الارهاب السيبرانى ومستقبل العلاقات الأمريكية الروسية

(سبتمبر 2021)

د. نـورهان الشيـخ*

أدت الطفرة التكنولوجية والاتجاه نحو الرقمنة والاقتصاد الرقمى وإدارة البنى التحتية والخدمية فـى معظم دول العالم بواسطة شبكات الحاسب الآلـى إلـى أن أصبح الفضاء السيبرانى ساحة رئيسية للتفاعل بين الدول. وبقدر ما أوضحت أزمة كورونا كثير من إيجابيات العالم الإفتراضى الذى بات قناة التواصل شبه الوحيدة فى لحظة ما من التطور الحرج للأزمة، وكفل ذلك استمرار الشئون الحياتية للمليارات فـى أنحاء العالم الـذين إلتزمـوا بيـوتهم وأداروا كافـة جوانـب الحيـاة إفتراضياً، فإن الأمر لا يخلو من أبعاد سلبية. لعل من أبرزها تعرض البنى التحتية السيبرانية لهجمات سواء من قراصنة بغرض الفدية أو من جانب تنظيمات ارهابية مما أدى إلى بروز ما بات يُعرف بـ "الإرهاب السيبرانى"، ذلك النشاط الإجرامى الذى يتم تنفيذه من قبل الجماعات والتنيظمات الإرهابية من خلال استخدام الحاسب الآلى ويكون الهدف هو أيضاً المنظومات الإلكترونية مسبباً خسائر واسعة النطاق لا تقل من حيث التأثير عن تلك الناجمة عن الارهاب التقليدى بل وقد تفوقها من حيث الحجم والاتساع.

وعند الحديث عن البعد السيبرانى فى العلاقات الأمريكية الروسية قد يميل البعض إلى استخدام مصطلح "الحرب السيبرانية" واعتبار الهجمات السيبرانية أحد أنماط الحروب الجديدة غير التقليدية، إلا إنه بالنظر إلى طبيعة هذه الهجمات وعدم ثبوت تورط الهيئات الحكومية أو الاستخباراتية ورائها يظل مصطلح "الجريمة السيبرانية" أو "الهجمات السيبرانية" هو الأنسب لتوصيفها خاصة وأن معظمها يكون بهدف الفدية. وفي هجمات الفدية السيبرانية، يخترق القراصنة شبكة الكمبيوتر ويهددون بتعطيلها أو حذف ملفات مهمة منها ما لم يتم دفع فدية مالية لهم، أو يقومون بتشفير بيانات الضحايا ثم يطالبون بدفع فدية غالبا بواسطة عملة البيتكوين مقابل مدهم بمفتاح فك التشفير وإعادتها إلى أصحابها، وتهدد تلك الجماعات، أحيانا، بنشر المستندات المسروقة على موقعها الإلكتروني مثل "HappyBlog" إذا لم تستجب الضحية لمطالبها.

* أستاذ العلاقات الدولية، جامعة القاهرة

ولأكثر من ثلاثة عقود، يُعتقد أن قراصنة مرتبطين بموسكو حاولوا سرقة أسرار الولايات المتحدة عبر الإنترنت، وشهدت السنوات الأخيرة تغيراً نوعياً فى هذه الهجمات حيث باتت تطول قطاعات شديدة الحساسية والتأثير وتضخمت الخسائر الناجمة عنها، ناهيك عن التأثير السلبى على سمعة الولايات المتحدة التى عجزت عن تأمين نفسها ضد هذه الاختراقات، يضاف إلى هذا تكرار الهجمات الكبرى على نحو ملحوظ وكأنها محاولة للإجهاز على الأمن السيبرانى الأمريكى. فمنذ منذ عام 2013، تصاعدت التهديدات السيبرانية لتصبح واحدة من أكبر تهديدات الأمن القومي الأمريكى، مما دفع واشنطن إلى إصدار وثيقة مستقلة حول "استراتيجية الأمن السيبرانى للولايات المتحدة الأمريكية" فى سبتمبر 2018.[1]

