المركز العربي للأبحاث ودراسة السياسات
Arab Center for Research & Policy Studies

تقييم حالة | 26 أيار/ مايو، 2022

عمليات ضبط المعلومات في الفضاء السيبراني الإيراني: استراتيجية الحرب الناعمة

ميليندا كوهون

وحدة الدراسات الإيرانية

عمليات ضبط المعلومات في الفضاء السيبراني الإيراني: استراتيجية الحرب الناعمة

سلسلة: تقييم حالة

26 أيار/ مايو، 2022

وحدة الدراسات الإيرانية

ميلندا كوهون

طالبة دكتوراه في برنامج دراسات الشرق الأدنى والأوسط في جامعة واشنطن. تتركز اهتماماتها البحثية في عمليات ضبط المعلومات ومحبّي الألعاب الإلكترونية وصناعتها في إيران والخارج. أما أطروحتها التي موّلها برنامج الزمالة للتفوّق في معهد روشان للدراسات الفارسية ومنحة برنامج الزمالة لمجلس أبحاث العلوم الاجتماعية عن أطروحة البيانات الاجتماعية، وعنوانها «التعقيدات العاطفية: محبّو الألعاب الإلكترونية الإيرانيون على وسائل التواصل الاجتماعي والألعاب الإلكترونية»، فتكشف كيف تولّد التجربة اليومية للعقوبات والرقابة مشاعرَ متقلّبة وشعورًا بالانتماء لدى محبّي هذه الألعاب الإيرانيين. وعملت كوهون على نحو واسع أيضًا على مشاريع الإنسانيات الرقمية، ونشرت في عام 2020، في المجلّة الأكاديمية المحكّمة *Interdisciplinary Digital Engagement in Arts & Humanities, IDEAH* (وهي مجلّة للمشاركة الرقمية المتعدّدة التخصّصات في الفنون والعلوم الإنسانية) دراسةً عنوانها «إيران الرقمية: قوّة ناعمة وتأثير الألعاب الإلكترونية».

المركز العربيّ للأبحاث ودراسة السّياسات مؤسّسة بحثيّة عربيّة للعلوم الاجتماعيّة والعلوم الاجتماعيّة التطبيقيّة والتّاريخ الإقليميّ والقضايا الجيوستراتيجية. وإضافة إلى كونه مركز أبحاثٍ فهو يولي اهتمامًا لدراسة السّياسات ونقدها وتقديم البدائل، سواء كانت سياسات عربيّة أو سياسات دوليّة تجاه المنطقة العربيّة، وسواء كانت سياسات حكوميّة، أو سياسات مؤسّسات وأحزاب وهيئات.

يعالج المركز قضايا المجتمعات والدول العربيّة بأدوات العلوم الاجتماعيّة والاقتصاديّة والتاريخيّة، وبمقاربات ومنهجيّات تكامليّة عابرة للتّخصصات. وينطلق من افتراض وجود أمن قوميّ وإنسانيّ عربيّ، ومن وجود سماتٍ ومصالح مشتركة، وإمكانيّة تطوير اقتصاد عربيّ، ويعمل على صوغ هذه الخطط وتحقيقها، كما يطرحها كبرامجَ وخططٍ من خلال عمله البحثيّ ومجمل إنتاجه.

المركز العربيّ للأبحاث ودراسة السّياسات

شارع الطرفة، منطقة 70

وادي البنات

ص. ب: 10277

الظعاين، قطـر

هاتف: 40354111 974 +

www.dohainstitute.org

المحتويات

البنية التحتية البيروقراطية لشبكة الإنترنت في إيران 2

الضغط لضبط المعلومات على شبكة الإنترنت في أثناء الاحتجاجات 4

«مشروع قانون حماية مستخدمي الفضاء السيبراني» 6

المراجع 8

يشكّل الفضاء السيبراني حيّزًا رمزيًّا عالميًّا تحدث فيه التطوّرات على شبكة الإنترنت. وهو أيضًا الواقع الافتراضي، حيث يترجم الأفراد معنى الصور والكلمات وأشرطة الفيديو، ويتواصلون فيما بينهم عبر الرسائل الفورية أو البريد الإلكتروني. كما يمارسون الألعاب الافتراضية وينشئون مواقع إلكترونية، حتّى إنهم ينشئون عوالم افتراضية تستند إلى أماكن خيالية أو واقعية. صحيحٌ أنّ الإنترنت في إيران يتألّف من «أمكنة عدّة» ليست بالضرورة «'إيرانية' بأي شكلٍ مباشرٍ»، لكنّ الفضاء السيبراني الإيراني يحوي فوارق دقيقة خاصة به، تتعلّق بالتجارب التي يعيشها المواطنون الإيرانيون والخيارات السياسية التي تتّخذها الحكومة[1]. لذلك، يمكن وصفه بأنه مجموعة من الأمكنة على شبكة الإنترنت المتوافرة ضمن فضاءٍ سيبراني عالميٍ شامل، يسعى من خلاله المواطنون الإيرانيون، المنتسبون إلى هذا الفضاء، للتعبير عن ذواتهم عبر الإنترنت بطرائقٍ اجتماعية سياسية وثقافية، وعبر منصّات رقمية وعوالم افتراضية. في الإطار نفسه، تعمل العديد من الهيئات الحكومية الإيرانية على تثبيت وجودها عبر الفضاء السيبراني لممارسة القمع الإلكتروني على المواطنين الإيرانيين، من خلال تدابير قمعية وفرض شروطٍ قانونية، بما في ذلك على سبيل المثال لا الحصر، شنّ هجماتٍ إلكترونية عدائية والسجن والعنف وتصفية محتويات الإنترنتFiltered Internet والإبطاء المتعمد لسرعته (ما يُعرف بالاختناق Throttling)، وصولاً إلى الانقطاع الكليّ لشبكة الإنترنت. لذلك، يشكّل الفضاء السيبراني الإيراني حيّزًا وجوديًّا وسياقًا حقيقيًّا يتعلّق تحديدًا بالتجربة الاجتماعية الثقافية للمواطنين، ويرتبط بعمليات ضبط الحكومة للمعلومات. ولا تستند استراتيجية ضبط المعلومات هذه إلى توسّع القوة الناعمة في إيران وفي جميع أنحاء العالم فحسب، بل تعتمد أيضًا على الحرب الناعمة (جنگِ نرم باللغة الفارسية).

