التحديات الإلكترونية والأمن السيبراني في الوطن العربي

Electronic threats and cyber security in the Arab world

بلعسل بنت نبي ياسمين¹، عمروش الحسين²

Belacel bent nabi yasmine¹, Amrouche Houssine²

¹ جامعة الدكتور يحي فارس المدينة - كلية الحقوق (الجزائر)، belacel.yasmine@univ.medea.dz

² جامعة الدكتور يحي فارس المدينة - كلية الحقوق (الجزائر)، LSMLAW213@YAHOO.FR

تاريخ الاستلام: 2021/02/25 تاريخ القبول: 2021/05/08 تاريخ النشر: 2021/06/01

ملخص:

كانت المنطقة العربية على مر التاريخ منطقة لمختلف الصراعات والتحديات سواء تقليدية كانت أم جديدة. فلم يعد إطار القضايا الأمنية بأبعادها المتعددة محددًا داخليًا لأي دولة، بل امتد إلى الإطار الإقليمي والدولي، فأساليب التعامل الممكنة تتأثر هي الأخرى بالعديد من المتغيرات الخارجية والتي أصبحت من الصعب تجاهل آثارها، في ظل الثورة الرقمية وما صاحبها من تطور مس جميع المجالات وامتدادها كليا للفضاء السيبراني تغيرت وفقه خصائص الأمن والصراع في المنطقة العربية خاصة بعد سنة 2011 وما تبعها من ثورات الربيع العربي التي تزايدت من خلالها مختلف التهديدات الأمنية الجديدة خاصة الإلكترونية منها فحولت حلبة الصراع من أرض الواقع إلى الفضاء الأزرق.

كلمات مفتاحية: التهديد، القضايا الأمنية، الثورة الرقمية، الحرب الإلكترونية، الفضاء السيبراني، المنطقة العربية.

Abstract:

Throughout history, the Arab region has been a region of various conflicts and threats, whether traditional or new. The framework of security issues in their dimensions is no longer defined internally for any country, but has extended to the regional and international framework. And in light of the digital revolution and the accompanying development that touched all fields and the total sweep of cyberspace, the characteristics of security and conflict in the region changed, especially after the year 2011 and the subsequent Arab spring revolutions, through which various new security threats, especially electronic ones, increased, thus transforming the arena of conflict from the ground to reality. Blue space.

Keywords: threat; security issues; the digital revolution; electronic warfare; cyberspace; the Arab region.

المؤلف المرسل: بلعلل بنت نبي ياسمين، الإيميل: yasmine38yasmine00@gmail.com

1. مقدمة :

فرضت الثورة التكنولوجية العديد من التهديدات والتحديات في المجالات المختلفة لأنها شملت كافة مجالات الحياة، فهي تعتبر إحدى أحدث التطبيقات العلمية، وكأي تطبيق له الكثير من المنافع والعديد من الأضرار بسبب الاستخدام السيء لها، وأصبح من يمتلك التكنولوجيا الآن هو من يملك القوة والسيطرة، فظهرت البنوك والحكومات الإلكترونية، وانتشرت التجارة الإلكترونية والتعليم الإلكتروني ومختلف الوسائط الإلكترونية.

برز في السنوات الأخيرة مخاطر عسكرة الفضاء الإلكتروني، وسعيًا لدرء هذه التهديدات وجب التطور في مجال سياسات الدفاع والأمن الإلكتروني، والسباق نحو التسليح السيبراني، وتبني سياسات دفاعية سيبرانية لدى الأجهزة المعنية بالدفاع والأمن في مختلف الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.

فقد حاولت الدول العربية كغيرها من الدول مواكبة دول العالم في الاستخدامات المتعددة للثورة الرقمية، لكن باعتبارها منطقة لمختلف النزاعات واجهت نوعًا من الصعوبة في التأقلم مع هذه التكنولوجيا، ومع استمرارية تطويرها ونشرها في جميع أنحاء الوطن العربي وركبه في المقابل تنامي التهديدات السيبرانية لمختلف القطاعات العامة والخاصة.

الهدف من دراسة هذا الموضوع هو تبيان مجمل الأخطار والتهديدات التي تنتج عن الفضاء الإلكتروني، بالإضافة إلى اعتباره من المواضيع المهمة على الساحة الدولية نظرا لكثرة الصراعات والتجاذبات على المستوى الداخلي أو الإقليمي والدولي.

ففي ظل انتشار الثورة الرقمية بشكل كبير ومختلف انعكاساته على جميع القطاعات من جهة، وكثرة الصراعات والنزاعات في أغلب الدول العربية من جهة ثانية، فيما تتمثل تحديات المنطقة العربية في ظل التحديات الإلكترونية من أجل تعزيز الأمن السيبراني؟ للإجابة عن هذه الإشكالية وتساؤلات أخرى اعتمدنا على المنهج الوصفي والمنهج التاريخي المناسبين لمثل هذه الدراسات من أجل الإلمام بمختلف جوانب الموضوع والوقوف على أهم التحديات التي تواجه المنطقة العربية لتعزيز أمنها السيبراني. وبناء على ذلك، سنحاول دراسة الموضوع من خلال العناصر الآتية:

2. الإطار المفاهيمي للتحديات الإلكترونية والأمن السيبراني

تعتبر قضية العالم الافتراضي والفضاء السيبراني من أهم القضايا التي باتت تشغل العالم اليوم، فهو أضحى واقعا موازيا للعالم الحقيقي، وقد انتقل جزءا كبيرا من الصراعات بين القوى العظمى من ميادين القتال الكلاسيكية إلى العالم الرقمي.

