

## "سيناريوهات المواجهة الناعمة بين الولايات المتحدة والصين"

إعداد الباحث:

حامد محمود خضرة

باحث دكتوراه- قسم العلوم السياسية- كلية الحقوق والعلوم السياسية- جامعة بيروت العربية- بيروت - لبنان.

<https://doi.org/10.36571/ajsp8023>

## الملخص:

تسعى هذه الدراسة الى شرح سيناريوهات المواجهة الناعمة الناتجة عن الحرب التكنولوجية القائمة بين الولايات المتحدة الأمريكية والصين، عبر التطرق الى الحرب الاقتصادية والحرب السيبرانية باعتبارهما المظهرين الاساسين لهذه المواجهة.

تخلص الدراسة الى أن المواجهة الناعمة بين الولايات المتحدة الأمريكية والصين، وبالرغم من كونها المسار الأرجح لمستقبل المواجهة بين القطبين، فان ذلك لا يفي كليا احتمال تدحرج الأمور الى صدامات عسكرية غير محسوبة النتائج تكون شرارة لحرب عسكرية كبرى بينهما.

**الكلمات المفتاحية:** الحرب التكنولوجية؛ المواجهة الناعمة؛ الحرب الاقتصادية؛ الحرب السيبرانية؛ الولايات المتحدة؛ الصين.

## المقدمة:

ان المواجهة التكنولوجية بين الولايات المتحدة والصين تشكل تحولاً هاماً في العلاقات الدولية وتؤدي الى صراعات مستقبلية بين الدولتين لما يشكله الصعود التكنولوجي الصيني اللافت من مخاوف للعديد من الدول وفي مقدمتها الولايات المتحدة، (ريببكا فانين، 2010 ص 5) (1) اذ تتجاوز هذه المنافسة، المواجهات العسكرية التقليدية لتشمل المجالات الاقتصادية والسيبرانية التي تشكل أساس الحرب الناعمة غير المسلحة. تشمل المواجهات غير المسلحة مجموعة من الاستراتيجيات والتكتيكات التي قد تستخدمها الدولتان لتأكيد هيمنتها، والتأثير على النظام العالمي، ورسم مستقبل التكنولوجيا.

ان الحرب الناعمة بمفهومها العام " تتضوي تحت مفهوم القوة الناعمة مع استخدام التكتيكات التي لا تصل الى حد الهجوم المسلح" (Micheal Gross, 2017, Page 1) (2). فمن خلال الحروب الناعمة، يسعى المتحاربون الى فرض ارادتهم وهيمنتهم والوصول الى أهدافهم من دون الانخراط في العمل العسكري المباشر الذي يتمظهر في استخدام القوة المفرطة والوسائل الحربية والأسلحة الفتاكة. ان الحرب الناعمة هي أحد أبرز سيناريوهات نتائج الصراع التكنولوجي بين الولايات المتحدة والصين حيث تكتسب تكتيكات الحرب الناعمة، بما في ذلك الحرب السيبرانية والعقوبات الاقتصادية، أهمية متزايدة في نظريات الحروب الحديثة. (Micheal Gross, 2017 Page 4) (3)

## مشكلة البحث

ان الحرب التكنولوجية القائمة اليوم بين الولايات المتحدة الأمريكية والصين باتت من أهم المواضيع الداهمه في مجال العلاقات الدولية. ولقد تجلت هذه الحرب في مواجهة مباشرة بين البلدين على أكثر من صعيد. وبالرغم من ان المواجهة لاتزال ضمن الأطر الناعمة ولم تتدحرج بعد الى مواجهة عسكرية، فان ذلك يفتح أمامنا المجال للأسئلة التالية:

(1) ريببكا فانين، (2010)، التنين الصيني وسباق التكنولوجيا، ترجمة، محمد فتحي، محمد جبريل، مجموعة النيل العربية، القاهرة ص 5.

(2) Michael Gross and Tamar Meisels, (2017), *Soft War, The Ethics of Unarmed Conflicts*, Cambridge University Press, UK. Page 1.

(3) المرجع نفسه ص 4.

- 1- ما هي مظاهر المواجهة الناعمة بين الولايات المتحدة والصين؟
- 2- ما هو مستقبل الحرب التكنولوجية بين البلدين؟
- 3- ما هي احتمالات تدحرج المواجهة الناعمة الى حرب عسكريه؟

### أهداف البحث

يهدف هذا البحث الى شرح سيناريوهات الحرب الناعمة القائمة بين الولايات المتحدة الأمريكية والصين ثم التطرق الى احتمالات تطور هذه المواجهة الى حرب عسكريه كبرى.

### أهمية البحث

لا شك بأن الحرب التكنولوجية بين الولايات المتحدة والصين تحتل حيزا مهما في رسم مشهد الصراع الدولي القائم في عالمنا اليوم. فالتنافس الاميركي الصيني هو من محددات معالم النظام الدولي الجديد. ولهذا فان التطرق الى مظاهر الصراع الحالي واحتمالية تدحرجه الى مواجهة عسكريه يمكن أن يوضح لنا مستقبل النظام الدولي ومعالم العلاقات الدولية وتوازنها.

### منهجية البحث

في هذا البحث، سوق يتم استخدام المنهج التحليلي في سبيل شرح مظاهر المواجهة الناعمة بين الولايات المتحدة والصين واستشراف مستقبل المواجهة وامكانيه تحولها الى صدام عسكري.

### تقسيم البحث

المطلب الأول: الحرب الاقتصادية

الفرع الأول: الحرب التجارية المباشرة (الرسوم الجمركية)

الفرع الثاني: سياسة القيود على الاستثمارات الخارجية

المطلب الثاني: الحرب السيبرانية

الفرع الأول: استراتيجيات وتكتيكات الحرب السيبرانية

الفرع الثاني: تداعيات الحرب السيبرانية على الامن العالمي

## المطلب الأول

### الحرب الاقتصادية

ان الحرب الاقتصادية هي احدى وسائل الحرب الناعمة الناتجة عن تفاقم الصراع التكنولوجي بين الولايات المتحدة والصين. تشير الحرب الاقتصادية إلى الاستخدام الاستراتيجي للوسائل الاقتصادية لتقويض اقتصاد الخصم مع تعزيز اقتصاد الطرف الآخر. ونظراً لترابط الاقتصاد العالمي، من المرجح أن تستخدم كل من الولايات المتحدة والصين تكتيكات اقتصادية وإجراءات تجاربه تستهدف الصناعات التكنولوجية لكل منهما وتقوض اقتصاد الآخر، بينما تسعى كل منهما إلى حماية وتعزيز صناعاتها الخاصة. في هذا المطلب، سوف نتطرق الى الحرب التجارية المباشرة (فرع اول) وسياسة القيود على الاستثمارات (فرع ثان).

### الفرع الأول

#### الحرب التجارية المباشرة (الرسوم الجمركية)

ان الحرب التجارية بين الولايات المتحدة الأميركية والصين هي أحد اهم مظاهر الحرب الاقتصادية بين البلدين. يمكن إرجاع الحرب التجارية بين الولايات المتحدة والصين، والتي تصاعدت حداثها بشكل ملحوظ بدءاً من عام 2018، إلى تنافس عميق صلبه التكنولوجيا التي تشكل الدافع الأساسي للتوترات. تُؤد الحرب التجارية المتصاعدة بين العملاقين الاقتصاديين انعدام ثقة استراتيجي، وتُزعزع قواعد التجارة ومنظمة التجارة العالمية في جو جيوسياسي مشحون حيث تسعى الدولتان إلى انتزاع الريادة التكنولوجية العالمية. (Muhammad Baig et Al, 2023, P 13)<sup>(4)</sup> تُمثل الحرب التجارية بين الولايات المتحدة والصين، المتجذرة في التنافس التكنولوجي، منعطفًا حاسمًا في العلاقات الاقتصادية العالمية. وبينما تواجه الدولتان تداعيات هذا الصراع، فإن خياراتهما لن تُشكل مستقبلهما الاقتصادي فحسب، بل المشهد العام للتجارة والدبلوماسية الدولية. فالتقدم التكنولوجي الذي كان أساسًا للتعاون، أصبح الآن ساحة معركة للمنافسة، مُغيرًا بذلك طبيعة العلاقة بين هاتين القوتين العظميتين العالميتين. وسيطلب حل هذه التوترات في المستقبل توازنًا دقيقًا بين المنافسة والتعاون، وهي مهمة محفوفة بالتحديات، لكنها ضرورية لاقتصاد عالمي مستقر ومزدهر.

ولهذا الصراع تداعيات بعيدة المدى، ليس فقط على الدولتين، بل على الاقتصاد العالمي والنظام الدولي أيضًا. فالحرب التجارية التي بدأت في العام 2018 من المرجح ان تستمر وتتصاعد كنتيجة حتمية للصراع التكنولوجي بين البلدين حيث تبدي الولايات المتحدة قلقا جديا إزاء التطور التكنولوجي الصيني. (Muhammad Baig et Al, 2023 Page 13)<sup>(5)</sup> لقد بدأت الحرب التجارية بين الولايات المتحدة الأميركية والصين بشكلها الرسمي العلني في تشرين الثاني من العام 2018 حين أعلن الرئيس الاميركي دونالد ترمب سلسلة من التعريفات الجمركية والقيود التجارية على الصين بهدف تغيير سلوكها تجاه الولايات المتحدة فيما اعتبره ممارسات غير

Muhammad Ali Baig, Dost Barresh and Talal Shabbir, (2023) *The US–China Trade War: Hard Implications of a Soft War*, BTTN Journal, Vol 2, (4)

Issue 1, Page 13.