وفي الوقت الذي تستخدم فيه جمهورية إيران الإسلامية الفضاء السيبراني لممارسة الرقابة على مواطنيها ومراقبتهم، بما في ذلك الحرب الإلكترونية لإلحاق الضرر بنُظم المعلومات خارج البلاد، فإنها تسعى باستراتيجية القمع الإلكتروني للحرب الناعمة التي تتّبعها إلى الحدّ من تداول المعلومات عبر شبكة الإنترنت لمنع «نشر الأفكار والثقافة والتأثيرات الأجنبية باعتماد تكنولوجيا المعلومات والاتصالات» داخل البلاد[2]. إن الحرب الناعمة هي استراتيجية لضبط المعلومات التي تحظر صراحةً على الأجانب، مثل الغرب والولايات المتحدة الأميركية تحديدًا، الوصول إلى المعلومات، وفي الوقت نفسه، منع انتشار المعلومات الصادرة عن الغرب بين المواطنين الإيرانيين. وإضافة إلى نشر المعلومات المضلّلة، تسعى استراتيجية الحكومة لضبط المعلومات الخاصة بالقوة الناعمة، لتقديم سردية الدولة من خلال حملتها الأيديولوجية المرتبطة ارتباطًا وثيقًا بإرثها الإمبريالي الفارسي وأساطيرها وتاريخها، أو بعبارة أخرى، السيطرة على الثقافة[3]. وقد برز إلى الواجهة أجندة إيران المحافظة والمتعلّقة بضبط المعلومات، في محاولتها الأخيرة لعزل البلاد عن الفضاء السيبراني من خلال «قانون حماية حقوق مستخدمي الفضاء السيبراني». وتحول العقوبات الأميركية دون وصول الإيرانيين إلى أدوات التكنولوجيا الرئيسة ومواقع إلكترونية أساسية مثل أمازونAmazon ، وغوغل Google، وآبل Apple، والألعاب الإلكترونية المتعدّدة اللاعبين على الإنترنت مثل لعبةWorld of Warcraft ؛ ما يؤدي فعليًّا إلى فصل الإيرانيين عن الفضاء السيبراني. وما يفاقم الأمور سوءًا، هو أنّ الإيرانيين يعيشون أصلًا استراتيجية الحرب الناعمة والقوة الناعمة التي أطلقتها الحكومة لعزلهم أكثر فأكثر عن الفضاء السيبراني العالمي. وتسهّل العقوبات الأميركية من جهتها عملية المراقبة والرقابة في إيران؛ إذ إنها تحجب عن المواطنين إمكانية الوصول إلى مختلف المنصّات والبرمجيات والأدوات على الإنترنت. ولا تزال حرية المواطنين الإيرانيين باستخدام الإنترنت مهدّدة بسبب الدعم المتزايد لـ «قانون حماية حقوق مستخدمي الفضاء السيبراني»، والذي من شأنه أن ينشئ شبكة إنترنت محلية حقيقية معزولة عن الفضاء السيبراني العالمي.

---

1 Niki Akhavan, *Electronic Iran: The Cultural Politics of an Online Evolution* (New Brunswick: Rutgers University Press, 2013), p. 2.

2 E.L. Blout, "Soft War: Myth Nationalism, and Media in Iran," *The Communication Review*, vol. 20, no. 3 (2017), p. 212, accessed on 10/3/ 2021, at: https://bit.ly/3rMeCGO

3 Seth G. Jones & Danika Newlee, "The United States' Soft War with Iran," *CSIS Briefs*, Center for Strategic & International Studies (June 2019), p. 1, at: https://bit.ly/37DjUhb