1.2 التهديد الإلكتروني والأمن السيبراني:

1.1.2 تعريف التهديد الإلكتروني:

يعرف التهديد لغة على أنه من الفعل هدد، يهدد تهديدا وهو ناتج عن إلحاق الأذى والضرر، أي أن التهديد يتعلق بكل ما من شأنه أن يعرقل عملية بناء الأمن أو يؤدي إلى إنقاص الشعور به (صباح، 2020)، ويشير المعنى اللغوي للتهديد في اللغة الإنجليزية إلى Threat، أما في اللغة الفرنسية فهو يشير إلى معنى الخطر Menace، وفي اللغة اللاتينية Trudere، يرادف معنى الدفع، ووفقا لقاموس وبستر فالتهديد هو: تصريح أو تعبير عن نية لإيذاء أو تدمير أو معاقبة في الانتقام أو الترهيب، وحسب معجم le Petit Robert هي الطريقة التي يرسم بها الرعب على وجه شخص ما، مع وجود النية لجعله يخشى الأذى التي أراد إلحاقها به (موقع العلاقات الدولية، 2019).

أما التهديد من الناحية الاستراتيجية فهو بلوغ تعارض المصالح والغايات القومية مرحلة يتعذر معها إيجاد حل سلمي يوفر للدولة الحد الأدنى من أمنها السياسي والاقتصادي والاجتماعي والعسكري مقابل قصور قدراتها لموازنة الضغوط الخارجية، الأمر الذي قد يضطر الأطراف المتصارعة اللجوء إلى استخدام القوة العسكرية، معرضة أطراف أخرى للتهديد (حربي، 2017).

تعرف التهديدات الأمنية اصطلاحاً من طرف ريتشارد أولمن: تهديد الأمن القومي هو عمل /فعل أو سلسلة من الأحداث التي تؤدي بشكل كبير، وعلى فترة زمنية قصيرة نسبياً، إلى النقص من نوعية حياة مواطني الدولة أو تساهم بشكل كبير في تطبيق نطاق الخيارات السياسية المتاحة أمام حكومة دولة أو الهيئات الخاصة والمنظمات غير الحكومية داخل الدولة (صباح، 2020).

أما التهديدات الإلكترونية فيقصد بها تلك الهجمات التي تتم باستخدام آليات وشبكات إلكترونية كالإنترنت والحواسيب وتهدف إلى إلحاق الضرر بأجهزة أو شبكات إلكترونية أخرى أو سرقة المعلومات الموجودة عليها، ويعنى بإلكترونية التهديد الإشارة إلى كل من أداة الهجوم أي الآليات المستخدمة في شنه، وإلكترونية الهدف المتعرض له، فقد تتعرض أهداف إلكترونية إلى هجمات غير إلكترونية كالهجمات الحركية والمادية... (شفيق، 2020).

وتعرف أيضاً بأنها استغلال الحاسبات وتكنولوجيا المعلومات في تخريب وتدمير البنية المعلوماتية للخصوم، بل وتعطيل شبكات الدفاع الجوي واختراق أنظمة المعلومات للبريد الإلكتروني لمكاتب رؤساء الدول والتجسس عليهم وفق خطة منهجية (البناء، 2018).

2.1.2 تعريف الأمن السيبراني:

يتكون الأمن السيبراني من لفظتين هما الأمن والسيبراني، فالأمن هو نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أَمِنَ أَمْنًا وَأَمَانًا وَأَمَنَةً: أي اطمئنان النفس وسكون

القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه، وقد عرفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يهدد القيم النادرة.

أما السيبراني: فمصطلح السيبرانية في الوقت الحالي من أكثر المصطلحات ترددا في معجم الأمن الدولي، وتشير كلمة cyber إلى أنها لفظة يونانية الأصل مشتقة من كلمة kybernetes بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازا للمتحكم governor، وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي norbert wiener وذلك للتعبير عن التحكم الآلي (قره، 2015).

ويعرف أيضا بأنه عبارة عن مجموعة من التقنيات والأنظمة والحديثة التي تهدف إلى حماية الشبكات والأنظمة الإلكترونية والأدوات التكنولوجية الحديثة للمؤسسات ومختلف القطاعات، للحد من الهجمات الإلكترونية بغير وجه حق (مجلة رواد الأعمال، 2020).

ويعرف الأمن السيبراني أو أمن تكنولوجيا المعلومات بأنه حزمة عمليات وإجراءات تتوخى تأمين وحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو التلف أو السرقة والوصول غير المصرح به (الأمير، 2018).

فالأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني (شكري، 2019).