(5) المرجع نفسه ص 13،

عادلة و سرقة حقوق الملكية الفكرية. (Anna Swanson, 2018)<sup>(6)</sup> تعتبر هذه القرارات الأميركية من أكثر القضايا سخونة في العلاقات الدولية الحديثة. (Muhammad Baig et Al, 2023 Page1)<sup>(7)</sup> ان هذه التعريفات والقيود لم تكن الا جزء من حملته كان قد وضعها البيت الأبيض من قبل، وأحد مواضيعها الاقتصادية الرئيسية كان خطة لشن حرب تجاريه ضد الصين. (رمزي محمود، 2022، ص 217)<sup>(8)</sup>

لقد فرضت الولايات المتحدة رسوماً جمركية على سلع صينية بقيمة 34 مليار دولار. ردًا على ذلك، ردت الصين بفرض رسوم جمركية على سلع أمريكية، مما أدى إلى تصعيد في الحرب التجارية الى مستويات متقدمة. (BBC, 2018)<sup>(9)</sup> وبحلول منتصف عام 2019، شملت الرسوم الجمركية تجارةً بمئات المليارات من الدولارات، مما أثر على العديد من الصناعات في كلى الاقتصادين. (Chetean Ahya, 2018)<sup>(10)</sup> وقد أدت الحواجز التجارية إلى اضطرابات كبيرة في سلسلة التوريد، مما دفع الشركات إلى إعادة النظر في استراتيجياتها التشغيلية والنظر في نقل إنتاجها بعيدًا عن الصين.

ان الحرب التجارية بين الولايات المتحدة والصين ليست مجرد صراع اقتصادي، بل هي مظهر من مظاهر التنافس الاستراتيجي على الهيمنة العالمية. وقد اعتبرت الولايات المتحدة صعود الصين تحديًا لهيمنتها، الامر الذي عزز الحرب التجارية وجعلها في سلم أولويات الحكومة الأميركية. فالحرب التجارية التي قامت لم تهدأ من الولاية الأولى للرئيس ترمب حتى الان. ومجريات الاحداث وتسلسلها يشيران الى انها لن تهدأ في الأمد القريب بل ستتعمق وتتسع وستكون من سمات المواجهة الأميركية الصينية في المستقبل. ومن الأمثلة الراهنة التي تؤكد على ذلك، ما أعلنه الرئيس الاميركي مؤخرًا في السابع من نيسان عام 2025 عن نيته فرض تعريفات جمركية اضافية بقيمة 50% على الصين في حال لم تتراجع عن التعريفات الجمركية المضادة التي فرضتها على الولايات المتحدة. (Reuters, 2025)<sup>(11)</sup> ولقد تبعه ذلك فرض ترمب لرسوم جمركية على الصين بقيمة 104% بعد ان رفضت الصين التراجع عن التعريفات الجمركية المضادة. (سي ان ان، 2025)<sup>(12)</sup> ان هذا يشير بوضوح الى منحى تصادي مستقبلي في الحرب التجارية بين البلدين بحيث سيكون الاقتصاد العالمي ملعبا لهذه التوترات الاقتصادية والسياسية الخطيرة.

Anna Swanson, New York Times website, **Trump's Trade War with China Is Officially Underway**, 05/07/2018, <sup>(6)</sup>

<https://www.nytimes.com/2018/07/05/business/china-us-trade-war-trump-tariffs.html> تاريخ الزيارة: 10/04/2025.

<sup>(7)</sup> مرجع سابق، Muhammad Ali Baig, Dost Barresh and Talal Shabbir، ص 1.

<sup>(8)</sup> رمزي محمود، (2022)، صراع أمريكا والصين على عرش الاقتصاد العالمي، دار التعليم الجامعي، القاهرة، ص 217.

<sup>(9)</sup> BBC News website, **China hits back after US imposes tariffs worth \$34bn**, 06/07/2018, <https://www.bbc.com/news/business-44707253> تاريخ الزيارة: 08/04/2025.

Chetean Ahya, Morgan Stanley website, **Why Trade Tariffs Could Rattle the Global Supply Chain?** 22/08/2018, <sup>(10)</sup>

<https://www.morganstanley.com/ideas/trade-tariffs-supply-chain> تاريخ الزيارة: 15/04/2025.

Reuters Website, **Trump threatens additional tariffs on China, terminates talks**, 07/04/2025, <https://www.reuters.com/world/us/trump-threatens-additional-tariffs-china-terminates-talks-2025-04-07/> تاريخ الزيارة: 07/04/2025.

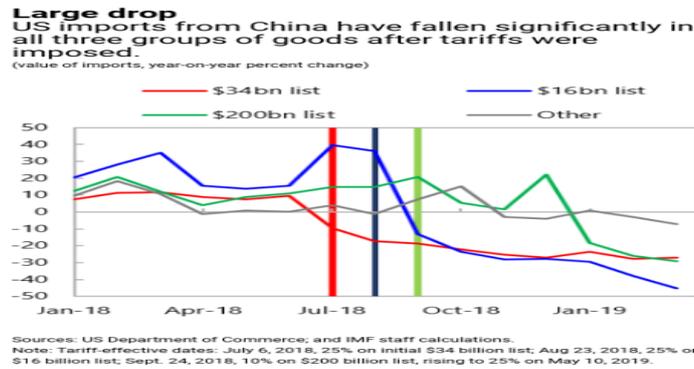
<sup>(12)</sup> موقع سي ان ان بالعربية، أول رد من الصين بعد دخول تعريفات الـ 104% لتراحم حيز التنفيذ، 09/04/2025، <https://arabic.cnn.com/world/article/2025/04/09/china-vows-resolute-measures-trumps-104-tariffs-take-effect> تاريخ الزيارة: 08/05/2025.

ان للحرب التجارية تداعياتٌ جمة على الاقتصاد الأمريكي. فعلى الرغم من ان الحرب التجارية والتعريفات الجمركية هدفت الى حماية الاقتصاد الأمريكية ومواجهة التمدد الصيني، إلا أنها رفعت أيضًا التكاليف على المستهلكين والمصنعين المعتمدين على الصادرات الصينية واضرت بالقدرة التنافسية للمزارعين الاميركيين. (Swiss info, 2025)<sup>(13)</sup> تكبدت القطاعات الزراعية الأمريكية، وخاصةً تلك المعتمدة على الصادرات إلى الصين، خسائر فادحة.

هذا الامر دفع الحكومة الأمريكية إلى تخصيص مليارات الدولارات كمساعدات للمزارعين المتضررين من حرب الرسوم الجمركية اذ " كشف الرئيس الأمريكي دونالد ترمب عام 2019 عن خطة إنقاذ بقيمة 16 مليار دولار للمزارعين المتضررين من حربه التجارية مع بكين"، (Anna Swanson, 2025)<sup>(14)</sup> في دلاله واضحة إلى استمرار الحرب التجارية في المستقبل والتوجه الى انسحاب الشركات الأمريكية من السوق الصينية.

ومن الملاحظ انه منذ بدء الحرب التجارية بين البلدين، شهدت معدلات التبادل التجاري بينها انخفاضات ملحوظة وكبيره كانت لها انعكاسها على التجارة والاقتصاد العالمي. (الملحق 1)

الملحق ادناه يوضح ان الرسوم الجمركية التي فرضتها الولايات المتحدة عام 2018 والتي كانت على ثلاث قوائم من السلع الصينية، مستهدفةً أولاً واردات سنوية بقيمة ٣٤ مليار دولار، ثم ١٦ مليار دولار إضافية، وأخيراً ٢٠٠ مليار دولار إضافية. (Eugenio Cerutti et Al, 2025)<sup>(15)</sup> ونتيجةً لذلك، انخفضت واردات الولايات المتحدة من الصين انخفاضًا حادًا في جميع فئات السلع الثلاث التي فُرضت عليها الرسوم.



## الملحق رقم 1

<sup>(13)</sup> Swiss Info website المزارعون الأمريكيون "قلقون" من تأثير الرسوم الجمركية على مداخيلهم، 06/04/2025، [https://www.swissinfo.ch/ara/%d8%a7%d9%84%d9%85%d8%b2%d8%a7%d8%b1%d8%b9%d8%b4](https://www.swissinfo.ch/ara/%d8%a7%d9%84%d9%85%d8%b2%d8%a7%d8%b1%d8%b9%d8%b4/d8%a7%d8%b1%d8%b9%d8%b4) تاريخ الزيارة: 08/04/2025.

<sup>(14)</sup> Anna Swanson, New York Times website, **Trump Gives Farmers \$16 Billion in Aid Amid Prolonged China Trade War**, 23/05/2025، <https://www.nytimes.com/2019/05/23/us/politics/farm-aid-package.html> تاريخ الزيارة: 10/08/2025.

<sup>(15)</sup> Eugenio Cerutti, Gita Gopinath and Adil Mahmoud, IMF Blog website, **The Impact of US-China Trade Tensions**, 23/05/2019، <https://www.imf.org/en/Blogs/Articles/2019/05/23/blog-the-impact-of-us-china-trade-tensions> تاريخ الزيارة: 11/04/2025.