البنية التحتية البيروقراطية لشبكة الإنترنت في إيران

كان تاريخ الجمهورية الإسلامية الإيرانية في مراقبة المعلومات الآتية من جميع أنحاء العالم، وفي وسائل الإعلام المحلية، واضحًا منذ تأسيسها في عام 1979. لكن مع ظهور الإنترنت في تسعينيات القرن العشرين، إضافة إلى التوترات بين العديد من الوكالات البيروقراطية في إيران، ركّزت الدولة على جودة خدمات الشبكة والوصول إليها[4]. وخلال فترة انتشار مقاهي الإنترنت في أوائل العقد الأول من القرن الحالي، بات التدوين الذي كان رائجًا وسيلةً قوية لإيصال الأصوات السياسية المعارضة للدولة؛ ما أدّى إلى اعتقال مدوّنين مثل سينا مطلبي في عام 2003 وحسين درخشان في عام 2008، وتسبّب في تعزيز المراقبة على المعلومات المتوافرة على الإنترنت. وبعد اقتراحات قدّمت في عام 2005 للحدّ من ظاهرة المعارضة بين المدوّنين، أصدر المرشد الأعلى، آية الله علي خامنئي، أمرًا بإنشاء مركز بيروقراطي للشبكة الداخلية (إنترانت Intranet) الوطنية عُرف باسم شبكة المعلومات الوطنية National Information Network بهدف تطوير شبكة إنترانت إيرانية وطنية تنعم ببنية تحتية تقدّم خدمات للقطاعَين العام والخاص في عام 2006. وتمنع شبكة المعلومات الوطنية أساسًا الأجانب من الوصول إلى الفضاء السيبراني الإيراني، وذلك من خلال مفاتيح التحويل وأجهزة التوجيه ومراكز البيانات، وهي تحثّ في الوقت نفسه الجمهور الإيراني على استخدام المواقع الإلكترونية ومواقع التواصل الاجتماعي المحلية. ويحافظ برنامج شبكة المعلومات الوطنية التابع للحكومة الإيرانية، الذي بلغت تكلفته مليارات الدولارات، على سير عمل الإنترنت من خلال محرّكات البحث والبريد الإلكتروني ووسائل الإعلام، أو بالأحرى شبكة محلية لتصفية محتوى الإنترنت، والتضييق في الوقت نفسه على الحركة الدولية لمرور البيانات عبر شبكة الإنترنت، بخاصةٍ أثناء الاحتجاجات. وفرضت نُظُم الحظر الدولية، التي بدأت بحملة ضغط قصوى مارستها الولايات المتحدة وصولًا إلى العقوبات، على شبكة المعلومات الوطنية أن تعتمد استراتيجيات أكثر تطوّرًا على مرّ السنوات، ولا سيّما بغية منع أيّ تدخل أجنبي، بينما تعمل على زيادة سرعات الإنترنت[5]. وقد تجلّى ذلك في سياسة الأمن القومي التي تتبنّاها إيران في الحرب الناعمة وتدابير القوة الصلبة (مثل العنف وأحكام بالسجن) التي تنتهجها في حق المواطنين من خلال دفعهم لاستخدام شبكة المعلومات الوطنية[6]. وفي الوقت الذي يقتصر دور هذه الأخيرة على تنظيم محتوى الإنترنت ومراقبته والإشراف عليه، تتشكّل البنية التحتية لعملية مراقبة المعلومات لدى الحكومة الإيرانية من أهداف تتضارب فيما بينها بشدّة؛ إذ أنها تسعى لزيادة سرعة الإنترنت، بتوسيع عرض النطاق الترددّي Bandwidth، من خلال شركة الاتصالات السلكية واللاسلكية الإيرانية[7].

ليست شبكة المعلومات الوطنية الهيئة الحكومية الوحيدة في إيران التي تدعم المنافسة الاستراتيجية، وتساعد على التأثير الإقليمي في عملية المراقبة والرقابة على شبكة الإنترنت؛ للإبقاء على السيطرة الجيوسياسية، وتعزيز النزعة الإقليمية للفضاء السيبراني الإيراني من خلال الحرب الناعمة. وتتّخذ العديد من الهيئات الحكومية الأخرى تدابير فعّالة، بما في ذلك الشرطة السيبرانية الإيرانية، والمجلس الأعلى للفضاء السيبراني الإيراني، وقيادة الدفاع السيبراني الإيراني، والمنظمة الوطنية للدفاع السلبي الإيراني، والمركز الوطني للفضاء السيبراني الإيراني، وفيلق حرس الثورة الإسلامية (سپاه) ومنظمة الحرب الإلكترونية والدفاع السيبراني التابعة للحرس الثوري الإيراني، ومجلس الباسيج السيبراني، إضافة إلى تعيين مجموعات بالوكالة

4 Babak Rahimi, "Cyberdissent: The Internet in Revolutionary Iran," *Middle East Review of International Affairs*, vol. 7, no. 3 (2003), p. 102, accessed on 23/5/2022, at: https://bit.ly/3LdHGPt

5 Loqman Salamatian et al., "The Geopolitics behind the Routes Data Travel: A Case Study of Iran," *Journal of Cybersecurity*, vol. 7, no. 1 (2021), p. 8, accessed on 23/5/2022, at: https://bit.ly/3Kby0DN

6 Farzan Sabet & Roozbeh Safshekan, "Soft War: A New Episode in the Old Conflicts Between Iran and the United States," *Iran Media Program* (2013), p.18, accessed on 23/5/2022, at: https://bit.ly/3L9RoCg

7 "Iran Orders Bandwidth Expansion to Boost Internet Speed," *PressTV*, 23/2/2022, accessed on 10/4/2022, at: https://bit.ly/3PB4Qlj

لشنّ عمليّات سيبرانية[8]. فعلى سبيل المثال، تراقب الشرطة السيبرانية الإيرانية، المعروفة بـ «فتا» (وهو المختصر باللغة الفارسية لمصطلح پليس فضای توليد وتبادل اطلاعات ايران، أو پليس فتا)، نشاطات الإيرانيين على الشبكة الإلكترونية؛ ما يؤدي إلى الملاحقة القضائية للمعارضين المزعومين الناشطين على الشبكة الإلكترونية، وإغلاق المواقع الإلكترونية التي تراها الشرطة الإلكترونية غير إسلامية ومبتذلة. وفي الوقت نفسه، تتحكّم اللجنة المكلّفة بتحديد المحتويات المسيئة بسياسات الرقابة، وتحدّث تباعًا قوائم المواقع الإلكترونية الخاضعة للرقابة، في حين تمنع منظمة الحرب الإلكترونية والدفاع السيبراني التابعة لفيلق حرس الثورة الإسلامية، المعروفة بالجيش السيبراني الإيراني، الهجمات الإلكترونية، وتنفّذ هجمات مضادّة على المستوى العالمي. وتشكّل شركات الاتصالات وجهات فاعلة، مثل شركة الاتصالات المتنقّلة الإيرانية [وهي شركة تشغيل شبكات الاتصالات للهواتف المحمولة]، بالتنسيق مع هذه الهيئات الحكومية والهيئات الوكيلة، جزءًا لا يتجزأ من البنية التحتية لعملية الرقابة على شبكة الإنترنت، ولا سيّما في ظل طمس يحول دون انتشار المعلومات عبر تكنولوجيا الاتصالات وأجهزة الهواتف المحمولة، وتعمل كلها بتفويض من شركة الاتصالات السلكية واللاسلكية الإيرانية التي تتحكّم جميعها في مستخدمي الإنترنت الذين يبلغ عددهم 57.4 مليون مستخدم من أصل ما يزيد على 82 مليون شخص يعيشون في إيران[9].