2.2 التهديدات الإلكترونية والهجمات السيبرانية:

1.2.2 أنواع التهديد الإلكتروني والهجوم السيبراني:

لقد أدى التطور التكنولوجي من انتشار الإنترنت والأجهزة النقالة، وتوافر الحزمة العريضة للإنترنت عبر الأجهزة النقالة وتدني كلفتها، إلى ارتفاع أعداد مستخدمي الإنترنت وتزايد الاعتماد على هذه التكنولوجيات في التنمية الاقتصادية والاجتماعية، إلا أن الانفتاح الذي يميز شبكة الإنترنت والفضاء السيبراني عموماً، جعلها عرضة للتعديات والأنشطة الإجرامية ومختلف التهديدات والهجمات الإلكترونية من قبل مخترقي الشبكات.

الفضاء الإلكتروني: الفضاء أو المحتوى والبديل الكوني الذي يمكن الناس من المشاركة فيه، ويصفه وليام جيبسون بأن: العالم الرقمي هو عبارة عن شبكات الكمبيوتر والاتصالات الإلكترونية وعبرة عن شبكة كمبيوتر خيالية تحتوى على كم هائل من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة، وأصبحت قوة الكمبيوتر تتزايد مما جعل الناس يرون في الفضاء الإلكتروني أنه عالم مواز للواقع الذي نعيش فيه(العباسي، 2016).

- **الإرهاب الإلكتروني:** يعرفه دورثي دينينغ بأنه: عبارة عن التقاء الإرهاب وعالم الكمبيوتر وأنه الاستخدام غير المشروع للقوة والتهديدات بضرب أجهزة الكمبيوتر والشبكات والمعلومات المختزنة فيها من أجل ترويع وإكراه الحكومات وشعوبها من أجل تحقيق أهداف سياسية واجتماعية، ولكي يعتبر ذلك إرهاب لا بد أن يؤدي إلى ترويع وإكراه الحكومات والأشخاص والممتلكات أو على الأقل التسبب في الضرر والخوف، وكذلك إحداث ضحايا وإيذاء بدني وانفجار وأضرار اقتصادية جسيمة.. (سليمان، 2020)، بحيث يتضمن الإرهاب الإلكتروني بهذا المعنى أعمال اختراق المواقع وأنظمة المعلومات والقرصنة، نشر الرعب ومختلف أشكال التهديد، استقطاب الأفراد للانخراط في التنظيمات الإرهابية (حكيم، 2018).

-**الحرب الإلكترونية:** هي مجموعة الإجراءات الإلكترونية المتضمنة استخدام بعض النظم والوسائل الإلكترونية الصديقة في استطلاع الإشعاع الكهرومغناطيسي الصادر من نظم العدو ووسائله ومعداته الإلكترونية المختلفة مع الاستخدام المتعمد للطاقة الكهرومغناطيسية

في التأثير على هذه النظم والوسائل لمنع العدو أو حرمانه أو تقليل استغلاله للمجال الكهرومغناطيسي، فضلا عن حماية الموجات الكهرومغناطيسية الصادرة من النظم والوسائل الإلكترونية الصديقة من استطلاع العدو لها، أو التأثير عليها (موسوعة مقاتل من الصحراء، 2020).

التجسس الإلكتروني: أو ما يعرف بحرب التجسس المعلوماتي وهي عبارة عن عدة طرق لاختراق المواقع الإلكترونية ومن ثم سرقة بعض المعلومات التي قد تكون في قائمة الأهمية والخطورة للطرف المتلقي والمسروق منه، فقد يكون الاختراق من أشخاص عابثين ليس إلا بغرض سرقة معلومات مهمة مثل ما حدث لوزارة الدفاع الأمريكية البنتاغون في العامين الماضيين من قبل أشخاص لا يتبعون للقاعدة، والاختراق ليس محصور على المؤسسات العسكرية فقط، فقد تتعرض له المؤسسات النقدية وخصوصا البنوك المركزية والمؤسسات العملاقة (موقع موسوعة ويكيبيديا، 2019).

2.2.2 التهديدات التي تواجه الأمن الإلكتروني

تتزايد أهمية الأمن السيبراني بسبب الاعتماد المتزايد على أنظمة الكمبيوتر والإنترنت مع تزايد نمو مختلف الأجهزة الذكية، ومن أجل تأمين النظام الإلكتروني، ينبغي فهم التهديدات (الأمير، 2018) التي يمكن أن يتعرض لها، ويمكن تصنيف هذه التهديدات إلى:

-**التنصت :** التنصت هو القيام بالاستماع خلسة إلى محادثة خاصة بين اثنين أو أكثر من مستخدمو الشبكة. ويتم ذلك من خلال استخدام برامج معدة لذلك.

-**الانتحال :** الانتحال هو القيام بالتكرار ككيان ساري المفعول من خلال تزوير البيانات من أجل الوصول إلى المعلومات التي يكون الشخص المنتحل غير مصرح له بالحصول عليها.

التلاعب: من خلال التلاعب يجري التعديل الضار للمنتجات.

تجاوز الصلاحيات: في هذه الحالة يسعى المهاجم الذي يمتلك مستوى معين من النفاذ والوصول المقيد للنظام إلى تجاوز المستوى المتاح له من دون ترخيص.

التصيد الاحتيالي: وهو محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان مباشرة من المستخدمين.

