مركز دراسات الخليج والجزيرة العربية
تأسس عام ١٩٩٤م - جامعة الكويت

التهديدات السيبرانية وتأثيراتها على الأمن الخليجي

إعداد
فاطمة محمد الأمين موسى

التقرير الاستراتيجي
العدد (١٨)

فبراير ٢٠٢٢م

مركز دراسات الخليج والجزيرة العربية
تأسس عام ١٩٩٤م - جامعة الكويت

التهديدات السيبرانية وتأثيراتها على الأمن الخليجي

إعـــداد
فاطمة محمد الأمين موسى
باحث دكتوراه في العلوم السياسية

التقرير الاستراتيجي
العدد (١٨)

فبراير ٢٠٢٢م

الآراء الواردة في هذه الدراسة لا تعبّر بالضرورة عن اتجاهات يتبناها مركز دراسات الخليج والجزيرة العربية بجامعة الكويت

الناشر

مركز دراسات الخليج والجزيرة العربية

جامعة الكويت

ص.ب: ٦٤٩٨٦ الشويخ (ب) الرمز البريدي: ٧٠٤٦٠ ، الكويت

هاتف : ٢٤٩٨٤٦٣٩ ـ ٢٤٩٨٤٦٥٨ (٩٦٥+)

البريد الإلكتروني Gulf_center@yahoo.com

الموقع الإلكتروني www.cgaps.ku.edu.kw

الطبعة الأولى

الكويت ـ ٢٠٢٢م

أعضاء مجلس إدارة
مركز دراسات الخليج والجزيرة العربية

د. علي راشد المطيري
القائم بأعمال نائب مدير جامعة الكويت للأبحاث (رئيس مجلس الإدارة)

د. فيصل أبو صليب
مدير المركز ـ نائب رئيس مجلس الإدارة

داخل جامعة الكويت

أ. د. يوسف ذياب الصقر
قسم الفقه المقارن والسياسة الشرعية
كلية الشريعة والدراسات الإسلامية
جامعة الكويت

أ. د. عبيد سرور العتيبي
رئيس قسم الجغرافيا ـ كلية العلوم الاجتماعية
جامعة الكويت

أ. د. فايز منشر الظفيري
قسم المناهج وطرق التدريس ـ كلية التربية
جامعة الكويت

أ. د. عبدالله محمد الهاجري
عميد كلية الآداب بالإنابة
جامعة الكويت

خارج جامعة الكويت

سعادة السفير/ جمال عبدالله الغانم
مساعد وزير الخارجية للشؤون الإدارية
وزارة الخارجية ـ دولة الكويت

تمهيد:

باتت دول العالم ومؤسساتها ومنشآتها الحيوية كافة في غضون سنوات قلائل من مطلع القرن الحادي والعشرين، هدفاً لا يصعب الوصول إليه من «على بُعد» من خلال أقل عدد ممكن من العناصر البشرية وفي زمن قياسي، فيما يُعرف في الدراسات المعاصرة بـ «الحروب السيبرانية».

وتندرج هذه النوعية الجديدة من الحروب ضمن الفئة الواسعة من آليات الصراع الدولي والإقليمي المعروفة بحروب الجيل الخامس، والتي يفوق حجم ما تسفر عنه من تداعيات كارثية على مختلف أركان الدولة ومؤسساتها، تلك الخسائر الضخمة التي كانت تنتج عن الحروب التقليدية التي سادت العالم حتى نهاية القرن العشرين.

ولا شك أن دول الخليج العربي ليست استثناء من بقية أعضاء المجتمع الدولي من حيث تعاظم مخاطر تعرضها لمثل هذه الهجمات وتلك الحروب، لاسيما في ضوء أهميتها الاستراتيجية، وحساسية موقعها الجغرافي، ما يجعلها ربما عرضة أكثر من غيرها لمثل هذه التهديدات.

في ضوء ذلك، يقدم مركز دراسات الخليج والجزيرة العربية هذا «التقرير الاستراتيجي»، الذي يعرض للتهديدات السيبرانية، وتأثيراتها على الأمن عموماً وعلى الأمن في الخليج العربي خصوصاً، وصولاً إلى التأكيد على كيفية التأهيل الخليجي بما يضمن التصدي الفعال لمثل هذه التهديدات المحتملة.

د. فيصل أبو صليب

مدير المركز

المحتويات	رقم الصفحة

- ملخص ١٣
- مقدمة ١٥
- **المحور الأول**: قراءة في تحولات الصراع والقوة وصولًا إلى عصر الرقمنة والحروب السيبرانية ١٩
- **المحور الثاني**: ماهية التهديدات السيبرانية ومدى تأثيرها على الأمن الوطني والدولي ٢٥
- **المحور الثالث**: واقع الهجمات غير المرئية في دول مجلس التعاون الخليجي ٣١
- **المحور الرابع**: التأهيل الخليجي في عصر التهديدات السيبرانية ٣٦
- الخاتمة ٤٥
- المراجع العربية والأجنبية ٤٧

المحتويات

- الجدول رقم (١): ترتيب دول الخليج العربي في مؤشر الأمن السيبراني لعام ٢٠٢٠م.

- الجدول رقم (٢): أبرز ضوابط الأمن السيبراني في دول مجلس التعاون الخليجي.

- الشكل رقم (١): تطور حوادث التهديدات السيبرانية.

- الشكل رقم (٢): معلومات عن المركز الإقليمي للأمن القومي.

مركز دراسات الخليج والجزيرة العربية

التهديدات السيبرانية وتأثيراتها على الأمن الخليجي

ملخص:

في زمن كانت الدول تتجسس على دول صديقة كانت أم عدوة من خلال أشخاص، أصبح هذا الأسلوب التقليدي لا يسمع عنه إلا ما نُدر، وتحولت حرب الجاسوسية إلى حرب إلكترونية تُدار في الفضاء الإلكتروني بتقنيات سهلة ومتنوعة. ووسط تزايد الهجمات الإلكترونية، بلغ حجم الإنفاق العالمي على الأمن السيبراني خلال عام ٢٠٢١م ١٥٠ مليار دولار، وفقًا للبيانات الصادرة عن شركة (جارتر) الإسبانية للأبحاث التكنولوجية.

وبات يتردد كثيرًا في الآونة الأخيرة مفاهيم كالحروب السيبرانية، الهجمات الإلكترونية، تهديدات الفضاء غير المرئي، الصراعات الرقمية ... إلخ من هذه المسميات، التي وإن اختلفت في مدلولها اللفظي فإنها تحمل في مضمونها معنى واحدًا، وتشير إلى تلك الصيغة الجديدة من الهجمات الإلكترونية التي يشهدها القرن الحادي والعشرين، والتي تُعد أخطر أنواع الهجمات وأشدها فتكًا، نظرًا لاعتمادها على تكنولوجيا المعلومات والاتصالات التي تمكنها من اختراق الحدود الجغرافية بسرعة هائلة لإلحاق الضرر أو تدمير الخصم. كما وأن مخاطر تأثيرها متعددة الأبعاد، فهي أمنية، واجتماعية، واقتصادية، وثقافية، وفكرية. وتختلف هذه الهجمات وفقًا لأهمية الهدف التي تسعى إلى تحقيقه، والمجال التي تعتزم استهدافه.

ولقد توالت هذه الهجمات خاصةً مع دخول مختلف الدول في سباق لتبني الحكومات الإلكترونية والمُدن الذكية، واتساع نطاق وتزايد عدد مستخدمي الإنترنت في العالم، فأصبحت قواعد البيانات القومية أكثر عرضة للهجمات والتهديدات السيبرانية. هذا بجانب حملات نشر الشائعات والمعلومات المضللة أو الدعوة لأعمال تحريضية أو دعم المعارضة أو الأقليات، الأمر الذي يساهم في تلاشي سيادة الدول ويضعف من قدرتها على الحفاظ على أمنها القومي.

ولم تكن دول مجلس التعاون الخليجي بمنأى عن تداعيات هذه الهجمات، وتهديدها الصريح لأمنها الوطني، وعليه فقد تسارعت هذه الدول في استقطاب شركات عالمية متخصصة في أمن وتقنية المعلومات، هذا إلى جانب اعتمادها للعديد من الخطط والاستراتيجيات المواجهة لخطر هذا الجيل الجديد من التهديدات. وعلى هذا الأساس، تبلور الهدف الأساسي من إعداد هذا التقرير، والذي يسلط الضوء على إحدى الموضوعات المعاصرة التي تتمتع بأهمية بالغة في حقل الدراسات الأمنية والاستراتيجية، والتي تجسد المظهر الجديد لصراعات المستقبل، ألا وهي الهجمات السيبرانية مع التركيز على واقعها كأحد أبرز مهددات منظومة الأمن الوطني الخليجي.

مقدمة:

طالما وجد الإنسان يظهر التنافس، يبرز الصراع، تندلع الحروب، ولا يمكن إغفال جوانب الصلح والتعاون والاتحاد، فالخير والشر، والأبيض والأسود من سمات الحياة منذ الوجود عبر مختلف الأزمنة والأمكنة. وفي عصر تسوده الهيمنة التكنومعلوماتية وتأثير التكنولوجيات الجديدة مثل الذكاء الاصطناعي، وإنترنت الأشياء، والروبورتات، والواقع المعزز، والبلوك تشين، ... وغيرها، أضحى الفضاء الإلكتروني مرشحًا قويًّا لأن يكون الساحة الجديدة للصراعات والتهديدات التي تُدار بأسلحة وأدوات تختلف من حيث الشكل والمضمون عن تلك التهديدات التي تعتمد على الأسلحة التقليدية.