<https://www.imf.org/en/Blogs/Articles/2019/05/23/blog-the-impact-of-us-china-trade-tensions>

المصدر:

ومن الملاحظ انه بالرغم من الحرب التجارية المستعرة بين البلدين، وبالرغم من الانخفاض الكبير في التبادل التجاري بينهما، فان التبادل لم يتوقف نظرا لحاجة كل طرف الى الآخر. الا انه انخفض بشكل ملحوظ.. فالعلاقة التجارية بين الولايات المتحدة والصين معقده وتحكمها العديد من العوامل الشائكة. فعلى سبيل المثال لا الحصر، " تستحوذ الصين على ما لا يقل عن نصف صادرات فول الصويا الأميركي وأكثر من الذرة الرفيعة اذ أنفقت بكين عام 2024 أي ست سنوات بعد بداية الحرب التجارية، 24,7 مليار دولار على المنتجات الزراعية الأميركية، بما في ذلك الدجاج ولحوم البقر ومحاصيل أخرى." (Eugenio Cerutti et Al, 2025) (16)

علاوةً على ذلك، دفع عدم اليقين في السياسات التجارية، العديد من الشركات إلى تقلبات في الأسواق وتراجع ثقة المستهلكين والمستثمرين وتأجيل الاستثمارات، مما قوّض النمو الاقتصادي. (CNBC Arabia, 2025) (17)

في المقلب الآخر، وبالرغم من أن الصين بدت مقاومةً للضغوط الأمريكية، إلا أنها واجهت تحديات اقتصادية جسيمة. فقد أدت الحرب التجارية الاولى عام 2018 ومن ثم تجدها عام 2025، إلى تفاقم المشكلات القائمة في الاقتصاد الصيني. فالاقتصاد الصيني اليوم يعتمد بشكل أساسي على الطلب الخارجي المتمثل بالصادرات مما يخلق تحديات جوهريه مثل الانكماش الاقتصادي، وضعف الاستهلاك المحلي، وتفاقم أزمة العقارات، بالإضافة الى ضغط على العملة الوطنية، وارتفاع مستويات الديون وتراجع النمو المحلي. (مصطفى مقلد، 2025) (18)

## الفرع الثاني

### سياسة القيود على الاستثمارات التكنولوجية

ان الحرب الاقتصادية بين الولايات المتحدة والصين عبر ادوات الحرب التجارية المباشرة مثل فرض رسوم وتعريفات جمركيه، تُستكمل على صعيد آخر بسياسة القيود على الاستثمارات التكنولوجية. فبما ان التكنولوجيا هي في جوهر الصراع بين البلدين وبما ان الحرب الاقتصادية هي من أبرز تداعيات الصراع التكنولوجي القائم، لجأت الولايات المتحدة في صراعها مع الصين الى استهداف مباشر لكل ما يتعلق بنقل التكنولوجيا الصينية وتوريدها والاستثمار فيها، اذ يواجه المستثمرون الأمريكيون المهتمون بالاستثمار في شركات التكنولوجيا الصينية المتقدمة الآن، قيودًا بسبب إطلاق الحكومة الأمريكية لقاعدة الاستثمار الخارجي المتعلقة بالتكنولوجيا الصينية والتي

(16) المرجع نفسه.

(17) CNBC Arabia website, تقرير لـ QNB: عدم اليقين بشأن السياسات الأمريكية التجارية والمالية يثير مخاوف الركود، 23/03/2025.

www.cnbcarabia.com/135810/2025/23/03/تقرير-لـ-QNB:-عدم-اليقين-بشأن-السياسات-الأمريكية-التجارية-والمالية-يثير-مخاوف-الركود تاريخ الزيارة: 12/04/2025.

(18) مصطفى مقلد، مركز شاف للدراسات المستقبلية وتحليل الازمات والصراعات، الحرب التجارية الصينية: من التكيف الى المواجهة، 08/04/2025.

https://shafcenter.org/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8- تاريخ الزيارة: 13/04/2025.

دخلت حيز التنفيذ في 2 كانون ثاني 2025. (Holland and Knight, 2025)<sup>(19)</sup> تفرض هذه القاعدة قيودًا على استثمارات المستثمرين الأمريكيين في بعض التقنيات الإلكترونية المتقدمة إذ تُصنّف بعض الاستثمارات أنها محظورة بشكل كامل، بينما يتطلب بعضها الآخر إخطارًا للسلطات الأمريكية بعد إتمام الصفقة. (Paul Edelberg, 2025)<sup>(20)</sup>

من أهم دوافع الحد من الاستثمارات التكنولوجية الصينية، هي قضايا الامن القومي والاعتقاد الراسخ بأن هذه الاستثمارات تُشكل خطرًا على الأمن القومي. (John Bateman, 2022 Page 1)<sup>(21)</sup> وقد سلط المسؤولون الأمريكيون الضوء على مخاوفهم من أن الشركات الصينية، وخاصةً تلك المملوكة للدولة، قد تجمع معلومات حساسة أو تُشكل تهديدًا إلكترونيًا. وقد ازداد هذا القلق مع صعود شركات التكنولوجيا العملاقة مثل هواوي وزد تي إي، اللتين اتُهما بالتجسس وإمكانية تمكين الحكومة الصينية من المراقبة. (Noah Berman et Al, 2023)<sup>(22)</sup>

وهنا، من المهم التطرق الى لجنة الاستثمار الأجنبي في الولايات المتحدة (CFIUS)، وهي فرقة عمل متعددة الوكالات مسؤولة عن مراجعة الاستثمارات الأجنبية في الشركات الأمريكية. (US–Treasury)<sup>(23)</sup> لقد اوعز الرئيس الاميركي دونالد ترمب في 21 شباط 2025 الى هذه اللجنة، التدقيق بشكل خاص في المعاملات التي تشمل شركات صينية وفرض قيود على الاستثمارات الصينية في القطاعات الحساسة وفي طبيعتها القطاعات التكنولوجية. (Guillermo Christensen et Al, 2025)<sup>(24)</sup> وتتمتع اللجنة بسلطة منع الصفقات التي تهدد الأمن القومي، مما يعكس حذرًا متزايدًا تجاه التدخل الأجنبي في التقنيات الحيوية.

من الدوافع المهمة الأخرى للقيود الأمريكية على الاستثمارات الصينية التكنولوجية، الرغبة في الحفاظ على القدرة التنافسية الاقتصادية. فمع استثمار الصين بكثافة في التقنيات الناشئة، مثل الذكاء الاصطناعي والحوسبة الكمومية والتكنولوجيا الحيوية، ازداد

Holland and Knight website, **Outbound Investment Screening Rule Goes into Effect, Final Rule Targets U.S. Investment in Chinese or Chinese Owned Companies**, 10/01/2025, <https://www.hklaw.com/en/insights/publications/2025/01/outbound-investment-screening-rule-goes-into-effect> تاريخ الزيارة: 15/04/2025.

Paul Edelberg, Fox Rothschild website, **Investments in Chinese Technology Companies Limited by New US Outbound Investment Rule**, 13/01/2025, <https://www.foxrothschild.com/publications/investments-in-chinese-technology-companies-limited-by-new-us-outbound-investment-rule> تاريخ الزيارة: 09/04/2025.

John Bateman, (2022), **US–China Technological Decoupling, A Strategy and Policy Framework**, Carnegie Endowment for International Peace, Washington, Page 1.

Noah Berman, Lindsay Miazland, and Andrew Chatzky, **Is China’s Huawei a Threat to U.S. National Security?**, 08/02/2023, <https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security> تاريخ الزيارة: 10/04/2025.

The US Department of the Treasury, **The Committee on Foreign Investment in the United States (CFIUS)**, <https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius> تاريخ الزيارة: 11/04/2025.

Guillermo S. Christensen, Steven F. Hill, Brian J. Hopkins, Nathaniel B. Bolin, David R. Allman and Jeffrey Orenstein, K&L Gates website, **Trump Administration Directs CFIUS to Tighten Restrictions on Investment From Certain Countries While Easing National Security Reviews of Investments From Allies and Partners**, 26/02/2025, <https://www.klgates.com/Trump-Administration-Directs-CFIUS-to-Tighten-Restrictions-on-Investment-From-Certain-Countries-While-Easing-National-Security-Reviews-of-Investments-From-Allies-and-Partners-2-26-2025> تاريخ الزيارة: 26/02/2025.

قلق الحكومة الأمريكية من أن وصول الصين غير المقيد إلى التكنولوجيا الأمريكية قد يُفوّض قيادة الولايات المتحدة في هذه القطاعات إذ لجأت الإدارة الأمريكية المتحدة عام 2024 خلال فترة ولاية الرئيس الأميركي السابق جو بايدن إلى وضع إطار تنظيمي يستهدف الاستثمارات في الذكاء الاصطناعي وأشباه الموصلات والحوسبة الكمومية. وتقرض هذه الإجراءات، التي دخلت حيز التنفيذ في كانون ثاني ٢٠٢٥، حظرًا على بعض المعاملات مثل تلك المرتبطة بالحوسبة الكمومية وتتطلب إخطارات إلزامية لمعاملات أخرى تتعلق بأنظمة الذكاء الاصطناعي عالية الأداء والإلكترونيات الدقيقة المتقدمة. (Giulia Interesse, 2025) (25)

إلا أن اللافت في هذا السياق تمكن الصين من تجاوز القيود الأمريكية المفروضة على التصدير والتي تستهدف بالمباشر التضيق على القطاع التكنولوجي الصيني وخلق تحديات تقنية وعراقيل أمام التقدم. ومن الأمثلة المهمة على تمكن الصين من أحداث خرق تقني كبير في ظل التضيق الأميركي المتصاعد في مجال التكنولوجيا، تطوير برنامج "ديب سيك" للذكاء الاصطناعي والذي بعد منافسا جديا لبرنامجي "غوغل" و "أوبن إيه آي" الأميركيين. (سكاي نيوز بالعربية، 2025) (26)

لقد جسّد هذا البرنامج التفوق التكنولوجي الصيني وقدرات الصين على الالتفاف على الإجراءات الأميركية والتأقلم معها ومنافسة الولايات المتحدة على احتكار الهيمنة التكنولوجية العالمي إذ اعتبر نقله نوعيه في مجال تكنولوجيا المعلومات. (PJ Kumar, 2025) (Page 2) (27)

فالتنافس بين الولايات المتحدة والصين ليس مجرد منافسة اقتصادية، بل هو أيضًا صراع جيوسياسي على النفوذ والهيمنة. في هذا السياق، تُعتبر قيود الاستثمار التكنولوجي أداة أساسية غير عسكرية لمواجهة النفوذ الصيني المتنامي. وبذلك فإن مواجهة القدرات التكنولوجية الصينية هو أفضل طريق لمنع الصين من توسيع نطاق حضورها العالمي وهيمنتها الدولية، وتغيير النظام العالمي من باب الريادة التكنولوجية.

