مجلة الكوفة للعلوم القانونية والسياسية

ISSN

٢٠٧٠٩٨٣٨ (مطبوع) ٣٠٠٦٧٦٧٧ (إلكتروني)

العدد الثالث/ المجلد السابع عشر

تاريخ النشر

٢٠ / ٩ / ٢٠٢٥

مراجعة ونقد دراسة الجيوسيبرانية العالمية والتحولات في أبعاد وخصائص القوة: آليات التوظيف في الاستراتيجية الروسية والصينية د. إيهاب عياد

Review and critique of the study of global geocybernetics and transformations in the dimensions and characteristics of power: Mechanisms of employment in Russian and Chinese strategy

م.د فاطمة حسن جاسم

Fatima.hassan@nahrainuniv.edu.iq

Abstract

The study begins with an introduction explaining how cyberspace redistributes power balances and injects new forms of influence, disruption, and deterrence. It is based on the general premise that "cyber power" is a double-edged sword that can either enhance a nation's interests or exacerbate its vulnerabilities. The study then outlines three main objectives: to analyze the relationship between geocyber, power shifts, and their mechanisms of deployment; to trace the rise of Russian capabilities; and to examine the rise of Chinese capabilities and their deployment mechanisms. The study presents a comprehensive methodological framework that blends national interest approaches, case studies, and descriptive methodologies to address the phenomenon from multiple perspectives. It then moves to an applied section that includes tables of the most prominent threats and attacks attributed to Russia and China over extended periods, concluding with a summary that highlights the differing approaches to soft and hard power employed by each side and calls for institutional and legal safeguards in cybersecurity.

الملخص

تعرض الدراسةُ تمهيداً يشرح كيف يعيد الفضاء السيبراني توزيع أوزان القوة ويضخّ أشكالاً جديدة من النفوذ والتعطيل والردع، وتستند إلى أطروحة عامة مؤداها أن "القوة السيبرانية" سلاحٌ ذو حدّين يعظّم مصالح الدول أو يفاقم هشاشتها. ثم تصوغ الدراسة ثلاثة أهداف رئيسة: تحليل العلاقة بين الجيوسيبرانية وتحولات القوة وآليات التوظيف؛ وتتبّع صعود القدرات الروسية؛ وفحص صعود القدرات الصينية وآلية توظيفها. وتُفصح الدراسة عن "إطارٍ منهجي متكامل" يمزج منهج المصلحة الوطنية ودراسة الحالة والمنهج الوصفي، بغية الإحاطة بالظاهرة من زوايا متعددة. وتنتقل لاحقاً إلى جزءٍ تطبيقي يتضمن جداول لأبرز التهديدات والهجمات المنسوبة إلى روسيا والصين عبر فترات زمنية ممتدة، مع خلاصةٍ تُقرِّر اختلاف المزج بين القوة الناعمة والصلبة لدى الطرفين، وتدعو إلى تحصيناتٍ مؤسسية وقانونية في الأمن السيبراني.

المقدمة

تتناول هذه القراءةُ النقديّة دراسةً منشورةً في مجلة البحوث المالية والتجارية بعنوان: "الجيوسيبرانية العالمية والتحولات في أبعاد وخصائص القوة: آليات التوظيف في الاستراتيجية الروسية والصينية". تُحدِّد الدراسةُ موضوعها في رصد أثر الفضاء السيبراني على تصوّر القوة وتوظيفها، مع تطبيق مقارن على حالتي روسيا والصين. وتستندُ الدراسة إلى بناءٍ نظريّ يبرز تحوّلات القوة في ظل الثورة الرقمية، وإلى سردٍ وصفيّ لحوادث ووقائع سيبرانية ترسم – من وجهة نظر الباحث – صورةً عن آليات التوظيف الروسي والصيني. وتغدو أهميةُ هذه المراجعة في أنها تُعيد تفكيك البناء المفاهيمي والمنهجي للدراسة، وتُقيِّم صلاحية الشواهد المستخدمة ومتانة الاستدلال، ثم تُقترح بدائل عملية لرفع القيمة العلمية والقدرة التفسيرية للنص.

التحليل والنقد: تتقدّم هذه القراءة النقدية عبر أربعة مستويات: صياغة المشكلة والأهداف، التأصيل النظري، التصميم المنهجي ونوعية الأدلة، ثم صلاحية المقارنة ووجاهة الخلاصات.

