

تقارير

النزاعات والمواجهات السيبرانية في فضاء منطقة الخليج العربي





إسرائيل من رواد الحروب السيبرانية بمنطقة الخليج (رويترز)

مقدمة

يدرك المتخصصون في مجال الأمن السيبراني أن ثمة حربًا سيبرانية غير معلنة تدور رحاها في الفضاء السيبراني لدول الخليج العربي، تسهم في إزالتها قوى كبرى، وجهات إقليمية متعددة تسعى إلى تنازع الهيمنة في منطقة تعد المصدر الأساسي لموارد الطاقة في عالمنا المعاصر.

وتحرص الجهات المتصارعة على عدم الإفصاح عن السجال السيبراني المحتدم فيما بينها، والذي أضحى نهجًا يُستخدم عندما لا تتوافر أمام القوى الكبرى، الولايات المتحدة بالخصوص، القدرة على حسم صراعاتها مع دول إقليمية، أو لتكثيف الضغط على الدول المناهضة لسياساتها. وهو النهج الذي بدأت إيران في توظيفه للتقليل من حجم الضغوط التي تمارس على سياساتها بالمنطقة، أو لتخفيف وطأة المعارضة ضد برنامجها النووي، وبرامج صواريخها الباليستية، من خلال الضغط بواسطة سلطاتها السيبرانية المتزايدة على دول الخليج العربي التي تتميز بعلاقات متينة مع الولايات المتحدة ودول من الاتحاد الأوروبي.

لقد تطورت التهديدات والهجمات السيبرانية بعد الهجمة الشرسة التي شنتها الولايات المتحدة الأمريكية على مشروع تخصيب اليورانيوم الإيراني، وتصاعدت وتيرتها حتى تحولت دفتها باتجاه تهديدات منشآت النفط والغاز في منطقة الخليج العربي، والبنى التحتية المهمة، وأضحت تهدد اقتصادات الدول وتنبئ ب بروز خارطة نزاع جيوسياسي سيبراني من نمط جديد.

فضاء النزاعات والمواجهات السيبرانية

برزت مخاطر أمنية وعسكرية من نمط جديد نتيجة لانبساط سلطان الفضاء السيبراني وتكاثر أدواته. ونشب عن ذلك تشكيل ساحة سيبرانية للنزاعات والتجاذبات، بدأت تحفل بالتهديدات، والهجمات. وتحول السعي إلى التنقيب عن الثغرات الرقمية

المقيمة في الفضاء السيبراني وأدواته، شيئاً فشيئاً إلى ممارسات تتم عن الرغبة في إحداث أضرار متفاوتة في الكيانات الرقمية التي تقيم في الفضاء السيبراني.

ونتيجة لتصعيد التهديدات وتكاثر الهجمات، بدأت الدول الكبرى بتوجيه جل اهتمامها نحو ترسيخ أمن نسيجها الشبكاتي، مع تطوير ألتها السيبرانية (الدفاعية والهجومية) لضمان بسط سلطانها وسطوتها السيبرانية قبالة التهديدات المتكررة والمؤثرة، فتحوّلت دائرة النزاع، تدريجياً، من ساحة المواجهة التقليدية، بمجالاتها البرية والبحرية والجوية، إلى المجال السيبراني المستحدث.

وتحول الفضاء السيبراني، إلى فضاء تغزوه التهديدات، وتساfer في فضائه المفتوح الهجمات، التي استثمر أصحابها سماته الفريدة، وانفتاحه غير المحدود، في ممارسة هجمات مؤثرة، قد ينشأ عنها تخريب جزئي أو كلي في الكيانات الرقمية المستهدفة، سواء كان مستقرها في فضاءات سيبرانية تعود إلى مؤسسات عسكرية، أو أمنية، أو مواقع حكومية، أو بحثية، أو صحية، أو تعليمية. لقد أضحت جميع الكيانات المقيمة في الفضاء السيبراني عرضة للتهديدات والهجمات التي تسافر مع قنوات الفيض الرقمي الذي يتدفق في الفضاء السيبراني الجديد (1).