وتعتبر الهجمات السيبرانية التى تتهم واشنطن روسيا بالتورط فيها وإيواء الجماعات التى تقوم بها تحدي رئيسي في العلاقات بين البلدين خاصة وأن بايدن يعطى الملف السيبرانى أولوية واضحة وانتقد إدارة ترامب التى لم تتمكن، من وجهة نظره، من جعل الأمن السيبراني ضمن أولويتها. ورغم أن بايدن أقر أن الحكومة الروسية قد لا تفعل ذلك بنفسها لكنها تقدم الحماية لمن يفعل ذلك،[2] فإنه حمل نظيره الروسي فلاديمير بوتين مسؤولية وقف مثل هذه الهجمات السيبرانية، وسلمه خلال قمة جنيف فى يونيو الماضى قائمة تتضمن 16 قطاعا حيويا للبُنى التحتية، تمتد من الطاقة إلى المياه وغيرها، ينبغي ألا تتعرض لهجمات سيبرانية. وإزاء هجمات يوليو الماضى أشار بايدن إلى عدم التأكد من هوية الجهة المسؤولة عن الهجوم، وأن "الاعتقاد المبدئي أنها ليست الحكومة الروسية ولكنه شدد على أن الولايات المتحدة سترد إذا خلص إلى أن روسيا هي المسؤولة عن الهجوم.

وكان بايدن قد أكد فى 28 ديسمبر 2020 أن الولايات المتحدة يجب أن تكيف أولوياتها الدفاعية على خلفية "التعقيدات الاستراتيجية المتزايدة التي خلقتها روسيا والصين ... وأنه يجب الابتكار وإعادة التفكير في التهديدات المتزايدة في مجالات جديدة مثل الفضاء السيبرانى"[3]. وهدد بايدن "أن الولايات المتحدة سترد بشكل قوي على تورط الحكومة الروسية في أنشطة خبيثة[4]." وأن موسكو "ستدفع الثمن" إذا استمرت الهجمات السيبرانية على الولايات المتحدة من أراضيها. وأكد أن الولايات المتحدة سترد على الهجمات السيبرانية التي "تأتي من روسيا"، لكنه استبعد استخدام القوة العسكرية ردا على الهجمات السيبرانية، وامتنع عن التعليق على ما إذا وجهت إدارة بايدن الأجهزة المختصة باستهداف الخوادم الروسية المستخدمة في الهجمات السيبرانية على الشركات والهيئات الأمريكية. إلا إنه فى 28 يوليو 2021 تحدث بايدن عن احتمالات دخول الولايات المتحدة حربا جديدة بسبب التكنولوجيا، وأنه "إذا انتهى المطاف بحرب حقيقية، مع قوة عظمى،

فسيكون ذلك نتيجة لخرق سيبرانى".[5] وأكد من منبر الأمم المتحدة في نيويورك، يوم 21 سبتمبر، أن واشنطن تحتفظ بحق الرد على هجمات سيبرانية تهدد أمن الولايات المتحدة أو حلفائها.

وكانت الولايات المتحدة قد اتهمت روسيا بالعديد من الهجمات السيبرانية من أبرزها التدخل في الانتخابات الأمريكية 2016، واختراق صن بيرست (الانفجار الشمسي) لشبكات الحواسيب التابعة لشركة سولارويندز وعملاءها من الشركات الخاصة والأجهزة الحكومية الأمريكية الذى بدأ فى مارس وتم اكتشافه فى ديسمبر 2020 واعتبر أسوأ اختراق على الإطلاق للحكومة الأمريكية وطال وزارة الخزانة الأمريكية ووزارتي الأمن الداخلي والدفاع ووزارة الطاقة الأمريكية وهي الجهة المسؤولة عن إدارة الأسلحة النووية الأمريكية، وهجوم رانسوم وير الذي أغلق خط أنابيب "كولونيال بايبلاين" الذى يوفر حوالي 45% من الوقود المستهلك على الساحل الشرقي للولايات المتحدة، في مايو الماضي، واختراق موقع "سينيكس" الذي تستخدمه اللجنة الوطنية للحزب الجمهوري الأمريكي، واختراق وزارة الخارجية الأمريكية فى أغسطس وغيرها.