أولاً: صياغة المشكلة والأهداف: تُحسن الدراسةُ التقاط سؤالٍ مركزي حول صلة الفضاء السيبراني بمنطق القوة، وتُبلور أهدافاً واضحة ثلاثية المحاور. غير أنّ الصياغة، على وضوحها، لا تُحوَّل إلى فرضياتٍ قابلة للاختبار، ولا تُصرِّح بوحدة التحليل ومستوى التحليل والإطار الزمني الملزِم، ما يُبقي البناء البحثي في حيز "الوصف الناظم" أكثر من كونه "تصميماً اختبارياً". ويُضيف غيابُ مؤشراتٍ تشغيلية لتعريف "تحول القوة" و"آلية التوظيف" مشكلةَ قياسٍ تُضعف إمكانية التعميم أو المقارنة الممنهجة عبر الزمن أو القطاعات. كان يمكن للدراسة – كي تُغلق هذه الفجوة – أن تُعرّف مخرجات القوة في الحقل السيبراني (ردع قابل للقياس، كلفة اقتصادية مُقدَّرة، تنازل سياسي في مفاوضة محددة) وتربطها بمؤشرات قابلة للرصد. تتعهدُ مقدمةُ الدراسة ببيان أهمية التحولات الرقمية في إعادة تعريف القوة، وهذا تعهّد وجيه، لكنه يحتاج ترجمةً إجرائية داخل جدول مؤشرات مرتبط بالأهداف.

ثانياً: التأصيل النظري: تُقدِّم الدراسة إطاراً عاماً يُبرز انتقال الصراع إلى الفضاء الإلكتروني ويُشدد على أن أدواته قد تُنتج خسائر اقتصادية وتعطيل بنى تحتية، وتُومئ إلى الردع السيبراني. وتُعد هذه المدخلات ضرورية لإنشاء خطٍّ نظري يربط "الفضاء" بـ"القوة". غير أن التأصيل يتوقف عند المستوى التعريفي/الوصفي، ولا يُدخل مدارس نظرية مفسِّرة (الواقعية الهجومية، القوة المعيارية، نماذج الردع بالمنع والعقاب، حوكمة الإنترنت متعددة الأطراف) بما يسمح بتعدد عدسات القراءة، ولا يُنشئ نموذجَ "آليات" يوضح كيف يُنتج فعلٌ سيبرانيّ معين أثراً سياسياً/اقتصادياً محدّداً عبر حلقات سببية. تُفيد نصوص المقدمة في استحضار الثيمة الكبرى عن حدَّي القوة السيبرانية، لكنّ الاكتفاء بذلك يُبقي المساحة النظرية أقلّ رسماً للآليات وأكثر استدعاءً للصور العامة. إدراجُ خريطة علاقات تربط "طبقات الفضاء" (المادي/المنطقي/الاجتماعي) بوظائف القوة (استطلاع/تعطيل/تأثير/ردع/شرعنة) كان سيمنح النص قدرةً تفسيرية أوسع. يعالج كوهل الانتقال من "الفضاء السيبراني" إلى "قوّة سيبرانية" بوضع تعريف تشغيلي يربط الموارد والشبكات والمهارات البشرية بمخرجات سياسية قابلة للرصد؛ ما يبرّر مطالبتك بإعلان "وحدة التحليل" و"مستوى التحليل" ومقياسًا زمنيًا ملزِمًا داخل الدراسة، حتى لا يبقى الوصف معلّقًا دون اختبار. (Kuehl, 2009). علاوة على ذلك، تؤكّد أدبيات القوّة السيبرانية أنّ الموارد الرقمية تُنتِج في الوقت ذاته قوّة ناعمة (جذبٌ وإقناع عبر الدبلوماسية العامة والمنصّات) وقوّة صلبة (إيذاء مادّي للبنى التحتيّة والتحكّم في أنظمة SCADA)، وهو ما يدعم تحويل أطروحة "السلاح ذو الحدّين" إلى مؤشرات أثر قابلة للقياس. يوضّح ناي أنّ اختيار المزج بين الناعم والصلب يعتمد على سياق التوظيف وأهدافه. (Nye, 2010). انظر أيضًا الجدول (١) في الدراسة (ص. ١٢٦).