وعلى هذا الأساس، ظهر ما يسمى بـ «تهديدات الفضاء الإلكتروني» أو «الحروب السيبرانية»، والتي تمتلك قواعد جديدة غيَّرت في طبيعة الحروب ذاتها، فهي بذلك لا تستهدف تدمير الآلات والمعدات العسكرية والقوات العسكرية البشرية، ولا تطمح في الاستيلاء على أرض الخصم واحتلاله، بل تنطلق لإلحاق الضرر البالغ في البنى التحتية والشبكات المعلوماتية، كما ساهمت مزياها المتمثلة في سهولة استخدامها وتكلفتها المنخفضة في زيادة قدرتها على التأثير في مختلف المجالات سواء السياسية، الاقتصادية، العسكرية، الاجتماعية وحتى الأيديولوجية، وبات جليًّا أن من يمتلك

آليات توظيف البيئة السيبرانية يصبح أكثر قدرة على تحقيق أهدافه والتأثير في سلوك الفاعلين المشاركين له في إطار هذه البيئة.

وعلى هذا المنوال، أضحي المجتمع الدولي أمام العديد من التحديات والتهديدات التي لم يشهدها من قبل، كتلك التي تُعرف بالتهديدات اللا تماثلية أو اللا تناظرية العابرة للحدود التي لا تعترف لا بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، الأمر الذي حاز على محور اهتمام الباحثين والمهتمين بدراسة حقل الدراسات الأمنية والاستراتيجية وكذلك على مستوى الممارسات السياسية، خاصةً وأن هناك من الهجمات السيبرانية المعقدة التي لا يمكن ردعها مهما اجتهدت الدول في إنشاء جدران إلكترونية على بياناتها وعالمها الرقمي، ويرجع ذلك إلى براعة بعض الخبراء التقنيين، وبعض الهواة أيضًا، الذين قد ينتمون لدولة بعينها أو لبعض الجهات أو الجماعات، ويتمتعون بقدرات فائقة تمكنهم من اختراق الشبكات الحمائية وتحقيق أهدافهم بسهولة ويسر.

ومن هذا المنطلق، تنامت العلاقة بين الأمن والتكنولوجيا، وتزايدت إمكانية تعرض المصالح الاستراتيجية للدولة للتهديدات السيبرانية، ومن ثمَّ تحويل الفضاء السيبراني لوسيط ومصدر لأدوات جديدة للصراع الدولي متعدد الأطراف، الأمر الذي أثار اهتمام المجتمع الدولي سعيًا لضمان أمن فضائه السيبراني. ومع ذلك، لم يقتصر اهتمام الدول بالأمن السيبراني على البعد التقني، بل تجاوزه ليشمل أبعادًا أُخرى تشمل الثقافية والاجتماعية والاقتصادية والعسكرية ... إلخ.

وهو ما يؤكد الفرضية التي تتلخص في أن الاستخدام غير السلمي للفضاء الإلكتروني يؤثر على الرخاء الاقتصادي والاستقرار الاجتماعي

لجميع الدول التي باتت تعتمد على البنية التحتية للمعلومات. كما أن تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد أثر بدوره على سيادة الدول، خاصة مع تعاظم دور الشركات التكنولوجية العابرة للحدود الدولية، وما يوازيها من زيادة حدة مخاطر القرصنة والجرائم السيبرانية والتهديدات الإلكترونية.

وعليه، جاء هذا التقرير ليُسلط الضوء على خطورة هذه التهديدات لما تشكله من تحديًا كبيرًا للأمن الوطني، وخاصة في منطقة الخليج العربي، باعتبارها من أكثر المناطق المستهدفة من قِبل القراصنة السيبرانيين، والتي تجاوزت ممارساتهم التسلية الشخصية، ثمَّ جني المال، لتصل اليوم إلى مرحلة التخريب والتدمير وإلحاق الضرر بالمؤسسات الحيوية والبنى التحتية التكنولوجية وأنظمة المعلومات. ثمّ ينتقل هذا التقرير ليشير إلى أبرز جهود وخطط دول مجلس التعاون الخليجي لتأمين فضائها السيبراني، لينتهي بمجموعة من الاقتراحات لرفع كفاءة الأداء بما يُساهم في التصدي لكافة أنواع هذه التهديدات أو الهجمات.

المحور الأول

قراءة في تحولات الصراع والقوة وصولًا إلى عصر الرقمنة والحروب السيبرانية

يعد الصراع بمثابة السمة السائدة في العلاقات الدولية، وخاصةً عند الحديث عن تضارب المصالح الجيوبوليتية بين القوى الدولية، والتي يسفر عنها اختلال معدلات التوازن الاستراتيجي العسكري. وعلى هذا الأساس، تُبرر الدول لجؤها إلى استخدام القوة لتحقيق أهدافها ومصالحها القومية، ومن المعلوم أن الحرب هي وسيلة من وسائل استخدام القوة، ومن ثمَّ فإن العديد من التحولات الجذرية قد طرأت في مفاهيم الحرب ونظرياتها على مدار العصور، فمن الحروب التقليدية التي اعتمدت على الرماح والسيوف، إلى البنادق والرشاشات، ثمَّ القنابل النووية، إلى الصواريخ العابرة للقارات، وصولًا إلى نوع جديد من الحروب، وهي «الحروب السيبرانية»، والتي تستهدف تطويع التقنيات الرقمية والوسائل التكنولوجية وتحويلها إلى أسلحة تكتيكية تلحق دمار يوازي دمار الأسلحة التقليدية، بل قد يفوقه في كثير من الأحيان.

وفي هذا الصدد، جاء ألفين Alvin وهايدي توفلر Heidi Toffler في مؤلفهما «أشكال الصراعات المقبلة: حضارة المعلوماتية وما قبلها»[1]، ليطلق على أجيال الحروب المتعاقبة مصطلح «موجات الحروب». وأوضح

هـذا المؤلـف بـأن حروب الجيـل الأول، أو حـروب الموجـة الأولى، ظهرت في البدايـة عـلى مستوى المجتمعـات الصغيـرة عـلى شكل صراعات عنيفـة بدافع الثأر أو السيطرة عـلى مصـادر الغـذاء. وتابـع المؤلـف بـأن الثـورة الزراعيـة انطلقـت لتعـد نقطـة تحـول جوهريـة في التاريـخ البـشري، لمسـاهمتها في دفـع المجتمعـات نحـو الإنتـاج لتأمـين مظهـر تطـور الدولـة، كـما تطـورت أشـكال الصراعـات لتشـمل جيوشًـا تحمـل الأسـلحة البدائيـة كالرمـاح والسـيوف والمطـارق والحجـارة، وقـد اتسـمت هـذه الصراعـات بسـوء التنظيـم والقيـادة لاعتمادهـا عـلى القـوة العضليـة والاشـتباك الجسـدي، وتعكـس هـذه الحـروب بسـاطة نمـط الحيـاة والتفكـير السـائد خـلال هـذه الفـترة.

وتابـع المؤلـف بأنـه مـع انـدلاع الثـورة الصناعيـة وانتشـار المصانـع والآلات البخاريـة بنهايـة القـرن السـابع عـشر، تجـلى الاتجـاه إلى أهميـة تطويـع اسـتراتيجيات الحـرب المكتسـبة مـن المـدارس الحربيـة والمهـارات الفنيـة لضـمان احترافيـة وتطويـر الجيـوش وصـولاً إلى مسـتويات متقدمة تتماشـى مع التحـولات السـائدة عـلى السـاحة الدوليـة خـلال الفـترة التي أعقبـت الحربين العالميتين الأولى والثانيـة. وتجلـت الموجـة الثالثـة مـن الحـروب مـع انـدلاع حـرب الخليـج عـام ١٩٩١، وتميـزت بأنهـا حـروب معلوماتيـة تنطـوي عـلى اسـتخدام الصواريـخ التوماهـوك، والقنابـل الموجهة بالليـزر لتحديد ضربات الخصـم وتوجيههـا بدقـة. ويُلاحـظ تعاظـم اسـتخدام القـوة العسـكرية لتُميـز حركـة التفاعـلات الدوليـة في عهـد الحـرب البـاردة. ومـع ذلـك، فقـد أكـد المؤلـف بـأن مصـادر قـوة الدولـة وأشـكالها تتغـير مـع مـرور الوقـت، وتبـين في أعقـاب الاهتـمام بالقـوة الصلبـة المتمثلـة في القـدرات العسـكرية، بتزايـد الاهتـمام بالأبعـاد غـير الماديـة، حيـث تجلـت القـوة الناعمـة في نهايـة تسـعينيات

القرن المنصرم وتعاظمت فاعليتها في الإقناع والتأثير، ومن هنا ظهرت القوة بأشكالها الجديدة الاقتصادية والثقافية والتكنولوجية.

أما مع التطور التقني الذي شهده العالم في العقود الأخيرة، وزيادة اعتماد الدول على أدوات تكنولوجيا المعلومات والاتصالات لإدارة وتوجيه مختلف أنشطتها، فقد انتقلت تداعيات هذه الثورة الرقمية وما يرتبط بها من تكنولوجيا متطورة إلى ميدان الحرب وأدواتها في إطار ما يعرف بـ «الحروب السيبرانية» ذات التأثير الواضح على المستويين المحلى والدولي.

