

إعادة هندسة الاقتصاد عبر الأمن السيبراني في ظل العقوبات الدولية: إيران أنموذجاً بعد عام 2018

م. م. آية علي عبدالله

كلية القانون والعلوم السياسية، جامعة ديالى، ديالى، 32001 ، العراق.

ayaali2023@uodiyala.edu.iq

المخلص

يتناول هذا البحث مفهوم الهندسة الاقتصادية للأمن السيبراني في ظل العقوبات الدولية، من خلال دراسة الحالة الإيرانية بعد عام 2018. وتتمثل إشكاليته في التساؤل حول كيفية تمكن دولة خاضعة لعقوبات شديدة من إعادة اقتصادها باستخدام الأدوات الرقمية والسيبرانية، وما حدود فاعلية هذا النموذج في الاستمرار والتكيف. وهدف البحث إلى توضيح الكيفية التي دفعت بها العقوبات إيران إلى بناء قنوات اقتصادية موازية عبر بنوك الظل، وشركات الواجهة، والعملات المشفرة، والبنى السيبرانية الداعمة لها. واعتمد البحث المنهج الاستقرائي والأسلوب الوصفي-التحليلي في تفسير العلاقة بين العقوبات الدولية وصعود الاقتصاد الرقمي الموازي في إيران. وخلصت الدراسة إلى أن الأمن السيبراني لم يعد مجرد وسيلة دفاعية، بل أصبح جزءاً من إدارة الاقتصاد وإعادة هندسته في بيئة العقوبات، إذ أسهم في تمكين استمرار التدفقات المالية والتجارية عبر قنوات بديلة. كما أظهرت النتائج أن هذا النموذج حقق قدراً من التكيف والاستمرارية، لكنه بقي مرتفع الكلفة وهشاً أمام تطور أدوات الرقابة الدولية والتتبع المالي. ويستشرف البحث ثلاثة مسارات مستقبلية، يبقى بينها سيناريو الاستمرار التكيفي هو الأقرب للواقع.

الكلمة المفتاحية: العقوبات الدولية، الاقتصاد الموازي، بنوك الظل، العملات المشفرة، الأمن السيبراني، شركات الواجهة.

Reengineering the Economy through Cybersecurity under International Sanctions: Iran as a Model after 2018

Assist. Lect. Aya Ali Abdullah

College of Law and Political Science, University of Diyala, Diyala, 32001, Iraq

ayaali2023@uodiyala.edu.iq

Abstract

This study examines the concept of economic reengineering through cybersecurity under international sanctions, focusing on the Iranian case after 2018. Its central research problem concerns how a state subjected to severe sanctions has been able to reengineer its economy through digital and cyber tools, and the extent to which this model can remain effective in terms of continuity and adaptation. The study aims to explain how sanctions have driven Iran to establish parallel economic channels through shadow banks, front companies, cryptocurrencies, and the cyber infrastructure supporting them. The study adopts an inductive approach and a descriptive-analytical method to examine the relationship between international sanctions and the emergence of Iran's parallel digital economy. The study concludes that cybersecurity is no longer merely a defensive instrument; rather, it has become an integral component of economic management and reengineering in a sanctions

environment, contributing to the continuation of financial and commercial flows through alternative channels. The findings also demonstrate that this model has achieved a certain degree of adaptability and continuity; however, it remains costly and vulnerable to the development of international monitoring mechanisms and financial-tracking technologies. The study anticipates three possible future trajectories, among which the adaptive-continuity scenario appears to be the most realistic.

Keywords: International sanctions, parallel economy, shadow banks, cryptocurrencies, cybersecurity, front companies.

المقدمة

شهد النظام الاقتصادي الدولي في السنوات الأخيرة تزايداً في توظيف الأدوات الاقتصادية وأهمها العقوبات المالية والتجارية، بوصفها آلية للضغط السياسي وإعادة تشكيل سلوك الدول المستهدفة. وفي هذا السياق، تبرز الحالة الإيرانية باعتبارها نموذجاً لتفاعل دولة خاضعة لعقوبات واسعة مع القيود المفروضة عليها من خلال مسارات لا تقتصر على التكيف التقليدي، بل تمتد إلى إعادة بناء بنيته الاقتصادية الرقمية وتكييفها سبيرانياً.

فقد أسهمت العقوبات، ولا سيما بعد عام 2018، في تقليص قدرة إيران على الوصول إلى النظام المالي العالمي، الأمر الذي دفعها إلى تطوير قنوات اقتصادية موازية عبر بنوك الظل وشركات الواجهة ومنصات العملات المشفرة. وفي هذا السياق، أصبح الأمن السبيري جزءاً من البنية الداعمة لهذه القنوات، بما يبرر دراسته بوصفه أحد مكونات إعادة تنظيم الاقتصاد في بيئة العقوبات.

أولاً/ أهمية البحث

تتبع أهمية البحث من عدة اعتبارات علمية وعملية، أبرزها:

1. تسليط الضوء على نمط جديد من التكيف الاقتصادي يعتمد على الأدوات الرقمية والسبيرية في مواجهة العقوبات.
2. الإسهام في تطوير فهم أعمق للعلاقة بين الأمن السبيري والاقتصاد السياسي الدولي.
3. تحليل دور الاقتصاد الموازي والعملات المشفرة كآليات لإعادة تشكيل التدفقات المالية.
4. تقديم إطار تحليلي يمكن تطبيقه على حالات مشابهة لدول خاضعة للعقوبات.
5. استشراف مستقبل هذا النموذج في ظل تطور أدوات الرقابة والتتبع الدولية.

ثانياً/ هدف البحث

يسعى هذا البحث إلى تحقيق مجموعة من الأهداف أبرزها:

1. تحليل دور الأمن السبيري في إعادة تشكيل الاقتصاد الإيراني ضمن بيئة العقوبات.
2. دراسة البنية المؤسسية والأدوات السبيرية المستخدمة وتقييم فاعلية هذه الأدوات في تجاوز القيود الدولية.
3. تقييم فاعلية هذا النموذج وحدوده واستشراف الافاق المستقبلية في ظل المتغيرات الدولية.

ثالثاً/ إشكالية البحث

تتمحور إشكالية البحث حول التحول في طبيعة العلاقة بين الأمن السبيري والاقتصاد في ظل العقوبات الدولية، حيث لم يعد الأمن السبيري مقتصرًا على حماية الأنظمة، بل أصبح جزءاً من عملية إعادة تشكيل الاقتصاد نفسه. وعليه، تتمثل مشكلة البحث في التساؤل عن: كيف يمكن للدول الخاضعة لعقوبات شديدة أن تعيد هندسة اقتصادها باستخدام الأدوات السبيرية، وما حدود فاعلية هذا النموذج؟ ويتفرع منه مجموعة من التساؤلات الفرعية:

1. ما المقصود بمفهوم الهندسة الاقتصادية للأمن السبيري؟
2. كيف تؤثر العقوبات الدولية في إعادة تشكيل البنية الاقتصادية للدول؟
3. ما دور بنوك الظل وشركات الواجهة في الاقتصاد الإيراني؟ وكيف تُستخدم العملات المشفرة كبديل للنظام المالي التقليدي؟
4. ما هي الأدوات السبيرية التي تعتمد عليها إيران في إدارة اقتصادها الموازي؟
5. ما حدود فاعلية هذا النموذج في ظل تطور الرقابة الدولية، وما المشاهد المستقبلية المحتملة؟

رابعاً/ فرضية البحث

ينطلق البحث من الفرضية الرئيسية الآتية: كلما تصاعدت العقوبات الاقتصادية زاد اعتماد إيران على الأدوات الرقمية والسيبرانية كأداة لإعادة هندسة اقتصادها، بما يؤدي إلى نشوء اقتصاد رقمي- مالي موازٍ قادر نسبياً على التكيف مع القيود، إلا أن فاعلية هذا النموذج تبقى نسبية ومقيدة بتطور أدوات التتبع والضغط الدولي.

خامساً/ منهجية البحث

يعتمد البحث على استخدام المنهج الاستقرائي عبر تحليل المعطيات والبيانات الواقعية المتعلقة بتجربة إيران في توظيف الأدوات السيبرانية والرقمية، للوصول إلى استنتاجات عامة حول طبيعة هذا النموذج. كما تم اعتماد أسلوب وصفي-تحليلي في عرض البيانات وتفسيرها، من خلال وصف بنية المنظومة الاقتصادية-السيبرانية وتحليل آليات عملها وتقييم فاعليتها.

سادساً/ هيكلية البحث

تم تقسيم البحث إلى مقدمة وثلاثة مباحث رئيسية على النحو الآتي: يتناول المبحث الأول الإطار النظري للهندسة الاقتصادية والأمن السيبراني، بينما يركز المبحث الثاني على تأثير العقوبات في إعادة تشكيل البنية الاقتصادية-الرقمية في إيران، في حين يعالج المبحث الثالث منظومة الهندسة الاقتصادية للأمن السيبراني من حيث البنية والأدوات والافاق المستقبلية، وصولاً إلى خاتمة تتضمن أبرز الاستنتاجات.

المبحث الأول

الإطار النظري للهندسة الاقتصادية والأمن السيبراني

يُعد فهم العلاقة بين الهندسة الاقتصادية والأمن السيبراني أساسياً لتحليل كيفية استجابة الدول الخاضعة للعقوبات للقيود الخارجية. هذا المبحث يهدف إلى تأسيس مرجع مفاهيمي ونظري يمكن عبره تفسير التحولات التي تجري داخل البنية الاقتصادية-الرقمية للدول المتأثرة بالعقوبات، مع التركيز على آليات التحول من وظائف تقنية بحتة إلى وظائف سياسية-اقتصادية استراتيجية.