ولعل من السمات الفريدة، والخصائص المميزة للفضاء السيبراني، بوصفه مجالاً جديداً للنزاع والمواجهة كونه: متعدد الموجودات السيبرانية مع تباين وتباعد أماكن توطنها السيبراني، وغياب هوية حضور المستخدمين؛ ويتميز بوجود فرصة لتغيب هوية الحضور السيبراني من خلال الأقنعة المتخيلة Avatar للكيانات السيبرانية المقيمة فيه فتغيب بصمة حضورها عن مشهد الممارسات الهجومية سواء نشأت عن كيانات منفردة، أو مجاميع؛ يضاف إلى ذلك انخفاض كلف الأدوات السيبرانية التي يمكن أن تستخدم في الهجمات وقدرتها الفائقة على إحداث تأثيرات ضارة، مع توافر عدد كبير منها بالمجان في مواقع الإنترنت. إضافة إلى كل ذلك، فإن الفضاء السيبراني تغيب عنه بالكلية الحدود الجغرافية والسياسية، وتنصهر في بوتقته الكثير من العوامل التي يمكن أن تعتمد في تحديد ملامح الممارسات العدوانية وأسبابها، وغاياتها، ومواردها، في فضاء متخيل لا تنطبق حدوده على مساحة فضاء الواقع بل باتت تهديداته وهجماته قادرة على الوصول والتخارج إليه، والتأثير عليه (2).

الجهات المساهمة في النزاعات السيبرانية بمنطقة الخليج العربي

يقيم في فضاء النزاعات والحروب السيبرانية عدد كبير من الكيانات المتخيلة (أفراداً، ومجاميع، وميليشيات سيبرانية، وجيوشاً) والذين قد سخروا طاقاتهم ومعرفتهم العميقة بالرمز الجديد من الحروب الرقمية، لتحقيق غايات شخصية من خلال تحقيق كسب مالي غير مشروع، أو للتعبير عن توجهات سياسية، أو مناهضة فئة أو تيار محدد، أو يتوجه نشاطهم نحو ممارسة تهديدات وهجمات سيبرانية موجعة على مستوى المؤسسات المالية والحكومية، أو التصعيد باتجاه إحداث ضرر على مستوى البنى التحتية والآلة الاقتصادية للفضاء السيبراني الذي يخص البلدان التي تستهدفها هجماتهم.

ويحفل الفضاء السيبراني لمنطقة الخليج العربي بعدد كبير من الكيانات الرقمية التي تستوطن فضاء النزاعات التي تنشط في مجاله الرقمي، والتي قد آثرت الوجود فيه لتحقيق غايات ذات بعد سياسي، أو عسكري، أو أممي، أو اقتصادي، من خلال ممارسة أنشطة التسلل، والتلصص، واختراق المواقع الحساسة، أو إيقافها عن العمل من خلال هجمات رفض الخدمة DoS، أو نشر الخلل والخراب في المعمارية الرقمية لكياناتها السيبرانية (3). انظر الجدول (1).

الجدول (1) يبين أهم الجهات المساهمة في التهديدات والهجمات السيبرانية في الفضاء السيبراني لدول الخليج العربي

الجهة	التوطن السيبراني	طبيعة التهديدات	الجهات المستهدفة	حجم التأثير
جيش إيران السيبراني	الفضاء السيبراني الإيراني	شن هجمات منسقة لإحداث خلل على مستوى البنية التحتية والمؤسسات الحكومية والمالية والنفطية الحساسة.	الولايات المتحدة، وإسرائيل، ودول الخليج العربي	هجمات بالغة التأثير
جيش اليمن السيبراني	فضاء اليمن السيبراني	شن هجمات ضد دول التحالف	السعودية، والإمارات، والبحرين	هجمات متوسطة التأثير
الجيش السوري الإلكتروني	فضاء سوريا السيبراني	شن هجمات ضد الدول الخليجية التي تناهض سياسات وممارسات النظام السوري.	قطر، والسعودية، والإمارات، والبحرين.	هجمات مؤثرة
فصائل القرصنة السيبرانية الإيرانية	فضاء إيران السيبراني	شن هجمات متنوعة لإحداث خلل جزئي أو شبه كلي في مواقع حكومية وأخرى تعود لقطاع التجارة والأعمال بقصد التكبسب المادي أو تعبيراً عن نزعة عقديّة أو وطنية.	الولايات المتحدة، ودول أوروبية، والسعودية، والإمارات، والبحرين، والكويت، وقطر.	هجمات مؤثرة
قرصنة سيبرانيون عرب	الفضاء السيبراني العربي	ممارسة اختراقات وهجمات محدودة للتعبير عن توجهات عقديّة أو سياسية.	دول خليجية متعددة	منخفضة التأثير
ناشطون سيبرانيون عرب	الفضاء السيبراني العربي	مجموعة من الناشطين السيبرانيين الذين يحاولون الإفصاح عن معارضتهم لممارسات النظم الحاكمة من خلال استغلال البيئة المفتوحة وتغييب الهوية في الفضاء السيبراني.	دول خليجية متعددة	منخفضة التأثير