الاحتيال المصرفي: وهو شكل من أشكال الهجمات الإلكترونية المتطورة التي تستهدف نقاط التواصل بين البنوك العالمية، وذلك من خلال استهداف التحويلات المصرفية العالمية التي تتدفق عبرها مليارات الدولارات يوميا، ومن ثم تحويل الأموال إلى حسابات المجرمين.

3. الهجمات السيبرانية في الوطن العربي: أنماط وتحديات

في السنوات الأخيرة الماضية شهد العالم تطورا هائلا في تكنولوجيا المعلومات الذي مس جميع المجالات وبدوره ألقى ظلاله على العلاقات الدولية، فتحول الفضاء الإلكتروني إلى مجال جديد لمختلف الصراعات الدولية.

1.3 التحولات الكبرى لهجمات الفضاء الإلكتروني

1.1.3 التغير في مهددات الأمن العالمي

ظهرت العلاقة ما بين الفضاء الإلكتروني والأمن الدولي، خاصة مع التوسع في تبني الحكومات الإلكترونية من جانب العديد من الدول، واتساع نطاق مستخدمي وسائل الاتصال وتكنولوجيا المعلومات في العالم، حيث تصبح قواعد البيانات القومية في حالة انكشاف خارجي، وهذا ما يعرضها لخطر التعرض لهجمات الفضاء الإلكتروني إلى جانب الدعاية والمعلومات المضللة ونشر الشائعات أو الدعوة لأعمال تحريضية.

وأصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، والتي تشمل الطاقة والاتصالات والنقل والخدمات الحكومية والتجارة الإلكترونية والمصارف والمؤسسات المالية، حيث جعل الفضاء الإلكتروني من تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة والتي تعرف بالبنية التحتية القومية للمعلومات وأصبح يتعلق

الأمن العالمي بمدى قدرة المجتمع الدولي على اتخاذ إجراءات الحماية ضد التعرض للأعمال العدائية جراء الاستخدامات السيئة للفضاء الإلكتروني (الصادق، 2018).

وجاءت تلك المظاهر لتبرز استخدامات غير السلمية للفضاء الإلكتروني وما يمثله ذلك من تهديد للأمن الإلكتروني العالمي من جانب كافة الفاعلين في مجتمع المعلومات، وأصبح من الممكن لأي طرف متصل بشبكة تكنولوجيا الاتصال والمعلومات أن يتأثر إما بالأطراف الأخرى المتصلة على الشبكة نفسها أو بطبيعة الأخطار التي تعترض هذه الشبكة وتهدد طبيعة عملها (الصادق، الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي، 2019)

ودفعت كذلك المزايا الاستراتيجية لهجمات الفضاء الإلكتروني إلى إمكانية توظيفها عسكريا في ظل اعتماد الدول على الأنظمة الإلكترونية في جميع منشأتها الحيوية، والعمل على توظيفه في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى بالاستراتيجية السيبرانية للدول، ومن جهة ثانية أدت عملية تصاعد المخاطر إلى بروز دور الشركات العاملة في مجال الأمن الإلكتروني (الصادق، الهجمات السيبرانية-أنماط وتحديات جديدة للأمن العالمي، 2018).

2.1.3 تحولات مفاهيم الأمن والصراع في عصر الفضاء الإلكتروني

أثر الفضاء الإلكتروني في تغير طبيعة وخصائص الأمن والقوة والصراع في المشهد الدولي سواء على المستوى النظري أو التطبيقي، وأصبح له تأثيرات وشواهد واضحة في العلاقات الدولية، تمثلت (الصادق، الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي، 2019) في:

-الأمن الإلكتروني لم يعد مقتصرًا على البعد التقني فقط بل تعداه إلى أبعاد أخرى في ظل تراجع سيادة الدولة، وتزايد العلاقة بين الأمن والتكنولوجيا بصفة عامة، خاصة مع إمكانية تعرض المصالح الاستراتيجية للدول إلى أخطار وتهديدات، قد فرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي للدولة، والذي يعني حماية قيم المجتمع الأساسية

وإبعاد مصادر التهديد عنها، وغياب الخوف من خطر تعرض هذه القيم للهجوم. ومن جهة أخرى فإن تحول الفضاء الإلكتروني إلى ساحة عالمية، جعل هناك ارتباط عضوي بين الأمن الداخلي وأمن الفضاء الإلكتروني، وهو ما يشكل أساس الأمن الجماعي العالمي.

- لعب الفضاء الإلكتروني دورا هاما في تعظيم القوة، أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية، حيث أصبح التفوق في ذلك المجال عنصرا حيويا في تنفيذ مختلف العمليات، واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة التكنولوجية، بحيث بات مسرحا لشن هجمات تخريبية ترتبط بنشر المعلومات المضللة والحرب النفسية، والتأثير في توجهات الرأي العام، والنشاط السري والاستخباراتي.

- الفضاء الإلكتروني وعلاقته ببروز أنماط جديدة من الصراع، كمجال تنشأ فيه نزاعات بين الفاعلين المختلفين وتعبيرا عن تعارض المصالح والقيم سواء بين الفاعلين من الدول أو غير الدول، فيعتبر الفضاء الإلكتروني عابر للحدود وسهولة الدخول إليه، وقد اتسعت دائرة الصراعات السيبرانية وازداد عدد المهاجمين وظهور الصراع حول امتلاك أدوات الحماية والدفاع، وتطوير القدرات الهجومية الإلكترونية...