المطلب الأول

مفهوم الهندسة الاقتصادية

يشير مفهوم الهندسة الاقتصادية إلى عملية إعادة تصميم الهياكل والمؤسسات والآليات الاقتصادية بصورة مقصودة من أجل تحقيق أهداف استراتيجية محددة، مثل الكفاءة، والاستقرار، والقدرة على التكيف، والاستقلال الاقتصادي. ويقوم هذا المفهوم على فرضية أساسية مفادها أن الاقتصاد ليس بنية جامدة، بل منظومة قابلة لإعادة التشكيل وفقاً لأولويات الدولة ومتغيرات البيئة الداخلية والخارجية، بما يجعل التدخل المؤسسي والتخطيطي جزءاً من عملية بناء القدرة الاقتصادية وليس مجرد استجابة ظرفية للأزمات [1].

وفي الأدبيات الاقتصادية والمؤسسية، ورد هذا المفهوم بصيغ متقاربة. فالبنك الدولي ينظر إلى الهندسة الاقتصادية بوصفها عملية إعادة تصميم للمؤسسات والسياسات الاقتصادية بما يعزز الكفاءة والقدرة على التكيف ويحقق الأهداف التنموية والاستراتيجية للدولة [2]. ويُفهم من هذا التعريف أن جوهر الهندسة الاقتصادية يتمثل في العلاقة بين المؤسسة والنتيجة، أي بين طريقة بناء النظام الاقتصادي والقدرة على إنجاز الأهداف العامة للدولة. أما الاقتصادي الأمريكي داني رودريك (Dani Rodrik) فيربط المفهوم بتدخل الدولة المقصود في تصميم الهياكل الاقتصادية والمؤسسات والأسواق بما يحقق أهداف التنمية والقدرة التنافسية، وهو تعريف يبرز البعد السياسي للدولة بوصفها فاعلاً موجهاً لا مجرد منظم محايد [3].

وتتلاقى هذه التعريفات، رغم اختلاف زاوية النظر فيها، عند فكرة أساسية مفادها أن الهندسة الاقتصادية هي عملية عقلانية ومقصودة لإعادة تنظيم الاقتصاد أو جزء منه من أجل تحقيق نتيجة أفضل أو أكثر ملاءمة لغايات الدولة. غير أن أهمية هذا المفهوم تتضاعف عندما يُستخدم في سياق الدول الخاضعة للعقوبات، لأن الموضوع هنا لا يعود متعلقاً فقط بتحسين الكفاءة أو رفع الإنتاجية، بل بإعادة بناء القنوات التي يمر عبرها المال والسلع والمعلومات في بيئة تتعرض فيها الدولة لضغط خارجي مباشر. في هذه الحالة تصبح الهندسة الاقتصادية أداة لصون القدرة على العمل الاقتصادي، لا مجرد وسيلة لتحسين أدائه. وقد اتسع هذا المفهوم في الأدبيات الحديثة ليشمل البعد المؤسسي والاستراتيجي للدولة، لا سيما في ظل التحولات التي فرضتها العولمة المتقطعة، والتوترات

الجيوسياسية، وتزايد أهمية المرونة الاقتصادية. وتشير تقارير منظمة التعاون الاقتصادي والتنمية إلى أن الأمن الاقتصادي، والمرونة المؤسسية، والتحول الرقمي أصبحت عناصر متداخلة في بناء القدرة الوطنية، ولم تعد تُفهم بوصفها مجالات منفصلة. ولم تعد الهندسة الاقتصادية تقتصر على تحسين كفاءة المشروعات أو تقليل الكلف، بل ترتبط بإعادة تشكيل العلاقات بين الدولة والسوق والبنية الرقمية لتحقيق الاستقرار والسيادة الاقتصادية[4].

ومن هنا، فإن الفرق بين الهندسة الاقتصادية في الدول العادية والدول الخاضعة للعقوبات يصبح فرقاً في الغاية والوظيفة. ففي الدول العادية، ينصرف هذا المفهوم إلى تحسين الكفاءة، وتخفيض التكاليف، وتعزيز التنافسية، وتطوير البنية المؤسسية للنمو. أما في الدول الخاضعة للعقوبات، فإنه يتحول إلى أداة للبقاء الاقتصادي، وإعادة تنظيم قنوات التبادل، وخلق مسارات بديلة للتمويل والتجارة والاستيراد، بحيث يصبح الهدف المركزي هو حماية الاقتصاد من الانقطاع وإبقاء النظام الاقتصادي قابلاً للعمل رغم القيود الخارجية[5]. وعليه، تُستخدم الهندسة الاقتصادية في هذا البحث بوصفها إطاراً تفسيريّاً لإعادة تنظيم الموارد والقنوات والعلاقات الاقتصادية، بما يجعل الفضاء الرقمي جزءاً من عملية إعادة بناء الاقتصاد في الدول الخاضعة للعقوبات.

المطلب الثاني

مفهوم الأمن السيبراني

يشير مفهوم الأمن السيبراني إلى مجموعة من الإجراءات والآليات والتقنيات التي تستهدف حماية الأنظمة والشبكات والبيانات من الاختراق أو التعطيل أو الاستغلال غير المشروع. وقد شهد هذا المفهوم توسعاً واضحاً في السنوات الأخيرة، إذ لم يعد محصوراً في كونه مسألة تقنية تتصل بحماية البنية المعلوماتية، بل أصبح جزءاً من البنية التي يقوم عليها الاقتصاد الحديث، لأن العمليات المالية والتجارية والخدمية باتت تعتمد بصورة متزايدة على القنوات الرقمية[6]. وعند النظر إليه كأصل اقتصادي استراتيجي، يمكن تمييز ثلاث وظائف رئيسية ومتداخلة[7]:

1. الوظيفة الوقائية: حماية الأنظمة البنكية والبنى التحتية الحيوية وشبكات الاتصالات والطاقة والنقل من الهجمات، بما يضمن استمرارية النشاط الاقتصادي ويحد من الخسائر.
2. الوظيفة التمكينية: تمكين الاقتصاد الرقمي، بما في ذلك التجارة الإلكترونية والدفع الإلكتروني والعملات المشفرة والتحويلات المالية، من العمل في بيئات عالية المخاطر، وهو ما يمثل شرطاً ضرورياً لعمل اقتصاد رقمي-مالي في الدول الخاضعة للعقوبات.
3. الوظيفة الهجومية: استخدام القدرات السيبرانية في عمليات هجومية قد تستهدف الحصول على مكاسب مالية أو إلحاق خسائر اقتصادية بالخصوم.

وتكتسب هذه الوظائف أهمية خاصة عند الربط بين الأمن السيبراني والاقتصاد الرقمي. فالأخير لا يمكن أن يعمل بكفاءة من دون مستوى عالٍ من الثقة في القنوات التي تنتقل عبرها القيمة والبيانات. ولهذا فإن أنظمة الدفع الإلكتروني، والمنصات التجارية، والخدمات المصرفية الرقمية، والبنى السحابية، كلها تحتاج إلى بيئة سيبرانية مستقرة حتى تتمكن من أداء دورها. ومن ثم، فإن الأمن السيبراني لا يمثل عنصراً مكملاً للاقتصاد الرقمي، بل يعد شرطاً أساسياً لاستمراره وفاعليته[8].

وتبرز هذه العلاقة بشكل أوضح في الدول الخاضعة للعقوبات. ففي هذه الدول تتراجع فاعلية القنوات المالية الرسمية، ويزداد الاعتماد على بدائل رقمية وموازية، الأمر الذي يجعل البنية السيبرانية جزءاً من استراتيجية التكيف الاقتصادي. وفي مثل هذه البيئات، لا يقتصر الأمن السيبراني على حماية الشبكات والأنظمة، بل يمتد إلى ضمان استمرار القنوات التي تُدار عبرها التحويلات المالية، والتبادل التجاري، والوساطة الرقمية. لذلك يتضاعف الطلب على الأمن السيبراني، لأن أي خلل في هذه البنية قد يؤدي إلى تعطيل قنوات بديلة يعتمد عليها الاقتصاد في الاستمرار والعمل[9]. ومن الناحية النظرية، يمكن تفسير هذه الظاهرة عبر ثلاثة أطر مترابطة وهي:

الإطار الأول: يتمثل في الاقتصاد السياسي للعقوبات، الذي ينظر إلى العقوبات باعتبارها أداة لإعادة توزيع القوة عبر التحكم في الوصول إلى الأسواق والتمويل والتكنولوجيا. وعندما تُغلق القنوات الرسمية أمام دولة ما، فإنها تلجأ عادة إلى بناء بدائل رقمية ومالية تقلل من أثر العزل الاقتصادي. وهذا ما يفسر توسع استخدام المنصات المشفرة، وبنوك الظل، وشبكات الوساطة غير التقليدية في بعض الدول الخاضعة للعقوبات[10].

أما الإطار الثاني: وهو مفهوم الأمن الاقتصادي، الذي يربط بين حماية الموارد الاقتصادية وحماية الدولة ذاتها. فالأمن الاقتصادي لا ينفصل عن الأمن القومي، لأن تعطل تدفق العملة الصعبة أو انقطاع سلاسل الإمداد أو فقدان السيطرة على المنصات

الرقمية يمكن أن ينعكس مباشرة على الاستقرار السياسي والأمني. ومن هذا المنظور، يصبح الأمن السيبراني أداة لحماية البنية الاقتصادية بقدر ما هو وسيلة لحماية البنية المعلوماتية، وهو ما يفسر اندماج الاعتبارات الأمنية والاقتصادية في سياسات الدول التي تواجه ضغوطاً خارجية [11].

الإطار الثالث: يتمثل في نظرية الاعتماد المتبادل المُسلَّح، التي تفسر كيف يمكن للشبكات الاقتصادية العالمية أن تتحول إلى أدوات ضغط عندما تسيطر عليها قوى مركزية عبر نقاط اختناق رئيسية، مثل أنظمة الدفع، والدولار، والمنصات التقنية، والخدمات السحابية. وفي المقابل، تحاول الدول الواقعة تحت الضغط تقليل هشاشتها عبر بناء شبكات بديلة أو أقل مركزية، وهو ما يفسر لجوء بعض الدول إلى توظيف التقنيات الرقمية والمنصات المشفرة كجزء من بنية اقتصادية موازية. ومن ثم، فإن الأمن السيبراني في هذا السياق لا يعود مجرد وسيلة للحماية، بل يصبح جزءاً من استراتيجية أوسع لإعادة تشكيل العلاقة مع النظام الاقتصادي العالمي [12].