المصدر : أعده الباحث

وبالإضافة إلى هذه الكيانات، تنشط في فضاء الخليج العربي وحدات وفصائل سيبرانية تعود إلى الدول الكبرى، مثل: الولايات المتحدة الأمريكية، وروسيا، والصين، وكوريا الشمالية في سعيها الدائم للهيمنة على الفضاء السيبراني والحفاظ على توازن

القوى في المنطقة. ويبقى الحضور السيبراني الأميركي مكثفًا قبالة حضور بقية الدول لمواجهة أنشطة إيران في منطقة الخليج العربي، والسعي إلى عرقلة برنامجها النووي، والدفاع عن حلفائه بالمنطقة، كما يوجد عدد كبير من المقاتلين السيبرانيين الذين يعملون في وحدة الدفاع السيبراني بجيش الدفاع الإسرائيلي لممارسة تهديداتهم وهجماتهم المستمرة على الفضاء السيبراني الإيراني.

التحديات السيبرانية في منطقة الخليج العربي

في البداية، كانت التهديدات والهجمات السيبرانية محدودة التأثير مارسها مستخدمون هواة حاولوا إثبات قدراتهم وخبراتهم في مجال الفضاء السيبراني، ثم تحولت إلى بيئة خصبة جذبت قراصنة المعلومات، ومستخدمين لديهم نزعات جرمية، قبل أن ترتقي في مستويات تأثيراتها من سعي فردي لإحداث خلل بسيط، أو إيقاف مواقع عن العمل لمدة قصيرة، إلى عمليات منسقة وممنهجة تسعى المجاميع والفصائل السيبرانية التي تمارسها إلى التجسس على مواقع حكومية وسرقة بيانات من مستودعاتها الرقمية، أو إحداث آثار تخريبية على مستوى البنى التحتية الحيوية.

بيد أن ولادة الدودة الخبيثة، التي أطلق عليها اسم Stuxnet، والتي عكف على تصنيعها فريق مشترك من خبراء أمن المعلومات وتصنيع البرمجيات الخبيثة بالولايات المتحدة وإسرائيل لشن هجمة شرسة على موقع مفاعل نطنز الإيراني لتخصيب اليورانيوم، ونجاحها بالفقر خارج حدود الفضاء السيبراني باتجاه المسيطرات الموجودة في مجمع تخصيب اليورانيوم الشهير، وإحداثها أضرارًا جسيمة في أجهزة الطرد المركزي المستخدمة في عملية التخصيب، عُدَّ طفرة نوعية وبداية لعهد جديد في ميدان التهديدات والهجمات السيبرانية التي تحولت إلى سلاح تستخدمه الدول ضد خصومها أو الدول التي تناهض سياساتها(4).

من أجل هذا، يمكن أن نعد ولادة هذه البرمجية الخبيثة الشرارة الأولى التي أوقدت نار النزاعات السيبرانية في منطقة الخليج العربي، بعد أن اتخذها النظام الإيراني ذريعة لمهاجمة أهداف متعددة في دول منطقة الخليج العربي بسبب العلاقة التي تربطها بالولايات المتحدة الأمريكية، بالإضافة إلى سعيه لإثبات سلطانه السيبراني بالمنطقة.