فقد شهد المجال السيبراني في المنطقة العربية دورا كبيرا في إحداث عدد من المتغيرات ذات الطبيعة السياسية والأمنية خاصة بعد عام 2011، وهو ما كان له تأثيرات كبرى على المجتمع وعلى علاقته بالدولة بل بالتأثير المباشر على الدول العربية ككل، بإفصالها وانهايار مؤسساتها خاصة الدول التي تشهد تراجع في الحداثة والتنمية مثل حالة اليمن وليبيا، بينما أخذت للعب دورا سياسيا في دول أخرى مثل حالة مصر وتونس، وقد جمعت استخدامات المجال السيبراني بين الدور السياسي والعسكري في الحالة السورية.

وتعرضت المنطقة العربية عبر المجال السيبراني إلى حروب نفسية استهدفت التأثير على الكتلة الحرجة من الشباب عبر الشبكات الاجتماعية سواء من قبل فرقاء على أساس

الاختلاف السياسي أو الديني أو المذهبي، وفي المقابل مارست قوى خارجية التدخل سيبرانيا للتأثير على الأمن والاستقرار بواسطة تغذية النزاعات الطائفية مثل الدور الذي تلعبه إيران في تغذية حسابات على شبكات التواصل الاجتماعي لدعم الشيعة في دول الخليج وتحريضهم سياسيا، أو عبر توظيف المجال السيبراني لتعزيز الرقابة والتجسس على دول المنطقة من قبل قوى إقليمية مثل إسرائيل وإيران وتركيا أو عبر التجسس من قوى دولية أخرى (الصادق، الهجمات السيبرانية: أنماط وتحديات جديدة للأمن العالمي، 2019).

كما شهدت المنطقة العربية ما يعرف بنمو ظاهرة الجيوش الإلكترونية والتي لا تعني أن لها أية أبعاد عسكرية بل أنها عبارة عن كتائب تحاول التأثير المتبادل في الآخر عبر توظيف الفضاء السيبراني في الصراع بين الفاعلين، ومن أهم التهديدات والهجمات السيبرانية (الرزو، 2019) التي لحقت ببعض الدول العربية، نذكر مثلا:

- في سنة 2012 قام فريق من القرصنة السيبرانيين الإيرانيين أطلق على نفسه اسم سيف العدالة القاطع Cutting Sword of Justice بإقحام فيروس خبيث أطلق عليه اسم شمعون 01 Shamoon في شبكة المعلومات الداخلية لشركة أرامكو السعودية النفطية، فقام بإلغاء بيانات مهمة في أكثر من 30,000 حاسب من حواسيب الشركة.

- في عام 2014 نفذت أخطر الهجمات الإلكترونية في منطقة الشرق الأوسط والخليج والتي سميت بعملية كليفر Opération Cleaver على قطاع النفط والغاز بالإضافة إلى المطارات ومواقع حكومية حساسة وشركات الاتصالات، وتعد من أشد الهجمات السيبرانية تأثيرا على المنطقة.

- 2017 هاجم فيروس الصخرة الدوارة Stone Drill السعودية حيث استهدف قطاع الطيران والبتروكيماويات، وقد أحدث هذا البرنامج الخبيث تأثيرات كبيرة على شركات الطيران وشركات البتروكيماويات في السعودية.

في 2019 تم تنفيذ تهديدات سيبرانية متقدمة مستمرة APT وهي هجمات سيبرانية بالغة التأثير، مارسها قراصنة إيرانيون سيبرانيون لاستهداف شبكات المعلومات وبنيتها التحتية في كل من قطر والكويت والسعودية والامارات والبحرين، وخلال مدة زمنية متطاوله، لضمان بلوغ أهدافها وتعميق مستويات تأثيرها.

2.3 تحديات الدول العربية لمكافحة الجرائم السيبرانية

1.2.3 التعاون العربي لمكافحة جرائم المعلوماتية لتعزيز الأمن السيبراني

حسب تقرير صادر عن بوز ألن هاملتون فإن استمرار تطوير التكنولوجيا ونشرها في جميع أنحاء منطقة الشرق الأوسط وشمال أفريقيا، يواكبه تنامي التهديدات السيبرانية كعمليات الغش لسحب البيانات وتعريضها للاختراق، ما يمثل تحديا للشركات والمنظمات، بحيث ستحتاج إلى تحويل مقاربتها للأمن السيبراني من مجرد التركيز على الامتثال الأمني إلى تطوير ثقافة شاملة للأمن الاستباقي عبر النطاق الأوسع للمؤسسات (صحيفة الرؤية، 2019)، كما يبرز ذات التقرير توقعات حول التهديدات السيبرانية لعام 2019 في منطقة الشرق الأوسط وشمال إفريقيا أهم توجهات التهديدات التي ينبغي أن تكون المنظمات في المنطقة على علم بها لكي تتمكن من منع حوادث الأمن السيبراني، وتجنب الضرر بالسمعة والخسائر المالية الناجمة عن الانتهاكات والحفاظ على الوعي الأمني (صحيفة الرؤية، 2019).