وبهذا المعنى، فإن الأمن السيبراني في هذا البحث لا يُستخدم بمعناه التقني الضيق، بل بوصفه أداة اقتصادية-استراتيجية تدخل في بنية إعادة التنظيم الاقتصادي داخل الدول الخاضعة للعقوبات. إن الحالة الإيرانية تمثل مثلاً واضحاً على كيفية تحول الأمن السيبراني من وسيلة حماية إلى عنصر من عناصر إدارة الاقتصاد الموازي وإعادة هندسته في بيئة دولية شديدة القبود.

المبحث الثاني

إيران بين العقوبات وإعادة تشكيل بنيتها الاقتصادية-الرقمية

تمثل العقوبات الاقتصادية العامل الرئيس الذي دفع إيران إلى إعادة هندسة اقتصادها، إذ لم تقتصر آثارها على تقليص الموارد، بل أدت إلى إعادة تشكيل بنيتها، ما دفعها للبحث عن قنوات بديلة لإدارة التدفقات الاقتصادية.

المطلب الأول

طبيعة الاقتصاد الإيراني ومؤشراته في ظل العقوبات

يمثل الاقتصاد الإيراني نموذجاً لاقتصاد كبير على المستوى الإقليمي، ويتميز بتنوع نسبي في قاعدته الانتاجية تتوزع بين قطاعات الهيدروكربونات والزراعة والخدمات والصناعات التحويلية والخدمات المالية. ويُقدَّر الناتج المحلي الإجمالي الاسمي لإيران بنحو 475.25 مليار دولار في عام 2024 [13]، وهو ما يجعلها من أكبر الاقتصادات في الشرق الأوسط من حيث الحجم الكلي، كما ينعكس ذلك في اتساع السوق المحلية وحجم القاعدة الاقتصادية للدولة. وتستند الى قاعدة واسعة من الموارد الطبيعية والبشرية، ويعتمد تاريخياً على النفط والغاز والبتروكيماويات بوصفها المصادر الأهم للعملة الصعبة والإيرادات العامة. ويتميز هذا الاقتصاد بوجود سوق داخلية واسعة، وقاعدة صناعية وخدمية، وموارد بشرية وفنية كبيرة كما أنها تمتلك احتياطيات طبيعية ومعدنية ضخمة تُقدَّر بنحو 27.5 تريليون دولار وتحتل المرتبة الخامسة عالمياً [14]، غير أن عناصر القوة هذه تقابلها نقاط ضعف بنيوية واضحة، أهمها: الاعتماد المرتفع على صادرات الطاقة لاسيما الوقود الأحفوري، وارتفاع مستويات التضخم [15]، وهشاشة الاندماج في النظام المالي العالمي، بسبب تعرضه المستمر للتقلبات السياسية والعقوبات الاقتصادية. كما أن هذا النمط من الاقتصاد يجعل أي صدمة خارجية، ولا سيما العقوبات، ذات أثر مباشر وسريع في الاقتصاد وهو ما يوضحه الجدول رقم (1).

جدول رقم (1): أبرز المؤشرات الاقتصادية في إيران قبل وبعد إعادة فرض العقوبات الأميركية

المؤشر الاقتصادي	2017	2018	2019	2024
نمو الناتج المحلي الإجمالي الحقيقي (%)	3.3	-3.75	-2.36	3.66
نمو نصيب الفرد من الناتج الحقيقي (%)	2.8	-3.1	-4.1	2.9
معدل البطالة (%)	13.5	12.2	10.7	7.6
معدل الفقر (عند 3 دولار يومياً) (%)	2.7	3.2	4.3	3.52
التضخم، متوسط السنة (%)	9.7	34.8	41.2	32.5
نمو الناتج غير النفطي (%)	4.0	-1.8	1.7	2.4
نمو الناتج النفطي (%)	5.2	-14.7	-36.2	3.7
نمو الصادرات من السلع والخدمات (%)	14.4	-1.1	-31.6	3.7
نمو الواردات من السلع والخدمات (%)	15.3	-13.3	-7.4	5.3
رصيد الحساب الجاري (% من الناتج المحلي)	3.0	7.9	-0.6	2.7

32.3	42.7	34	45	الدين الحكومي العام (% من الناتج المحلي)
600,000	140,000	120,000	31,771	سعر الصرف الاسمي (1 دولار مقابل الريال)

المصدر: من اعداد الباحثة بالاعتماد على بيانات: World Development Indicators, World Bank, Iran Economic Monitor International Monetary Fund (IMF).

من بيانات الجدول يظهر تحول واضح في أداء الاقتصاد الإيراني بعد إعادة فرض العقوبات عام 2018؛ إذ انتقل النمو من مستويات موجبة إلى الانكماش، ولا سيما في القطاع النفطي، مع ارتفاع التضخم وتراجع التجارة الخارجية. وفي المقابل، شهد الاقتصاد لاحقاً تحسناً في النمو والبطالة، مع استمرار مستويات التضخم المرتفعة. وتوضح المؤشرات أن العقوبات أحدثت صدمة اقتصادية أولية دفعت إيران إلى إعادة التكيف وتنويع قنوات النشاط الاقتصادي. تعرّضت إيران لآلاف التدابير والعقوبات الاقتصادية والمالية فرضتها الولايات المتحدة والاتحاد الأوروبي ومجلس الأمن منذ عام 1979، وتركزت على حظر قطاعات الطاقة، وتجميد الأصول، وعزل النظام المالي [16]، ويمكن مطالعة أهم هذه العقوبات في الجدول الآتي:

جدول رقم (2): أبرز العقوبات الاقتصادية المفروضة على إيران

المرحلة الزمنية	الجهة الفارضة	الاجراءات
1980_1979	الولايات المتحدة	فرض قيود أولية على العلاقات الاقتصادية والمالية مع إيران عقب الثورة وأزمة الرهائن، وتجميد أصول إيرانية في الولايات المتحدة
1984	الولايات المتحدة	إدراج إيران ضمن الدول التي أثمرت بدعم الإرهاب، وفرض قيود على المساعدات والتجارة والتمويل
1995	الولايات المتحدة	الأمر التنفيذي 12959 الذي حظر التجارة والاستثمار الأمريكيين في إيران
1997	الولايات المتحدة	الأمر التنفيذي 13059 وتوسيع القيود على تصدير السلع إلى إيران بصورة مباشرة أو غير مباشرة
2006-2000	الأمم المتحدة	تشديد عقوبات عدم الانتشار واستهداف نقل التكنولوجيا والمعدات المرتبطة بأسلحة الدمار الشامل والصواريخ، والقطاع العسكري
2013_2010	الولايات المتحدة/ الاتحاد الأوروبي/ دول أخرى	توسيع العقوبات لتشمل النفط، المصارف، البنك المركزي، التأمين، الشحن والطاقة
2015_2013	الولايات المتحدة/ الاتحاد الأوروبي	تشديد العقوبات المالية والقطاعية، بما فيها استهداف الريال الإيراني وقطاع السيارات والطاقة والشحن والكيانات المرتبطة بالانتشار النووي
2016	الولايات المتحدة/ الأمم المتحدة/ الاتحاد الأوروبي	تنفيذ الاتفاق النووي (JCPOA) وتعليق جزء مهم من العقوبات النووية، مع استمرار عقوبات أخرى مرتبطة بالإرهاب وحقوق الإنسان.
2018	الولايات المتحدة	الانسحاب من JCPOA وإصدار الأمر التنفيذي 13846 وإعادة فرض العقوبات التي رُفعت بموجب الاتفاق وتوسعتها لتشمل قطاعات أكثر
2019	الولايات المتحدة	توسيع العقوبات لتشمل المعادن والصلب والألمنيوم والنحاس، شبكات القيادة والتمويل.
2022_2021	الولايات المتحدة وحلفاؤها	استمرار العقوبات على الكيانات الإيرانية وشبكات التمويل، وإضافة عقوبات مرتبطة بحقوق الإنسان والأنشطة الإقليمية والعسكرية وقطاع التكنولوجيا.
2025	الأمم المتحدة/ مجلس الأمن/ فرنسا/ ألمانيا/ المملكة المتحدة	عودة مسار العقوبات النووية الدولية من خلال آلية Snapback بعد انتهاء الإطار الزمني للقرار 2231 وعدم التوصل إلى تسوية بشأن الملف النووي.

المصدر: إعداد الباحثة بالاعتماد على: <https://www.unitedagainstnucleariran.com/international-iran-sanctions-database>

من الجدول يتضح لنا ان العقوبات منذ الثورة الإسلامية دخلت في مراحل متعددة، الا أن أكثرها تأثيراً كان مرتبطاً بتصادم الملف النووي ثم بالانسحاب الأمريكي من الاتفاق النووي عام 2018 وإعادة تفعيل سياسة "الضغط الأقصى". ولم تكن العقوبات في هذه المرحلة موجهة إلى قطاع واحد، بل استهدفت مجموعة من القطاعات الحيوية التي تشكل العمود الفقري للاقتصاد الإيراني، الأمر الذي جعل أثرها يتجاوز الضغط المالي إلى إعادة تشكيل البنية الاقتصادية نفسها. ويمكن تفصيل القطاعات المتضررة على النحو الآتي [17]:

1. قطاع النفط والغاز والبتروكيماويات: وهو القطاع الأهم لأنه المصدر الرئيس للعملة الصعبة، ولأن عوائده تمثل قاعدة التمويل الأساسية للموازنة والدعم والاستيراد. وعندما تُفرض عليه العقوبات، تقل قدرة الدولة على البيع المباشر، وترتفع الكلفة، وتنتج إلى البيع عبر وسطاء وبخصومات كبيرة، ما يخفض الفائدة الحقيقية من التصدير.
2. النظام المصرفي والبنك المركزي: شملت العقوبات البنك المركزي وعدداً من المصارف الحكومية والتجارية، وهو ما قلص قدرتها على إجراء التحويلات الدولية، والوصول إلى الدولار، وتسوية المدفوعات في الأسواق العالمية، وأجبرها على استخدام شبكات غير مباشرة وواجهات مالية خارجية.
3. الشحن والتأمين والنقل البحري: أدى استهداف هذه القطاعات إلى إرباك حركة الصادرات والواردات، ورفع تكلفة التأمين والنقل، وإضعاف قدرة إيران على إيصال منتجاتها إلى الأسواق الخارجية بصورة نظامية.
4. التكنولوجيا والبرمجيات والخدمات الرقمية: أدت القيود على التكنولوجيا المتقدمة والبرمجيات والخدمات السحابية إلى عرقلة التحديث التقني، وإبطاء التحول الرقمي، وزيادة الاعتماد على قنوات بديلة أقل كفاءة وأكثر كلفة.
5. الشركات والأفراد المرتبطون بالحرس الثوري وشبكات التمويل غير الرسمية: استهدفت العقوبات الكيانات التي تلعب دوراً في إدارة التجارة غير المباشرة، وتمويل العمليات، والتنسيق بين الداخل والخارج، وهو ما جعل الاقتصاد الإيراني أكثر اعتماداً على الشبكات الظلية والوسطاء والشركات المسجلة في دول ثالثة.