ثالثاً: التصميم المنهجي ونوعية الأدلة: تُعلن الدراسةُ صراحةً استخدام "الإطار المنهجي المتكامل" الذي يجمع مناهج متعددة، وتُسند تحليلها إلى جداول حوادث وتهديدات عبر فترات زمنية. ويُحسبُ لها أنها تُصرّح بالأدوات المنهجية وتُحاول بناء صورة تركيبية لروسيا والصين. لكنّ هذا الدمج، في صيغته الحالية، يظلّ غير محكوم ببروتوكول ترميز واضح: لا تُذكر معايير إدراج/استبعاد للحوادث، ولا تُصنَّف العمليات

بحسب الشدة/القطاع/الأثر، ولا تُبيَّن درجات الثقة في الإسناد (Attribution). كما لا يُقدَّم مصدرٌ تقنيّ محكّم لكل حادثة (تقارير مراكز استجابة وطنية، ENISA، CISA، CCDCOE، قواعد CVE/ICS)، بل تُدرَج أحياناً روابط صحفية عامة، الأمر الذي يُضعف القوّة الاستدلالية ويعرّض النتائج لتحيزات المصدر. وإذ تُسجّل الجداول تنوعاً زمنياً وقطاعياً، فإنها تبقى "قوائم أحداث" أكثر من كونها "لوحة بيانات" قابلة للاختبار، فلا تُستثمَر في ربط التواتر الزمني بمحطات سياسية، ولا تُسندها تقديرات تكلفة/تعطل أو مقاييس زمنية (MTTR، MTTD) التي تسمح بقياس أثرٍ حقيقي على القوة. ينبّه ليبيكي إلى أنّ فاعليّة الردع السيبراني ترتبط بشروط قابلة للقياس: إمكان الإسناد (Attribution)، والكلفة المتوقّعة، واحتمال تكرار الهجوم. لذا فإن اقتراحك "لوحَة ترميز/بيانات" تتضمّن نوع العملية، القطاع المستهدَف، زمن التعطّل، والكلفة التقديرية ينسجم مع منطق الردع والتحليل السببي في دراسات القوّة السيبرانية. (Libicki, 2009).

رابعاً: مقارنة روسيا والصين : تُظهر الدراسةُ –بصورة موفقة– أن الصين لا "تحذو حذو" روسيا في نمط التوظيف؛ إذ تمزج بين أدوات القوة الناعمة ضمن مبادرة "الحزام والطريق" وبين القوة الصلبة عبر هجمات سيبرانية واستهداف للبنى التحتية، بينما تُستعاد الصورة الروسية في إطار أكثر هجومية وتوظيفاً للردع والاختراق. ويُثري هذا التفريقُ السردَ المقارن، لكنه يظل بحاجة إلى مصفوفة معايير قابلة للقياس: بنية القيادة والسياسات (عقيدة المعلومات الروسية/سيادة الفضاء الرقمي في الصين)، القدرات التقنية (APT، يوم-صِفري، سلاسل توريد)، القطاعات المستهدفة، مؤشرات الأثر، ومخاطر الارتداد (عقوبات/عزل/فكّ الاعتمادية). ويُحسِّن التحليلَ أن تُعاد صياغة الجداول في جدولٍ مقارن موحّد يضع الطرفين على محاور واحدة، مع أمثلة موثَّقة ومصادر ذات موثوقية عالية. كما تظهر الدراسة، يوثّق جيبني أنّ أوكرانيا شكّلت "ساحة تدريب" للعمليات الروسية، وأنّ هجمات ٢٠١٥–٢٠١٦ عطّلت شبكات الطاقة لساعات، ما يساند خلاصة الدراسة عن الدور المركزي للهجوم السيبراني الهجومي في العقيدة الروسية، ويدعم دعوتك لإرفاق قياسات أثر ملموسة بدلًا من السرد العام. (Gibney, 2022). أخيرا

توضح الدراسة نفسها أن عليّ زياد العلّي يبين أنّ "الحزام والطريق" يتضمّن بعدًا سيبرانيًا يُوسّع البنية الرقمية للدول الشريكة ويُكرّس السيادة الرقمية للصين؛ ما يفسّر مزجها أدوات القوّة الناعمة مع ممارسات صلبة انتقائية، ويبرّر اقتراحك لمصفوفة مقارنة تُظهر اختلافات البنية والسياسات بين الصين وروسيا. (العلّي، ٢٠١٩).