وقد قدرت خسائر منطقة الشرق الأوسط نتيجة الجرائم الإلكترونية بأكثر من مليار دولار، وتعد منطقة الخليج العربي الأكثر تعرضا للهجمات في الشرق الأوسط، حيث احتلت السعودية في نهاية عام 2017 المرتبة الثالثة عالميا في التعرض للهجمات الإلكترونية في جميع مرافقها الحكومية والخاصة من جهات خارجية، حيث وصل عدد الهجمات إلى 54 ألف هجمة سنويا، وتواجه قطاعات الخدمات المالية، والرعاية الصحية، والنفط والغاز معظم التهديدات الإلكترونية، ومن المتوقع أن يبلغ حجم الإنفاق العربي على أمن المعلومات

نحو 9.2 مليار دولار عام 2018 نتيجة ازدياد مستوى التهديدات الإلكترونية بنسبة 25% بحسب مشاركون في فعاليات مؤتمر التكنولوجيا والابتكار والمجتمع "سايفاي أفريقيا 2018"، في حين يعتبر القطاع المصرفي من أبرز القطاعات المستهدفة، وبالتالي تبرز أهمية تبني استراتيجية لاحتواء مخاطر التهديدات الإلكترونية (اتحاد المصارف العربية، 2018).

وتوقعت مؤسسة جارنتر أن يصل إنفاق منطقة الشرق الأوسط وشمال إفريقيا على تكنولوجيا المعلومات ككل إلى 155 مليار دولار خلال العام 2018، بزيادة قدرها 3.4% عن العام 2017. وفي العام 2018 فإن القطاع الرئيسي الذي سيعزز من نمو الإنفاق على تكنولوجيا المعلومات في المنطقة هو قطاع البنوك والأوراق المالية الذي سينمو إنفاقه بنسبة 3.6%.

ونظرا إلى ارتفاع مؤشر هذه الجرائم وتضاعف أعدادها وتطور أساليبها وأنواعها وما رافقها من استحداث أشكال جديدة لم تكن معروفة قبلا بسبب التطور المضطرب والمتسارع في تكنولوجيا المعلومات، فقد حرصت الأمانة العامة لمجلس وزراء الداخلية العرب على مكافحة هذه الجرائم بوضع استراتيجية عربية تتبثق من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي اعتمدها مجلس وزراء الداخلية العرب في القاهرة في دورته الـ 31 بتاريخ 21/12/2010 (اتحاد المصارف العربية، 2010)، وقد تضمنت هذه الاستراتيجية:

-تشريعات وطنية خاصة بمكافحة جرائم تقنية المعلومات.

-الحرص على إيجاد آلية وطنية للتعاون والتنسيق بين الجهات المعنية بمكافحة هذه الجرائم، بدءا من مرحلة تقييم المخاطر، رصد ومتابعة تلك الجرائم وتبادل المعلومات في شأنها، مروراً بعمليات التحري والملاحقة والتحقيق وتبادل المعلومات إلى تقديم مرتكبيها للمحاكمة.

-التعاون والتنسيق مع جميع وسائل الاعلام المرئية والمسموعة والمقروءة لتوعية المواطنين بأخطار جرائم تقنية المعلومات وأضرارها الاقتصادية والاجتماعية على الفرد والمجتمع.

وحسب لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا (الإسكوا) فإن الأفعال المصنفة جرائم سيبرانية تتمثل في: التعدي على البيانات المعلوماتية والأنظمة المعلوماتية، إساءة استعمال الأجهزة أو البرامج المعلوماتية، الجرائم على الأموال، الاستغلال الجنسي للقاصرين، جرائم البطاقات المصرفية والنقود الالكترونية... (اتحاد المصارف العربية، 2010).

ومع تزايد تعرض المنطقة العربية إلى الهجمات والقرصنة الإلكترونية خاصة في الخليج العربي، الأمر الذي دفع بها إلى زيادة الانفاق والاستثمار في الأمن السيبراني، وتشكيل هيئات وطنية للأمن السيبراني بالسعودية في شهر نوفمبر 2017، ناهيك عن وجود المركز الاقليمي للأمن السيبراني في سلطنة عمان بدعم من الاتحاد الدولي للاتصالات (الصادق، الهجمات السيبرانية-أنماط وتحديات جديدة للأمن العالمي، 2018).

حيث انعقد المؤتمر الإقليمي الثامن للأمن السيبراني يومي 27 و 28 أكتوبر 2019 بسلطنة عمان، تحت شعار ثورة الأمن السيبراني، مع مشاهدة ملامح تطبيقات الثورة الصناعية الرابعة من خلال مجموعة التقنيات المكونة لها من ذكاء اصطناعي وشبكة الجيل الخامس والصناعات الروبوتية والطباعة ثلاثية الأبعاد والتحول الرقمي للأعمال وتطور التخاطب بين الآلات، مما جعل الدول والأفراد أكثر عرضة للهجمات الإلكترونية.