وقد أدت هذه العقوبات إلى إضعاف القدرة الرسمية لإيران على إجراء التحويلات المالية عبر النظام المصرفي العالمي ما أدى إلى تعطيل التجارة الرسمية، وانخفاض قيمة العملة الإيرانية بسبب شحة العملة الأجنبية وارتفاع الطلب عليها، وارتفاع مستويات التضخم نتيجة ارتفاع كلف الاستيراد وتراجع الاستقرار النقدي، وصعوبات في الاستيراد لاسيما في السلع الوسيطة والتكنولوجيا والدوائية. كما أجبرتها على بيع جزء كبير من نفطها بأساليب غير معلنة وبخصومات كبيرة تصل إلى 30% بعد أن انخفضت صادراتها من النفط بنسبة 80%، ودفعها نحو البحث عن قنوات غير تقليدية لتسوية المدفوعات وإدارة العائدات وكذلك تزايد الاقتصاد غير الرسمي بما فيه شبكات الظل وشركات الواجهة [18].

المطلب الثاني

العلاقة بين الاقتصاد الرسمي والاقتصاد الموازي في إيران

يمثل الاقتصاد الرسمي الإطار الرئيس للنشاط الاقتصادي الإيراني، ولا سيما قطاعات النفط والغاز والصناعة والخدمات، إلا أن العقوبات المالية والنفطية حدّت من قدرة المؤسسات الإيرانية على الوصول المباشر إلى النظام المالي الدولي وتسوية المدفوعات الخارجية. وفي المقابل، ظهرت شبكات مالية وتجارية عابرة للحدود، تضم بيوت صرافة وشركات واجهة وحسابات خارجية، لتسهيل بعض المعاملات المرتبطة بالنفط والتجارة. لذلك، لا يمثل الاقتصاد الموازي بديلاً عن الاقتصاد الرسمي، بل يتداخل معه في التمويل والتسوية والتحويل الخارجي، بما يعزز القدرة على التكيف مع العقوبات، مع ارتفاع تكاليف المعاملات والمخاطر المالية والقانونية [19].

أولاً: مصادر التمويل وإعادة توجيه الموارد

تستند الموارد الاقتصادية الإيرانية إلى قاعدة متنوعة تشمل النفط والغاز والبتروكيماويات، إلى جانب الزراعة والصناعة والخدمات. ولم تؤدّ العقوبات إلى توقف الموارد أو النشاط الاقتصادي بصورة كاملة، لكنها قيدت قدرة إيران على تحويل عائداتها واستخدامها من خلال القنوات المصرفية الدولية. ونتيجة لذلك، جرى توجيه جزء من هذه العائدات من خلال بيوت صرافة وشركات واجهة وحسابات خارجية وشبكات تجارية متعددة. وقد وثقت وزارة الخزانة الأمريكية استخدام هذه الآليات في إدارة المدفوعات المرتبطة بالنفط والبتروكيماويات والمعاملات التجارية الإيرانية. تؤدي القنوات الموازية وظيفة إعادة توجيه الموارد وتسوية المدفوعات أكثر من كونها مصدراً مستقلاً لها، إذ تربط بين الموارد المتولدة داخل الاقتصاد الإيراني وبين احتياجات التمويل والتجارة الخارجية. أن هذه الآلية تفرض تكاليف إضافية نتيجة تعدد الوسطاء وتعقيد مسارات التحويل [20].

ثانياً: قنوات التجارة وإعادة تنظيم التعاملات

امتد أثر العقوبات إلى تجارة النفط والمنتجات البتروكيماوية والنقل البحري، الأمر الذي دفع بعض الجهات المرتبطة بإيران إلى الاعتماد على وسطاء وشركات مسجلة خارج البلاد وشبكات شحن متعددة. وقد وثقت وزارة الخزانة الأمريكية استخدام سفن وشركات إدارة وملكية مسجلة في دول مختلفة لنقل النفط الإيراني إلى الأسواق الخارجية. وقد ساعدت هذه الترتيبات على استمرار جزء من التجارة الخارجية، لكنها جعلت عمليات التصدير أكثر تعقيداً وكلفة، بسبب زيادة الوسطاء والولايات القضائية المشاركة

وارتفاع مخاطر العقوبات وتجميد الأموال. وبذلك أصبحت بعض مراحل التجارة الإيرانية تجمع بين النشاط الرسمي في الإنتاج، والقنوات غير المباشرة في التسويق والنقل والتحويل [21].

ثالثاً: الرقابة والشفافية

تختلف درجة الرقابة والشفافية بين القنوات المصرفية الرسمية والشبكات المالية غير المباشرة. فالمؤسسات الرسمية تخضع للأطر القانونية والمصرفية المعمول بها، في حين تعتمد شبكات الالتفاف على العقوبات على شركات وحسابات ووسطاء موزعين على أكثر من ولاية قضائية، الأمر الذي يعقد تحديد الملكية المستفيدة ومسار الأموال. تعتمد الجهات الرقابية الدولية على إجراءات العناية الواجبة وتحليل المعاملات والتحقق من المستفيد الحقيقي وربط الشركات والحسابات والأطراف التجارية [22]. وقد دعا فريق العمل المالي FATF في عام 2025 إلى تطبيق تدابير مضادة تجاه إيران، من بينها تعزيز العناية الواجبة والقيود المرتبطة بالعلاقات المصرفية المراسلة، استناداً إلى المخاطر التي حددها في مجال غسيل الأموال وتمويل الإرهاب وانتشار الأسلحة. ومع انتقال جزء من المعاملات إلى البيئة الرقمية، أصبحت البيانات والسجلات الإلكترونية وتحليل المعاملات أدوات إضافية في الرقابة، في حين أصبحت حماية الأنظمة والمنصات من الاختراق والتعطيل وتسريب المعلومات عاملاً مؤثراً في استمرارية النشاط المالي الرقمي [23].

رابعاً: المخاطر الناتجة عن التداخل بين الاقتصاديين

وفر استخدام القنوات المالية والتجارية غير المباشرة لإيران قدرة نسبية على الاستمرار في بعض صور التجارة والتحويل الخارجي، إلا أن هذه القدرة ترتبط بمجموعة من المخاطر. أهمها [24]:

1. من الناحية الاقتصادية، يؤدي تعدد الوسطاء إلى زيادة تكاليف النقل والتسوية والتحويل، كما قد يؤدي الاعتماد على أطراف خارجية إلى تجميد الأموال أو تأخر وصولها أو فقدان جزء من قيمتها.
2. الناحية القانونية والمالية، يؤدي انتشار الشركات الوسيطة والحسابات الخارجية إلى تعقيد تحديد المستفيد النهائي من بعض المعاملات، ويزيد مخاطر العقوبات والامتنال وغسل الأموال والفساد والاحتتيال. كما أن استهداف هذه الشبكات بصورة متتابة يفرض عليها إعادة تنظيم علاقاتها التجارية والمالية بصورة مستمرة.
3. في الجانب الرقمي، فتظهر مخاطر مرتبطة باختراق المنصات وتعطيل الخدمات وسرقة البيانات وتتبع المعاملات. ومن ثم، فإن الاعتماد المتزايد على الوسائط الرقمية يجعل الأمن السيبراني جزءاً من إدارة المخاطر الاقتصادية المرتبطة بالقنوات البديلة، سواء من حيث حماية البيانات والأنظمة أو ضمان استمرارية الخدمات المالية والتجارية.

المطلب الثالث

صعود الاقتصاد الموازي والأدوات المالية – الرقمية البديلة

أبرزت العقوبات مجموعة من القنوات المالية والتجارية البديلة التي أصبحت جزءاً من آليات التكيف الاقتصادي الإيراني، وأبرزها. ويمكن توضيحها بالآتي [25]:

أولاً: شبكات الظل المصرفي وشركات الواجهة:

أصبحت من أهم أدوات الالتفاف على العقوبات، لأنها تسمح بتمرير الأموال وعائدات التجارة خارج النظام المصرفي التقليدي. وتعمل هذه الشبكات عادة عبر كيانات مسجلة في دول ثالثة، خصوصاً في الإمارات وهونغ كونغ وسنغافورة، تُستخدم شركات ظاهرية بوصفها غطاء قانونياً لتحويل الأموال وإخفاء الجهة المستفيدة الحقيقية منها. وقد أظهر تقرير مكتب FinCEN التابع لوزارة الخزانة الأمريكية الصادر في أكتوبر 2025 أن حجم النشاط الظلي المرتبط بإيران بلغ نحو 9 مليارات دولار خلال عام 2024 [26]، وهي قيمة موزعة على قنوات متعددة، أبرزها [27]:

- أ- شركات صورية transacted نحو 5 مليارات دولار.
- ب- شركات نفط أجنبية يُرجح ارتباطها بشبكات إيرانية transacted نحو 4 مليارات دولار.
- ت- معاملات إضافية بقيمة نحو 413 مليون دولار مرتبطة باقتناء تكنولوجيا خاضعة للرقابة والاستخدامات الدفاعية.