خامساً: الملخص والعرض : يُقدّم النص سرداً متدرجاً من المفاهيمي إلى التطبيقي، ويعرض جداول مفيدة بصرياً، غير أن الملخص – في النسخة الإنجليزية على وجه الخصوص – يحتاج إعادة تحرير لغوي وتخليصاً من التركيبات غير القياسية، كما يحتاج إلى تضمين موجزٍ صريح: المنهج، وحدة التحليل، الإطار الزمني، وأهم النتائج. ويُستحسن توحيد المصطلحات العربية (الجيوسيبرانية/الجيو-سيبرانية، الحرب السيبرانية/الإلكترونية) والإنجليزية على حد سواء. ويُستحسن كذلك تثبيت بيانات النشر والهوامش وفق نمط توثيقٍ موحّد. تُظهر صفحات المجلة والعنوان وبيانات الإصدار بوضوح، ما يُسهّل الضبط الببليوغرافي إن أُعيد تنسيق قائمة المراجع.

سادساً: المراجع والموثوقية : تُوظّف قائمة المراجع خليطاً من مصادر أكاديمية عربية ودراسات سياسات ومحتوى صحفي وروابط مواقع عامة، وتُورِد بعض الإحالات إلى مواقع إخبارية عند توثيق حوادث تقنية حسّاسة. ويُفضَّل – في موضوعات الإسناد السيبراني تحديداً – ترجيح التقارير التقنية المحكّمة ومصادر جهات CERT/ENISA/CCDCOE وشركات الأمن السيبراني ذات السمعة، وتقييد الاعتماد على الأخبار أو تدوينها بوصفها "مسانِدة" لا "حاكمة". كما يُستحسن ضبط صيغة الكتابة اللاتينية للأسماء والسنوات وتوحيد أسلوب التوثيق. إنّ تضمين روابط صحفية عامة (مثل مادة "روسيا اليوم العربية" المنقولة عن رويترز) في حقلٍ منهجي يتطلب دقة إسناد تقنية يُقلّص من صلابة الحجة.

سابعاً: صلاحية الاستدلال والخلاصة : تُقرر الخلاصة اختلاف آليات توظيف القوة بين روسيا والصين وتُبرِز اتساع أثر البيئة الرقمية. يظل هذا التقرير معقولاً على المستوى الوصفي، لكنه يحتاج دعماً سببيّاً يظهر "كيف" أدّى حدثٌ سيبراني بعينه إلى مكسب قوة قابل للقياس (سياسياً/اقتصادياً/عسكرياً). وتفيد

الدراسةُ كثيراً إن قادت القارئ عبر سلسلة آليات في دراسة حالة معمَّقة: من الاختراق/الهجوم → إلى درجة التعطيل والخسائر → إلى استجابة الخصم وتغيّر السلوك أو الكلفة التفاوضية. وبدون هذا "التتبّع السببي"، تبقى الحجّة أقرب إلى الانطباع التحليلي منها إلى الإثبات. يُظهر القسم الصيني، على سبيل المثال، استدعاءً صريحاً لمزج الناعم/الصلب، لكنه لا يُرفق قياساتٍ أو درجات ثقة لكل حدث تُعزّز قابلية التكرار.

التوصيات وفرص التحسين

١) تشغيليّة الأهداف وتحويلها إلى فرضيات

من الأنسب تحويل الأهداف الثلاثة المعلنة إلى فرضيات اختبارية محددة تقود مسار التحليل بدل أن تظل مؤشرات توجيهية عامة. يتحقق ذلك عبر تحديد: (أ) وحدة التحليل (حادثة سيبرانية مفردة، أو حملة ممتدة، أو قطاع مستهدف)، (ب) مستوى التحليل (استراتيجي يتصل بالعقائد والسياسات، أو عملياتي يتصل بآليات التنفيذ)، و(ج) الإطار الزمني الملزم الذي تُقاس ضمنه المتغيرات. ثم تُصاغ لكل هدف فرضية قابلة للرفض أو القبول وفق أدلة مرصودة. مثلًا: "يزداد تواتر التوظيف السيبراني الهجومي في سياقات الأزمات الجيوسياسية مقارنةً بفترات الاعتياد"؛ أو "تمزج الصين أدوات التأثير المعلوماتي مع إجراءات تقنية انتقائية على نحو يحقق مكاسب سياسية بتكلفة ارتداد أقل من النمط الروسي". كما ينبغي إعلان التعريف الإجرائي لمخرجات "القوة" في الفضاء السيبراني (زمن التعطيل، التكلفة المقدّرة، التغيير السلوكي للطرف المستهدف)، وربطها مباشرة بمقاييس الرصد والتحقق. هذا التحويل يتيح مقارنة زمنية وقطاعية صلبة، ويمنح الخلاصة قوة تفسيرية تتجاوز السرد الانطباعي.