وتناول المؤتمر التطور التقني للثورة الصناعية الرابعة، وتقييم التدابير اللازمة للتقليل من المخاطر في الأنظمة المترابطة بشكل تكاملي، ومناقشة أفضل الممارسات لتحديد سياسة الأمن السيبراني الوطنية والتنظيمية وعرض المنجزات عربيا، ومن أهم أهدافه الاطلاع على أفضل الممارسات من كبار الخبراء في مجال الأمن السيبراني.

كما تم تنظيم المؤتمر السنوي الحادي عشر لمنظمة التعاون الإسلامي لفرق الاستجابة لطوارئ الحاسبات خلال نفس الفترة، حيث يعد المؤتمر السنوي لمركز الأمن السيبراني لمنظمة التعاون الإسلامي (OIC-CERT) مبادرة مستمرة لتعزيز الأمن السيبراني

وزيادة الوعي من خلال التعاون الدولي بين الأعضاء والهيئات المختلفة لأمن المعلومات والشراكة بين الجهات المتخصصة في الأمن السيبراني لتعزيز الترابط المرن ومشاركة المعلومات وتحسين فاعلية الأعضاء، كما يقدم المؤتمر الفرصة لمناقشة التوجهات الاستراتيجية والتحديات المستقبلية (المركز العربي الإقليمي للأمن السيبراني ARCC، 2019).

وتبنت العديد من الدول العربية تشريعات وطنية لمكافحة الجرائم السيبرانية ومكافحة الإرهاب والتطرف أو محاولة تقنين الإعلام الإلكتروني، والسعي إلى بناء القدرات في مجال التدريب، ووفق تقرير الاتحاد الدولي للاتصالات والذي عمل على قياس ما سماه بالقوة السيبرانية وفق 25 مؤشر قام بتصنيف الدول إلى مراتب، فلقد جاءت أقوى الدول العربية من حيث الترتيب سلطنة عمان حيث احتلت المركز الأول، ويقاس الرقم القياسي العالمي للأمن السيبراني بمدى التزام البلدان في مجال الأمن السيبراني وفق التدابير القانونية والتقنية والتنظيمية وبناء القدرات والتعاون (موقع قناة الحرة، 2019).

ترتيب الدول العربية في الأمن السيبراني، موقع قناة الحرة، 2019/03/29.

الدولة	التقييم في 2017	التقييم في 2018
السعودية	46 عالميا و 05 عربيا	13 عالميا و 01 عربيا
سلطنة عمان	04 عالميا و 01 عربيا	16 عالميا و 02 عربيا
قطر	25 عالميا و 03 عربيا	17 عالميا و 03 عربيا
مصر	14 عالميا و 02 عربيا	23 عالميا و 04 عربيا
الإمارات	47 عالميا و 06 عربيا	33 عالميا و 05 عربيا
الكويت	138 عالميا و 17 عربيا	67 عالميا و 06 عربيا
البحرين	64 عالميا و 08 عربيا	68 عالميا و 07 عربيا

الأردن	92 عالميا و10 عربيا	74 عالميا و08عربيا
تونس	40 عالميا و04 عربيا	76 عالميا و09 عربيا
المغرب	49 عالميا و07 عربيا	93 عالميا و10عربيا
فلسطين	103 عالميا و13 عربيا	101 عالميا و11 عربيا
السودان	95 عالميا و11 عربيا	103 عالميا و12 عربيا
العراق	158 عالميا و19 عربيا	107 عالميا و13 عربيا
الجزائر	67 عالميا و09 عربيا	108 عالميا و14 عربيا
سوريا	101 عالميا و12 عربيا	114 عالميا و15 عربيا
ليبيا	104 عالميا و14 عربيا	117 عالميا و16 عربيا
لبنان	118عالميا و15عربيا	124 عالميا و17 عربيا
موريتانيا	124 عالميا و16عربيا	145 عالميا و18 عربيا

2.2.3 الجماعات الإرهابية وتهديدات الإرهاب الإلكتروني في الوطن العربي

أصبح الإرهاب جريمة عابرة للحدود القومية من حيث النشاط والخطط والتمويل والأعضاء، وتحول الارهاب إلى تهديد عالمي، إلا أنه تصاعد نشاط الجماعات الإرهابية عبر الفضاء الإلكتروني وتعزيز بعدها العالمي وتم استخدام المنجزات التكنولوجية في ممارسة الارهاب، فيستخدم هذا النوع الجديد من القوة لأغراض هجومية كاختراق مواقع إلكترونية أو التجسس الإلكتروني أو نشر الفيروسات، فمثلا في صيف 2011 استطاع جوليان أسانج صاحب موقع ويكيليكس من تسريب عدد كبير من برقيات الخارجية الأمريكية وأن أجهزة الاستخبارات الأمريكية يمكنها الحصول على معلومات عن أي مستخدم لمواقع الإنترنت الكبيرة في أي وقت تريده (عمر، 2012)، والأخطر من ذلك هو استخدام الجماعات الإرهابية الفضاء الإلكتروني للتخطيط وتنفيذ العمليات الإرهابية في مختلف دول العالم، فقد

ظهر التزاوج بين الإرهاب والإنترنت بشكل أكثر وضوحاً بعد أحداث 11 سبتمبر، ولكنه منذ عام 1999 كانت الجماعات الإرهابية حاضرة على الإنترنت بشكل كبير، فبعد عام 2001 كان هناك أكثر من 05 آلاف موقع إلكتروني وغرف محادثة إلكترونية تستخدمها للتأثير على الرأي العام أو للقيام بأعمال إرهابية (العباسي، 2016).