ويعني ذلك أن الظل المصرفي لم يعد مجرد آلية التفاف ثانوية، بل صار بنية تشغيلية متقدمة تدير جزءاً مهماً من التدفقات المالية الإيرانية خارج الشفافية المصرفية التقليدية. كما أن استمرار استهداف هذه الشبكات في 2026 من قبل وزارة الخزانة الأميركية يؤكد أنها ما تزال قناة مركزية في تمويل التجارة الإيرانية وتدوير عائدات النفط والبتروكيماويات.

ثانياً: القنوات التجارية غير المباشرة

لم يقتصر التكيف الإيراني على الجانب المالي، بل شمل إعادة تنظيم القنوات التجارية أيضاً. فقد اعتمدت إيران بصورة أكبر على الوسطاء التجاريين وشركات إعادة التصدير والمسارات البحرية غير المباشرة لتصريف صادراتها من النفط والبتروكيماويات واستيراد السلع الأساسية والوسيط. ويعمل هذا النمط من خلال طبقات متداخلة من الوسطاء، بحيث تُخفي الهوية الحقيقية للبائع والمشتري، وتُدار الصفقات عبر كيانات قانونية في ولايات قضائية متعددة، الأمر الذي يقلل من إمكانية التتبع لكنه يرفع كلفة المعاملة ومخاطرها [28].

وقد أظهرت بيانات الخزانة الأميركية أن هذه القنوات التجارية لا تعمل فقط على نقل السلع، بل تؤدي دوراً في إعادة تدوير العائدات وتوزيعها على شبكات مالية وتجارية تمتد عبر الخليج وشرق آسيا. وتكشف هذه المعطيات أن الاقتصاد الموازي الإيراني أصبح ذا بنية دولية مرنة، تعتمد على شبكات وسيطة أكثر من اعتمادها على التبادل المباشر، وهو ما يفسر استمرار تدفق بعض السلع الإيرانية إلى الأسواق الخارجية رغم العقوبات [29].

ثالثاً: العملات المشفرة والمنظومة الرقمية

يمثل استخدام العملات المشفرة أحد أبرز مظاهر التحول إلى الاقتصاد الرقمي الموازي، إذ وفرت هذه الأداة منفذاً أقل ارتباطاً بالبنوك التقليدية، وأكثر مرونة في البيانات الخاضعة للرقابة. وتشير تقارير شركة Chainalysis (هي شركة أميركية متخصصة في تحليل بيانات البلوك تشين وتتبع حركة العملات المشفرة) الصادرة في يناير 2026 إلى أن الاقتصاد المشفر الإيراني بلغ نحو 7.78 مليارات دولار خلال 2025 [30]، وهو رقم يعكس توسعاً سريعاً في الاعتماد على الأصول الرقمية كوسيلة لتسوية المعاملات وتحريك القيمة عبر الحدود. كما أشارت التغطيات والتحليلات المرتبطة ببيانات السلسلة إلى أن جزءاً مهماً من هذا النشاط ارتبط بتدفقات داخلية وخارجية تتعلق بالتجارة، وتمويل العمليات، وتبادل الأصول الرقمية مع وسطاء إقليميين. أن توظيف العملات المشفرة يتم ضمن منظومة مترابطة تقوم على ثلاث وظائف رئيسية [31]:

1. استخدام منصات تداول محلية وإقليمية لتجميع الأصول الرقمية من السوقين الداخلية والخارجية.
2. توظيف العملات المشفرة في تسوية جزء من المدفوعات المرتبطة بتجارة النفط والبتروكيماويات وبعض السلع الأخرى
3. تحويل جزء من هذه الأصول إلى عملات تقليدية عبر منصات ووسطاء في دول ثالثة، بما يسمح بإعادة إدخالها إلى الدورة الاقتصادية.

وهذا التحول لا يعني أن العملات المشفرة أصبحت بديلاً كاملاً عن النظام المالي التقليدي، لكنه يوضح كيف تحولت إلى أداة عملية لتقليل الاعتماد على البنوك والممرور عبر أنظمة مالية يمكن تعقبها بسهولة أكبر. ومن ثم، فإن المنظومة الرقمية لم تعد ملحقةً ثانوياً بالاقتصاد الموازي، بل صارت جزءاً بنيوياً من طريقة عمله.

يتضح مما سبق إن صعود الاقتصاد الموازي في إيران لم يكن نتيجة خيار اقتصادي عادي، بل حيلة مباشرة لتأثير العقوبات في قنوات التمويل والتجارة. وقد تمثل هذا الصعود في ثلاثة مسارات مترابطة: شبكات الظل المصرفي، والقنوات التجارية غير المباشرة، والمنظومة المالية-الرقمية المشفرة. وأنتجت هذه المسارات اقتصاداً مرناً نسبياً في مواجهة العقوبات، لكنه أكثر كلفة وأكثر عرضة للملاحقة وأكثر اعتماداً على الوساطة الخارجية من الاقتصاد الرسمي. هذه التحولات تمثل في جوهرها "هندسة اقتصادية" تُعاد فيها هيكل العلاقات بين الفاعلين الاقتصاديين والقنوات المالية، بمساعدة أدوات رقمية وسيريرية، وهو ما يمهد للانتقال إلى المبحث الثالث الذي يركز على دور الأمن السيبراني تحديداً في هذه المنظومة.

المبحث الثالث

الهندسة الاقتصادية للأمن السيبراني في إيران – البنية، الأدوات، والفاعلية

يتناول هذا المبحث توظيف الأمن السيبراني في إعادة تنظيم بعض القنوات الاقتصادية الإيرانية، من خلال تحليل بنيته المؤسسية وأدواته ووظائفه وحدوده وآفاقه المستقبلية.

المطلب الأول

الفاعلون والبنية المؤسسية-السيبرانية والادوات التقنية

شكلت العقوبات الاقتصادية والتهديدات الأمنية المتزايدة عاملاً رئيساً في تسريع تطور القدرات السيبرانية الإيرانية خلال العقدين الأخيرين، ولا سيما مع اتساع اعتماد الدولة على البنية الرقمية في إدارة قطاعات الطاقة والاتصالات والقطاع المالي. وفي هذا السياق، برزت إيران بوصفها قوة سيبرانية إقليمية صاعدة، إذ اتجهت إلى بناء قدرات دفاعية وهجومية متقدمة نسبياً بالاعتماد على تطويرها الذاتي، في محاولة لتقليل أثر القيود الخارجية وتعزيز قدرتها على حماية مصالحها الاقتصادية والأمنية.

وقد أسهمت أحداث مفصلية، وفي مقدمتها الهجوم بفيروس Stuxnet عام 2010 الذي استهدف البنية التحتية النووية، وكشف لصانعي القرار الإيرانيين أن البنية الرقمية يمكن أن تكون هدفاً استراتيجياً مباشراً لا مجرد أداة مساعدة في إدارة الاقتصاد. وقد أدى هذا التحول إلى توسيع الاستثمار في الأمن الرقمي، وتطوير كوادرات متخصصة، وإنشاء مؤسسات وطنية أكثر ارتباطاً بإدارة المجال السيبراني بوصفه مجالاً أمنياً واقتصادياً في آن واحد [32]. وتُظهر المؤشرات الدولية أن هذه الجهود لم تكن شكلية أو محدودة الأثر، إذ احتلت إيران المرتبة العاشرة عالمياً في مؤشر القوة السيبرانية لعام 2024 الصادر عن مركز بيلفر، وهو ما يعكس مستوى متقدماً من التراكم المؤسسي والتقني في هذا المجال [33].

كما تمتلك إيران اليوم قدرات ملحوظة في مجالات الدفاع السيبراني، وجمع المعلومات، والعمليات الإلكترونية الهجومية، مقارنةً بمعظم دول الشرق الأوسط. وتشير تقارير أمنية دولية متعددة إلى أن طهران طوّرت خلال السنوات الأخيرة مجموعات سيبرانية ذات خبرة في الاختراق والتجسس الرقمي وهجمات الفدية والعمليات الموجهة ضد أهداف حكومية واقتصادية خارجية. ولا تقتصر أهمية هذه القدرات على بعدها الأمني المباشر، بل تمتد إلى كونها أداة لحماية البنية الاقتصادية الرقمية التي أصبحت جزءاً من استراتيجية الدولة في التكيف مع العقوبات ومواجهة أثارها. ومن أبرز المسارات التي أسهمت في بناء القدرات السيبرانية الإيرانية [34]:

- 1- القاعدة العلمية والتطوير المحلي: طورت إيران قدراتها من خلال تنمية الكوادر التقنية والاستفادة من الجامعات ومراكز البحث والاستجابة للحوادث؛ إذ توجد مراكز CERT في جامعات مثل شريف للتكنولوجيا وأمير كبير وأصفهان للتكنولوجيا وشيراز، وتشارك في منظومة OIC-CERT. وهذا وفر قاعدة بشرية وأكاديمية لدعم تطوير الأمن السيبراني محلياً. OIC-CERT – الأعضاء
- 2- الخبرة العملية والفاعلون السيبرانيون: أسهم تعرض إيران لهجمات متكررة في تراكم الخبرة وتطوير قدرات أكثر تنظيماً، وظهرت مجموعات سيبرانية مرتبطة بمؤسسات أمنية إيرانية تمارس التجسس والاختراق والعمليات الهجومية. وأصبحت الخبرة المكتسبة من البيئة العملية أحد مصادر تطور القدرة السيبرانية الإيرانية.
- 3- التعاون وتبادل الخبرات الدولية: إلى جانب التطوير الداخلي، استفادت إيران من أطر التعاون السيبراني الإقليمية والدولية، وشاركت مراكز إيرانية في OIC-CERT لتبادل الخبرات والاستجابة للحوادث، كما وقعت مع روسيا في عام 2021 اتفاقاً للتعاون في مجال أمن المعلومات. ويشير ذلك إلى أن بناء القدرة الإيرانية جمع بين الاعتماد على الموارد المحلية والاستفادة الانتقائية من التعاون الخارجي.