٢) إنشاء مصفوفة ترميز و"لوحة بيانات" : تحويل الجداول الحالية إلى قاعدة بيانات معيارية سيضاعف فائدتها. تتضمن مصفوفة الترميز حقولًا ثابتة: معرف الحادثة، نوع العملية (استطلاع، اختراق، DDoS، استغلال ثغرة، تخريب أنظمة صناعية)، القطاع المستهدف (طاقة، اتصالات، مالية، حكومة، صحة، نقل...)،

جغرافيا الهدف، قناة الدخول (تصيّد، سلسلة توريد، ثغرة يوم-صِفري...)، شدّة الحادثة على مقياس من خمس درجات، زمن التعطل إن وُجد، مؤشرات الأثر الاقتصادي/الاجتماعي، إضافة إلى "درجة الثقة في الإسناد" مع وصف موجز لأساسها. تُستكمل القاعدة بـ"سجل مصدر" يحفظ تاريخ جمع المعلومة ونوع المصدر وطريقة التحقق. بعد ذلك تُبنى لوحة تحكم تفاعلية تُظهر اتجاهات زمنية، خرائط حرارية للقطاعات المستهدفة، ومصفوفات ارتباط بين نوع الهجوم والسياق السياسي. بهذه الصورة تنتقل الجداول من "قوائم أحداث" إلى "لوحة بيانات" تمكّن من الاختبار والاستدلال وتوليد أسئلة بحثية تالية.

٣) تدعيم الموثوقية المصدرية : يقترح اعتماد هرميّة واضحة للمصادر تضمن الحد الأدنى من الصلابة: مصادر مؤسسية متخصصة وتقارير تقنية تُقدَّم على الروابط الخبرية العامة؛ وعند الاضطرار لاستخدام محتوى إعلامي يُشار إليه كمساند لا كحاكم. كما يُنصح بتطبيق "التثليث" عبر مقارنة الحدث الواحد في أكثر من مصدر مستقل، وتسجيل أي تناقضات أو فجوات. وجود "سجل إسناد" داخل الملحق يبيّن تاريخ الاطلاع، وملخص المنهجية التي اتُّبعت في التحقق، وأي تحديثات لاحقة على توصيف الحادثة. هذا الانضباط لا يحسّن موثوقية النتائج فحسب، بل يزيد من قابليتها للتكرار ويقلل تحيزات التغطية أو إعادة تدوير نفس الخبر بأشكال مختلفة. كما يجدر وضع بروتوكول لمعالجة الحالات الغامضة: إذا كان الإسناد "منخفض الثقة" يُذكر ذلك صراحة ويُستبعد الحدث من التحليلات الحساسة، مع بقائه في قاعدة البيانات لأغراض الرصد.

٤) توسيع العدسات النظرية : لرفع القدرة التفسيرية، يُستحسن بناء إطار نظري مركّب يزاوج بين مدارس متعددة: منظور واقعي هجومي يفسّر دوافع التوسّع أو الردع بالقوة؛ منظورات الردع السيبراني (بالمنع وبالعقاب) لتقدير حسابات الكلفة/العائد؛ منظور القوة المعيارية لفهم أدوات الإقناع والشرعنة عبر المنصّات الرقمية؛ ومنظورات حوكمة الإنترنت لفكّ اشتباك الأدوار بين الدول، الشركات، والهيئات الدولية. يُترجم هذا الإطار في "سلسلة آليات" تُظهر كيف ينتقل الفعل السيبراني من القدرة التقنية إلى الأثر السياسي: قدرة/مورد → عملية/تكتيك → أثر مادّي/معلوماتي/معياري → نتيجة استراتيجية

قابلة للرصد. بهذه السلسلة يمكن تفسير الاختلاف بين النمط الروسي الأكثر هجومية واندفاعًا، والنمط الصيني الذي يمزج أدوات ناعمة مع تدخلات تقنية محسوبة في سياقات مبادرات اقتصادية وسيادية أوسع.