إن المنافسة في ميادين التكنولوجيا المتطورة يتصاعد يوما بعد يوم نظرا لتأثير التكنولوجيا المباشر على الاقتصاد والقدرات العسكرية. لذلك فإن تقييد وصول الصين إلى التقنيات المتقدمة يمكن أن يمنعها من تحقيق النمو الاقتصادي المرجو وبالتالي يقلص

Giulia Interesse, China Briefing website, **S Investment Ban on China: What it Means Now That it's in Effect**, 15/01/2025, <https://www.china-briefing.com/news/us-investment-ban-on-china-what-it-means-now-that-its-in-effect>، تاريخ الزيارة: 10/04/2025. (25)

(26) موقع سكاي نيوز بالعربية، الريادة الأمريكية في الذكاء الاصطناعي تحت تهديد 'ديب سيك'، 29/01/2025، <https://www.skynewsarabia.com/business/1773018>، تاريخ الزيارة: 09/04/2025.

PJ Rosario Kumar, (2025) **REVOLUTIONIZING THE SEARCH GAME HOW DEEPSEEK IS TRANSFORMING INFORMATION-SEEKING BEHAVIOR IN THE DIGITAL AGE**, International Journal of Scientific Research in Engineering and Management, Volume: 09 Issue: 02, Page 2. (27)

نفوذها العالمي. (Mariano Florentino, 2024, Page 11) (28) ولذلك، فإن الوتيرة التصاعدية لهذه القيود، هدفها حماية مصالح الولايات المتحدة والحفاظ على توازن القوى في العلاقات الدولية.

لقد اتخذت الحكومة الأمريكية مجموعة متنوعة من التدابير لتقييد الاستثمارات التكنولوجية الصينية التي من المحتمل ان تساهم في تعزيز القدرات العسكرية الصينية، اذ اتبعت نهجا صارما في آليات التصدير لإدارة تدفق التكنولوجيا الحساسة إلى الصين. وينظم مكتب الصناعة والأمن (BIS) التابع لوزارة التجارة، صادرات التكنولوجيات التي يمكن أن تكون لها تطبيقات عسكرية. فقد وسّعت الولايات المتحدة قائمة التقنيات الخاضعة لضوابط التصدير، مما أدى إلى تشديد القيود على المنتجات التي قد تعزز القدرات العسكرية للصين. (Bureau of Industry, 2024) (29)

ان سياسة القيود الأمريكية على الاستثمارات الصينية التكنولوجية تزيد من التوترات في العلاقات الثنائية وتعقد مسارها المستقبلي. تُمثل هذه القيود محاولةً أمريكيةً لكبح جماح صعود الصين وإعاقة تطلعاتها للريادة التكنولوجية العالمية. وقد استكملت الولايات المتحدة حملتها ضد الصين بسلسلة من الرسوم الجمركية القاسية التي لاقت استهجانا دوليا كبيرا، اذ اتهمت الصين الولايات المتحدة بممارسة سياسة حمائية اقتصادية وان هذه الرسوم تؤدي الى ضرب استقرار الانتاج العالمي وسلاسل التوريد. (سكاي نيوز بالعربية، 2025) (30)

في المقابل، ترى الولايات المتحدة أن هذه الإجراءات ضرورية لحماية أمنها القومي. تُسهم القيود المستمرة في تنامي العداء بين البلدين، والذي قد يتفاقم إلى توترات جيوسياسية أوسع نطاقاً.

## المطلب الثاني

### الحرب السيبرانية

تتميز المواجهة الناعمة بين القطبين الولايات المتحدة الأمريكية والصين، نتيجةً للصراع التكنولوجي العميق، بوجه آخر غير الحرب الاقتصادية هي الحرب السيبرانية.

Mariano Florentino Cuellar and Christopher Chivis, (2024) **U.S.–China Relations for the 2030s: Toward a Realistic Scenario for Coexistence**, (28) Carnegie Endowment for International Peace Publications Department 1779 Massachusetts Avenue NW Washington, DC 20036, Page 11.

Bureau of Industry and Security, **Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications**, 02/12/2024, <https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semiconductors-military> تاريخ الزيارة: 12/04/2025.

(30) موقع سكاي نيوز بالعربية، الصين تتهم أميركا بـ "الحمائية" و"التنمر الاقتصادي" 07/04/2025، <https://www.skynewsarabia.com/world/1788407> تاريخ الزيارة: 04/202515.

تعرف الحرب السيبرانية انها " سلسلة من الهجمات السيبرانية ضد دولة قومية، تُلحق بها أضرارًا جسيمة. قد يشمل هذا الضرر تعطيل أنظمة حاسوبية حيوية." (Alexander Gillis)<sup>(31)</sup> ولا يقتصر تعريف الطرف المسؤول عن الحرب السيبرانية على الدول فقط انما يمتد ليشمل منظمات وكيانات ومجموعات غير حكومية.<sup>(32)</sup> تحمل الحرب السيبرانية القدرة على التسبب في أضرار للبنية التحتية الحكومية والمدنية، مما قد يؤدي إلى تعطيل الأنظمة الحيوية وإلحاق الضرر بالأمة أو خسارة الأرواح. (Paul Chakarian et Al, 2013, Page 2)<sup>(33)</sup>

لا تقل الحرب السيبرانية اهمية عن تلك الاقتصادية خاصة ان كلتي الحربين تعتبران وسيلتين للمواجهة بعيدتين عن استخدام الأسلحة التقليدية والوسائل العسكرية. فمع استمرار تحول المشهد العالمي نحو نموذج أكثر ترابطاً وتقدماً تكنولوجياً، اشتدت المنافسة بين الولايات المتحدة والصين في عدة مجالات، أبرزها التكنولوجيا والتي نتج عنها قدرات سيبرانية متقدمة وذات ضرر كبير. لقد أدى تزايد وتيرة العمليات السيبرانية والهجمات المعلوماتية وتطورها إلى ظهور شكل جديد غير تقليدي من الحرب، له تداعيات سياسية واقتصادية واجتماعية كبيرة. يتطرق هذا المطلب الى أبرز استراتيجيات وتكتيكات الحرب السيبرانية (فرع اول) والى تداعياتها على الامن العالمي (فرع ثان).

## الفرع الاول

### استراتيجيات وتكتيكات الحرب السيبرانية

ان الحرب السيبرانية الحالية بين الولايات المتحدة والصين ما هي الا تجسيد لنتائج التوترات الجيوسياسية الناتجة عن الصراع التكنولوجي المتفاحم. وقد فتح ظهور الإنترنت والاتصالات الرقمية في التسعينيات وأوائل الألفية الثانية آفاقاً جديدةً لأساليب الحرب والصراع. لطالما اعتُبرت الولايات المتحدة رائدة الإنترنت في العالم، وسعت بكل الوسائل الى بسط تفوقها في المجال السيبراني. ومع ازدياد عدد الدول التي طورت قدراتها السيبرانية وفي مقدمتها الصين، طغت على العقل الأميركي مخاوف بشأن الأمن السيبراني وإمكانية استخدامه ضدها وإلحاق الأذى بمصالحها القومية اذ تتوقع شركة Cybersecurity Ventures أن ترتفع تكاليف الجرائم الإلكترونية العالمية بنسبة 15% سنويا على مدى السنوات الخمس المقبلة، لتصل إلى 10.5 تريليون دولار أميركي سنويا بحلول عام 2025، مقارنة بـ 3 تريليون دولار أميركي في عام 2015. (Steve Morgan, 2020)<sup>(34)</sup>

(31) Alexander S. Gillis, TechTarget website, **what is Cyberwarfare?** <https://www.techtarget.com/searchsecurity/definition/cyberwarfare> تاريخ الزيارة: 10/04/2025

(32) Paulo Shakarian, Jana Shakarian and Andrew Ruef, (2013), **Introduction to Cyber Warfare, A Multidisciplinary Approach**, Syngress, 225 Wyman Street, Waltham, MA, USA, Page 2.

(33) مرجع سابق، Alexander S. Gills.

(34) Steve Morgan, Cyber Security Ventures website, **Cybercrime to Cost the World \$10.5 Trillion Annually By 2025**, 13/11/2020, تاريخ الزيارة: 15/04/2025. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016>

تتصوي الحرب السيبرانية القائمة بين الولايات المتحدة الأمريكية والصين على استراتيجيات وتكتيكات تشكل النواة الأساسية للمواجهة. فيما يلي أبرز هذه الاستراتيجيات:

أولاً: العمليات السيبرانية الهجومية

تتمحور استراتيجية الولايات المتحدة الأمريكية تجاه العمليات السيبرانية على مبدأ الدفاع والردع والهجوم التي تقوم بها القيادة السيبرانية للولايات المتحدة الأمريكية. هذه القيادة هي "قيادة عسكرية تعمل عالمياً ضد خصوم مصممين وقادرين. تضم القيادة قدرات عسكرية واستخباراتية وتقنية معلوماتية، مهمتها توجيه ومزامنة وتنسيق تخطيط وعمليات الفضاء الإلكتروني للدفاع عن المصالح الوطنية وتعزيزها بالتعاون مع الشركاء المحليين والدوليين." (US Cybercommand) (35) تنفذ هذه القيادة عمليات سيبرانية هجومية تستهدف الخصوم لتعطيل قدراتهم وحماية المصالح الرقمية الأمريكية وشملت هذه العمليات، التي غالباً ما تُصنّف ضمن السرية، تدابير مضادة للهجمات السيبرانية، وحملة تضليل إعلامي، وهجمات على بنى تحتية حيوية.