وفي هذا السياق، تتكون منظومة الأمن السيبراني والاقتصادي في إيران من شبكة متداخلة من المؤسسات الرسمية والأمنية والجهات التقنية الخاصة، حيث تتوزع الأدوار بين التخطيط والتنظيم والتشغيل والحماية التقنية. ويمكن تحديد أبرز الفاعلين في هذه المنظومة على النحو الآتي [35]:

1. المؤسسات الرسمية: مثل البنك المركزي وبعض الوزارات الاقتصادية، التي تضع الإطار العام وتتعامل مع العقوبات على المستوى الرسمي، وقد تغض الطرف عن بعض أنشطة الاقتصاد الموازي طالما أنها تخدم أهداف الدولة.
2. الحرس الثوري والأجهزة الأمنية: التي تمثل العمود الفقري لشبكات شركات الواجبة وبنوك الظل، وتملك نفوذاً واسعاً على منصات الكريبتو والبنية الرقمية الحساسة، وتلعب دوراً محورياً في توجيه الموارد عبر الاقتصاد الموازي.
3. القطاع التقني والمالي الخاص: الذي يشمل شركات برمجيات وأمن سيبراني ومنصات تداول عملات مشفرة ومزودي خدمات سحابية واتصالات آمنة، ويقوم بتصميم وتشغيل البنى التحتية الرقمية-السيبرانية التي تعتمد عليها الدولة في إدارة اقتصادها الموازي.

هذا التداخل بين الرسمي والأمني والخاص يخلق منظومة هجينة يصعب الفصل فيها بين ما هو "اقتصادي" وما هو "أمني"، إذ يتحول المهندس السيبراني والخبير المالي في شركة خاصة إلى جزء من شبكة أوسع تخدم أهداف الأمن الاقتصادي للدولة. تعتمد هذه المنظومة على عدة أدوات تقنية متداخلة [36]:

1. **طبقة الاتصالات الآمنة:** وتشمل أدوات الاتصال الآمن شبكات VPN، وبروتوكولات مثل WireGuard، وقنوات مراسلة مشفرة، وهي أدوات تستخدم لنقل المعلومات الحساسة بين الفاعلين في شبكات بنوك الظل وشركات الواجهة ومنصات الكريبتو.
2. **طبقة إدارة الأصول الرقمية:** وتشمل المحافظ الرقمية المتعددة التوقيع، وأنظمة إدارة مفاتيح التشفير، ولوحات التحكم في تدفقات العملات المشفرة عبر عشرات أو مئات العناوين، وأدوات تجزئة المدفوعات واستخدام خدمات خلط (Mixers) لتقليل إمكانية التتبع.
3. **طبقة الدفاع السيبراني:** وتشمل أنظمة كشف التسلل، والجدران النارية المتقدمة، وفرق الاستجابة للحوادث، وإجراءات النسخ الاحتياطي واستعادة البيانات، التي تحمي منصات التداول والبنوك والمراكز الحساسة من الهجمات الخارجية، سواء كانت بدافع مالي أو سياسي.

كل طبقة من هذه الطبقات تمثل دورها مجالاً لنشاط اقتصادي وتقني؛ فهناك شركات وخبراء وموازنات مخصصة لإنشائها وصيانتها وتطويرها، ما يعزز فكرة الأمن السيبراني كقطاع اقتصادي قائم بذاته داخل الدولة.

المطلب الثاني

الأمن السيبراني كأداة تمكين لاقتصاد الموازي وتحقيق عوائد اقتصادية

أصبح الأمن السيبراني في الحالة الإيرانية أداة تمكين رئيسة للاقتصاد الموازي، لأنه يوفر البيئة الضرورية لاستمرار شبكات الظل المصرفي وشركات الواجهة ومنصات تداول الأصول الرقمية. فهذه الكيانات لا تستطيع العمل بفعالية من دون بنية آمنة تسمح بتبادل الوثائق وتنظيم المعاملات وتدوير الأموال والتواصل بين الفاعلين عبر الحدود، وأي خلل في هذه البيئة يرفع مخاطر الكشف والتتبع ويهدد استمرارية القنوات البديلة التي يعتمد عليها الاقتصاد في ظل العقوبات. تتجلى وظيفة الأمن السيبراني هنا في ثلاث وظائف مترابطة:

1. **حماية قنوات بنوك الظل وشركات الواجهة:** تعتمد شبكات تحويل الأموال وتدوير العوائد على مراسلات حساسة وبيانات مالية وعقود ووثائق تمر عبر أنظمة رقمية. ولذلك فإن تأمين هذه البنية يسهم في تقليل احتمالات الاختراق أو التسريب أو الاستخدام القانوني لهذه البيانات من قبل الجهات الرقابية الدولية. وتكشف بيانات FinCEN أن إيران اعتمدت عام 2024 على شبكة ظل مصرفي عابرة للحدود بلغت قيمتها التقديرية نحو 9 مليارات دولار عبر الحسابات المراسلة الأميركية، وأن الجزء الأكبر من هذه التدفقات مر عبر شركات وهمية تداولت نحو 5 مليارات دولار، فيما ارتبطت شركات نفطية خارجية يُحتمل ارتباطها بشبكات إيرانية بنحو 4 مليارات دولار أخرى، إضافة إلى نحو 413 مليون دولار في معاملات مرتبطة باقتناء تكنولوجيا خاضعة للرقابة [37].
2. **تأمين منظومة العملات المشفرة (الكريبتو):** منصات التداول والمحافظ والأدوات المرتبطة بها هي عصب الاقتصاد الرقمي الموازي، وأي اختراق واسع لها يمكن أن يؤدي إلى خسائر مالية كبيرة وانهيار الثقة لدى المستخدمين. لذلك، يتوجب الاستثمار المستمر في حماية هذه المنصات من الاختراق والسرقة، وتأمين بنى تحتية موثوقة لإدارة الأصول الرقمية. وتشير التقديرات الأميركية في 2026 إلى أن منصات إيرانية رئيسة، وعلى رأسها Nobitex وهي أكبر منصة إيرانية لتداول العملات المشفرة، كانت مسؤولة عن أكثر من 50% من التدفقات المشفرة الداخلة إلى إيران خلال 2025، وأن الخزنة الأميركية جمّدت أو صادرت ما يقارب مليار دولار من الأصول المشفرة الإيرانية ضمن حملة الضغط المالي المتصاعد [38].
3. **ضمان استمرارية الخدمات الاقتصادية-الرقمية:** إذ يمكن الأمن السيبراني من استمرار عمل أنظمة الدفع الإلكتروني، والتجارة الإلكترونية، والخدمات المصرفية الرقمية، حتى في ظل هجمات خصوم خارجيين أو تشديد داخلي للرقابة، ما يحافظ على حيوية جزء من الاقتصاد الذي أصبح يعتمد بشكل متزايد على الوسائط الرقمية. وتكتسب هذه النقطة أهمية خاصة إذا أخذ في الاعتبار أن التقديرات الحديثة تشير إلى أن الاقتصاد الرقمي في إيران يمثل قرابة 5 إلى 6% من الناتج المحلي، وأن الانقطاع

الواسع للإنترنت قد يكلف الاقتصاد عشرات ملايين الدولارات يومياً، مع خسائر كبيرة في التجارة الإلكترونية والأنشطة المرتبطة بالمنصات الرقمية [39].

إلى جانب الدور الدفاعي والتمكيني، تشير معطيات عدة إلى أن إيران طوّرت قدرات سيبرانية هجومية ذات عائد اقتصادي، من خلال [40]:

1. هجمات الفدية التي تستهدف شركات ومؤسسات في دول أخرى، حيث يتم تشفير بياناتها والمطالبة بفدية غالباً ما تُدفع بعملة مشفرة يصعب تتبعها.
2. عمليات اختراق تستهدف منصات مالية، أو شركات تكنولوجيا، أو بنوك، بهدف الاستيلاء على أموال أو بيانات يمكن بيعها في الأسواق السوداء الرقمية.

رغم أن حجم العائدات المباشرة من هذه العمليات يصعب تقديره بدقة، إلا أن تقارير أمنية دولية تشير إلى أن بعض مجموعات الرانسوموير المرتبطة بإيران حققت نسب أرباح مرتفعة في حملات متتالية تصل إلى 50 مليون دولار سنوياً [41]، ما يدل على احتراف متزايد في توظيف القدرات الهجومية لأهداف مالية. ومع أن هذه العوائد قد لا تضاهي عوائد النفط المخفّى أو الكريبتو المرتبط بالتجارة، إلا أنها تظل جزءاً مكتملاً لمنظومة التمويل في ظل العقوبات، وتؤكد أن الأمن السيبراني أصبح – في بعض جوانبه – قناة لإنتاج القيمة وليس فقط لحمايتها.

المطلب الثالث

فاعلية منظومة الهندسة الاقتصادية للأمن السيبراني وحدودها والآفاق المستقبلية

أولاً: فاعلية المنظومة

تظهر المعطيات أن الهندسة الاقتصادية للأمن السيبراني في إيران حققت عدداً من الأهداف [42]:

1. تمكين استمرار تدفقات مالية بمليارات الدولارات عبر شبكات بنوك الظل والكريبتو، رغم القيود الرسمية على النظام المصرفي.
2. تقليل الاعتماد على القنوات المالية التقليدية الخاضعة لسيطرة القوى الكبرى، واستبدالها جزئياً بقنوات رقمية-سيبرانية أكثر مرونة.
3. الحفاظ على القدرة على تمويل سياسات إقليمية وبرامج عسكرية وأمنية، ما يشير إلى نجاح نسبي في تحييد جزء من آثار العقوبات.