وبسبب البيروقراطية المفرطة في عمليات ضبط المعلومات في إيران، يعاني المواطنون الإيرانيون تدابير تقنية وتنظيمية شديدة، من خلال قطاع صناعة الاتصالات السلكية واللاسلكية، بما في ذلك شبكة المعلومات الوطنية. فهذه الشبكة تتيح للمستخدمين الوصول إلى الفضاء السيبراني. ومنذ نشأتها، سعت الشبكة لاستبدال الشبكة العامة للإنترنت العام كلّيًّا، بشبكة إلكترونية داخلية (إنترانت)، ومن ثمّ عزل المواطنين الإيرانيين عن الشبكة العالمية للإنترنت، في إطار استراتيجية الحكومة في حربها وقوّتها الناعمتين على الصعيدين المحليّ والعالمي. وأشار المسؤولون، بداية، إلى أن عزل إيران لن يؤدي إلى شلّ العديد من المؤسسات الإيرانية فحسب، بل يعرقل حركة اقتصاد الدولة من خلال عملية معقّدة. وفي مبادرة مماثلة لمبادرة «جدار الحماية العظيم الصيني»Great Firewall of China [10]، ارتأت الحكومة الإيرانية في عام 2006 أن تواصل شبكة المعلومات الوطنية في تطبيق استراتيجيتها بعيدة المدى في السيطرة على وسائط الإعلام والاتصالات الإلكترونية التي يستخدمها المواطنون الإيرانيون من خلال «شبكة مغلقة»[11]. إلى جانب شبكة المعلومات الوطنية، تحافظ العديد من الهيئات البيروقراطية الحكومية والجهات الوكيلة على هذه الشبكة المغلقة المعروفة بشبكة «الإنترنت الحلال» Halal Internet [12]، من خلال أدوات وأنظمة مراقبة لإدارة تصفّح المواطنين للفضاء السيبراني. جرى إطلاق شبكة الإنترنت الحلال في عام 2011، بهدف الترويج لنسخة متطوّرة من الشبكة الإلكترونية الوطنية الداخلية، بحجّةٍ رئيسة، مفادها أنّ استخدام المواطنين للشبكة العنكبوتية العالمية World Wide Web يقيّد حريتهم، ومن ثمّ يتطلّب تصفية محتوى الإنترنت وضبطه[13]. كانت شبكة الإنترنت الحلال التي أطلقها علي آغا محمدي، المعاون السابق لنائب الرئيس الإيراني للشؤون الاقتصادية والنائب في مجلس الشورى، تشمل أيضًا خطةً رئيسة لتعزيز تطوير الإنترنت وتكنولوجيّات الاتصالات، فضلًا عن الرقابة على

8 Congressional Research Service, “Iranian Offensive Cyber Attack Capabilities, IF11406· VERSION 1,” 13/1/2020, p. 1, at: https://bit.ly/37DjWWl

9 ARTICLE 19, “Iran: Tightening the Net 2020: After Blood and Shutdowns” (Creative Commons License 3.0, 2020), p. 13, accessed on 23/5/2022, at: https://bit.ly/3OJ3zIC

10 هي مبادرة تديرها وزارة الأمن العام في الحكومة الصينية، منذ عام 1998. وتسعى لمراقبة محتويات شبكة الإنترنت وتصفيتها وتقييدها من خلال تقنيات متطوّرة.

11 Center for Human Rights in Iran, “10 Things You Should Know about Iran’s Multi-Billion Dollar National Internet Project,” 3/10/2016, accessed on 23/5/2022, at: https://bit.ly/3Lao5zG

12 تسعى شبكة الإنترنت الحلال لتأمين تصفّح إلكتروني آمن تشرف عليه الحكومة الإيرانية من خلال مراقبتها محتويات المواقع الإلكترونية، على أن تراعي تلك المواقع المتوافرة في تلك الشبكة قواعد الدين الإسلامي وضوابطه.

13 Farid Shirazi, “Interrogating Iran’s Restricted Public Cloud: An Actor Network Theory Perspective,” *Telematics and Informatics*, vol. 31, no. 2 (May 2014), p. 1, accessed on 23/5/2022, at: https://bit.ly/3KbbvPp

الإنترنت بإنشاء نظام محميّ ومغلق كلّيًا. وبصورة رئيسة، قدّمت شبكة الإنترنت الحلال نفسها على أنها فرصة تتيح للنخبة السياسية التنافس على السلطة، وذلك فيما يتعلّق بمستخدمي الإنترنت الإيرانيين في الفضاء السيبراني. ويمكن أن تُعزى عملية تنفيذ شبكة الإنترنت الحلال إلى أنّها تندرج ضمن الحرب الناعمة، بوصفها ردًّا على الحركة الخضراء الإيرانية في عام 2009، والتي شملت احتجاجات شعبية ضد إعادة انتخاب محمود أحمدي نجاد رئيسًا لإيران. وأدّت الطبيعة المقيّدة لسياسات الرقابة الإيرانية إلى التشكيك في حرية استخدام الإنترنت في إيران.