ومع مرور الوقت، بدأت سلسلة من عمليات الاستتسال التي استثمرت البصمة الجينية للفيروس الخبيث Stuxnet والتي أفرزت ولادة برمجيات أشد خبثًا وتأثيرًا على الكيانات الرقمية المقيمة في الفضاء السيبراني بدول منطقة الخليج العربي، والفضاء العولمي على حدٍ سواء.

أما إذا أردنا التوجه صوب الكشف عن أهم الهجمات التي شهد الفضاء السيبراني الخليجي خلال السنوات الأخيرة، سنجد أنفسنا قبالة كَمٍّ كبير من التهديدات والهجمات المتنوعة التي تباينت ألياتها، وتنوعت جغرافية أهدافها، وتعددت هويات المساهمين بشنها على مستوى الأفراد، والفصائل والجيش السيبرانية للقوى المتصارعة على بسط هيمنتها على هذه المنطقة الحيوية، انظر الجدول (2).

الجدول (2) يبين أهم التهديدات والهجمات السيبرانية في فضاء دول الخليج العربي

السنة	التهديد أو الهجمة	دول الخليج المستهدفة	القطاع المستهدف	الوصف
2012	شمعون 1 Shamoon I	السعودية	شركة أرامكو	قام فريق من القرصنة السيبرانيين الإيرانيين أطلق على نفسه اسم "سيف العدالة القاطع Cutting Sword of Justice" في شهر أغسطس/آب من عام 2012 بإقحام فيروس خبيث أطلق عليه اسم Shamoon في شبكة المعلومات الداخلية لشركة أرامكو السعودية النفطية، والذي باشر على الفور نشاطه التخريبي فقام بإلغاء بيانات مهمة في أكثر من 30,000 حاسب من حواسيب الشركة، بالإضافة إلى إدراج صورة لعلم الولايات المتحدة الأمريكية الذي التهمته النيران.
2014	Rocket Kitten	دول خليجية ودول عربية أخرى	شبكات الاتصالات والمعلومات	قامت هذه المجموعة من قرصنة المعلومات باختراق شبكات المعلومات والاتصالات في دول خليجية وأصابتها بأضرار جسيمة.
	عملية كليفر Operation Cleaver	قطر، والكويت، والسعودية، والإمارات	النفط والغاز، والمطارات، ومواقع حكومية حساسة، وشركات الاتصالات	تعد من أشد الهجمات السيبرانية تأثيرًا، وقد قامت بها مجاميع متعددة من القرصنة السيبرانيين الإيرانيين على دول متعددة من الخليج بالإضافة إلى الولايات المتحدة الأمريكية ودول أوروبية، وقد حُطِّط لأن تكون ذات تأثيرات جسيمة على قطاعات حيوية في دول الخليج ودول أخرى.
2016	شمعون 2 Shamoon II	السعودية	شركة أرامكو	يعد هذا البرنامج الخبيث نسخة مطورة من البرنامج الذي استهدف شركة أرامكو السعودية عام 2012 وقد توسعت قطاعات تأثيره إلى قطاعات مضافة إلى قطاعي النفط والغاز.

2017	الصخرة الدوارة Stone Drill	السعودية	قطاعا الطيران والبتروكيماويات	أحدث هذا البرنامج الخبيث تأثيرات كبيرة على شركات الطيران وشركات البتروكيماويات في السعودية.
	فيروس مامبا للفدية Mamba Ransomware	دول خليجية متعددة	القطاع المالي	يعد من برمجيات الفدية الخبيثة التي أحكمت قبضتها على حواسيب موجودة في القطاع المالي لدول خليجية متعددة وأورتتها خللاً كبيراً.
2018	تريتون Triton	دول خليجية متعددة	قطاعا النفط والغاز والصناعات البتروكيماوية	يعد هذا البرنامج الخبيث من الأنسال الجديدة التي حملت آثاراً خطيرة على قطاعي النفط والغاز والصناعات البتروكيماوية في دول خليجية مع وجود تهديدات باتجاه إحداث تفجيرات ممنهجة يمكن أن تؤدي بحياة العاملين في مواقع العمل
2019	التهديدات السيبرانية المتقدمة APT	قطر، والكويت، والسعودية، والإمارات، والبحرين	البنى التحتية المهمة	هجمات سيبرانية بالغة التأثير، مارسها القراصنة الإيرانيون السيبرانيون لاستهداف شبكات المعلومات وبنيتها التحتية، وخلال مدد زمنية متطاولة، لضمان بلوغ أهدافها وتعميق مستويات تأثيرها