كما وقد تنوعت صور هذه الحرب وأساليب إدارتها وحتى أهدافها، إذ انتقل العديد من وسائل السيطرة والتحكم من العالم المادي إلى الحاسوب الآلي، مثلما انتقل جانب من المواجهات والهجمات إلى العالم الافتراضي، حتى أمكن تبني افتراض مفاداه أن الصيغة المستقبلية للحرب تتلخص في القوة السيبرانية وباستخدام الشبكة الدولية للمعلومات. وفي هذا الإطار، يعد جوزيف. س ناي Joseph S Nye. من أبرز المهتمين بالقوة السيبرانية، حيث يُعرّفها بأنها «القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأُخرى وذلك عبر أدوات سيبرانية»[٢].

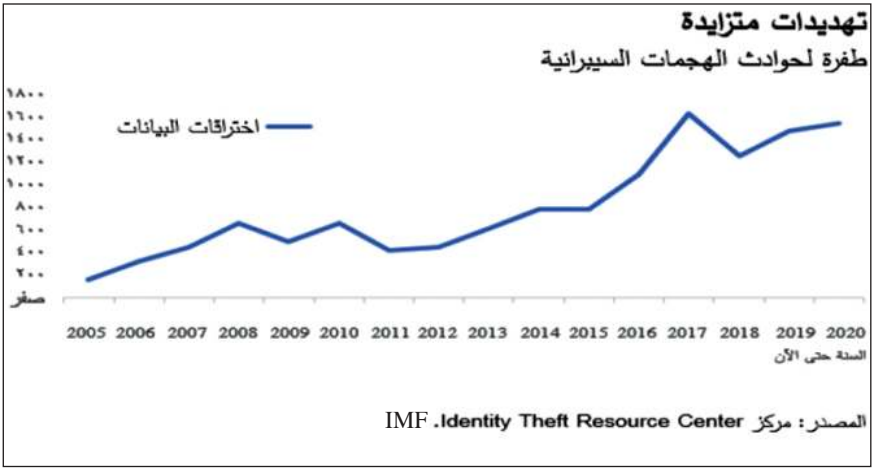
وبالتالي، إن حروب الجيل الرابع قد جاءت لتشكل تغييرًا جذريًّا لشكل الحروب، حيث أصبحت لا تستهدف أرضًا أو جنودًا، وإنما الأفكار، والأُطر القانونية، ووسائل الإعلام والوكالات الدولية، والأنشطة الاقتصادية والاتفاقيات، مع التدمير المادي والمعنوي لأفراد المجتمعات. كما ساهمت

في إعادة هيكلة مفهوم الحرب، والفواعل، والأسلحة المستخدمة، وأساليبها واستراتيجياتها.

وعلى هذا الأساس، فقد ساهم الفضاء السيبراني في اختصار حاجز الزمان والمكان، وخلق مساحات للتفاعلات المحلية والدولية في الواقع الافتراضي، ومن ثمّ نشأت فضاءات جديدة للصراع بأدوات مستحدثة، وأنماط جديدة تختلف عن الصراعات التقليدية. وهو ما اتضح خاصةً بعد أحداث ١١ سبتمبر ٢٠٠١ لكونها الحدث المفصلي في تاريخ العلاقات الدولية لبداية لجوء الجماعات الإرهابية للإنترنت بشكل بارز للترويج عن المبادئ والأفكار المتطرفة، وأصبح الفضاء السيبراني ساحة للصراع والقتال بين تنظيم القاعدة والولايات المتحدة الأمريكية.

ثمّ توالت بعد ذلك حوادث الهجمات غير المرئية، حيث اندلعت عام ٢٠٠٨ العمليات الهجومية العدائية بين روسيا وجورجيا في الفضاء السيبراني، ثمَّ تجلت تداعيات الهجوم السيبراني بـ «فيروس ستاكسنت Stuxnet» على برنامج إيران النووي عام ٢٠١٢، هذا بالإضافة إلى الدور الكبير الذي لعبته شبكات التواصل الاجتماعي في ظل الثورات العربية بدءًا من عام ٢٠١١. وفي خضم هذه الأحداث المتتالية والتي تؤكد على قوة الأسلحة السيبرانية في التأثير على التفاعلات وتطورها، جاء الشكل رقم (١) ليوضح بأن عام ٢٠١٧ قد مثل طفرة في عدد حوادث الهجمات السيبرانية.

الشكل رقم (١)
تطور حوادث التهديدات السيبرانية



ونخلص مما سبق بأن الفضاء السيبراني قد أضحى ساحة جديدة للصراع بشكله التقليدي ولكنه ذو طابع إلكتروني، ويتميز بتمدده داخل شبكات الاتصالات والمعلومات متجاوزًا الحدود التقليدية وسيادة الدول، كما يعكس أساليب جديدة للصراعات الدولية، فهناك صراع سيبراني تُحركه دوافع سياسية ويأخذ شكلًا عسكريًّا ويعتمد على استخدام قدرات هجومية ودفاعية عبر الفضاء السيبراني، كما يوجد صراع سيبراني يندرج في إطار القوة الناعمة ويستهدف الحصول على المعلومات أو التأثير في الأفكار والمعتقدات من خلال شن حروب إعلامية وسيكولوجية، ويمكن أن يأخذ الصراع السيبراني طابعًا تنافسيًّا بهدف الاستحواذ على سبق التقدم التكنولوجي، أو سرقة حقوق الملكية الفكرية والعلمية أو السعي لاختراق الأمن الوطني للدول من خلال الحصول على معلومات سرية، كالهجمات

التي تشنها قراصنة الكمبيوتر والتجسس، والتي قد يترتب عليها تدمير الاقتصاد والبنية المؤسساتية بنفس القوة التي قد يُسببها تفجير تقليدي مدمر.

المحور الثاني

ماهية التهديدات السيبرانية ومدى تأثيرها على الأمن الوطني والدولي

في عصر المعلوماتية والرقمنة الآلية وما أسفر عنه من تهديدات وجرائم سيبرانية أصبحت تُشكّل تحديًا كبيرًا للأمن الوطني وكذلك الدولي، أثار الفضاء السيبراني الجدل في أوساط العلماء والمهتمين في أرجاء كثيرة من العالم إلى أن اعتبره الكثيرون بمثابة المجال الخامس في الحروب، إضافة إلى المجالات التقليدية الأربعة : البحر، اليابسة، الجو، الفضاء[٣].

ويتجلى في هذا السياق أهمية الاطلاع على الجهود الفكرية لعدد من المعنيين بالدراسات السيبرانية، فضلًا عن أهمية الاطلاع على التفسيرات المطروحة لهذا الجيل من التهديدات، خاصةً مع التحذيرات من ارتفاع معدلات هذه الهجمات التي تستهدف الشركات وجهات حكومية وأجهزة الاستخبارات في الدول، بما يُساهم في احتدام الصدام بين القوى العالمية ويهدد الأمن القومي للاعبين على الساحة الدولية. ويُلاحظ في هذا السياق عدم وجود تعريفات واضحة وشاملة وموحَّدة بين أعضاء المجتمع العلمي لمثل هذه المفاهيم المعقدة والمتشابكة في أبعادها.

وبإمعان النظر إلى الفضاء السيبراني، تجدر الإشارة إلى أن مسألة تفسيره تعد مسألة نسبية حيث تتوقف على طبيعة إدراك وفهم كل دولة أو جهة بعينها وفقًا لرؤيتها واستراتيجيتها وقدرتها على استغلال المزايا المتاحة ومواجهة المخاطر الكامنة من هذا الفضاء. فعرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه: « فضاء التواصل الناتج من الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية»[٤]، ويُلاحظ أن هذا التعريف قد ركز على الجانب التقني غافلًا العامل البشري على الرغم من أهميته لفهم الفضاء السيبراني. بينما وصفه الاتحاد الدولي للاتصالات بأنه: «المجال المادي وغير المادي الذي ينتج من عدة عناصر وهي: أجهزة الحاسوب، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو جميع هذه العناصر»[٥]. كما أن هناك مَن عرَّفه بوصفه الذراع الرابعة للجيوش الحديثة.

وتقودنا دراسة الفضاء السيبراني إلى ضرورة الاطلاع على ماهية الحروب السيبرانية، فعرفها كل من جون أركويلا John Arquilla وديفيد رونفيلت David Ronfeldt بأنها: «إجراء أو استعداد لإجراء عمليات عسكرية بالاعتماد على المبادئ والآليات المعلوماتية، ما يعني تعطيل أو تدمير نظم المعلومات والاتصالات في الدولة الخصم»[٦]. كما عرفتها ماريا روزاريا Maria-rosaria Taddeo، الباحثة في معهد أكسفورد للأنترنت بأنها: «حرب تعتمد على استخدامات ذات طبيعة خاصة لتكنولوجيا المعلومات والاتصالات، وذلك في إطار استراتيجية عسكرية هجومية أو دفاعية تقرها الدولة، وتستهدف التعطيل الفوري أو السيطرة على معلومات مهمة عن

الخصم، ويختلف مستوى الدمار الذي يترتب عليها وفقاً لطبيعة وحجم الهجوم»[٧].