٥) بناء مقارنةٍ معيارية :بدل جداول منفصلة لكل طرف، يُفضَّل إنشاء جدول مقارن موحّد يضع روسيا والصين على مؤشرات واحدة مع تعريفات دقيقة لكل مؤشر: بنية القيادة والسياسات (عقيدة المعلومات، الأطر القانونية، مؤسسات الإشراف)، منظومات الفرق المتقدمة والهندسة التقنية، أدوات التأثير المعلوماتي والدبلوماسية الرقمية، القطاعات المستهدفة وتوزيعها النسبي، مؤشرات الأثر (تعطيل، كلفة، تغيير سلوك)، وكلف الارتداد (عقوبات، عزلة تقنية، حظر توريد). يمكن إدخال "نظام ترقيم/ترجيح" مبسط يمنح كل مؤشر درجة من ١ إلى ٥ وفق معايير مُعلنة، ثم عرض النتائج في رادارات/جداول تُظهر الفوارق البنيوية لا السردية فحسب. هذا النهج يُسهل استخلاص خلاصات معيارية متّسقة، ويعطي المقارنة عمقًا قابلاً للقياس والتتبّع عبر الزمن.

٦) ضبط الملخص والمصطلحات : يستفيد النص من ملخص ثنائي اللغة مُحكم يعكس تصميم الدراسة ومنهجها ووحدة تحليلها وزمنها وأبرز نتائجها العملية. ويُنصح باعتماد "قائمة مصطلحات" داخلية تُوحِّد المقابلات العربية/الإنجليزية للمفاهيم الجوهرية (الجيوسيبرانية، الردع بالمنع/بالعقاب، السيادة الرقمية...)، مع توحيد طريقة كتابة الأسماء الأجنبية عبر المتن والهوامش. كما تُعتمد صيغة تحريرية موحّدة للمراجع والهوامش والعناوين الفرعية، وتُراجع لغة الملخص الإنجليزي بعناية لسلامة التعبير ودقّته. هذا الضبط التحريري ليس تجميليًا فحسب، بل يؤثر مباشرة في وضوح الحُجّة وقابليتها للاقتباس، ويقلّل اللبس عند القارئ المتخصص وغير المتخصص على السواء.

٧) إدراج دراسات حالة معمّقة : مع الحفاظ على النظرة الشاملة، يحتاج النص إلى طبقة "غاطسة" من التحليل تقدم حالتين أو ثلاثًا تُدرس آليًا خطوةً بخطوة. تُختار الحالات وفق معايير تمثّل تباينًا في القطاع (مثل الطاقة والاتصالات)، وفي طبيعة الأثر (تعطيل مادّي مقابل تأثير معلوماتي)، وفي نمط التوظيف

بين الطرفين. تُبنى لكل حالة "سلسلة زمنية" دقيقة: سياق ما قبل الحادثة، آلية الاختراق أو الهجوم، حجم التعطيل وزمنه، الاستجابة التقنية والمؤسسية للطرف المستهدف، ثم الانعكاس السياسي أو الاقتصادي إن وُجد. ويُبرز التحليل البدائل المقابلة (ماذا لو لم يحدث الهجوم؟) لإظهار القيمة المضافة. بهذه المقاربة يتجسّد "أثر القوة" في أمثلة قابلة للقياس، ويتحوّل السرد إلى استدلال سببي مدعوم بالدليل.

٨) وضع حدودٍ منهجية وأخلاقية: من المهم تضمين فقرة صريحة تُقرّ بقيود الإسناد المفتوح المصدر، وباحتمالات التحيّز في التغطية بين البيئات الإعلامية المختلفة، وبالاختلالات الناتجة عن فجوات الشفافية التقنية. تُحدّد الفقرة سياسة التعامل مع حالات عدم اليقين، ومع المواد الحساسة أو التي قد يسبّب نشرها ضررًا أمنيًا أو قانونيًا. كما تُوضّح الاعتبارات الأخلاقية المتعلقة بخصوصية الأفراد والمؤسسات، وبتوازن العرض بين الأطراف المتنازعة، وبضرورة تجنّب "تسييس" الوقائع خارج نطاق الأدلة المتاحة. إعلان هذه الحدود يعزّز شفافية النتائج ويمنع إساءة قراءتها، ويمنح القارئ إطارًا واضحًا لفهم ما يمكن وما لا يمكن استنتاجه على ضوء المادة المتاحة.