وفي هذا السياق، لم تقتصر فاعلية هذه المنظومة على الاستمرارية فقط، بل امتدت إلى تحقيق عوائد اقتصادية مباشرة وغير مباشرة، نتيجة توظيف الأمن السيبراني والعملة الرقمية كأدوات ضمن الاستراتيجية الاقتصادية. تتوزع هذه العوائد والأرباح على عدة مسارات استراتيجية مترابطة وعلي النحو الآتي [43]:

1. الالتفاف على العقوبات والتمويل الموازي:

- أ- اقتصاد الظل الرقمي: بلغ إجمالي نشاط العملات الرقمية في إيران نحو 7.8 مليار دولار، مع تقديرات تشير إلى أن الكيانات المرتبطة بالحرس الثوري تستحوذ على ما يقارب نصف هذا النشاط.
- ب- تمويل الواردات: سمح اعتماد العملات المشفرة في تسوية بعض المعاملات التجارية بتجاوز القيود المفروضة على النظام المصرفي العالمي، بما في ذلك القيود المرتبطة بنظام (SWIFT)، مما وفر قناة بديلة لتمويل الواردات.

2. عوائد تعدين البيتكوين (تحويل الطاقة إلى قيمة رقمية) اعتمدت إيران على استغلال مواردها من النفط والغاز في توليد كهرباء مدعومة تُستخدم في تعدين البيتكوين، وهو ما يمثل آلية لتحويل الموارد الطبيعية إلى أصول رقمية يصعب تعقبها أو تجميدها، تشير التقديرات إلى أن قطاع التعدين يمكن أن يولد ما بين 700 مليون إلى مليار دولار سنوياً لصالح الخزنة العامة [44].
3. الجباية والرسوم السيبرانية: منها رسوم الملاحاة بالبيتكوين ظهرت تقارير تشير إلى أن إيران بدأت في طلب دفع مبالغ ضخمة من عملة البيتكوين كرسوم مرور للسفن عبر مضيق هرمز لضمان عدم تعقب هذه الأموال أو مصادرتها بسبب العقوبات.
4. التجسس الاقتصادي وسرقة البيانات: تُستخدم القدرات السيبرانية للحصول على بيانات وملكية فكرية تقلل كلف التطوير. تستهدف مجموعات مثل (Seedworm) و (MuddyWater) قطاعات حيوية كالصحة والطاقة والتكنولوجيا.

5. **التحوط المالي ضد تدهور العملة:** برزت العملات المشفرة كأداة للتحوط المالي في ظل تراجع العملة المحلية. وتمثل ملاذاً آمناً يلجأ جزء من المجتمع إليها لحماية المدخرات، مما يوفر سيولة تدعم الاقتصاد الرقمي.

ثانياً: حدود المنظومة وهشاشتها

تعاني هذه المنظومة من عدد من القيود البنيوية الواضحة [42]:

1. تطوّر أدوات تحليل سلاسل الكتل والرقابة الدولية على منصات الكريبتو، ما يزيد القدرة على تتبّع التدفقات المرتبطة بإيران وإغلاق بعض القنوات.
2. تعرّض المنصات المحلية والخدمات الرقمية لهجمات مضادة من خصوم خارجيين، ما يهدّد الأصول الرقمية ويضعف ثقة المستخدمين.
3. خطر إساءة الاستخدام الداخلي، والفساد، وتضارب المصالح بين الفاعلين المختلفين داخل المنظومة.
4. الاقتصاد الرقمي الموازي ليس اقتصاداً بلا تكلفة، بل اقتصاداً عالي الكلفة من حيث التشغيل والصيانة والحماية وإخفاء الأثر وإدارة المخاطر. وكلما توسعت الشبكات غير الرسمية، زادت الحاجة إلى طبقات أعمق من التشفير والوساطة والتأمين، ما يرفع كلفة المعاملة ويقلل من كفاءة الاقتصاد الكلية.

ثالثاً: الآفاق المستقبلية وفق منهج بناء السيناريوهات

يتحدد مستقبل الهندسة الاقتصادية للأمن السيبراني في إيران وفق تفاعل مجموعة من المتغيرات، أبرزها مستوى العقوبات والضغط الدولي، وتطور قدرات التتبع والرقابة على التدفقات المالية الرقمية، ومستوى التعاون الدولي في مواجهة قنوات الالتفاف، وقدرة إيران على تطوير بنيتها التقنية والمؤسسية. وتكتسب هذه المتغيرات أهمية خاصة مع استمرار تعرض البنية الرقمية والمالية الإيرانية للضغط؛ فقد فرضت الولايات المتحدة في يونيو 2026 عقوبات على منصات أصول رقمية إيرانية رئيسية، من بينها Nobitex، وربطت الإجراءات باستخدامها في معاملات مرتبطة بالالتفاف على العقوبات [45]، في حين تؤكد الدراسات الحديثة استمرار تطور أدوات الرقابة والتحكم في البنية الرقمية الإيرانية. وبناءً على ذلك، يمكن استشراف ثلاثة مسارات مستقبلية رئيسية:

- 1- **سيناريو التحول الرقمي الاستراتيجي:** يفترض نجاح إيران في تطوير بنيتها الرقمية والمالية بما يعزز استخدام الأصول الرقمية والأمن السيبراني في إدارة جزء من معاملاتها الاقتصادية. ويتحقق هذا المسار مع استمرار قدرتها على الابتكار وتوسيع البنية الرقمية المحلية والاستفادة من القنوات البديلة، مع بقاء العقوبات دون مستوى الإغلاق الكامل. وفي هذه الحالة، قد يتشكل نظام مالي-رقمي هجين يمنح الاقتصاد الإيراني قدرة أكبر على التكيف مع القيود الخارجية، وإن ظل معرضاً للرقابة والتتبع الدوليين.
- 2- **سيناريو الاستمرار التكيفي:** يقوم على استمرار النموذج الحالي القائم على الجمع بين القنوات الرسمية والبديلة، دون تحول جذري في بنية الاقتصاد أو انهياره. وتستمر إيران في استخدام الوسطاء والأدوات الرقمية والقنوات المالية غير المباشرة، مع إعادة تشكيلها كلما تعرضت للضغط. ويبدو هذا السيناريو الأكثر ترجيحاً في ضوء استمرار قدرة الشبكات الإيرانية على التكيف، مقابل ارتفاع تكاليفها ومخاطرها نتيجة العقوبات وتطور أدوات الرقابة. وتدعم الإجراءات الأمريكية الأخيرة ضد منصات الأصول الرقمية الإيرانية استمرار هذا التوازن بين التكيف والضغط.
- 3- **سيناريو الانكشاف والتقييد الحاد:** يفترض تصاعد العقوبات وتكامل جهود الرقابة الدولية مع تطور تقنيات تتبع التدفقات المالية والرقمية، بما يؤدي إلى تضيق القنوات الموازية واستهداف بنيتها التحتية. وفي هذا المسار، ترتفع كلفة استخدام الوسطاء والمنصات الرقمية، وتراجع قدرة الاقتصاد الموازي على أداء وظائفه، خصوصاً مع تعرض بنيته السيبرانية للاستهداف. وقد يؤدي ذلك إلى زيادة الضغوط على الاقتصاد الإيراني وتعميق هشاشته، رغم إمكانية لجوء طهران إلى قنوات بديلة جديدة.

تكشف السيناريوهات الثلاثة أن مستقبل الهندسة الاقتصادية للأمن السيبراني في إيران لن يتحدد بعامل واحد، بل بنتيجة التفاعل بين الضغط الخارجي والابتكار الداخلي والقدرة على إعادة تشكيل القنوات المالية والرقمية. وبالاستناد إلى الاتجاهات الحالية، يبدو سيناريو الاستمرار التكيفي هو الأكثر ترجيحاً؛ إذ تشير المعطيات إلى استمرار استخدام القنوات الرقمية والمالية البديلة بالتوازي مع تصاعد إجراءات الرقابة والعقوبات، بما يرجح استمرار حالة التكيف تحت الضغط بدلاً من التحول الجذري أو الانهيار الكامل.

الخاتمة والاستنتاجات

خلصت الدراسة إلى أن العقوبات الدولية، ولا سيما بعد عام 2018، لم تقتصر على إضعاف الاقتصاد الإيراني أو تقييد اندماجه في النظام المالي العالمي، بل دفعت إيران إلى تبني مسارات جديدة لإعادة تنظيم اقتصادها على أسس رقمية وسيبرانية. وأن الأمن السيبراني لم يعد مجرد وسيلة لحماية الأنظمة والشبكات، بل تحول إلى عنصر بنوي في إدارة الاقتصاد الموازي، وتأمين شبكات بنوك الظل، وشركات الواجهة، ومنصات العملات المشفرة، بما يجعل مفهوم الهندسة الاقتصادية للأمن السيبراني إطاراً مناسباً لفهم الحالة الإيرانية.

كما بينت الدراسة أن هذا النموذج حقق قدراً من الفاعلية في تمكين الاقتصاد الإيراني من الاستمرار تحت الضغط، لكنه بقي نموذجاً هشاً وعالي الكلفة، يقوم على الوساطة والتشهير وإخفاء الأثر أكثر مما يقوم على الكفاءة والاستقرار. ومن ثم، فإن الهندسة الاقتصادية للأمن السيبراني في إيران تمثل استجابة تكيفية ناجحة نسبياً، لكنها لا ترقى إلى مستوى الاستقلال الاقتصادي الكامل، خاصة مع تطور أدوات الرقابة والتتبع وتزايد الضغوط الجيوسياسية والمالية. ووصلت الدراسة إلى مجموعة من الاستنتاجات:

1. العقوبات الدولية بعد عام 2018 كانت عاملاً رئيساً في دفع إيران إلى إعادة تشكيل بنيتها الاقتصادية والمالية، لا سيما عبر القنوات الرقمية والموازية.
2. تبين أن الأمن السيبراني في الحالة الإيرانية تجاوز وظيفته التقليدية الدفاعية، وأصبح أداة لتمكين الاقتصاد الموازي وحماية تدفقاته المالية والتجارية.
3. أن شبكات بنوك الظل وشركات الواجهة لعبت دوراً محورياً في إبقاء جزء مهم من النشاط المالي الإيراني خارج النظام المصرفي التقليدي.
4. أظهرت البيانات أن العملات المشفرة أصبحت قناة اقتصادية فعلية لإعادة تدوير الأموال وتحريك القيمة، وليست مجرد أداة هامشية أو تجريبية.
5. أسهمت القنوات الرقمية والموازية في استمرار بعض الأنشطة الاقتصادية والمالية الحيوية، رغم ارتفاع تكاليفها ومخاطرها.
6. أن النموذج الإيراني يمثل مثلاً واضحاً على قدرة الدول الخاضعة للعقوبات على ابتكار أدوات اقتصادية وسيبرانية بديلة، لكنه مثال على البقاء تحت الضغط أكثر من كونه نموذجاً للاستقلال أو الازدهار المستدام.