المصدر : أعده الباحث

لقد تحول الفضاء السيبراني لدول الخليج العربي إلى ساحة تصفية حسابات، وبيئة خصبة للتنزعات المحتملة بين الولايات المتحدة الأميركية وإيران، وأضحت منشآت النفط والغاز، وفضاءات المؤسسات الحكومية الحساسة ومواقعها، وبيئة الاقتصاد والمال في هذه الدول عرضة للتراشق الرقمي الذي تطور خلال السنوات الأخيرة باتجاه تهديدات سيبرانية بالغة الخطورة يمكن أن تنتشب عنها أضرار جسيمة في الكيانات المقيمة بالفضاء السيبراني لهذه الدول.

إن انتهاج الولايات المتحدة الأميركية سياسة ممارسة الهجمات السيبرانية ضد منظومات عسكرية إيرانية متعددة في إيران بدلاً من استخدام آلتها العسكرية التقليدية، هذه الأيام، وبالخصوص بعد إسقاط طائراتها الاستطلاعية (5)، يعد شاهداً على توظيف فضاء النزاعات السيبرانية في الرد بدلاً من تأجيج الصراع في منطقة الخليج العربي، الذي يمكن أن تتطور تداعياته بحيث لا يمكن احتواؤها.

الصراع السيبراني وجيوبولتيك الخليج العربي

نشأ عن هيمنة الدور الذي يمارسه الفضاء السيبراني في حياتنا المعاصرة، وتغلغله على جميع المستويات، وتكاثر أجهزة الاتصالات والمعلومات الثابتة والمحمولة، وولادة إنترنت الأشياء، ترسيخ خطاطته المميزة التي جاءت بمبدأ غياب سمة التساوق في إدارة الصراع بين القوى المتصارعة Asymmetries وغيّبت خاصية التوازن بين الفاعلين الكبار (الدول أو

المؤسسات التي تمارس العمل العسكري) من جهة، وبين الفاعلين الصغار (دول نامية، أو مجاميع قرصنة المعلومات وحتى المستخدمين العاديين) أثناء حدوث صراع داخل حدود الفضاء السيبراني، من جهة أخرى(6).

وأسهمت خصائص الفضاء السيبراني في قولبة أنموذج جديد لتوازن القوى الجيوسياسية نتيجة لتداخل الخاصية المتخيلة مع مفردات الواقع الصلبة، وتراجع كلفة الوصول إلى مجال النزاع السيبراني، فتقلصت الفوارق بين موازين القوى التي ترسخت لدينا (على أساس مبدأ القوى العظمى والدول النامية)، ولم تعد القدرة على إحداث الضرر في أحد الخصوم مرتبهة بمفهومنا التقليدي لإدارة النزاعات، لأن الخصوم الصغار (مثل قرصنة المعلومات) أصبحوا بفضل ما يتسم به فضاء المعلومات من مميزات فريدة، قادرين على إحداث ضرر في لاعبين كبار على مستوى الحكومات أو الدول الأربع الكبرى (على سبيل المثال) وبمديات لا يمكن مقارنتها بالتأثير المقابل الذي يمكن أن ينشأ عن استجابة هذه الدول وتعاملها مع التهديدات. كما لم تعد حوكمة مجال النزاع بيد جهة دون غيرها، ومهما كان مستوى السطوة التي تتمتع بها داخل حدود الفضاء السيبراني، أو خارجه، ذلك لأن حضور أطراف النزاع أضحى خارج نطاق سلطة الغير، وبعيداً عن مجال هيمنة الجهات المتصارعة، ومهما كانت هويتها ومقدار سلطانها متجاوزة خطاطة القولبة الضيقة التي تولدت منذ قرون بناء على مبادئ الانتماءات القومية، والسياسية، والجغرافية (7).