أما مجلس الأمن الدولي فقد عرفها بأنها: «استخدام لأجهزة الحاسوب، أو الوسائل الرقمية، من قِبلُ حكومة الدولة أو بمعرفتها أو بموافقة صريحة منها ضد دولة أُخرى أو ملكية خاصة داخل دولة أُخرى، بما يشمل الوصول المتعمد لمعلومات وبيانات أو اعتراضها أو تدميرها، أو إلحاق الضرر بالبنية التحتية الرقمية، أو إنتاج وتوزيع الأجهزة والتطبيقات الإلكترونية التي تستهدف الأنشطة المحلية».[٨] وعرفتها وزارة الدفاع الأمريكية بأنها: «توظيف القدرات السيبرانية بهدف الأهداف أو الآثار العسكرية في الفضاء السيبراني أو من خلاله»[٩].

كما يتجلى أيضًا في هذا السياق، مفهومان وهما: الهجمات السيبرانية والجرائم السيبرانية، وتعرف الأولى بكونها عمليات التسلل إلى أنظمة الحواسيب الآلية وجمع البيانات، وتتبعها، أو تدميرها، أو تغييرها، أو تشفيرها، كما ينطوي الأمر على زرع تطبيقات وبرمجيات خبيثة للتجسس. كما تعد هذه الهجمات بمنزلة اعتداء مباشر على السيادة الوطنية (الإلكترونية)، لما تحمله من تهديد صريح على خصوصية الأفراد باختراقه لحساباتهم البنكية أو هواتفهم وأجهزة حاسباتهم، أو على الأمن الوطني للدول في حال القرصنة على مواقع أو مؤسسات حكومية.

أما بالنسبة إلى الجرائم السيبرانية، فهي مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الممارسات التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها

ومقاضاة فاعليها. فهي الجريمة المتصلة باستخدام الكمبيوتر، أي تصرف غير قانوني، يرتكب باستخدام تقنيات المعلومات والاتصالات.

وفي ضوء الترابط الوثيق بين مصالح الدول القومية وبنيتها التحتية الحيوية، ومن ثمّ فإن أي هجوم على إحدى تلك المصالح يترتب عليه خلل استراتيجي وتهديد خطير على أمن الدولة القومي. كما أن الفضاء السيبراني قد فرض إعادة التفكير في مفهوم الأمن، بحيث لم يقتصر الأمر على ضرورة تمكين الدولة لردع خطر التعرض للهجوم، وتوفير إجراءات الحماية ضد تعرض منشآتها الحيوية وبنيتها التحتية للتهديد، بل امتد ليشمل ضرورة التسلح بالإمكانيات التكنولوجية لضمان توفير سياسات حمائية تستطيع التصدي لعمليات استهداف أنظمتها المعلوماتية.

وهو ما دفع العديد من الدول إلى إدراج إشكالية الأمن السيبراني في نطاق استراتيجيتها للأمن الوطني، فضلًا عن إضافته كبُعد جديد في أجندة حقل الدراسات الأمنية. فنجد على سبيل المثال أن الاختراق الإلكتروني الذي تعرضت له الولايات المتحدة الأمريكية في منتصف ديسمبر ٢٠٢٠، ووصف بأنه الأسوأ في تاريخ واشنطن حيث ما تزال تداعياته مستمرة إلى الآن، بما يفسر خطورة تلك التهديدات الإلكترونية وتزايدها وتوسع نطاقها.

وعليه، فقد تجاوزت مخاطر مثل هذه الهجمات بكونها تحديًا تقنيًّا، بل أضحت ترتبط بالأمن الوطني للدول بشكل وثيق لقدرتها على تعطيل أجهزة رئيسية في الدولة، كما أصبح جزءًا لا يتجزأ من آليات التعاون الأمني بين الدول، فجاءت على سبيل المثال لا الحصر في مقدمة المجالات التي تضمنتها المناورات العسكرية التي استضافتها الأردن، بعنوان «الأسد

المتأهب» خلال الفترة من ٢٥ أغسطس إلى ٥ سبتمبر ٢٠١٩، بمشاركة ٢٩ دولة.[١٠] وبالتوازي، فقد تنبهت الدول الكبرى ومنظمات الأمن الإقليمي إلى تداعيات التهديدات الإلكترونية، ووصل الأمر إلى تضمينها في نطاق العمليات الإرهابية التي قد تعصف بكافة المرافق الحيوية في البلاد، وهو ما تعرضت له إسبانيا عام ٢٠٠٧، مما دفع حلف شمال الأطلسي «الناتو» إلى تطوير سياسة للردع الإلكتروني، الأمر الذي يعكس جاهزية الحلف لتقديم الدعم الفوري في حال تعرض أي من الدول الأعضاء لمثل هذا الهجوم.

كما أولى الاتحاد الأوروبي قضية الأمن السيبراني أولوية قصوى، وهو ما اتضح من خلال اللقاءات المختلفة لممثلي الاتحاد، هذا إلى جانب جهود الوكالة المسؤولة عن الأمن الإلكتروني في الاتحاد الأوروبي. كما خاضت الدول الأوروبية بصورة منفردة خطوات بارزة في إطار الدفاع الإلكتروني، خاصة في كل من ألمانيا وفرنسا حيث أسست الأخيرة قيادة للعمليات المعلوماتية تقع في إطار اختصاصات قيادة الأركان، لتشرف على حوالي ٢٦٠٠ مقاتل رقمي.

كما ينبغي في هذا السياق أيضًا التطرق إلى مفهوم الردع السيبراني، ولعل التعريف الأبرز والأشهر له - والمتداول بكثرة في الأدبيات - هو تعريف الجنرال «أندريه بوفر» بأنه «القدرة على منع الدولة الخصم من اتخاذ قرار بالتحرك ضدها - أو بصورة أعم - منعها من العمل أو الرد إزاء موقف معين باتخاذ مجموعة من التدابير والإجراءات التي تشكل تهديدًا كافيًا حيالها، والنتيجة التي يراد الحصول عليها بواسطة التهديد هي نتيجة سيكولوجية نفسية»[١١]. كما يعتبر أبرز الآليات التي تستخدم لمنع الممارسات والأنشطة

الإجرامية ضد الأصول الوطنية في الفضاء والبنى التحتية التي تدعم مختلف العمليات الإلكترونية، ويجب أن ينطوي الردع السيبراني على ثلاث ركائز أساسية، وتتمثل في: مصداقية الدفاع Credible Defense، والقدرة على الانتقام An Ability to Retaliate، والرغبة في الانتقام A Will to Retaliate [١٢].

ويمكن أن نستخلص مما سبق بأن التهديدات السيبرانية تقع في إطار الممارسات التي تستهدف نظم المعلومات والاتصالات، ويمارسها الفاعلين من الدولة، أو الكيانات من غير الدول، وتتسم في الحالة الأخيرة بصعوبتها وتعذر إمكانية تحديد الخصم أو الجهة المهاجمة. كما أضحت جزءًا من أساليب وتكتيكات الصراعات الهجينة الرامية إلى مزج أدوات متعددة في تنفيذ الهجمات، مع عدم الارتكاز فقط على الأسلحة التقليدية.

المحور الثالث

واقع الهجمات غير المرئية في دول مجلس التعاون الخليجي

حمل العقدان الآخيران من القرن الحادي والعشرين في طياته العديد من التحديات لمنطقة الشرق الأوسط وشمال أفريقيا في الكثير من المجالات، لاسيما في نطاق الهجمات السيبرانية. ومقارنةً مع سائر المناطق، لم تكن منطقة الخليج بعيدة عن مخاطر الإرهاب السيبراني، بل اعتبرها الكثيرون بمثابة أرضًا خصبة ومسرحًا لتنفيذ عمليات القرصنة والجرائم الإلكترونية، هذه الأخيرة أضحت تهدد الأمن الإلكتروني في كافة أنحاء العالم اليوم أكثر من أي وقت مضى بفضل تنوع وتعدد الوسائل والأجهزة المستهدفة ما بين الهواتف النقالة، وأجهزة الحاسبات والمعلومات ... إلخ، والتي ترتبط إجمالاً بإقحام برمجيات خبيثة تلحق أضراراً بخوادم الإنترنت أو الأجهزة الذكية.

وقد بات جليًّا غزو عدد كبير من الكيانات الرقمية الفضاء السيبراني للدول الخليجية من خلال ممارسة أنشطة التسلل واختراق المواقع الحيوية، أو إيقافها عن العمل، أو إلحاق الخلل أو الضرر بالكيانات الرقمية، وذلك لتحقيق أهداف ذات أبعاد متعددة سياسية، أو عسكرية، أو أمنية، أو اقتصادية، وهو ما آثار قلق المعنيون في مجال الأمن السيبراني وخاصة ما

يتعلق بتداعياتها غير المعلنة والتي تدور رحاها في الفضاء الإلكتروني لدول الخليج العربي، وتسهم في إذكائها قوى كبرى، وجهات إقليمية متعددة تسعى إلى تنازع الهيمنة في منطقة.

إن ثمة عوامل قد ساهمت في استهداف هذه المنطقة، ويتقدمها التوجه الخليجي نحو البيئة الرقمية بامتياز والاعتماد على التكنولوجيا بشكل متزايد في كافة القطاعات والمستويات الاجتماعية والحكومية والاقتصادية، ويتمثل العامل الثاني في أهمية هذه المنطقة باعتبارها موقعًا حيويًّا لإقامة الاستثمارات التجارية وتأسيس الشركات والمؤسسات، إضافة إلى كونها إحدى المنابع الرئيسة لموارد الطاقة في عالمنا المعاصر، وهو ما يفسر إشارة العديد من الدراسات بأن غالبية تلك الهجمات تستهدف قطاعي الغاز والنفط، والمؤسسات المالية.