المصادر

- [1] Dani Rodrik (2007), One Economics, Many Recipes: Globalization, Institutions and Economic Growth, Princeton University Press, P58.
- [2] World Bank, (2002). World Development Report 2002: Building Institutions for Markets, Washington, D.C. P34.
- [3] Dani Rodrik, (2007) One Economics, Many Recipes: Globalization, Institutions and Economic Growth, Princeton University Press, P62.
- [4] Organisation for Economic Co-operation and Development (OECD). (2022), OECD Policy Framework on Digital Security: Cybersecurity for Prosperity (Paris: OECD Publishing, 2022), <https://doi.org/10.1787/a69df866-en>
- [5] Financial Crimes Enforcement Network (FinCEN), (2026), FinCEN Alert on the Use of Front Companies, Financial Facilitators, and Digital Asset Infrastructure by Iran's Islamic Revolutionary Guard Corps to Evade Sanctions and Launder Proceeds, FIN-2026-Alert002 (Washington, DC: U.S. Department of the Treasury, May 11, 2026). <https://www.fincen.gov/system/files/2026-05/FinCEN-Alert-IRGC.pdf>
- [6] Singer, P. W., and Allan Friedman. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, P23-35.
- [7] OECD. (2022) Cybersecurity Policies for the Digital Economy. Paris: OECD, p 25-40.
- [8] قاسمي، شعيب و بلغيث، فؤاد. (2020). الاستراتيجيات الدولية في مكافحة الجريمة السيبرانية دراسة حالة الجزائر، رسالة ماجستير مقدمة لكلية الحقوق والعلوم السياسية / جامعة العربي التبسي - تبسة. الجزائر.

- [9] OECD, (3February, 2026). Economic Security in a Changing World (Paris: OECD Publishing, 2025); Reuters, "Iran's Surging Crypto Activity Draws US Scrutiny".
- [10] نيكولاس مولدر، (2022)، سلاح العقوبات الاقتصادية، مجلة التمويل والتنمية، صندوق النقد الدولي، يونيو، ص23، متاح على الرابط: <https://www.imf.org/-/media/files/publications/fandd/article/june/ar/mulder.pdf2022>
- [11] OECD, (2025). Economic Security in a Changing World, Ibid.
- [12] Henry Farrell and Abraham L. Newman, (2023) Underground Empire: How America Weaponized the World Economy (New York: Henry Holt, P89.
- [13] World Bank. (2024). *GDP (current US\$) - Iran, Islamic Rep.* World Bank Open Data. <https://data.albankaldawli.org/indicator/NY.GDP.MKTP.CD?locations=IRdata.albankaldawli>
- [14] إيران برس. (1February, 2025). إيران تحتل المرتبة الخامسة عالميًا في الموارد الطبيعية والمنجمية. <https://arabic.iranpress.com>
- [15] Statistical Center of Iran. (2025). Consumer price index reports for 2025. Tehran, Iran.
- [16] United Against Nuclear Iran. (n.d.). International Iran sanctions database. Retrieved August 9, 2026, from <https://www.unitedagainstinucleariran.com/international-iran-sanctions-database>
- [17] محمد، احمد فاروق عباس، تامر فكري عطيفه النجار، (2025)، الاقتصاد الإيراني الواقع والتحديات، المجلة العلمية للبحوث التجارية، العدد الثاني، الجزء الثاني، ابريل.
- [18] عزيز، فوزية اكرم، (2025)، اثر العقوبات الاقتصادية الدولية على التنمية الاقتصادية ايران انموذجاً، مجلة الريادة للمال والاعمال، المجلد السادس، العدد 1.
- [19] U.S. Department of the Treasury. (2025, June 6). "Treasury Sanctions Iranian Network Laundering Billions for Regime Through Shadow Banking Scheme." Washington, DC: U.S. Department of the Treasury. <https://home.treasury.gov/news/press-releases/sb0159>
- [20] U.S. Department of the Treasury. (2025, April 18). Treasury imposes additional sanctions on Iran's shadow fleet as part of maximum pressure campaign. <https://home.treasury.gov/news/press-releases/sb0026>
- [21] U.S. Department of the Treasury. (2025, April 16). Treasury increases pressure on Chinese importers of Iranian oil. <https://home.treasury.gov/news/press-releases/sb0090>
- [22] Financial Action Task Force. (2025, June 13). High-risk jurisdictions subject to a call for action: 13 June 2025. <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-june-2025.html>
- [23] Financial Action Task Force. (2025). Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers. <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Udate-VA-VASPs.pdf.coredownload.pdf>
- [24] World Bank. (2023). Iran Economic Monitor, Spring/Summer 2023: Moderate growth amid economic uncertainty. World Bank. <https://openknowledge.worldbank.org/server/api/core/bitstreams/1c94cb80-5f40-408f-a5c7-c7cfd97dc438/content>
- [25] النجار، زينة عبدالكريم، (2024)، العقوبات الاقتصادية وتأثيراتها على الاقتصاد الرقمي: دراسة مقارنة (العراق وايران انموذجاً)، مجلد 4 عدد 37، مجلة تكريت للعلوم السياسية، جامعة تكريت.
- [26] Financial Crimes Enforcement Network (FinCEN)(2025). Illicit Finance Risk Assessment,p.32
- [27] Fathi, Abdelaziz.(2025), "FinCEN: Iran Used Dubai, Hong Kong, Singapore to Move \$9B Despite Sanctions." FinanceFeeds, November 7, 2025. FinanceFeeds
- [28] التميمي، علي ثجيل يوسف، محمد بيدار برجين عليا،(2024)، دور الاقتصاد المقاوم في تعزيز استقرار الاداء الاقتصادي جمهورية ايران الاسلامية انموذجاً، مجلة الجامعة العراقية، العدد 69، الجزء 3.
- [29] Schneider, Friedrich, and Dominik H. Enste.(2013), The Shadow Economy: An International Survey. Cambridge: Cambridge University Press.p216.

- [30] Chainalysis.(2026), Crypto Crime Report 2025. New York: Chainalysis,p.45
- [31] بوثلجة، ياسين. (2024). الاقتصاد الإيراني بين تأثير العقوبات الأمريكية وأساليب المواجهة. مجلة السياسة العالمية، المجلد(8)، العدد(1)، ص514.
- [32] Jon R. Lindsay,(2013), "Stuxnet and the Limits of Cyber Warfare," Security Studies 22, no. 3,p365–404, <https://doi.org/10.1080/09636412.2013.816122>
- [33] Raphael S. Cohen et al.,(2026) "National Cyber Power Index 2024" (Harvard Belfer Center, forthcoming/cited in commentary), <https://www.belfercenter.org/>
- [34] عبدالمنعم، وسن احسان، احمد قيس احمد، 2022، تكنولوجيا المعلومات والامن السيبراني، ط1، بغداد: مطبعة الرفاه، ص86.
- [35] عزي، محمد فريد،(2021) النشاط السيبراني الايراني مابين السرية والعلن، مركز تريندز للبحوث والاستشارات، 5ديسمبر 2021، متاح على الرابط: [TRENDS Research & Advisory - النشاط السيبراني الايراني: ما بين السرية والعلن](https://www.trendsresearch.com/iranian-cyber-activity)
- [36] Rapid Labs. (2026) "Iran's Cyber Playbook in the Escalating Regional Conflict." Rapid7, March 12, 2026. <https://www.rapid7.com/blog/post/tr-iran-cyber-playbook-escalating-regional-conflict/>
- [37] FinCEN,(2025), "FinCEN Identifies 9\$Billions of Iranian Shadow Banking Activity in 2024," October 22, 2025, <https://www.fincen.gov/news/news-releases/fincen-identifies-9-billion-iranian-shadow-banking-activity-2024>
- [38] Chainalysis,(2026), "OFAC Sanctions Nobitex and Iranian Cryptocurrency Exchanges," June 2, 2026, <https://www.chainalysis.com/blog/ofac-sanctions-iranian-crypto-exchanges-june-2026/>
- [39] Iran International, "Iran's digital economy battered by prolonged blackout," April 13, 2026, <https://www.iranintl.com/en/202604149190>
- [40] عبدالحميد، نغم مجدي،(2025)، تحولات المواجهة: قراءة في الاتجاهات السيبرانية الإيرانية والمواجهة مع إسرائيل، مركز شمس للاستشارات والبحوث الاستراتيجية، أغسطس 20. ص187.
- [41] The Record.(2025). "Iranian Ransomware Group Pay2Key.I2P Offers Bigger Payouts." July 7.p4.
- [42] الرزوي، حسن مظفر (2023) ، تأثير تحولات ايران على الاستراتيجيتها السيبرانية وانعكاساتها المحتملة على المجال الجيوسياسي السيبراني، مجلة مدارات ايرانية،المركز الديمقراطي العربي، المجلد8، العدد 22، ص93_94.
- [43] Abdallah Al Jouaid,(10.03.2026) Iran's Crypto Sector Was a Lifeline Through Sanctions. War Could Shut It Down Newsletter, , <https://www.wired.me/story/irans-crypto-sector-was-a-lifeline-through-sanctions-war-could-shut-it-down>
- [44] Tangermann, Victor. (April 8, 2026) "Iran Demanding Huge Bitcoin Payments to Pass Through Strait of Hormuz." Futurism. <https://futurism.com/future-society/iran-demanding-bitcoin-payments-pass-strait-of-hormuz>
- [45] U.S. Department of the Treasury. (2026, June 2). Economic Fury targets Iran's largest digital asset exchange for terror finance and sanctions evasion. <https://home.treasury.gov/news/press-releases/sb0519>