وفى مطلع يوليو من العام الجارى اتهمت الاستخبارات الأمريكية والبريطانية الإدارة العامة للاستخبارات الروسية بتنفيذ هجمات سيبرانية على مئات المؤسسات الحكومية والخاصة في مختلف أنحاء العالم، وأنه منذ أواسط عام 2019 حتى مطلع 2021 استخدمت الإدارة العامة للاستخبارات الروسية والوحدة العسكرية 26165 خلية Kubernetes لتنفيذ محاولات واسعة وموزعة ومجهولة المصدر للوصول إلى مئات المؤسسات الحكومية والخاصة في العالم، وأن الهجمات نفذت على أيدي مجموعات هاكرز مرتبطة بالاستخبارات الروسية، ومن المرجح أن هذه العمليات مازالت مستمرة.

جاء ذلك إثر تعرض نحو 200 شركة أمريكية لهجوم إلكتروني "موسع" ببرمجيات الفدية الخبيثة فى 2 يوليو استهدف شركة تكنولوجيا المعلومات كاسيا بولاية فلوريدا ثم انتشر بين الشبكات المؤسسية التي تستخدم برمجيات الشركة، ويوجد موقع شركة كاسيا في عشر دول ولديها أكثر من عشرة آلاف عميل، ورجحت مؤسسة هانتريس لابس لأمن الإنترنت أن جماعة "ريفيل" المرتبطة بروسيا وفيروس الفدية الذي تطوره تقف وراء هذا الهجوم. وسبق أن دفعت شركة "كولونيال" مبلغ 4.4 مليون دولار فدية بعد الهجوم عليها. وتُعد جماعة ريفيل، المعروفة أيضا باسم سودينوكيبي، من أكبر جماعات الجريمة السيبرانية وأكثرها تحقيقا للأرباح على مستوى العالم. واتهمها مكتب التحقيقات الفيدرالي الأمريكى بأنها نفذت هجوما إلكترونيا في الولايات المتحدة في مايو الماضي، تسبب في حالة من الشلل في عمليات شركة جي بي إس، أكبر موردي اللحوم في العالم. كما ربطت تقارير بين اسم ريفيل وعشرات الهجمات السيبرانية

المنظمة التي تعرضت لها أجهزة حكومية محلية في ولاية تكساس الأمريكية عام 2019. كما أثيرت شكوك من قبل حول مجموعة قرصنة روسية تُدعى (Cozy Bear) أو (APT 29)، والتي يُعتقد أن لها علاقات بوكالات التجسس في البلاد، واتهمت باختراق خوادم البريد الإلكتروني في وزارة الخارجية والبيت الأبيض عندما كان باراك أوباما رئيسا.

وقد اتهمت واشنطن موسكو بعدم اتخاذ إجراءات صارمة ضد هذه الجرائم السيبرانية، وأشار وزير الخارجية أنتوني بلينكين إلى إنه: "لا ينبغي لأي دولة مسؤولة أن تشارك بأي شكل من الأشكال في إيواء المنظمات الإجرامية المنخرطة في الهجمات السيبرانية، بما في ذلك برامج الفدية التي تعمل من الأراضي الروسية".[6]