وبالرغم من ذلك، واجهت هذه التدابير تحديات في ظلّ التطور السريع للمشهد السيبراني بحيث أظهرت القدرات السيبرانية الصينية تطورات في تكتيكات مثل الهجمات متعددة النواقل، والبرمجيات الخبيثة المتطورة المُصمّمة لاختراق الشبكات وهجمات التصيد الإلكتروني، إذ أكد مكتب التحقيقات الفيدرالي الأميركي ان الصين منخرطة في هذه الأنشطة السيبرانية المريبة بهدف احداث فوضى في البنية التحتية الأمريكية مثل شبكات الكهرباء والمرافق الحيوية المختلفة. (Christopher Bing, 2024) (36)

كذلك تشير تحذيرات من مديرة وكالة الأمن السيبراني وأمن البنية التحتية (CISA) جين إيستلي والمدير الوطني للأمن السيبراني هاري كوكر إلى " أن القرصنة الصينيين يقومون بتحول استراتيجي لاستهداف البنية التحتية الحيوية، ومن المرجح أن يكونوا قادرين على شن هجمات إلكترونية يمكن أن تؤدي إلى شلل تلك البنية التحتية، وأنهم يستغلون بشكل متزايد المعلومات الخاصة للأمركيين". (Hadley Spadaccini, 2024) (37)

(35) US Cyber Command website, <https://www.cybercom.mil/About/History>, تاريخ الزيارة: 15/04/2025.

(36) Christopher Bing, Reuters website, **FBI says Chinese hackers preparing to attack US infrastructure**, 19/04/2024, <https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18>, تاريخ الزيارة: 16/04/2025.

(37) Hadley Spadaccini, **Risks are higher than ever for US– China cyber war**, 18/04/2024, <https://responsiblestatecraft.org/us-china-cyberwar>, تاريخ الزيارة: 14/04/2025.

من الأمثلة المهمة الحديثة على العمليات الهجومية السيبرانية الصينية هي عملية " إحصار الملح " التي خطط لها ونفذها قرصنة صينيون. فالهجوم، الذي يعتقد المحققون الأميركيون أنه مرتبط بوزارة أمن الدولة الصينية، استهدف على الأقل تسع شركات اتصالات وتدير بنى تحتية حيوية في الولايات المتحدة، إضافة إلى أهداف عدة في عشرات البلدان الأخرى. (آدم سيغال، 2025)<sup>(38)</sup>

والجدير بالذكر، ان المحققين الاميركيين لم يتمكنوا من تحديد مدة العملية اذ تمكن القرصنة الإلكترونيون من تحديد مواقع جغرافية عدة وسجلوا مكالمات هاتفية لملايين الأميركيين، واخترقوا إلى الرسائل النصية والمكالمات الهاتفية لعدد من المسؤولين على مستوى العالم، من بينهم الرئيس الأميركي الحالي دونالد ترمب ونائب الرئيس جي دي فانس. (آدم سيغال، 2025)<sup>(39)</sup>

مثال ثان على عمليات الهجوم السيبرانية هو اختراق مكتب إدارة شؤون الموظفين الأمريكي عام 2015. أدى هذا الاختراق إلى سرقة بيانات حساسة لأكثر من ٢٠ مليون فرد، بمن فيهم موظفون ومتعاقدون فيدراليون اذ اعتبرت هذه العملية احدى أخطر الاختراقات السيبرانية في تاريخ الولايات المتحدة. (Dirk Shrader, 2025)<sup>(40)</sup>

حاولت إدارة الرئيس الأميركي باراك أوباما آنذاك جاهدة تقييم تأثير خرق البيانات الضخم الذي شمل الوكالة التي تتعامل مع التصاريح الأمنية وسجلات موظفي الحكومة الأميركية، مع توجيه الشكوك بسرعة إلى الصين، التي اتُهمت بتنفيذ عمليات تجسس إلكتروني ضد الولايات المتحدة في الماضي. (The Guardian, 2015)<sup>(41)</sup>

جسد اختراق مكتب إدارة شؤون الموظفين التطور المتزايد للعمليات الإلكترونية الصينية ونقاط الضعف في البنية التحتية للأمن السيبراني الأمريكي. وأبرز الحادث المخاوف المتعلقة بالتجسس وخصوصية البيانات وأمن المعلومات الشخصية، مما زاد من حدة التوترات بين القوتين.

مثال ثالث على العمليات السيبرانية الهجومية المهمة ما حدث عام 2017 باختراق سيبراني معقد لشركة إيكوفاكس الأميركية، والذي أضرّ بالمعلومات الشخصية لنحو 147 مليون أمريكي، اذ خلص تحقيق فيديريالي موسع أن قرصنة تابعين للدولة الصينية هم

<sup>(38)</sup> آدم سيغال، موقع اندبنتبث بالعربية، الصين تصعد تهديداتها في الفضاء السيبراني، 25/01/2025، [www.independentarabia.com/node/616375](http://www.independentarabia.com/node/616375) /أراء الصين-تصعد-تهديداتها-في-الفضاء-السيبراني تاريخ الزيارة: 15/04/2025.

<sup>(39)</sup> المرجع نفسه، آدم سيغال.

<sup>(40)</sup> Dirk Schrader, Netwrix Community website, **The Largest and Most Notorious Cyber Attacks in History**, 17/12/2024,

<https://blog.netwrix.com/biggest-cyber-attacks-in-history> تاريخ الزيارة: 10/04/2025.

<sup>(41)</sup> The Guardian website, **OPM hack: China blamed for massive breach of US government data**, 05/06/2015,

<https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances> تاريخ

الزيارة: 15/04/2025.

المسؤولون عن الاختراق، ووجهت وزارة العدل الأمريكية اتهامات لأربعة أفراد من الجيش الصيني لتورطهم. (Strong DM,2025) (42) وقد أبرزت الدعايات المتعددة لهذه الحادثة أهمية تأمين البيانات الشخصية، لا سيما فيما يتعلق بالأمن القومي والاستخبارات الاقتصادية.

ثانياً: تعزيز الوضع الدفاعي للأمن السيبراني

ركزت الولايات المتحدة الأمريكية والصين على تعزيز وضعيهما الدفاعيتين في المجال السيبراني. وقد طبقت الحكومة الأمريكية استراتيجيات لتعزيز الأمن السيبراني عبر تعزيز الشراكة بين القطاعين العام والخاص وتبادل المعلومات. وتُبرز الاستراتيجية الوطنية للأمن السيبراني الحاجة إلى المرونة في مواجهة التهديدات السيبرانية الخارجية، وضرورة التزام الشركات المحلية بأفضل ممارسات الأمن السيبراني. (Eugenia Lostri et Al,2022) (43)

من ناحية أخرى، ركزت الصين استراتيجياتها على تطوير دفاعات داخلية قوية في شتى المجالات المتعلقة بالأمن السيبراني سواء بالسيطرة على شبكة الانترنت او منصات التواصل، بالتزامن مع تنفيذ عمليات سيبرانية في الخارج. وتؤكد الحكومة الصينية على أهمية الأمن السيبراني باعتباره قضية أمن قومي، وتشجع شركات التكنولوجيا على الالتزام بالمبادئ التوجيهية للدولة، بما في ذلك قوانين توطين البيانات الصارمة ضمن معايير حماية عالية ومعقدة. (Intimedia, 2024) (44) فالحكومة الصينية، طبقت قانون الأمن السيبراني عام 2017 والذي يلزم شركات التكنولوجيا الأجنبية بتخزين بيانات المواطنين الصينيين داخل البلاد. يهدف هذا الإجراء إلى منع تسريب بيانات المواطنين الصينيين إلى الخارج والحد من احتمالية وقوع هجمات إلكترونية أجنبية. (Intimedia, 2024) (45) دخل القانون حيز التنفيذ في الأول من حزيران عام 2017 وبالإضافة إلى كونه يلزم مشغلي الشبكات بتخزين بيانات محددة داخل الصين، فإنه يسمح للسلطات الصينية بإجراء عمليات تفتيش عشوائية على عمليات شبكات الشركات، إذ تؤكد بكين أن القانون يهدف إلى مواكبة الصين لأفضل الممارسات العالمية في مجال الأمن السيبراني. (Jack Wagner, 2017) (46)

Strong DM website, **Equifax Data Breach: What Happened and How to Prevent It**, 06/03/2025, <https://www.strongdm.com/what-is/equifax-data-breach> تاريخ الزيارة: 10/04/2025.

Eugenia Lostri, James Andrew Lewis, and Georgia Wood, Center for Strategic and International Studies, **A Shared Responsibility: Public-Private Cooperation for Cybersecurity**, 2022.

Intimedia website, **Unveiling China's Cyber Defense: How China Protects Itself from International Cyber Attacks**, 07/08/2024, (44) <https://intimedia.id/read/unveiling-chinas-cyber-defense-how-china-protects-itself-from-international-cyber-attacks> تاريخ الزيارة: 11/04/2025.

(45) المرجع نفسه.  
Jack Wagner, The Diplomat website, **China's Cybersecurity Law: What You Need to Know**, 01/06/2017, (46) <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know> تاريخ الزيارة: 12/04/2025.

## الفرع الثاني

### تداعيات الحرب السيبرانية على الامن العالمي

ان للحرب السيبرانية بين الولايات المتحدة الأمريكية والصين كما للحرب الاقتصادية بشكل خاص وكما للحرب التكنولوجية بشكل عام، تداعيات على الامن العالمي والاستقرار على أكثر من صعيد. تمثل الحرب السيبرانية بين البلدين نموذجًا مصغراً للتنافس الجيوسياسي الاشملي. ويعكس التنافس التكنولوجي الذي يُحرك هذا الصراع مخاوف عميقة بشأن الاستقرار الاقتصادي والأمن القومي ومستقبل الحوكمة العالمية. ومع استمرار الدولتين في تعزيز قدراتهما السيبرانية، تُصبح الحاجة إلى استجابة منسقة لإدارة التهديدات السيبرانية أمرًا بالغ الأهمية. في عالم تتوسع فيه الحدود الرقمية باستمرار، قد يعتمد توازن القوى بين الدول بشكل متزايد على قدرتها على التعامل مع تعقيدات الحرب السيبرانية والدبلوماسية الدولية والمشهد التكنولوجي المتطور. وفي نهاية المطاف، لن يُشكل حل هذا التنافس السيبراني مستقبل العلاقات الأمريكية الصينية فحسب، بل ستكون له أيضًا عواقب بعيدة المدى على الاستقرار والأمن العالميين.