ولعل العامل الثالث، والأهم يتلخص في إيران واستراتيجيتها الرامية إلى تطوير قدراتها للتهديدات اللاتماثلية أو اللاتناظرية العابرة للحدود، وذلك تعويضًا لعدم امتلاكها للقدرات العسكرية اللازمة لخوض حرب تقليدية ضد خصومها. ويشير هذا النوع من التهديدات إلى التوازن الغير متكافئ بين القوى التي تعادي بعضها، وبالتالي يرغب الطرف الأقل قدرة على المواجهة المباشرة، في شن هجمات غير قابلة للكشف أو يصعب تحديد مصدرها، ولم ينحصر الأمر على لجوء الفواعل ذات الإمكانيات المحدودة لهذا النوع من الهجمات، بل شمل أيضًا الأقوياء على نحو أكثر انتشارًا وبتقنيات ووسائل أحدث وأكثر حسمًا.

ويمكن القول بأن إيران تعد الدولة الرائدة في استخدام هذه التكتيكات بالشرق الأوسط، خاصةً مع تصاعد حدة التوترات بينها من جانب

والولايات المتحدة وحلفائها في الخليج من جانب آخر. كما تبين أن الإتقان الذي بلغته القوات الإيرانية في نطاق التهديدات اللاتناظرية جعلها قادرة على تنفيذ هجمات إلكترونية على ٥٠ مؤسسة في ١٦ دولة بالعالم، هذا إلى جانب اختراقها لحسابات المعارضة الإيرانية كافة وعزلها عن العالم، والسيطرة على ما يقرب من ٣٠٠ ألف جهاز حاسوب داخل إيران عام ٢٠٠٩، بالإضافة إلى تنفيذ عدة عمليات قرصنة على مواقع التواصل الاجتماعي وخاصةً تويتر، وموقع بايدو «محرك البحث الصيني»، وموقع صوت أمريكا(١٣).

وفي ضوء ارتفاع وتيرة الهجمات الرقمية السيبرانية التي استهدفت عدد من الشركات ومؤسسات القطاعين: العام والخاص خلال السنوات الأخيرة بهدف التجسس، أو الاستيلاء على بيانات ومعلومات سرية، أو للحصول على الأموال، كشفت الإحصائيات الصادرة عن شركة أمن البيانات «فارونيس Varonis» لعام ٢٠١٩، بأن ٨٨٪ من الشركات العالمية لم تستطيع ردع هذه الهجمات، بينما ٥٪ فقط استطاعت حماية أنظمتها(١٤).

وعلى الصعيد الخليجي، كشف تقرير صدر في ١٦ يونيو ٢٠٢٠، من قِبل باحثون بشركة «كاسبرسكي Kaspersky» المتخصصة في الأمن الإلكتروني، عن تعرض دول مجلس التعاون الخليجي إلى ما يقرب من ٢٨٢ ألف هجمة إلكترونية على مستخدمي الهواتف الذكية خلال الفترة الممتدة من يناير إلى يونيو ٢٠٢٠. أما الهجمات التخريبية فقدر عددها بـ ١٦٠ ألفًا في المملكة العربية السعودية، و٧٠ ألفًا في دولة الإمارات العربية المتحدة، و٢٠ ألفًا بدولة الكويت، و٥ آلاف بدولة البحرين، و١٢ ألفًا بدولة قطر.(١٥) كما صرحت إحصائيات شبكة كاسبرسكي الأمنية Kaspersky Private Security Network في أكتوبر

٢٠٢٠ عن زيادة البرمجيات الخبيثة التي استهدفت المؤسسات المالية في جميع أنحاء دول الخليج بنسبة قدرت بـ ٤٥٪ في النصف الأول من عام ٢٠٢٠، مقارنة بالفترة ذاتها من العام السابق.(١٦)

ومن أبرز التهديدات السيبرانية التي استهدفت فضاء دول الخليج العربي، نذكر قيام فريق من قراصنة إيران السيبرانيين سمى بـ «سيف العدالة القاطع» بإقحام فيروس أطلق عليه شمعون ١، بشبكة المعلومات الداخلية لشركة أرامكو بالمملكة العربية السعودية النفطية في أغسطس ٢٠١٢، مما أدى إلى فقدان بيانات مهمَّة في أكثر من ٣٠٠٠٠ حاسب من حاسبات الشركة، بالإضافة إلى بث صورة لعلم الولايات المتحدة الأمريكية الذي تلتهمه النيران. كما اخترقت مجموعة Rocket Kitten عام ٢٠١٤ شبكات المعلومات والاتصالات في أكثر من دولة خليجية وإصابتها بأضرار بالغة.

وجاءت عمليات كليفر Operation Cleaver التي نفذت عام ٢٠١٤ لتتصدر قائمة الهجمات السيبرانية لإصابتها للعديد من القطاعات الحيوية كالنفط والغاز، إلى جانب العديد من المواقع الحيوية الحكومية والمطارات وشركات الاتصالات بأضرار جسيمة في دول الخليج، والولايات المتحدة الأمريكية، دول أُخرى أوروبية. وبالتوازي طور صانعي البرامج: الخبيث شامعون ٢؛ ليستهدف في نسخته الجديدة الصادرة عام ٢٠١٦ قطاعات أخرى بجانب قطاعي النفط والغاز. وفي عام ٢٠١٧، أحدث البرنامج الخبيث، المسمى بـ الصخرة الدوارة: Stone Drill تأثيرات بالغة في قطاعي: الطيران والبتروكيماويات بالمملكة العربية السعودية. كما أحكم فيروس مامبا للفدية Mamba Ransom ware قبضته على

حاسابات تابعة لمؤسسات مالية في عدد من الدول الخليجية وإلحق بهم خللاً كبيرًا.

وبالمثل، تسبب البرنامج الخبيث تريتون Triton عام ٢٠١٨ في أضرار مدمرة لعدة مؤسسات في قطاعي النفط والغاز والصناعات البتروكيماوية في دول خليجية، فضلًا عن تهديده باندلاع تفجيرات ممنهجة يمكن أن تودي بحياة العاملين في مواقع العمل. كما شن قراصنة إيرانيون سيبرانييون العديد من الهجمات بالغة التأثير APT عام ٢٠١٩ واستهدافها لشبكات معلومات وبنى تحتية مهمة في قطر والكويت والسعودية والإمارات والبحرين، وذلك خلال فترات زمنية متطاولة لضمان بلوغ أهدافها وتعميق مستوى تأثيرها.

ونخلص مما سبق أن الفضاء السيبراني لدول الخليج العربي قد تحول إلى بيئة خصبة للتهديدات، حيث أضحت منشآت النفط والغاز، ومؤسسات المرافق العامة، وقطاعات الخدمات المالية والاتصالات والرعاية الصحية، والمدن الذكية والبنى التحتية ومواقعها الحيوية في هذه الدول أشد عرضة للهجمات السيبرانية، الأمر الذي استدعى انتفاضة دول مجلس التعاون والتحرك لصقل قدراتها على التصدي لهذه التهديدات المتكررة.

المحور الرابع

التأهيل الخليجي في عصر التهديدات السيبرانية

في ظل تنامي اعتماد دول مجلس التعاون الخليجي على التكنولوجيا وآليات الحوسبة السحابية في مختلف القطاعات والصناعات، وتوسع نطاق التعامل بالعملة المشفرة أو الإلكترونية، سيتبعها بلا شك اتساع دائرة أنواع التهديدات والهجمات الإلكترونية والتجسس الصناعي، وانتهاكات أمن المعلومات والاحتيال في الهوية والاحتيال المالي والعديد من الأنشطة غير القانونية الأُخرى، مما يستدعي حتمية تأهيل هذه الدول حتى تتمكن من خلق فضاء سيبراني آمن حاضرًا ومستقبلًا.

ويُلاحظ أن دول مجلس التعاون الخليجي قد أولت اهتمامًا بالغًا لمواجهة هذه التهديدات، وهو ما يُشير إليه الجدول رقم (٢) والذي يوضح ترتيب دول الخليج في مؤشر الأمن السيبراني الذي صدر عن الاتحاد الدولي للاتصالات التابع للأمم المتحدة عام ٢٠٢٠، [١٧] والمعنى بقياس مدى جاهزية الدول لمواجهة هذه الهجمات ارتكازًا على معايير محددة، ليخلص إلى أن المملكة العربية السعودية ودولة الإمارات العربية المتحدة وسلطنة عُمان قد تصدرا قائمة الدول الأكثر نضجًا رقميًّا في هذا الشأن على مستوى المنطقة.

الجدول رقم (١)

ترتيب دول الخليج العربي في مؤشر الأمن السيبراني لعام ٢٠٢٠م

ترتيب دول الخليج في مؤشر الأمن السيبراني لعام ٢٠٢٠		
الدولة	الترتيب خليجيًّا	الترتيب عالمياً
المملكة العربية السعودية	١	٢
دولة الإمارات العربية المتحدة	٢	٥
سلطنة عُمان	٣	٢١
دولة قطر	٤	٢٧
مملكة البحرين	٥	٦٠
دولة الكويت	٦	٦٥

ومن الجهود المبذولة من قِبل الحكومات الخليجية في هذا الصدد، نوضح في الجدول رقم (٢) خططتها الاستراتيجية الرامية إلى تأسيس وحدات متخصصة لزيادة درجة مرونتها ورفع مستوى قدراتها في التصدي للهجمات السيبرانية كل دولة على طريقتها الخاصة، فضلًا عن توجه كل منها نحو مراجعة أمن نظم المعلومات بإجراء اختبارات الاختراق والتدقيق الأمني أُسوة بتجارب الدول والمنظمات الدفاعية التي استطاعت التصدي لهذا النوع من التهديدات.