فى المقابل نفت الحكومة الروسية أكثر من مرة الاتهامات الأمريكية والغربية بالقرصنة ضدها والتدخل في شؤونها الداخلية، مشيرة إلى عدم تقديم أي أدلة تدعم هذه الاتهامات، وأنه لا علاقة لها من قريب أو بعيد بالأنشطة الخبيثة التي تتحدث عنها الولايات المتحدة. وأعلن سكرتير مجلس الأمن القومي الروسي، نيكولاى باتروشيف، في نوفمبر 2020 أن روسيا تتعرض أيضاً لهجمات سيبرانية متزايدة وأن القراصنة هاجموا موارد المعلومات الروسية عام 2020 بأكثر من مرة ونصف مقارنة بعام 2019. وأشار رئيس لجنة حماية سيادة الدولة بمجلس الاتحاد الروسى أندريه كليموف أن نسبة الهجمات السيبرانية الأمريكية على أهداف روسية حساسة تبلغ ما بين 48 –52% من إجمالى الهجمات. كما اتهمت روسيا الولايات المتحدة بالتدخل في انتخاباتها البرلمانية التي جرت في الفترة من 17 إلى 19 سبتمبر، وقام نائب وزير الخارجية الروسى سيرجى ريابكوف بإبلاغ السفير الأمريكى فى موسكو جون سوليفان بأن الجانب الروسي لديه أدلة دامغة على انتهاكات القانون من جانب شركات الإنترنت الأمريكية العملاقة فيما يتعلق بانتخابات مجلس الدوما[7].

وفى السياق ذاته أشار الرئيس بوتين إلى أن أغلب الهجمات السيبرانية في العالم تنفذ من داخل الولايات المتحدة، وتأتي بعدها كندا، ثم أمريكا اللاتينية فبريطانيا، بينما روسيا ليست في قائمة الدول الأولى من حيث عدد مثل هذه العمليات. وأكد بوتين على أن الولايات المتحدة لم ترد على أي طلب للتوضيح وجهته روسيا بشأن الهجمات السيبرانية، وأنه خلال عام 2021 أرسلت موسكو 45 طلبًا للوكالات المعنية في الولايات المتحدة، لكن لم تتلق أي جواب. واعتبر بوتين أن الحوار والتشاور ضرورى لضمان الأمن السيبراني للبلدين وتحديد من يتحمل المسؤولية فى هذا الصدد[8]، مؤكداً أن موسكو على استعداد لتسليم مرتكبي الجرائم السيبرانية المطلوبين لدى الولايات المتحدة إلى واشنطن في حال إبرام الطرفين اتفاقية رسمية تنص على التزاماتهما

المتبادلة في هذا الصدد، وفي هذه الحالة تلتزم الولايات المتحدة، بالشروط نفسها، وتسلم المجرمين المطلوبين إلى روسيا.

وقد اتفق البلدان خلال قمة جنيف يوم 16 يونيو على إطلاق حوار ثنائي على مستوى الخبراء بشأن ضمان الأمن في المجال السيبراني، ومناقشة قضايا الأمن المعلوماتي ومكافحة الجرائم السيبرانية، وفى الاتصال الهاتفى بين بايدن وبوتين يوم 9 يوليو بحث الجانبين "الهجمات المستمرة المنفذة باستخدام برامج الفدية من قبل مجرمين متمركزين في روسيا والتي طالت الولايات المتحدة ودولا أخرى"، وشدد بايدن على "ضرورة اتخاذ روسيا إجراءات لمنع أنشطة هذه المجموعات مؤكداً أن "الولايات المتحدة ستتخذ كل الخطوات الضرورية لحماية شعبها وبنيتها التحتية الحيوية في مواجهة هذا التحدي المستمر".[9] وأكدت المتحدثة باسم البيت الأبيض فى 17 سبتمبر أن الولايات المتحدة تواصل الحوار مع روسيا حول قضية الأمن السيبراني، دون أن تتوقع نتائج فورية منه، وأشارت إلى مقولة بايدن "أننا لا نتوقع أن يحدث ذلك خلال ساعة واحدة.. المناقشات مستمرة وهي تجري على المستوى الدبلوماسي.. هذا الموضوع يعمل عليه فريقنا للأمن القومي." فإطلاق الحوار بين البلدين حول الأمن السيبراني خطوة إيجابية وهامة للتعاون فى هذا المجال الحيوى ولكنها لم تؤتى ثمارها بعد.