لقد تعمقت التأثيرات الجيوسياسية للفضاء السيبراني خلال السنوات الخمس الأخيرة، بعد أن مرت الحروب السيبرانية بسلسلة متلاحقة من التطورات، منذ حصول الهجمة الشرسة بواسطة البرنامج الخبيث Stuxnet على المشروع النووي الإيراني، ومن ثم الهجمة التي قامت بها روسيا ضد أهداف حيوية تقيم في الفضاء السيبراني لأوكرانيا، والهجمات التي مارسها جيش إيران السيبراني ضد منشآت شركة أرامكو السعودية.

ومما لا شك فيها أن هذه المواصفات ساهمت في التصعيد الجيوسياسي-السيبراني في منطقة الخليج العربي، مما سيعمق عدم الاستقرار في المنطقة، وسيلعب دوراً خطيراً في توسيع دائرة الأزمات التي تعصف ببلدانها. كما أن توجه التهديدات والهجمات السيبرانية خارج نطاق حدود الفضاء السيبراني وبلوغ أثارها لمنشآت النفط والغاز، ومواقع حكومية حساسة، وشركات الطيران، والمستودعات الرقمية الوطنية، بات يشكل مؤشراً خطيراً على وجود تهديدات أمنية غير مسبوقه لدول الخليج العربي، والتي تعد صناعتها النفطية، ومنظومتها الاقتصادية العصب الحيوي لموارد الطاقة والسوق المالية العالمية. ومما يزيد من خطورة التحولات الجيوسياسية في المجال السيبراني، هو تكاثر، وتنوع هوية الجهات التي تنشط في الفضاء السيبراني الخليجي، (سواء كانت ملتحقة بقوى كبرى، أو أخرى إقليمية، أو محلية) والتي تتنافس وتتجاذب فيما بينها في إدارة ملف الصراع المعقد وبين أهداف حساسة ومؤثرة على المستويات كافة بالمنطقة. كما أن الضغوط الأخيرة والتهديدات التي تمارسها الولايات المتحدة الأميركية على إيران لكف مشروعها النووي، وسلوكياتها في منطقة الخليج ودول الجوار، وسعي الطرفين المتنازعين إلى نقل جزء كبير من مشهد النزاع إلى الفضاء السيبراني الخليجي، وعدم وجود مؤشرات حول نزع فتيل الأزمات المتصاعدة فيما بينهما بات يشكل تهديداً أمنياً خطيراً نتوقع أن ينشب عنه ولادة أنماط جديدة من النزاعات والمدافعة الإقليمية التي ستنصبغ بصبغة سيبرانية، ستستبطن تأثيرات خطيرة وغير معلنة على المنطقة، وسترسم حدوداً لساحة نزاع سيبراني لا يمكن التنبؤ بالتداعيات المحتملة عنها على عموم المنطقة العربية والخليجية.

* حسن مظفر الرزوي، مدير مركز الموصل للدراسات الاستراتيجية والمستقبلية.

- (1) الرزوز، حسن مظفر، الحضور العربي-الرقمي: قراءة في مطالع تشكيل حضور محيطه المعرفي (OmniScriptum AraPers ،Noor Publishing) .الطبعة الأولى، 2017، Germany ،BahnhofstraBe ،GmbH .217.
- (2) الرزوز، حسن مظفر، الفضاء المعلوماتي (مركز دراسات الوحدة العربية، بيروت، 2007)، الطبعة الأولى، 125.
- (3) . Gazula, Mohan, **Cyber Warfare Conflict Analysis and Case Studies**, Working Paper CISL# 2017-10, (Cambridge, MIT,2017).
- (4) Symantec, **Internet Security Threat Report**, Volume 22, (California, Symantec, 2017)..
- (5) . Bohn, Dieter, **US Cyberattack Reportedly Hit Iranian Targets**, The Verge, June 22nd 2019, Accessed on July 14th 2019, Available At: <https://www.theverge.com/2019/6/22/18714010/us-cyberattack-iranian-targets-missile-command-report>.
- (6) Naval War College Ganapathi, Commodore, **Cyberwar – Viewed Through The Prism Of Clausewitzian Strategy**, (6) .Journal, 2016.pp.22
- (7) Bordelon, Emily, **Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law**, A Senior Thesis Submitted In Partial Fulfillment Of The Requirements For Graduation In The Honors Program, Liberty University, Fall 2016, pp.12.