com/news/home/20250723444318/en/Resecurity-Partners-with-Iraq-Cyber-Events-Response-Team-IQ-CERT-to-Advance-National-Cybersecurity-and-Threat-Intelligence.