من ناحية أخرى، تدرك موسكو وواشنطن أهمية التنسيق بينهما لمواجهة الهجمات السيبرانية من التنظيمات الارهابية والخطر المتزايد من تحول الإرهاب من التهديد المادي إلى التهديد الرقمي، إذ عززت هذه التنظيمات من برامج تجنيد المبرمجين ومهندسي الكمبيوتر، وقامت بتطوير برامج ضارة للتجسس والإختراق، وظهر شكل جديد من الإرهاب تحت اسم "الخلافة الإلكترونية الموحدة" التي تحاول شن هجمات سيبرانية وإيجاد منصات في كل مكان في العالم بما في ذلك أوروبا بهدف الهيمنة على الفضاء السيبرانى في المستقبل المنظور تحت شعار "الجهاد السيبرانى"، ولا يقتصر هدف التنظيمات الإرهابية على تنفيذ هجمات إرهابية سيبرانية، ولكن يتجاوز ذلك إلى إنشاء أمة افتراضية عالمية تؤمن بالأفكار والآيديولوجية المتطرفة، إذ تعهد تنظيم "داعش" الإرهابي بعد هزيمته في العراق وسوريا بمواصلة هجماته من خلال التأكيد على الترويج لـ "الخلافة الافتراضية".[10]

إن الفضاء السيبرانى سيظل أحد ساحات المواجهة الأمريكية الروسية، ورغم ما تفرضه التهديدات السيبرانية والارهاب السيبرانى من تعاون وتنسيق بين البلدين، إلا إن الطريق مازال طويلاً لبلوغ مثل هذه التفاهمات فى ضوء تمسك روسيا بقاعدة المعاملة بالمثل وتردد واشنطن فى هذا الخصوص.

الهوامش:

[1] National Cyber Strategy of the United States of America, September2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[2] Biden presses Putin to act on ransomware attacks, hints at retaliation, Reuters, July 10, 2021, (https://www.reuters.com/technology/biden-pressed-putin-call-act-ransomware-attacks-white-house-2021-07-09/)

[3] Байден призвал США ответить на "вызовы" со стороны России, РИА Новости, 29.12.2020, https://ria.ru/20201229/bayden-1591315120.html

[4] Biden warns Russia against 'harmful activities' at start of first official trip, BBC, 10 June 2021, (https://www.bbc.com/news/world-us-canada-57422348)

[5] Biden: If U.S. has 'real shooting war' it could be result of Cyber Attacks, Reuters, July 28, 2021, https://www.reuters.com/world/biden-warns-cyber-attacks-could-lead-a-real-shooting-war-2021-07-27/

[6] Blinken says Russia has an 'obligation' to stop ransomware attacks, CNN, 2 June 2021, https://edition.cnn.com/2021/06/02/politics/blinken-cnne-interview-russia-cyber/index.html

[7] МИД обвинил США во вмешательстве в выборы в Госдуму, РИА Новости, 21.09.2021, https://ria.ru/20210921/vybory-1751154078.html

[8] Путин заявил, что больше всего кибератак в мире идет с территории США, ТАСС, 16 ИЮН, 2021, https://tass.ru/politika/11667495

[9] Biden presses Putin to act on ransomware attacks, hints at retaliation, Reuters, July 10, 2021, (https://www.reuters.com/technology/biden-pressed-putin-call-act-ransomware-attacks-white-house-2021-07-09/)

[10] Christina Schori Liang, Unveiling the “United Cyber Caliphate” and the Birth of the E-Terrorist, Georgetown Journal of International Affairs, vol.XVIII, no.III, Fall 2017, file:///C:/Users/CompuCity27-12-20/Desktop/2y10J90JJDcWfuIrVEExJU5SuOkDgq8V08daYodqmvT26flfqCIibJmC.pdf