فعلى صعيد الاقتصاد، ومع اشتداد التنافس السيبراني، يتأثر الاقتصاد العالمي بشكل متزايد بالحرب السيبرانية إذ يساهم تصاعدها في تعزيز حالة عدم اليقين لدى الشركات متعددة الجنسيات العاملة في كلى السوقين. وقد دفعت المخاوف المتزايدة بشأن سرقة الملكية الفكرية خصوصية البيانات، والامتثال للأنظمة، والشركات إلى إعادة تقييم استراتيجياتها لإدارة المخاطر والعمل على ضمان توفير البيئة المنبئة امام التهديدات السيبرانية المحتملة عبر التوسع في الإجراءات الحمائية ورصد جزء من ميزانيتها لمواجهة المخاطر السيبرانية التي ممكن ان تطرأ على أنظمتها في أي لحظة في المستقبل. تواجه المؤسسات عالميًا تكاليف متزايدة تتعلق بتدابير الأمن السيبراني استجابةً للتهديدات. ووفقا لذلك، يتعين على الشركات تخصيص موارد كبيرة للدفاع ضد التهديدات السيبرانية بدلاً من الاستثمار في النمو والتطوير. فبالنسبة للعديد من الشركات، وخاصةً الصغيرة منها، قد يكون العبء المالي للحفاظ على الأمن السيبراني غير كافٍ، مما يؤدي إلى انخفاض قدرتها التنافسية. (سكاي نيوز بالعربية، 2023)<sup>(47)</sup> ان الحرب السيبرانية قد تكبد الشركات تكاليف إضافية ليست بالحساب لحماية موقعها في ظل تحديات الأمن السيبراني، الامر الذي يزيد من التكاليف الإجمالية الملقاة على عاتقها.

ومن ناحية أخرى، تخلق الحرب السيبرانية اضطرابات في سلاسل التوريد مما يحدث تأخيرات في حركة الشحن العالمي ويؤثر مباشرة على الأسواق وتوافر السلع كما حدث عام 2017 مع كبرى شركات النقل البحري الأمريكية ميرسك لاين حين أدى هجوم سيبراني متقن على شبكات حاسوب شركة ميرسك لاين الى اغلاقه لمدة أسبوعين حيث توقفت حركة النقل البحري للحاويات كليا في 17 مرفأ تابعه للشركة حول العالم وأدى الى خسائر اقتصادية تقدر ب ثلاثمئة مليون دولار أميركي. (Jordan–Novet, 2017)<sup>(48)</sup> فالنقل البحري وتحديدًا المتعلق بالحاويات يعتبر من ركائز سلاسل التوريد العالمية إذ يؤثر مباشرة بإمداد الأسواق العالمية بالسلع و المنتجات.

<sup>(47)</sup> موقع سكاي نيوز بالعربية، كيف يهدد تطور الهجمات السيبرانية الاقتصاد العالمي؟ 15/11/2023، [www.skynewsarabia.com/business/1670391](http://www.skynewsarabia.com/business/1670391) -يهدد-تطور-الهجمات-السيبرانية-الاقتصاد-العالمي؟ تاريخ الزيارة: 10/04/2025.

<sup>(48)</sup> Jordan Novet, CNBC website, **Shipping company Maersk says June cyberattack could cost it up to \$300 million**, 16/08/2017, <https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html> تاريخ الزيارة: 07/04/2025.

بالإضافة إلى ذلك، تبذل الشركات في القطاعات الأساسية، مثل القطاعين المالي والاتصالات، جهودًا أكبر لتأمين بنيتها التحتية في ظل العلاقات التجارية المعقدة بين الولايات المتحدة والصين. وغالبًا ما تتجاوز الآثار الاقتصادية للحرب السيبرانية الخسائر المباشرة، مما قد يُعيق الابتكار والتعاون.

ان الهجمات السيبرانية التي يقوم بها المهاجمون الإلكترونيون من شأنها ان تعطل الاقتصاد عبر اختراق الأنظمة الحيوية الضرورية للمعاملات المالية، مثل والبنوك والبورصات وأنظمة الدفع وأنظمة التداولات المالية العالمية اذ يمكن أن تؤدي هذه الهجمات إلى توقف المعاملات المالية، مسببةً أضرارًا اقتصادية ومالية ضخمة. (Sona Poghosyan, 2023)<sup>(49)</sup> و من الهجمات السيبرانية التي كان لها تداعيات اقتصادية عالمية خطيرة هجوم " واناكراي" الذي بدأ هجوم 12 مايو 2017، وهو غير مسبوق من حيث الحجم، حيث أثر بسرعة على ما يقرب من ربع مليون جهاز كمبيوتر في أكثر من 150 دولة. (Lawrence Trautman, 2018, Page 522)<sup>(50)</sup> احدث هذا الهجوم خسائر كبيرة في الأسواق المالية العالمية و في الشركات التي طالها هذا الهجوم بشكل مباشر او غير مباشر. (Sona Poghosyan, 2023)<sup>(51)</sup>

على صعيد آخر، تساهم الحرب السيبرانية في إعادة تشكل العلاقات الدبلوماسية حيث تعزز هذه الحرب الاصطفاف السياسي وتعيد ترتيب تموضع الدول بين من هو أقرب الى الولايات المتحدة ومن هو أقرب الى الصين اذ أصبح الأمن السيبراني ركيزة أساسية في العلاقات الثنائية، مؤثرًا على المناقشات حول التعاون الدفاعي، وتبادل المعلومات الاستخباراتية، والاتفاقيات التجارية. فالولايات المتحدة الاميركي وفي إطار مساعها الى مواجهة الخطر السيبراني الصيني وتقوية الردع وتعزيز الجاهزية، لجأت الى تمثين تعاونها مع حلفائها، وبالأخص الدول الاعضاء في حلف شمال الأطلسي. (شريفه كلاج، 2022، ص 1022)<sup>(52)</sup> وقد زادت الولايات المتحدة تركيزها على الأمن السيبراني في أجندتها للسياسة الخارجية، مما أثر على التحالفات والشراكات الدولية. لقد أصبح الأمن السيبراني عنصرًا أساسيًا في تعامل الولايات المتحدة مع حلفائها، كما يتضح من مبادرات مثل الحوار السيبراني بين الولايات المتحدة والاتحاد الأوروبي، وشراكات الأمن السيبراني مع دول منطقة المحيطين الهندي والهادئ.

اما الصين فعزيزت من تعاونها السيبراني مع روسيا في مواجهة التحالف الغربي منذ عام 2015 حين وقعت البلدان اتفاقية ثنائية للتعاون في مجال أمن المعلومات الدولي. تحدد هذه المعاهدة، التدابير التعاونية التي تتعهد الحكومتان باتخاذها فيما يخص الفضاء السيبراني، بما في ذلك تبادل المعلومات وتعزيز التعاون العلمي والأكاديمي. (Elaine Korzak, 2015)<sup>(53)</sup> وقد استمر هذا النهج من

Sona Paghosyan, *The Impact of Cyber Warfare on Global Financial Markets*, 27/04/2023, <https://plat.ai/blog/cyber-warfare-and-global-financial-market> (49) تاريخ الزيارة: 10/03/2025.

Lawrence Trautman and Peter Ormerod, (2018) *Wannacry, Ransomware, and the Emerging Threat to Corporations*, SSRN Electronic Journal, Vol 86, Page 522. (50)

(51) مرجع سابق، Sona Poghosyan.

(52) شريفه كلاج، الصراع الروسي الصيني الأمريكي للاستحواذ على الهيمنة في الفضاء السيبراني، مجلة السياسة العالمية، العدد 6، رقم 1، الجزائر 2022. ص 1022.

Elaine Korzak, Council on Foreign Relations website, *The Next Level for Russia-China Cyberspace Cooperation?*, 20/08/2015, (53) <https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation> تاريخ الزيارة: 15/04/2025.

التعاون وتعزز حيث أصبح التعاون وتبادل المعلومات في الفضاء السيبراني بين البلدين مدعاة للقلق والاهتمام الأميركي. (Bhagyashree Garekar, 2024)<sup>(54)</sup>

على صعيد آخر، سعت الصين إلى تعزيز صورتها كضحية للعدوان السيبراني الأمريكي. وانخرطت في إجراءات لمكافحة التجسس، وصاغت استراتيجيتها للأمن السيبراني ضمن سياق أوسع يمثل في حماية سيادة الدولة ورفض التدخلات الخارجية.

لا يزال مستقبل الحرب السيبرانية بين الولايات المتحدة الأمريكية والصين غامضاً، نتيجةً لبيئة متغيرة باستمرارٍ وتقدمٍ تكنولوجيٍّ سريع. ومع استمرار الدولتين في تطوير تقنياتٍ جديدة، ستزداد المخاطر المرتبطة بالعمليات السيبرانية.

مع استمرار التطور السريع للتكنولوجيا، أدى تأثيره على مختلف القطاعات، بما في ذلك الدفاع والتجارة والاتصالات، إلى سباقٍ محمومٍ على التفوق بين القطبين الولايات المتحدة والصين. وتشمل التقنيات الأساسية في قلب هذا الصراع البنية التحتية للاتصالات، وتقنيات الذكاء الاصطناعي، وشبكات الجيل الخامس المتطورة، والاقتصادات الرقمية. ترمي استراتيجيات كل دولة للسيطرة على هذه القطاعات، على إعادة تعريف التحالفات، وإعادة تشكيل العلاقات التجارية والسياسية، وتغيير ميزان القوى على الساحة العالمية. فالولايات المتحدة تسعى إلى الحفاظ على هيمنتها الدولية بينما تسعى الصين إلى تغيير الواقع الحالي السائد.