٩) ربط الجداول بالتحليل : ينبغي أن تتحوّل الجداول إلى نقطة انطلاق نحو تحليل منظّم. تبدأ العملية باشتقاق مؤشرات مشتقة: التواتر السنوي للهجمات بحسب القطاع، متوسط زمن الاكتشاف والاستجابة، شدّة الحوادث عبر مقياس معياري، وكثافة الاستهداف الجغرافي. ثم تُرسم اتجاهات زمنية وتُقارن بفترات التوتر السياسي أو محطات السياسات العامة، للكشف عن أنماط اقتران ذات دلالة. ويمكن توظيف مقاربات وصفية بسيطة (جداول عبور، معاملات ارتباط) لتدعيم الفرضيات دون الانزلاق إلى تعقيد إحصائي لا تتيحه البيانات. تُعرض هذه النتائج في رسوم واضحة تُحيل مباشرة إلى الأسئلة البحثية، وتُستخدم لاختبار الفرضيات المصاغة في التوصية الأولى. بهذه الخطوات ينتقل النص من "التجميع" إلى "الاختبار"، ومن العرض الخطي إلى التحليل التفسيري. ختاماً، عمليًا، يبدأ التحسين بتحديث المقدمة والمنهج لإعلان الوحدة والمستوى والإطار الزمني، ثم إنشاء مصفوفة الترميز ولوحة

البيانات، يليهما ضبط الملخص والمصطلحات. بالتوازي، تُبنى المقارنة المعيارية في جدول موحّد، وتُنتقى دراستان أو ثلاث كحالات معمّقة وفق معايير انتقاء شفافة. وأخيرًا تُولَّد المؤشرات المشتقة وتُربط زمنيًا بالسياقات السياسية، مع ذكر الحدود المنهجية والأخلاقية بوضوح. بهذا تتعزّز القيمة العلمية والنفع التطبيقي للدراسة: يتقوّى الاستدلال، وتتضح الفروق البنيوية بين الاستراتيجية الروسية والأخرى الصينية، وتغدو النتائج قابلة للقياس والمقارنة والتراكم في أبحاث لاحقة.

الخاتمة

تُقدّم الدراسةُ نصّاً تأسيسياً بالعربية في موضوعٍ بالغ الحداثة؛ فتُظهر كيف يُعيد الفضاء السيبراني تشكيل مشهد القوة وتوزيعاتها، وتُميِّز – بصورةٍ ذات دلالة – بين نمط التوظيف الروسي الأكثر هجومية والمزج الصيني بين الناعم والصلب في إطار استراتيجية أوسع. وتُسجِّل هذه المراجعة، في المقابل، أن قيمة الدراسة العلمية يمكن أن ترتفع بوضوح إذا انتقلت من "الوصف التجميعي" إلى "التحليل المنظَّم القابل للاختبار": بإدارة فرضياتٍ محددة، وبناء مصفوفة ترميز موثوقة ومصادر تقنية رصينة، وتركيب مقارنةٍ معيارية تُظهر الاختلافات البنيوية لا الاختلافات السردية فقط، وإدراج دراسات حالة تُثبت السلسلة السببية من الفعل إلى الأثر. وعندما تُعالج هذه الجوانب، تُصبح الدراسة مرجعاً عربياً متيناً في حقل العلاقات الدولية السيبرانية، وتُسهم في بلورة فهمٍ أدقّ لطرائق تحويل القدرات الرقمية إلى مكاسب قوة قابلة للقياس في الحالتين الروسية والصينية .

المراجع

- Joseph S. Nye, Jr. (2010). *Cyber Power*, (Cambridge, Belfer Center for Science and International Affairs, Harvard Kennedy School).
- Kuehl. Daniel T. (2009). *From cyber space to cyber power: defining the problem in cyber power and national security.* (Washington. D.C: national Defence up).

- Libicki. Martin C. (2009). *Cyberdeterrence and Cyberwarfare.* (RAND: Santa Monica).
- Gibney. E. (2022). *Where is Russia's cyberwarfare? Researchers deconstruct its strategy.* (Nature magazine on March 21).
- العلي، علي. (٢٠١٩). الجيوسيبرانية في استراتيجية طريق واحد حزام واحد الصينية. شبكة النبأ المعلوماتية. تاريخ الزيارة ٢٧-٧-٢٠٢٢. على https://annabaa.org/arabic/print/18538 :