الضغط لضبط المعلومات على شبكة الإنترنت في أثناء الاحتجاجات

في 12 حزيران/ يونيو 2009، أُعيد انتخاب أحمدي نجاد بنسبة 63 في المئة من الأصوات[14]. ردّت الحكومة الإيرانية على إعادة الانتخاب، بأن أغلقت مؤقتًا شبكة الإنترنت أثناء إعلان النتائج في 13 حزيران/ يونيو. ومع ذلك، رفض الإيرانيون الرئيس أحمدي نجاد المنتهية ولايته، مبلّغين عن مخالفات في أثناء عملية الاقتراع. ردًّا على ذلك، نفّذ بعض المواطنين الهجمات في شكل حجب الخدمة الموزّعة Distributed Denial-of-service (DDoS) Attack؛ أي تعطيل حركة المعلومات على الإنترنت لشبكة مستهدفة على نحوٍ خاص، وكانت تستهدف مواقع تدعم أحمدي نجاد وتسعى لتعبئة الاحتجاجات الحاشدة في طهران[15]. وهكذا اندلعت الاضطرابات الشعبية، التي شملت المواطنين الذين نزلوا إلى الشوارع متجاوزين عملية تصفية محتوى الإنترنت باستخدام أدوات مكافحة الرقابة مثل الشبكات الخصوصية الافتراضية Virtual Private Networks–VPNs[16] . وبنشر المواطنين للأحداث والتطوّرات على مواقع التواصل الاجتماعي مثل فيسبوك Facebook وتويتر Twitter، استطاعوا توثيق ما يعيشونه وتمكّنوا من بلورة خطاب عن وضعهم السياسي مع أقرانهم. كانت الشبكات الخصوصية الافتراضية، ولا تزال، وسيلة ضرورية للوصول الكامل إلى الفضاء السيبراني خارج النطاق الذي حدّده الفضاء السيبراني الإيراني. ويعود ذلك إلى حد بعيد إلى أنّ الحكومة الإيرانية تمتلك خوادم شبكة الإنترنت Internet Servers؛ ما يعني أنه ما لم يجرِ اعتماد شبكة خصوصية افتراضية، أو وسيلة لإخفاء الحركة عبر الإنترنت من خلال اتصالٍ مشفّر، فإنّ الحكومة قادرة على تحديد كل عنوان على الإنترنت يتفاعل معه المواطن في الفضاء السيبراني. وخلال الثورة الخضراء، سعت الدولة للسيطرة على السردية الثقافية، وحاولت معالجة عملية نشر المعارضة للمعلومات عبر الفضاء السيبراني الإيراني، وذلك بعرقلة عملية الوصول إلى الإنترنت وتعطيل الاتصالات الثابتة، بوصفهما جزءًا من استراتيجية حرب ناعمة لحظر استخدام الشبكة الخصوصية الافتراضية ونشر المعلومات. وإضافة إلى ممارسة التضييق (أو الاختناق) على عملية الاتصال بشبكة الإنترنت (أو إبطاء سرعات الإنترنت)، تضمّنت عملية القمع التي مارستها الحكومة ضد المتظاهرين العنف العسكري والتعذيب والاعتقالات ومسح بطاقات الذاكرة وتخريب أجهزة الحواسيب.

وعلاوة على انقطاع الإنترنت، عرقلت السلطات، إلى حدٍ بعيد، خدمة الرسائل النصّية القصيرة حتى لا يتمكّن المواطنون من إرسال رسائل تتضمّن آراء مناهضة للحكومة؛ ما يتيح تنظيم المعارضة بصفة أكبر. وللردّ على الانخراط السياسي للمواطنين في التحرّكات المعارضة للنظام، سعت الحكومة من خلال ما يسمّى شبكة الإنترنت الحلال إلى قمع أي معارضة، بما فيها حظر قيم غير مألوفة بالنسبة إلى الحكومة ولا تقع ضمن أهوائها السياسية، بوصفها تكتيكًا للقوة الناعمة. واندرج تكتيك شبكة الإنترنت الحلال أيضًا ضمن أجندة الحرب

14 Nergar Motaahedeh, *#iranelection: Hashtag Solidarity and the Transformation of Online Life* (Stanford: Stanford Briefs, 2015), p. 2.

15 Noah Shachtman, "Activists Launch Hack Attacks on Tehran Regime," *Wired*, 15/6/2009, accessed on 10/4/2022, accessed on 23/5/2022, at: https://bit.ly/3KbZUPX

16 هي تقنية تتيح التصفّح الآمن للإنترنت عبر توجيه مشفّر للمعلومات، بهدف ضمان خصوصية الإنترنت وحماية سرية بيانات المتصفّح وموقعه وهويته.

الناعمة للرقابة، وذلك، جزئيًا، بغية قمع الاحتجاجات المستقبلية التي قد تندلع بعد الانتخابات، وللتأكد من أنّ الإيرانيين لن يخضعوا لوجهات النظر الخارجية أو الداخلية المناهضة للحكومة. ويؤكد ذلك آية الله خامنئي، بعد مرور خمسة أشهر على انتخابات عام 2009، بقوله: «إنّ الأولوية الرئيسة في البلاد اليوم هي مواجهة الحرب الناعمة للعدو»، معزّزًا من ثمّ أهمية الحرب الناعمة في إيران[17]. لذلك، أصبحت التدابير السياسية السيبرانية هدفًا ضروريًا بعد عام 2009؛ ما دفع آية الله خامنئي في عام 2012 إلى إنشاء الهيئة المركزية للمجلس الأعلى للفضاء السيبراني. يراقب هذا المجلس الهيئات الحكومية المسؤولة عن الرقابة، وهي التالية: اللجنة المكلّفة بتحديد المحتويات المسيئة، والشرطة السيبرانية الإيرانية، وقيادة الدفاع السيبراني[18]. وتشكّل هذه الهيئات، معًا، إلى جانب العديد من المؤسسات والجهات الوكيلة الأخرى، بنية تحتية أشدّ تعقيدًا، تعمل على إبطاء الإنترنت بصفة متزايدة لمتصفّحي شبكة الإنترنت في منازلهم، باختطاف خادم أسماء المجالات Domain Name System–DNS hijacking[19]، وإعادة توجيهه، وتصفية الكلمات الرئيسة، وممارسة الاختناق.