تشكل الأدوات غير العسكرية جانبا مهما في المواجهة التكنولوجية الكبرى بين الولايات المتحدة الأمريكية والصين. فجزء أساسي من المواجهة بين البلدين يتمظهر من خلال حرب ناعمة لا تقل خطورة وديناميكية عن الحرب العسكرية بالأدوات الحربية التقليدية. فمن الحرب الاقتصادية التي تشمل مواجهات تجاربه حاده وقيود على الاستثمارات وصولاً إلى الحرب السيبرانية المستعرة التي تحاكي استثمار أحدث الوسائل التكنولوجية التي وصل إليها العلم الحديث لمواجهة الخصم واستهدافه في الفضاء السيبراني والعالم الافتراضي، بات جليا ان المواجه بين الطرفين سينحى منحى تصاعدي في المستقبل تكتسب من خلاله خيارات أخرى مثل الخيارات التصادم العسكري حيزا مهما في قراءة المشهد العام وآفاق مستقبل الصراع بينهما.

## الخلاصة

يشهد العالم اليوم حرباً تكنولوجية شديدة بين الولايات المتحدة الأمريكية والصين، يشكل فيها السعي لامتلاك التكنولوجيا الأكثر تطوراً، نوعاً جديداً من سباق التسلح بين القطبين كالذي جرى في الحرب الباردة بين الولايات المتحدة والاتحاد السوفياتي. ولكن هذه المرة، فإن التكنولوجيا هي محور هذا السباق.

لقد تطرق هذا البحث إلى مظاهر المواجهة الناعمة حيث تتمظهر الحرب التكنولوجية بين الولايات المتحدة والصين حالياً عبر سيناريوهات ناعمة لاتزال بعيدة عن الحرب العسكرية المباشرة. من أبرز مظاهر الحرب الناعمة الدائرة بين القطبين هي الحرب الاقتصادية

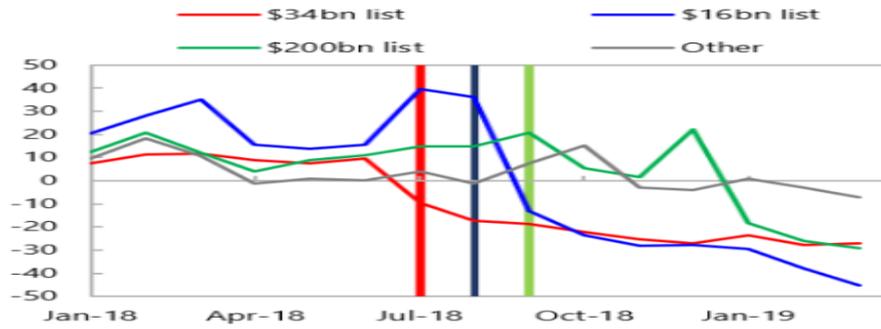
Bhagyashree Garekar, The Strait Times website, **China–Russia links in cyberspace are a source of concern, says America’s top cyber warrior**, 22/11/2024, <https://www.straitstimes.com/asia/east-asia/china-russia-links-in-cyberspace-are-a-source-of-concern-says-america-s-top-cyberwarrior> تاريخ الزيارة: 16/04/2025.

التي تقوم عبر الإجراءات التجارية الصارمة بين الطرفين، والحرب السيبرانية التي تقوم عبر الهجمات السيبرانية التي تستهدف البنى التحتية الأساسية للخصم، مع اشتداد معالم هذه التوترات في الأونة الأخيرة، تبرز أماننا احتماليه تدرج هذه التوترات الى مواجهة عسكريه مباشره. وإزاء هذا الاحتمال الذي لا يمكن استبعاد إمكانية حصوله بشكل قاطع، فإننا نخلص الى الاستنتاجات التالية:

- 1- ان الصراع الحالي بين الولايات المتحدة والصين سيستمر في المسار نفسه، أي المواجهة الناعمة، وسيتصاعد ضمن قواعد اشتباك محدده من دون التدرج الى حرب عسكريه مباشره بقناعة ضمنية مشتركة بينهما تفرضها الوقائع الجيوسياسية والواقعية في فهم الوضع القائم.
- 2- بالنسبة للولايات المتحدة الأمريكية، فان الوضع الجيوسياسي المعقد السائد والمتمثل ببؤر توتر وصراعات استراتيجيه قائمة مثل الحرب الروسية الأوكرانية والصراع العربي الإسرائيلي والملف النووي الإيراني، والتي تُعتبر الولايات المتحدة شريكاً أساسياً فيها كلها وتأتي في صلب اهتماماتها ومصالحها القومية، يحتم عليها منطقياً تجنب فتح مواجهة عسكريه مباشرة مع الصين قبل انقشاع نتائج الصراعات القائمة. فالصدام العسكري مع الصين هو قرار استراتيجي حساس وتترتب عليه نتائج خطيرة وهو بحاجة الى تفرغ كلي من الولايات المتحدة بكل مقدراتها وطاقاتها وإمكاناتها وعدم انشغالها في ملفات أخرى. ولذلك فإننا نرى ان الحرب العسكرية هو خيار مستبعد بالمدى المنظور وان الولايات المتحدة ستكتف من التصعيد عبر ادواتها الحالية وبخاصة الحرب الاقتصادية للضغط على الصين ومحاولة عرقلتها قدر الإمكان.
- 3- اما بالنسبة للصين، فإننا إذا نظرنا الى مقاربتها الاستراتيجية لجميع الملفات منذ عقود حتى الآن، نجد انها تتبع السياسة الناعمة وتوظف الأدوات الناعمة لتحقيق أهدافها الاستراتيجية بعيدة المدى. ان الصين تدرك حق الإدراك انها في وضعها العسكري الراهن ليس لها حظوظ في حسم أي مواجهة عسكريه مع الولايات المتحدة. فالأخيرة لاتزال تتمتع بتفوق عسكري ساحق لا يمكن مجاراته. ولهذا فان مصلحة الصين العليا تكمن في تجنب الصدام العسكري مع الولايات المتحدة والعمل على تغليب الحلول الدبلوماسية. اما فيما يخص الاستراتيجية الصينية لمواجهة الولايات المتحدة وحربها الاقتصادية، فان الصين ستستمر في مسار تحقيق اهداف رؤيتها الاستراتيجية المرسومة في مجال التكنولوجيا والاقتصاد عبر توظيف الأدوات الناعمة لمنافسة الولايات المتحدة وتعزيز موقعها في المعادلات الدولية.

## الملاحق

**Large drop**  
 US imports from China have fallen significantly in all three groups of goods after tariffs were imposed.  
 (value of imports, year-on-year percent change)



Sources: US Department of Commerce; and IMF staff calculations.  
 Note: Tariff-effective dates: July 6, 2018, 25% on initial \$34 billion list; Aug 23, 2018, 25% on \$16 billion list; Sept. 24, 2018, 10% on \$200 billion list, rising to 25% on May 10, 2019.

<https://www.imf.org/en/Blogs/Articles/2019/05/23/blog-the-impact-of-us-china-trade-tensions>

المصدر:

المراجع:

ريببكا فانين، التنين الصيني وسباق التكنولوجيا، (2010)، ترجمة، محمد فتحي، محمد جبريل، مجموعة النيل العربية، القاهرة.  
 Michael Gross and Tamar Meisels, (2017), **Soft War, The Ethics of Unarmed Conflicts**, Cambridge University Press, UK.

Muhammad Ali Baig, Dost Barresh and Talal Shabbir, **The US–China Trade War: Hard Implications**  
 Anna Swanson,(2023), New York Times website, **of a Soft War**, BTTN Journal, Vol 2, Issue 1.  
**Trump’s Trade War with, China Is Officially Underway**, 05/07/2018,  
 تاريخ الزيارة: <https://www.nytimes.com/2018/07/05/business/china-us-trade-war-trump-tariffs.html>  
 .10/04/2025

رمزي محمود،(2022)، صراع أمريكا والصين على عرش الاقتصاد العالمي، دار التعليم الجامعي، القاهرة، ص 217.  
 BBC News website, **China hits back after US imposes tariffs worth \$34bn**,06/07/2018,  
 تاريخ الزيارة: <https://www.bbc.com/news/business-44707253>  
 .08/04/2025

Chetean Ahya, Morgan Stanley website, **Why Trade Tariffs Could Rattle the Global Supply Chain?**  
 تاريخ الزيارة: 22/08/2018, <https://www.morganstanley.com/ideas/trade-tariffs-supply-chain>  
 .15/04/2025

Reuters Website, **Trump threatens additional tariffs on China, terminates talks**, 07/04/2025,  
<https://www.reuters.com/world/us/trump-threatens-additional-tariffs-china-terminates-talks-2025-07-04/>  
 تاريخ الزيارة: 07/04/2025.

موقع سي ان ان بالعربية، أول رد من الصين بعد دخول تعريفات الـ 104% لترامب حيز التنفيذ، 09/04/2025،  
<https://arabic.cnn.com/world/article/2025/04/09/china-vows-resolute-measures-trumps-tariffs-take-effect>  
 تاريخ الزيارة: 08/05/2025.

Swiss Info website المزارعون الأميركيون "قلقون" من تأثير الرسوم الجمركية على مداخلهم، 06/04/2025،  
<https://www.swissinfo.ch/ara/%d8%a7%d9%84%d9%85%d8%b2%d8%a7%d8%b1%d8%b9%d8%b1>  
 تاريخ الزيارة: 08/04/2025.

Anna Swanson, New York Times website, **Trump Gives Farmers \$16 Billion in Aid Amid Prolonged China Trade War**, 23/05/2025,  
<https://www.nytimes.com/2019/05/23/us/politics/farm-aid-package.html>  
 تاريخ الزيارة: 10/08/2025.

Eugenio Cerutti, Gita Gopinath and Adil Mahmoud, IMF Blog website, **The Impact of US-China Trade Tensions**, 23/05/2019,  
<https://www.imf.org/en/Blogs/Articles/2019/05/23/blog-the-impact-of-us-china-trade-tensions>  
 تاريخ الزيارة: 11/04/2025.