الجدول رقم (٢)
أبرز ضوابط الأمن السيبراني في دول مجلس التعاون الخليجي

الدولة	ضوابط الأمن السيبراني
المملكة العربية السعودية	- أنشأت هيئة وطنية للأمن السيبراني نهاية أكتوبر ٢٠١٧، لتحديث قدرة الأمن السيبراني السعودي وإنشاء منصةٍ وطنيةٍ مشتركةٍ بين الوكالات. وقد تمّ منح الهيئة تفويضًا شاملًا يضمّ صياغة الاستراتيجية الوطنية للأمن السيبراني والإشراف على تنفيذها ووضع أُطُر الأمن السيبراني والضوابط والامتثال وبناء وتشغيل المراكز التشغيلية وتطوير القدرات البشرية في مجال الأمن السيبراني وزيادة الوعي بالأمن السيبراني وتحفيز نمو قطاع الأمن السيبراني وتشجيع الابتكار والاستثمار فيه وإقامة علاقاتٍ مع الوكالات المماثلة في الخارج والكيانات الخاصة مِن أجل تبادل المعرفة والخبرات.
دولة الإمارات العربية المتحدة	- إنشاء مجلس للأمن السيبراني في نهاية نوفمبر ٢٠٢٠، بهدف اقتراح وإعداد التشريعات والسياسات والمعايير اللازمة للأمن السيبراني للقطاعات المستهدفة في الدولة. كما يختص بإعداد وتطوير وتحديث استراتيجية للأمن السيبراني وخطة وطنية متكاملة للاستجابة، وضمن ذلك الهجمات والتهديدات وتقييم جاهزيتها، ووضع الآلية لتبادل ومشاركة وحوكمة المعلومات المرتبطة بالأمن السيبراني بين الجهات والقطاعات المختلفة محلياً ودولياً.
سلطنة عُمان	- إنشاء مركز الدفاع الإلكتروني، في ١٠ يونيو ٢٠٢٠، بهدف حماية المعاملات الإلكترونية، ومكافحة جرائم تقنية المعلومات، ويتبع مباشرةً جهاز الأمن الداخلي.
مملكة البحرين	- إنشاء لجنة وطنية للأمن السيبراني، ككيان رسمي لمعالجة قضية الأمن السيبراني بشكل مشترك على أعلى مستوى. - إعداد استراتيجية وطنية للأمن السيبراني، والتي من المتوقع إطلاقها قريباً بغية التصدي لتهديدات الأمن الإلكتروني الحالية والمتزايدة والحد من مخاطرها ولتمثل التزامًا من الدولة لحماية مصالح المملكة في الفضاء الإلكتروني. - استحداث أنظمة لإدارة المخاطر في الأمن السيبراني وإبلاغ الجهات بالمخاطر والتهديدات الماسة بالأمن السيبراني.

دولة قطر	- إنشاء الوكالة الوطنية للأمن السيبراني، في ٦١ سبتمبر ٢٠٢٠، بهدف توحيد رؤى وجهود تأمين الفضاء السيبراني للدولة، والمحافظة على الأمن الوطني السبراني. - إعداد الاستراتيجية الوطنية للأمن السيبراني والمحافظة عليها.
دولة الكويت	- تتجه إلى تنفيذ مشروع إنشاء مركز للأمن الوطني السيبراني، بهدف حماية الشبكات والمعلومات والبيانات الرسمية والشخصية، وتأمين الاستخدام الآمن والصحيح للمواقع الإلكترونية، مراقبة الأصول والبنى التحتية الحيوية والمعلومات الوطنية، دعم مشاريع التحول الرقمي والميكنة بمختلف الجهات الحكومية.

كما أبرمت الدول الخليجية العديد من الاتفاقيات، وعقدت شراكات مع الدول الرائدة في هذا الشأن، وأبرزهم الولايات المتحدة الأمريكية، وروسيا والصين، على أساس أن تداعيات التهديدات السيبرانية عابرة للحدود، وبالتالي ليس بمقدور أي دولة مهما توافرت لديها الإمكانيات المادية والبشرية أن تتصدى لتلك المخاطر سوى بالتعاون الإقليمي والدولي. وعليه، فقد طورت دول مجلس التعاون حافظة منوّعة من الشركاء في مجال الإنماء التكنولوجي، خاصةً في القطاعات الحيوية، وتشمل مزيجًا متوازنًا من شركات تابعة لدول شريكة في آسيا وأوروبا فضلًا عن الولايات المتحدة الأمريكية.

وتجدر الإشارة إلى أن المملكة العربية السعودية تعد الدولة الأولى على مستوى دولة المنطقة الأكثر عرضة للهجمات الإلكترونية بارتفاع عدد محاولات اختراق أنظمتها إلى ٢٦٠٪، الأمر الذي دفعها إلى تكثيف استثماراتها في أنظمة الحماية، واعتماد البرامج التوعوية للقطاعات المستهدفة. كما استطاعت دولة الإمارات التصدي للعديد من الهجمات الرقمية التي ازدادت وتيرتها خاصةً مع أزمة كوفيد-١٩، والتي تنوَّعت ما بين برمجيات خبيثة بنسبة ٦٢٪، وثغرات أمنية بنسبة ٣١٪، والتصيُّد الإلكتروني ٧٪.

هـذا إلى جانـب، إحبـاط الهيئـة العامـة لتنظيم قطـاع الاتصـالات بالدولة ٩٤٤ ألفًا و٢٠٩ هجـمات إلكترونيـة خـلال عـام ٢٠٢٠.[١٨]

هـذا وقـد حـذَّرت الهيئـة مـن فتـح الروابـط المجهولـة أو المزيّفـة وإبـلاغ الجهـات الأمنيـة في حـل أي مشـكلة للتأكـد مـن المصـدر الرسـمي. وتعاونـت الهيئـة مـع مزودي خدمـات الاتصالات لحظر المواقع الإلكترونيـة الاحتيالية، إلى جانـب اختبـار مستوى الأمـان في التطبيقـات الذكيـة لـدى المؤسسـات والـشركات الحكوميـة ونـشر الوعـي حـول عـالم الأمـن السـيبراني.

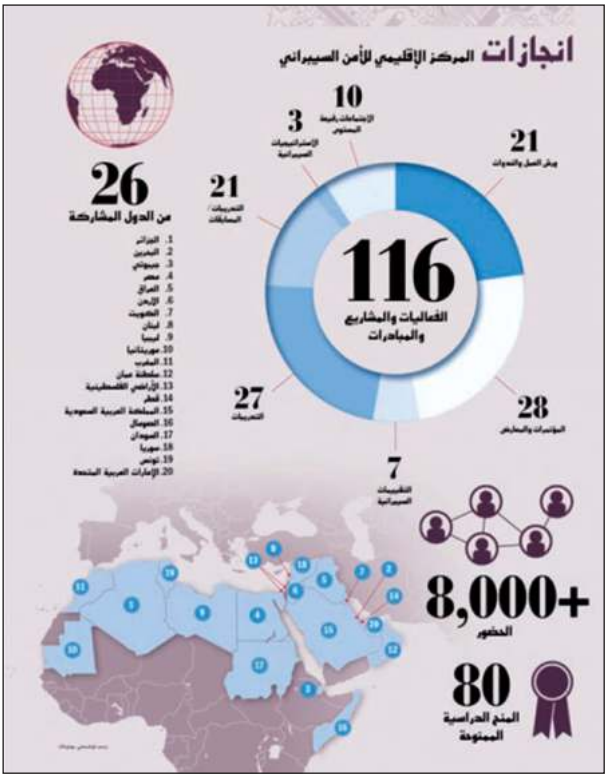
ونجحـت دولـة قطـر في التصـدي لنحـو ٤ ملايـين هجمـة إلكترونيـة خـلال النصـف الأول مـن العـام ٢٠٢٠، وتنوَّعـت مـا بـين الهجـمات عـلى البريـد الإلكـتروني، والمواقـع الإلكترونيـة URL، والبرمجيـات الخبيثـة. كـما تمكّنـت المؤسسـات والـشركات القطريـة مـن الاسـتمرار بأعمالهـا ومواجهـة التحديـات مـن خـلال ممارسـة أحـدث السياسـات الأمنيـة وتطبيـق أهـم البرامـج الخاضعـة لمعايـير عالميـة في الأمـن السـيبراني.

كـما أشـار تقريـر بشـأن «الرسـائل غـير المرغـوب فيهـا والتصيـد في الربـع الثـاني مـن عـام ٢٠٢٠» أعدتـه شركـة «كاسبرسـكي Kaspersky»، إلى أن مملكـة البحريـن قد نجحـت في التصدي لمحـاولات تصيد إلكـتروني «هجمات إلكترونيـة» بلـغ عددها ٦٧٥٨١ عملية خلال الربـع الثاني من عام ٢٠٢٠، في حين الكشـف عـن ٢,٥٧٨,٥٠١ محاولة تصيـد في كل من: مصر والإمارات والسـعودية والكويـت والبحريـن وعُـمان[١٩]. ويُعـدّ التصيُّد، أحد أقـدم أنواع الهجـمات الرقميـة القائمـة عـلى مـا يُعـرف بالهندسـة الاجتماعيـة، وأكثرهـا مرونـة، ويُسـتخدم بعـدَّة طـرق ولأغـراض مختلفـة للإيقـاع بالمسـتخدمين غـير الحذريـن عـبر جذبهـم إلى موقـع ويـب مـا وحثّهـم عـلى إدخـال معلوماتهـم

الشخصية، التي غالبًا ما تتضمن بيانات اعتماد مالية مثل كلمات المرور الخاصة بالحسابات المصرفية أو تفاصيل البطاقات البنكية أو تفاصيل تسجيل الدخول إلى حسابات وسائل التواصل الاجتماعي.