استمرت عملية الحدّ المتعمّد من سرعات الإنترنت، بوصفها تكتيكًا مركزيًا للرقابة على الإنترنت، في أثناء الانتخابات الرئاسية لعام 2013، وذلك بهدف الحفاظ على الهدوء؛ أو بعبارة أخرى، لمنع اندلاع الاحتجاجات[20]. وبما أنّ استخدام الشبكات الخصوصية الافتراضية يتيح الوصول إلى خوادم خارج إيران، فقد استمرّ حظرها بوصفها تدبيرًا مضادًا، لا لمنع السلوك المسيء سياسيًا، والذي يُعدّ سلوكًا إجراميًا أو مبتذلًا، فحسب، بل للسيطرة الكاملة على المحتوى بهدف الحفاظ على سردية الدولة. وقد فرضت السلطات الإيرانية مزيدًا من الرقابة على الجمهور لمنع الهجمات المستوحاة من الشبكات الاجتماعية؛ ومن ثمّ، كان الوصول إلى البريد الإلكتروني يشكّل تحدّيًا شديدًا للغاية خلال الانتخابات الرئاسية لعام 2013. وبالفعل، عمد المواطنون إلى تبادل محتويات الوسائط المتعدّدة عبر قنوات الاتصالات، وتلقّي أخبار من الخارج. وهكذا، فإن عملية التشويش على الاتصالات وحظرها جعلت الشبكات الخصوصية الافتراضية شبكات عديمة الفائدة، ومَنَعت حرية التعبير إلى حدّ كبير[21]. وبهدف ممارسة المزيد من الحرب الناعمة خلال فترة الانتخابات، استخدمت السلطات، على نطاق واسع، الهجمات عبر حجب الخدمة الموزّعة بوصفها وسيلة لمنع الوصول إلى مواقع الشبكة العنكبوتية، وفي الوقت نفسه، للتصيّد الاحتيالي للصحافيين والنشاطات [المعارضة] باستخدام برمجيات الترصّد أو الفيروسات[22]. وفضلًا عن ذلك، جرت تصفية الرسائل النصّية القصيرة التي تحتوي على شعارات سياسية محدّدة تشمل أسماء مثل [النائب الأول للرئيس الإيراني السابق أحمدي نجاد] إسفنديار رحيم مشائي، بصفة مكثّفة، حتى لا يتمكّن المواطنون من نشر معلومات تدعو إلى التنظيم الجمْعي[23].

احتج الإيرانيون أيضًا على الحكومة، خارج سياق الانتخابات، حينما واجهوا مشكلات اقتصادية. ففي أواخر عام 2017 حتى أوائل عام 2018، احتج المواطنون على ارتفاع أسعار السلع، فما كان من الحكومة إلّا أن حظرت استخدام تطبيقَي تلغرام Telegram وانستغرام Instagram مؤقتًا؛ كون هاتين المنصّتين أساسيّتين لتنظيم

17 ARTICLE 19, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran," 3/2/2017, p. 2, accessed on 23/5/2022, at: https://bit.ly/3K9ehob

18 Simurgh Aryan, Homa Aryan & J. Alex Halderman, "Internet Censorship in Iran: A First Look," *FOCI* (2013), p. 1, accessed on 23/5/2022at: https://bit.ly/36FcWaT

19 تُعد عملية اختطاف خادم أسماء المجالات DNS hijacking، وهي تُعرف أيضًا بعملية إعادة التوجيه، نوعًا من الهجوم يجري فيها حل جميع الاستفسارات على نحوٍ غير صحيح من أجل إعادة توجيه المستخدمين بصفة غير متوقّعة إلى مواقع إلكترونية ضارة.

20 Golnaz Esfandiari, "Iran Admits Throttling Internet to 'Preserve Calm' During Election," *RadioFreeEurope RadioLiberty*, 26/6/2013, accessed on 10/4/2022, at: https://bit.ly/3MtF3ZM

21 Collin Anderson, "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran," arXiv:1306.4361, 18/6/2013, p. 1, accessed on 23/5/2022at: https://bit.ly/3xOZBbm

22 James Ball & Saeed Kamali Dehghan, "Iran Accused of Using Online Censorship and Hacking to Sway Presidential Poll," *The Guardian*, 31/5/2013, accessed on 10/4/2022, at: https://bit.ly/39ezMar

23 Freedom House, "Freedom on the Net 2013 – Iran," 3/10/2013, accessed on 23/5/2022, at: https://bit.ly/3KePXkK

التجمّعات وتبادل وسائل الإعلام الرقمية عن العنف الذي تجيزه الدولة والموت في أثناء الاحتجاجات[24]. تسبّب حجم العقوبات الأجنبية، المرتبط بالفوضى المالية في إيران في ظلّ سياسات الضغط القصوى الجسيمة التي تمارسها الولايات المتحدة، في تدهور قيمة العملة الإيرانية تدهورًا حادًّا؛ ما أدّى إلى ارتفاع أسعار النفط. وبحلول عام 2019، ارتفعت أسعار المحروقات في إيران ارتفاعًا كبيرًا؛ ما أدّى إلى احتجاج المواطنين واتخاذ الحكومة تدابير قمعية، شملت إجراءات صارمة عنيفة وانقطاع الإنترنت، فيما عُرف بـ «احتجاجات نوفمبر»[25]. وخلال هذه الاحتجاجات، قطعت الحكومة خدمة الإنترنت عن ملايين الإيرانيين[26]. وفي أثناء مواجهتهم العقوبات القاسية، شهد المواطنون استفادة الدولة من تطبيق بروتوكول البوابة الحدودية Border Gateway Protocol[27] الذي منح الحكومة فعليًا القدرة على تشغيل شبكتها المحلية المستقلة، كما كان مخطّطًا له منذ عام 2006. ويراقب هذا التطبيق القدرة على الاتصال الإلكتروني بفاعلية ويستفيد منها[28]. وبحلول عام 2021، كانت السلطات لا تزال تواصل اعتداءاتها على المواطنين. وقد رافق هذه الهجمات انقطاع في شبكة الإنترنت، بسبب احتجاجات على نقص في المياه؛ ما دفع الحكومة إلى تصعيد الموقف بتعزيز الإجراءات القمعية على الإنترنت هادفةً إلى منع الوصول إلى الفضاء السيبراني العالمي.