CNBC Arabia website, تقرير لـ QNB: عدم اليقين بشأن السياسات الأميركية التجارية والمالية يثير مخاوف الركود،  
[www.cnbcarabia.com/135810/2025/23/03-QNB-عدم-اليقين-بشأن-السياسات-الأميركية-التجارية-والمالية-يثير-مخاوف-الركود](http://www.cnbcarabia.com/135810/2025/23/03-QNB-عدم-اليقين-بشأن-السياسات-الأميركية-التجارية-والمالية-يثير-مخاوف-الركود)  
 تاريخ الزيارة: 12/04/2025.

مصطفى مقلد، مركز شاف للدراسات المستقبلية وتحليل الازمات والصراعات، الحرب التجارية الصينية: من التكيف الى المواجهة،  
<https://shafcenter.org/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8-%D8%A7%D9%84%D8%AD%D8%B1%D8%A8>  
 تاريخ الزيارة: 08/04/2025  
 13/04/2025

Holland and Knight website, **Outbound Investment Screening Rule Goes into Effect, Final Rule Targets U.S. Investment in Chinese or Chinese-Owned Companies**, 10/01/2025,  
<https://www.hklaw.com/en/insights/publications/2025/01/outbound-investment-screening-rule-goes-into-effect>  
 تاريخ الزيارة: 15/04/2025.

Paul Edelberg, Fox Rothschild website, **Investments in Chinese Technology Companies Limited by New US Outbound Investment Rule**, 13/01/2025,

<https://www.foxrothschild.com/publications/investments-in-chinese-technology-companies-limited-by-new-us-outbound-investment-rule>  
تاريخ الزيارة: 09/04/2025.

John Bateman, (2022), **US-China Technological Decoupling, A Strategy and Policy Framework**, Carnegie Endowment for International Peace, Washington.

Noah Berman, Lindsay Miazland, and Andrew Chatzky, **Is China's Huawei a Threat to U.S. National Security?**, 08/02/2023, <https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security>  
تاريخ الزيارة: 10/04/2025.

The US Department of the Treasury, **The Committee on Foreign Investment in the United States (CFIUS)**, <https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius>  
تاريخ الزيارة: 11/04/2025.

Guillermo S. Christensen, Steven F. Hill, Brian J. Hopkins, Nathaniel B. Bolin, David R. Allman and Jeffrey Orenstein, K&L Gates website, **Trump Administration Directs CFIUS to Tighten Restrictions on Investment From Certain Countries While Easing National Security Reviews of Investments From Allies and Partners**, 26/02/2025, <https://www.klgates.com/Trump-Administration-Directs-CFIUS-to-Tighten-Restrictions-on-Investment-From-Certain-Countries-While-Easing-National-Security-Reviews-of-Investments-From-Allies-and-Partners-2-26-2025>  
تاريخ الزيارة: 26/02/2025.

Giulia Interesse, China Briefing website, **S Investment Ban on China: What it Means Now That it's in Effect**, 15/01/2025, <https://www.china-briefing.com/news/us-investment-ban-on-china-what-it-means-now-that-its-in-effect>  
تاريخ الزيارة: 10/04/2025.

موقع سكاى نيوز بالعربية، **الريادة الأميركية في الذكاء الاصطناعي تحت تهديد "ديب سيك"**, 29/01/2025, <https://www.skynewsarabia.com/business/1773018->  
تاريخ الزيارة: 09/04/2025.

PJ Rosario Kumar, (2025), **REVOLUTIONIZING THE SEARCH GAME HOW DEEPSEEK IS TRANSFORMING INFORMATION-SEEKING BEHAVIOR IN THE DIGITAL AGE**, International Journal of Scientific Research in Engineering and Management, Volume: 09 Issue: 02.

Mariano Florentino Cuellar and Christopher Chivis, (2024), **U.S.-China Relations for the 2030s: Toward a Realistic Scenario for Coexistence**, Carnegie Endowment for International Peace Publications Department 1779 Massachusetts Avenue NW Washington, DC 20036.

Bureau of Industry and Security, **Commerce Strengthens Export Controls to Restrict China's Capability to Produce Advanced Semiconductors for Military Applications**, 02/12/2024, <https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced-semiconductors-military> تاريخ الزيارة: 12/04/2025.

موقع سكاي نيوز بالعربية، الصين تتهم أميركا بـ "الحماية" و"التنمر الاقتصادي" 07/04/2025، [https://www.skynewsarabia.com/world/1788407-%D8%A7%D9%84%D8%B5%D9%8A%D9%86-%D8%AA%D8%AA%D9%87%D9%85-](https://www.skynewsarabia.com/world/1788407-%D8%A7%D9%84%D8%B5%D9%8A%D9%86-%D8%AA%D8%AA%D9%87%D9%85) تاريخ الزيارة: 15/04/2025.

Alexander S. Gills, TechTarget website, **what is Cyberwarfare?** <https://www.techtarget.com/searchsecurity/definition/cyberwarfare> تاريخ الزيارة: 10/04/2025.

Paulo Shakarian, Jana Shakarian and Andrew Ruef,(2013), **Introduction to Cyber Warfare, A Multidisciplinary Approach**, Syngress, 225 Wyman Street, Waltham, MA, USA.

Steve Morgan, Cyber Security Ventures website, **Cybercrime to Cost the World \$10.5 Trillion Annually By 2025**,13/11/2020, <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016> تاريخ الزيارة: 15/04/2025.

US Cyber Command website, <https://www.cybercom.mil/About/History> تاريخ الزيارة: 15/04/2025.

Christopher Bing, Reuters website, **FBI says Chinese hackers preparing to attack US infrastructure**, 19/04/2024, <https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18> تاريخ الزيارة: 16/04/2025.

Hadley Spadaccini, **Risks are higher than ever for US- China cyber war**, 18/04/2024, <https://responsiblestatecraft.org/us-china-cyberwar> / تاريخ الزيارة: 14/04/2025.

آدم سيغال، موقع اندبنت بالعربية، الصين تصعد تهديداتها في الفضاء السيبراني، 25/01/2025 [www.independentarabia.com/node/616375](http://www.independentarabia.com/node/616375) /آراء/الصين-تصعد-تهديداتها-في-الفضاء-السيبراني تاريخ الزيارة: 15/04/2025.

Dirk Schrader, Netwrix, Community website, **The Largest and Most Notorious Cyber Attacks in History**,17/12/2024, <https://blog.netwrix.com/biggest-cyber-attacks-in-history> تاريخ الزيارة: 10/04/2025.

The Guardian website, OPM hack: China blamed for massive breach of US government data, 05/06/2015, <https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances> تاريخ الزيارة: 15/04/2025.

Strong DM website, Equifax Data Breach: What Happened and How to Prevent It, 06/03/2025, <https://www.strongdm.com/what-is/equifax-data-breach> تاريخ الزيارة: 10/04/2025.

Eugenia Lostri, James Andrew Lewis, and Georgia Wood, (2022), Center for Strategic and International Studies, **A Shared Responsibility: Public-Private Cooperation for Cybersecurity.**

Intimedia website, **Unveiling China's Cyber Defense: How China Protects Itself from International Cyber Attacks**, 07/08/2024, <https://intimedia.id/read/unveiling-chinas-cyber-defense-how-china-protects-itself-from-international-cyber-attacks> تاريخ الزيارة: 11/04/2025.

Jack Wagner, The Diplomat website, **China's Cybersecurity Law: What You Need to Know**, 01/06/2017, <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know> تاريخ الزيارة: 12/04/2025.

موقع سكاى نيوز بالعربية، كيف يهدد تطور الهجمات السيبرانية الاقتصاد العالمي؟، 15/11/2023، [www.skynewsarabia.com/business/1670391](http://www.skynewsarabia.com/business/1670391) يهدد-تطور-الهجمات-السيبرانية-الاقتصاد-العالمي؟ تاريخ الزيارة: 10/04/2025.

Jordan Novet, CNBC website, **Shipping company Maersk says June cyberattack could cost it up to \$300 million**, 16/08/2017, <https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html> تاريخ الزيارة: 07/04/2025.

Sona Paghosyan, **The Impact of Cyber Warfare on Global Financial Markets**, 27/04/2023, <https://plat.ai/blog/cyber-warfare-and-global-financial-market> تاريخ الزيارة: 10/03/2025.

Lawrence Trautman and Peter Ormerod, (2018), **Wannacry, Ransomware, and the Emerging Threat to Corporations**, SSRN Electronic Journal, Vol 86.

شريف كلاع، (2022) الصراع الروسي الصيني الأمريكي للاستحواذ على الهيمنة في الفضاء السيبراني، مجلة السياسة العالمية، العدد 6، رقم 1، الجزائر 1022.

Elaine Korzak, Council on Foreign Relations website, **The Next Level for Russia–China Cyberspace Cooperation?**, 20/08/2015, <https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation> تاريخ الزيارة: 15/04/2025.

Bhagyashree Garekar, The Strait Times website, **China–Russia links in cyberspace are a source of concern, says America’s top cyber warrior**, 22/11/2024, <https://www.straitstimes.com/asia/east-asia/china-russia-links-in-cyberspace-are-a-source-of-concern-says-america-s-top-cyberwarrior> تاريخ الزيارة: 16/04/2025.

## “Scenarios of Soft Confrontation Between the United States and China”

**Researcher:**

**Hamid Mahmoud Khudra**

### **Abstract:**

This study seeks to explain the scenarios of soft confrontation resulting from the ongoing technological war between the United States and China by addressing economic warfare and cyber warfare as the two main aspects of this confrontation.

The study concludes that while a soft confrontation between the United States and China is the most likely expected path for the confrontation between the two poles, this does not entirely negate the possibility of the situation escalating into unforeseen military clashes that could spark a major military war between them.

**Keywords:** Technological War; Soft Confrontation; Economic War; Cyber Warfare; The United States; China.