ففي عالم الإنترنت الذي لا حدود له، يمكن أن تتسبب هذه التهديدات في دولة بعينها في إحداث موجة متتالية من الأضرار في جميع أنحاء العالم، الأمر الذي يطرح ضرورة التعاون والمشاركة في الأدوات والموارد وتبادل أفضل الممارسات لحماية الشبكات والبنى التحتية الحيوية، لضمان سرعة الاستجابة والمرونة في حالة حدوث مثل هذا الاختراق.

الشكل رقم (٢)
المركز الإقليمي للأمن القومي



وعليه، فقد استطاعت سلطنة عُمان إدارة أول مركز إقليمي للأمن السيبراني، تابع للوكالة المتخصصة بتكنولوجيا المعلومات والاتصالات التابعة للأمم المتحدة ـ الاتحاد الدولي للاتصالات ـ بهدف تهيئة بيئة أكثر أمنًا وتعاونًا للأمن السيبراني في المنطقة العربية وتعزيز دور الاتحاد الدولي للاتصالات في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات في المنطقة.

وكما يوضحه الشكل رقم (٢)[٢٠]، فهو يضمن عضوية ٢٦ دولة ويسعى إلى وضع أُطر وسياسات إقليمية ووطنية ؛ لتعزيز الأمن السيبراني من خلال العديد من الأنشطة والفعاليات الإقليمية، وقد تمكن هذا المركز من تحقيق العديد من الإنجازات والحصول على عدد من التقديرات.

وفي ضوء حتمية التأهيل والاستعداد لمواجهة مخاطر مثل هذه التهديدات، يمكن حصر التوجهات اللازمة لبناء استراتيجيات الدفاع السيبرانية، فيما يلي:

- **التوجه الأول**: يستهدف استغلال تقنيات البحث العلمي والتكنولوجي لتحسين الإمكانيات السيبرانية، من خلال استحداث البرامج الحمائية لضمان التفوق التقني، ورفع كفاءة نظم الأتمتة وتحليل البيانات.
- **التوجه الثاني**: ينطوي على تطوير القدرات الهجومية للتصدي للأعداء وردعهم، إما عبر بناء القدرات الذاتية أو بالاستعانة بالأفراد والشركات المتخصصة، هذا إلى جانب تطوير القدرة على اختبار مدى الجاهزية لمواجهة الهجمات الإلكترونية. ويقصد بهذا التوجه رفع معدلات الاستجابة وزيادة الاهتمام بالبنية التحتية الحيوية وتأهيلها لتكون أكثر قدرة على التكيف والتعامل مع الهجمات العنيفة.
- **التوجه الثالث**: يؤكد على ضرورة الاهتمام بالتحالفات والشراكات مع الهيئات الدولية والإقليمية التي تتمتع بقدرات إلزامية لتعديل السلوك في العالم السيبراني وتحثهم على الابتعاد عن الحروب السيبرانية.
- **التوجه الرابع**: يهتم بإعادة تشكيل البيئة الداخلية لمنظومة الدفاع السيبراني، شاملًا تعزيز الوعي السيبراني وثقافة الحماية بين العاملين في

مجال الدفاع، وتنمية مستويات مسؤوليتهم تجاه الأمن السيبراني، مع ضرورة إشراكهم في البحث عن حلول ذكية ومرنة ومنخفضة التكاليف للإشكاليات السيبرانية.

- **التوجه الخامس**: يرمي إلى الاستثمار في الثروة البشرية المتميزة في مجال الأمن السيبراني من خلال تقديم الدعم والتأهيل للاستفادة من إمكانياتهم على أفضل وجه ممكن، هذا بالإضافة إلى تفعيل دور الخبراء في هذا المجال ومسؤولياتهم.

وهكذا نجد أن الاستراتيجية المثلى، ذات الكفاءة العالية للاستعداد والحماية من مخاطر التهديدات الإلكترونية، هي تلك التي تعتمد على قوة سيبرانية، تنعم بالقدرة على المنافسة والردع، وتستطيع إيجاد حلفاء وشركاء من الداخل والخارج يسهمون في الحماية، وتتمتع ببيئة حماية تتميز بالوعي والمسؤولية وإعطاء دور في الحماية لكل فرد، فضلًا عن السعي إلى تنمية المواهب والخبرات وإدارتها إدارة حسنة تفعل الإبداع والابتكار. والخلاصة أخيرًا أن تأمين هذه المتطلبات أمر مستمر يبدأ، لكن لا ينتهي، بسبب التقدم العلمي ومعطياته المتجددة، وتفاعله مع شؤون التنافس والصراع.

الخاتمة :

في ضوء تعاظم الدور الذي أضحى يضطلع به الفضاء السيبراني وإمكانياته المتغلغلة في كافة جوانب حياتنا المعاصرة، بفعل تكاثر أجهزة الاتصالات والمعلومات وتنوعها، واستحداث إنترنت الأشياء، فقد ساهمت هذه الأمور مجتمعة في قولبة نموذج جديد في ميزان القوى الجيوسياسي، حيث تهاوت الركائز التقليدية الراسخة بشأن الفوارق بين القوى العظمى والدول النامية فيما يتعلق بالقدرة على إحداث الضرر بالخصم، حيث أصبح صغار الخصوم كقراصنة المعلومات يتمتعون بقدرات هائلة في اختراق أو تدمير لاعبين كبار على الساحة الدولية، وهو ما عُرف بمخاطر التهديدات السيبرانية، هذه الأخيرة مرت بسلسلة متتالية من التطورات حتى تجاوزت خطاطة القولب الضيقة التي تولدت منذ قرون وفقًا للحدود القومية، والسياسية، والجغرافية، وكبَّدت الاقتصاد العالمي حتى اليوم خسائر فادحة فاقت ٦ تريليونات دولار[٢١].

مما لا شك فيه أن توجه التهديدات والهجمات السيبرانية تجاه منشآت الغاز والنفط، وبنى النقل والاتصالات، ومواقع حكومية حيوية، وشركات الطيران، والمستودعات الرقمية الوطنية، بات يشكل مؤشرًا خطيرًا خاصةً على المنظومة الأمنية لدول منطقة مجلس التعاون الخليجي، والتي تعد صناعاتها النفطية ومنظومتها الاقتصادية بمثابة العصب الحيوي لاستقرارها.

ومما يزيد من الأمر خطورة هو تكاثر وتنوع هوية الجهات النشطة في الفضاء السيبراني الخليجي، سواء كانت تابعة لقوى كبرى أو أُخرى إقليمية أو محلية، والتي تتنافس وتتجاذب فيما بينها، بما سوف يساهم بالتبعية في توسيع دائرة الأزمات التي تعصف بهذه الدول الخليجية، تمهيدًا لأنماط جديدة من النزاعات التي ستصبغ بصبغة سيبرانية لا يمكن التنبؤ بتداعياتها المحتملة على المنطقة العربية والخليجية.

وعلى هذا الأساس، اتجهت دول هذه المنطقة منفردة إلى تطوير دفاعتها في مجال الأمن السيبراني، وإعداد استراتيجيات وقائية لحماية فضائها الإلكتروني عبر التصدي لهجمات الفاعلين من الدول أو غير الدول كالقراصنة والجمعات السيبرانية، والذي جلّ تركيزهم على الهجمات ضد دول مجلس التعاون في المقام الأول على مهام التجسس والتخريب والاحتيال الإلكتروني، فيما استهدفت هذه الهجمات منذ عام ٢٠١٧ قطاعات ذات أهمية استراتيجية كالنفط والاتصالات.

ويبدو أن ممارسات القرصنة وعناصر الاختراق والتسلل المنتشرة حاليًّا لن تختفي من على خريطة العالم بين عشية وضحاها من تلقاء نفسها، وإنما لا بد من تكاتف الجهود وتضافر الأنشطة لمواجهتها، حيث إن الأمر أصبح يتعدى فكرة إنشاء مؤسسات معنية بمواجهة مثل هذه التهديدات، وفرض ضرورة العمل بشكل متوازٍ وجماعي على عدة أصعدة، سواء تشريعية من حيث إقرار التشريعات اللازمة، أو إعلامية من حيث إقرار سياسات توعوية تدعو المواطنين بأهمية أمن المعلومات بشكل عام، أو من خلال الاستعانة بالكوادر البشرية المتخصصة والمدربة على أعلى مستوى لمواكبة أساليب عمل الجماعات والمنظمات الإجرامية التي تسعى دومًا لاختراق أنظمة المعلومات في أجهزة الدولة، خاصةً ما يرتبط منها بالمؤسسات: المالية والعسكرية والأمنية.

قائمة المراجع العربية والأجنبية:

أولاً ـ المراجع العربية.

ثانياً ـ المراجع الأجنبية.