«مشروع قانون حماية مستخدمي الفضاء السيبراني»

يواجه المواطنون باستمرار محاولات جمهورية إيران الإسلامية تعزيز الرقابة على الإنترنت، وتصفية المعلومات على الشبكة، وذلك من خلال التشريع، بذريعة الحرب والقوة الناعتين؛ ما يقوّض من ثمّ حق الإنسان في حرية التعبير والخصوصية الآمنة على شبكة الإنترنت. وقد مارس المشرّعون الإيرانيون ضغوطًا كبيرة على الإدارة القانونية في مجلس الشورى لتمرير «مشروع قانون حماية مستخدمي الفضاء السيبراني» بدءًا من عام 2021. وبموجب المادة 11، تملك السلطات والمؤسسات الحكومية إمكانية الوصول إلى المعلومات الخصوصية، عبر مراقبة مستخدمي شبكة الإنترنت، في حين تصنّف المادة 15 المستخدمين بناءً على توصيفهم الوظيفي، وتحدّد لهم مقدار الوصول إلى الإنترنت بناءً على مهاراتهم[29]. وعلاوة على ذلك، من شأن مشروع القانون تنظيم المعلومات الواردة على شبكة الإنترنت، ومنع الوصول إليها بحسب مستوى الإذن الصادر عن الحكومة بحسب كل مواطن. صحيحٌ أنه من المفترض أن يكون الوصول إلى الخدمات والمواقع العالمية الشهيرة مثل يوتيوب YouTube وتويتر غير ممكن، وبالنتيجة مقيّدًا بشدّة، إلا أنّ الشبكات الخصوصية الافتراضية كانت بمنزلة إجراء مضادّ فعّال ضد الحكومة الإيرانية. غير أنّ مشروع القانون يجرّم إلى حدّ بعيد توزيع الشبكات الخصوصية الافتراضية واستخدامها، وقد يؤدي إلى السجن وحظر استخدام منصّة إنستغرام؛ ما يتسبّب في عزل المواطنين على الصعيد الدولي، ويعرّضهم للمزيد من الاضطهاد ويخضعهم لبيئة إلكترونية معادية. ولقد تحدّث الرئيس إبراهيم رئيسي، إضافة إلى مسؤولين كبار آخرين، عن إنشاء «شبكات خصوصية افتراضية قانونية» في حالة تجريم استخدام هذا النوع من الشبكات[30]. ولحسن الحظ، أسقط صنّاع القرار مشروع القانون

---

24 Simin Kargar, "Iran's National Information Network: Faster Speeds, but at What Cost?" *Internet Monitor*, 21/2/2018, accessed on 10/4/2022, at: https://bit.ly/3LdNOah

25 Human Rights Watch, "Iran: No Justice for Bloody 2019 Crackdown, No Accountability, Threats Against Families," accessed on 17/11/2020, at: https://bit.ly/3k7PRkd

26 ARTICLE 19, "Iran," p. 12.

27 بروتوكول توجيه خارجي معياري جرى تصميمه لتبادل معلومات التوجيه وقابلية الوصول بين الأنظمة المستقلة على شبكة الإنترنت.

28 Salamatian et al., p. 1.

29 "The Full Text of the Latest Version for the 'Plan of Cyberspace Service Regulation System' (Protection): The Flaws Remain," *Shargh Daily*, 19/2/2022, accessed on 15/4/2022, at: https://bit.ly/38eDZdB

30 Sayeh Isfahani, "The Internet 'Protection Bill' Will Hurt All Iranians, But the Queer Community Will Have the Most to Lose," Atlantic Council, 12/4/2022, accessed on 15/4/2022, at: https://bit.ly/3EFhjiV

في شباط/ فبراير 2022، على الرغم من أنّ الضغوط لا تزال تتصاعد لتمريره. وفي الوقت الذي ستتأثر فيه بشدّة سرعات الإنترنت وإمكانية الوصول إلى المحتوى، ستواجه الشركات المحلية في إيران، التي تستخدم منصّة انستغرام بوصفها تقنية للترويج، عجزًا ماليًّا؛ ما يشكّل تهديدًا للتجارة الإلكترونية الإيرانية المزدهرة منذ ظهور جائحة فيروس كورونا المستجد (كوفيد–19)[31]. ولا يزال مستخدمو الإنترنت الإيرانيون يعانون اختناقًا شديدًا في سرعات الإنترنت، بصورة عشوائية في أغلبية الأوقات.