أولاً - المراجع باللغة العربية:

- إيفانز غراهام، نوينهام جيفري، **قاموس بنغوين للعلاقات الدولية**، ترجمة: مركز الخليج للأبحاث (الإمارات العربية المتحدة: مركز الخليج للأبحاث، ٢٠٠٤).
- الطيب مصطفى، **الفرق بين أمن المعلومات والأمن السيبراني** (مدونة علوم، ٨ أغسطس ٢٠١٩).
- الفتلاوي أحمد عبيس نعمة، **الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر** (مجلة المحقق الحلي للعلوم القانونية والسياسية، ٢٠١٦).
- بارة سمير، **الأمن السيبراني** cyber security **في الجزائر السياسات والمؤسسات** (المجلة الجزائرية للأمن الإنساني، ٢٠١٧).
- بوغرارة يوسف، **الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري** (مجلة الدراسات الإفريقية وحوض النيل، ٢٠١٨).
- جبور منى الأشقر، **السيبرانية هاجس العصر** (بيروت: جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، ٢٠١٦).
- حسن مظفر الرزو، **الفضاء المعلوماتي**، الطبعة الأولى (بيروت: مركز دراسات الوحدة العربية، ٢٠١٧).

- دحماني سليم، **أثر التهديدات السيبرانية على الأمن القومي.. الولايات المتحدة الأمريكية أنموذجًا، ٢٠٠١ ـ ٢٠١٧** (جامعة محمد بوضياف المسيلة، قسم العلوم السياسية، ٢٠١٨).
- زروقة إسماعيل، الفضاء السيبراني والتحول في مفاهيم القوة والصراع (مجلة العلوم القانونية والسياسية، ٢٠١٩).
- مرزوق عنترة، حرشاوي بن محيي الدين، **الأمن السيبراني كبُعد جديد في السياسة الدفاعية الجزائرية** (الجزائر: الملتقى الدولي حول: سياسات الدفاع الوطني بين الالتزامات السيادية والتحديات الإقليمية، ورقة بحثية، ٣٠- ٣١ يناير ٢٠١٧).

ثانياً ـ المراجع باللغة الإنجليزية:

- Alex S. Wilner, Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism (Journal of Strategic Studies, Vol. 34, No. 1, February 2011).

- Catherine Lotrionte, A Better Defense: Examining the United States New Norms-Based Approach to Cyber Deterrence (Georgetown Journal of International Affairs, 2013).

- Dieter Bohn, **US Cyber-attack reportedly Hit Iranian Targets** (The Verge, June 22nd 2019). Available At:

https://www.theverge.com/2019/6/22/18714010/us-cyberattack-iranian-targets-missile-command-report

- Griffiths, Jordan Luke, CYBER SECURITY AS AN EMERGING CHALLENGE TO SOUTH AFRICAN NATIONAL SECURITY, Master thesis (University of Pretoria, South Africa, 2016).

- Lehto Martti , Neittaanmäk Pekka, Cyber Security: Analytics, Technology and Automation (Switzerland : Springer International Publishing, 2015).

- Mohan Gazula, Cyber Warfare Conflict Analysis and Case Studies (Cambridge, working Paper CISL# 2017-10, MIT, 2017).

- Richard J. Harknett & John P. Callaghan & Rudi Kauffman, Leaving Deterrence Behind: War-Fighting and National Cyber security (Journal of Homeland Security & Emergency Management, Vol. 7, No. 1, 2010).

- Sven Herpig, **Strategic Operations in the Cyber Domain and their Implications for National Cyber Security** (GI-Jahrestagung, 2015).
- Symantec, Internet Security Threat Report (California, Symantec, Volume 22, 2017).
- Tim Stevens, A Cyber war of Ideas? Deterrence and Norms in Cyberspace (Contemporary Security Policy, Vol. 33, No, 1, 2015).
- Valeriano Brandon and C. Maness Ryan, **International relations theory and cyber security threats conflicts and ethics in an Emergent Domain in an emergent domain**, in Brown Chris and Eckersley Robyn, The Oxford Handbook of International Political Theory (United Kingdom: Oxford University Press, 2018).

الهوامش :

١ـ ألفين، هايدي توفلر، أشكال الصراعات المقبلة – حضارة المعلوماتية وما قبلها، ترجمة: صلاح عبد الله (بيروت : دار الأزمنة الحديثة، ١٩٩٨).

٢ـ صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية في التفاعلات الدولية، المعهد المصري للدراسات، دراسات سياسية، ٢٩ أكتوبر ٢٠١٦. متاح على: استخدام ـ القوة ـ الإلكترونية ـ فى ـ التفاعلات ـ الدولية.
(pdf eipss-eg.org)

٣ـ صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني؛ دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير(جامعة الشرق الأوسط: كلية الآداب والعلوم، قسم العلوم السياسية، تموز ٢٠٢١) ص.٤٧. متاح على: حروب الفضاء الإلكتروني .(pdf (meu.edu.jo)

4- Philippe VITEL and Henrik BLIDDAL, France Cyber Security and Defence: An Overview (Information & Security: An International Journal, vol.32, 2015, p. 3209-3. Available at: https://isij.eu/article/french-cyber-security-and-defence-overview

5- Available at: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.itu.int%2Fdms_pub%2Fitu-t%2Fopb%2Fres%2FT-RES-T.50-2012-MSW-A.docx&wdOrigin=BROWSELINK

6- John Arquilla, David Ronfeldt, Cyber war is coming! (Taylor & Francis Group: Comparative Strategy Journal, Vol 12, issue 2, 1993) p. 142. Available at: https://apps.dtic.mil/sti/pdfs/ADA485253.pdf

7- Mariarosaria Taddeo, An Analysis For A Just Cyber Warfare (UK: University of Hertfordshire, 2012 4th International Conference on Cyber Conflict, Department of Philosophy - School of Humanities, 2012) p.211. Available at: https://ccdcoe.org/uploads/2012/01/3_5_Taddeo_AnAnalysisForAJustCyberWarfare.pdf
8- Fred Schreier, On Cyber warfare (DCAF Horizon, Working Paper No. 7, 2015) p.31. Available at:
https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf
9- Ibid, p. 65.

١٠- متاح على:
https://caus.org.lb/ar/%D9%8A%D9%88%D9%85%D9%8A%D8%A7%D8%AA-2019-4/

١١- رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات (المركز الديمقراطي العربي، فبراير ٢٠١٧). متاح على:
https://democraticac.de/?p=43837&fbclid=IwAR0E3qdGSI13CGhr2ZaoVZ51dF5WoBnE-N5Uu-Byc9R9jlqezGqXxkHTocdI#_ftnref9

12- Ibid.

١٣- أحمد فوزي سالم، مساع خليجية لامتلاك خبرة روسيا في «الحرب غير المتكافئة»، ٢٨ أكتوبر ٢٠١٩. متاح على:
https://www.noonpost.com/content/29966

14- Statistics available at: https://www.varonis.com/blog/cybersecurity-statistics/

15- Statistics available at: https://www.zawya.com/mena/en/press-releases/story/Phishing_during_COVID19_outbreak_106245_attacks_in_Q2_in_Kuwait_report-ZAWYA20200819095049/

16- Statistics available at: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf

١٧- قراءة في تقرير مؤشر الأمن السيبراني العالمي لعام ٢٠٢٠، متاح على:
http://www.akhbar-alkhaleej.com/news/article/1257499

18- Available at: https://telecomreviewarabia.com/index.php/articles/reports-coverage/1679-the-cyber-attacks-pandemic-affects-the-gulf-countries-and-intensifies-efforts-to-confront-them

19- Available at:
https://alwatannews.net/article/885595/Bahrain/%D9%83%D8%A7%D8%B3%D8%A8%D8%B1%D8%B3%D9%83%D9%8A-%D8%A7%D9%84%D8%A8%D8%AD%D8%B1%D9%8A%D9%86-%D8%AA%D8%AA%D8%B5%D8%AF%D9%89-%D9%8467581-%D9%85%D8%AD%D8%A7%D9%88%D9%84%D8%A9-%D8%AA%D8%B5%D9%8A%D8%AF-%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D8%A8%D8%A7%D9%84%D8%B1%D8%A8%D8%B9-%D8%A7%D9%84%D8%AB%D8%A7%D9%86%D9%8A

20- Available at:
https://unipath-magazine.com/ar/%D8%B3%D9%84%D8%B7%D9%86%D8%A9-%D8%B9%D9%8F%D9%85%D8%A7%D9%86-%D8%B1%D9%8A%D8%A7%D8%AF%D8%A9-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3-%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A/

21- Available at:
https://alghad.com/6-%D8%AA%D8%B1%D9%8A%D9%84%D9%8A%D9%88%D9%86%D8%A7%D8%AA-%D8%AF%D9%88%D9%84%D8%A7%D8%B1-%D8%AE%D8%B3%D8%A7%D8%A6%D8%B1-%D8%A7%D9%84%D9%82%D8%B1%D8%B5%D9%86%D8%A9-%D8%A7%D9%84%D9%85%D8%AA%D9%88%D9%82/

قواعد النشر في سلسلة التقرير الاستراتيجي يصدر شهرياً

- أن يكون موضوع التقرير الاستراتيجي معنياً بالقضايا الاستراتيجية التي تهم دولة الكويت في المقام الأول، ودول منطقة الخليج والجزيرة العربية بشكل عام.
- ألا تقل عدد صفحات التقرير عن (١٥) صفحة (٣٧٥٠ كلمة).
- أن توضع الهوامش والمصادر العلمية والمراجع وفق المعايير البحثية المعتمدة.
- يمنح الباحث (١٠) نسخ من الإصدار.
- يمنح الباحث مكافأة مالية مقدارها (١٥٠ دينار كويتي).