أدّت الحرب الناعمة للفضاء السيبراني الإيراني، وعمليّات ضبط المعلومات ورصدها، إلى جعلها دعاية بوصفها سلاحًا [إذ تؤذي المتلقّي]؛ وهكذا تركت تأثيرًا في العالم الحقيقي فيما يتعلّق بوصول المواطنين إلى الفضاء السيبراني العالمي في أثناء أوقات الاحتجاجات وخارجها. صحيح أن الحكومة الإيرانية تعمد إلى تدابير مضادة تفرضها بنيتها التحتية المعقّدة المتعلّقة بالرقابة، للحفاظ على سردية الدولة ومنع انتشار المعلومات بين المواطنين، إلا أن متصفّحي شبكة الإنترنت الإيرانيين يستمرّون في إيجاد حلول للوصول إلى المواقع الإلكترونية الشعبية، ووسائل التواصل الاجتماعي، وحتى تطبيقات مثل تلغرام وواتساب WhatsApp، والتي تخضع للرقابة حاليًا. ونجح المواطنون الإيرانيون، الذين يستخدمون الشبكات الخصوصية الافتراضية والخوادم الوكيلة Proxy Servers، في تجاوز عوائق بسيطة مثل تصفية محتوى الإنترنت، بسهولة. ولكن مع تعزيز التعقيد في التدابير المضادة التي تتّخذها الدولة، تطوّرت أيضًا الأساليب التي يلجأ إليها المواطنون لتجاوز تلك العراقيل. فعلى سبيل المثال، يتيح تطبيق هاتف محمول، يعمل بنظام أندرويد Android يُسمّى ناهوفت Nahoft، أيّ «مخفي» باللغة الفارسية، للمستخدمين إرسال رسائل مشفّرة إلى آخرين عبر تطبيقات مثل تلغرام وواتساب، ويترجم تطبيق Nahoft الرسائل المشفرة، حتى ولو كان الوصول إلى الفضاء السيبراني العالمي محظورًا في إيران، بخاصةٍ إذا كان قد جرى تنزيل التطبيق على هاتف أندرويد[32]. صحيحٌ أنّ إضفاء الطابع الإقليمي على الفضاء السيبراني الإيراني يبقى على الأرجح استراتيجية جيوسياسية سيبرانية، إلاّ أنّ المواطنين الإيرانيين سيواصلون سعيهم لإيجاد طرائق للوصول الكامل إلى الفضاء السيبراني العالمي، على الرغم من مبادرات السلطات الإيرانية المعقّدة؛ إذ إنّ الاتصال عبر شبكة الإنترنت يشكّل أمرًا حيويًّا خلال حالات القمع الشديد. في الوقت الحالي، يستطيع الإيرانيون الاعتماد على تقنيات التهرّب لتجنّب الاضطهاد الذي تمارسه الدولة التي تسعى لرصد أولئك الذين ينتقدون المؤسسة وتوقيفهم.

31 Layla Hashemi, "Threats to Iranian Instagram: Analyzing Iran's Internet Landscape," *Fikra Forum*, 24/11/2021, accessed on 10/4/2022, at: https://bit.ly/3k9nt17

32 Lily Hay Newman, "A New App Helps Iranians Hide Messages in Plain Sight," *Wired*, 17/9/2021, accessed on 10/4/2022, at: https://bit.ly/3PQo46P.

المراجع

Akhavan, Niki. *Electronic Iran: The Cultural Politics of an Online Evolution*. New Brunswick: Rutgers University Press, 2013.

Anderson, Collin. "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran." arXiv:1306.4361. 182013/6/. at: https://bit.ly/3xOZBbm

ARTICLE 19. "Iran: Tightening the Net 2020: After Blood and Shutdowns." (Creative Commons License 3.0, 2020). at: https://bit.ly/3OJ3zIC

ARTICLE 19. "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran." 32017/2/. at: https://bit.ly/3K9ehob

Aryan, Simurgh, Homa Aryan & J. Alex Halderman. "Internet Censorship in Iran: A First Look." *FOCI* (2013). at: https://bit.ly/36FcWaT

Blout, E.L. "Soft War: Myth Nationalism, and Media in Iran." *The Communication Review*. vol. 20, no. 3 (2017). at: https://bit.ly/3rMeCGO

Center for Human Rights in Iran. "10 Things You Should Know about Iran's Multi-Billion Dollar National Internet Project." 32016/10/. at: https://bit.ly/3Lao5zG

Congressional Research Service. "Iranian Offensive Cyber Attack Capabilities, IF11406· VERSION 1." 132020/1/. at: https://bit.ly/37DjWWl

Freedom House. "Freedom on the Net 2013 – Iran." 32013/10/. at: https://bit.ly/3KePXkK

Human Rights Watch. "Iran: No Justice for Bloody 2019 Crackdown, No Accountability, Threats Against Families." at: https://bit.ly/3k7PRkd

Isfahani, Sayeh. "The Internet 'Protection Bill' Will Hurt All Iranians, But the Queer Community Will Have the Most to Lose." Atlantic Council. 122022/4/. at: https://bit.ly/3EFhjiV

Jones, Seth G. & Danika Newlee. "The United States' Soft War with Iran." *CSIS Briefs*. Center for Strategic & International Studies (June 2019). at: https://bit.ly/37DjUhb

Kargar, Simin. "Iran's National Information Network: Faster Speeds, but at What Cost?" *Internet Monitor*. 212018/2/. at: https://bit.ly/3LdNOah

Motaahedeh, Nergar. *#iranelection: Hashtag Solidarity and the Transformation of Online Life*. Stanford: Stanford Briefs, 2015.

Rahimi, Babak. "Cyberdissent: The Internet in Revolutionary Iran." *Middle East Review of International Affairs*. vol. 7, no. 3 (2003). at: https://bit.ly/3LdHGPt

Salamatian, Loqman et al. "The Geopolitics behind the Routes Data Travel: A Case Study of Iran." *Journal of Cybersecurity*. vol. 7, no. 1 (2021). at: https://bit.ly/3Kby0DN

Shirazi, Farid. "Interrogating Iran's Restricted Public Cloud: An Actor Network Theory Perspective." *Telematics and Informatics*. vol. 31, no. 2 (May 2014). at: https://bit.ly/3KbbvPp