فعلى الساحة العربية سعى تنظيم الدولة الإسلامية (داعش) إلى بسط سيطرته على أكبر قدر ممكن من المناطق الجغرافية ومد نفوذه إلى الدول المجاورة، ولم يدخر جهداً في تسخير إمكانياته وقدراته لاستغلال واحتلال الفضاء الإلكتروني لممارسة نشاطه الإعلامي ونشر إصدارته المتنوعة (الأفلام الوثائقية-وكالات الأنباء...)، حيث يعتبر داعش أن الإعلام الرقمي أداة قتال رئيسية في معركته مع الأعداء (العباسي، 2016).

فاستغل تنظيم الدولة (داعش) الإنترنت في بث عمليات الإعدام التي كان يقوم بتنفيذها في الأسرى لبث الرعب والفرع في نفوس أهالي المدن التي كان يرغب في السيطرة عليها وهو ما تحقق جزئياً في هروب واستسلام مدن وقرى له، كما استخدمه في تجنيد العديد من الشباب حول العالم (السعود، 2019).

وقد عمل داعش على تجنيد جيش إعلامي متخصص في الإعلام الإلكتروني، يعمل تحت تسميات مختلفة، مثل المراكز والمؤسسات والكتائب الإعلامية والمنشآت الجهادية لدعم الأهداف التي يقرها الإعلام المركزي الخاص بالتنظيم كمرکز الفجر للإعلام، ومؤسسة الفرقان الإعلامية... (حكيم، 2018)، بالإضافة إلى ذلك استخدم التنظيم الفضاء الإلكتروني من أجل التعبئة والحشد وتجنيد الإرهابيين الجدد، التنقيب عن المعلومات، إعطاء التعليمات والتلقين الإلكتروني، الحرب النفسية والتخطيط والتمويل.

في الأخير، لقد حول تنظيم الدولة الاسلامية الفضاء الإلكتروني إلى عنوان لهويته الإلكترونية ووسيلة للاختراق الإيدلوجي الذي يستهدفه واختراق المؤسسات السيادية (العباسي)، (2016).

4. خاتمة:

شهد المجال السيبراني في المنطقة العربية دورا كبيرا في إحداث عدد من المتغيرات ذات الطبيعة السياسية والأمنية خاصة بعد عام 2011، وهو ما كان له تأثيرات كبرى على المجتمعات العربية، وقد توصلنا إلى مجموعة من النتائج أهمها:

- يقصد بالتهديدات الإلكترونية استغلال الحاسبات وتكنولوجيا المعلومات في تخريب وتدمير البنية المعلوماتية للخصوم، بل وتعطيل شبكات الدفاع الجوي واختراق أنظمة المعلومات للبريد الإلكتروني لمكاتب رؤساء الدول والتجسس عليهم وفق خطة منهجية.

- أصبح الفضاء الإلكتروني مجال جديد للصراعات بين كل الأطراف سواء من الدول أو من غير الدول، وتبلورت الحروب السيبرانية في خصائص مغايرة للحروب التقليدية.

- من أجل مكافحة جرائم المعلوماتية اعتمدت الدول العربية الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 21 / 12 / 2010.

وفي الأخير نقدم بعض التوصيات منها :

- وضع آلية وطنية للتعاون والتنسيق بين الجهات المعنية بمكافحة الجرائم السيبرانية.

- إيجاد صيغة للتعاون والتنسيق مع جميع وسائل الاعلام المرئية والمسموعة والمقروءة لتوعية المواطنين بأخطار جرائم تقنية المعلومات وأضرارها على المجتمع.

- مشاركة المعلومات والتحديات المرتبطة بالأمن السيبراني وتحسين فاعلية الدول العربية وزيادة تأثيرهم من خلال رفع القدرات الإدارية والتقنية في مواجهة الحوادث المعلوماتية.

5. قائمة المراجع:

المقالات:

- عبد الله حربي سليمان، (2017)، مفهوم الأمن مستوياته وصيغته وأبعاده-دراسة نظرية في المفاهيم والأطر، المجلة العربية للعلوم السياسية، العدد 19؛

- العباسي ريهام عبد الرحمن رشاد، (2016)، أثر الإرهاب الإلكتروني على تغير مفاهيم القوة في العلاقات الدولية 2001-2015-دراسة حالة تنظيم الدولة الإسلامية في العراق والشام (داعش)، المركز الديمقراطي العربي، ألمانيا؛

- غريب حكيم، (2018)، الإرهاب السيبراني والأمن الدولي-التحديات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، المجلد 05، العدد 02؛

المدخلات:

- اتحاد المصارف العربية، أمن المعلومات-المخاطر وتحديات المستقبل، إدارة الدراسات والبحوث، بيروت، لبنان، 2018، متوفر على الموقع uabonline.org

- اتحاد المصارف العربية، تكاتف الجهود العربية لمكافحة الجريمة الإلكترونية وجرائم المعلوماتية وأثرها على العمليات المالية، بيروت، لبنان، 2010، متوفر على الموقع uabonline.org

- المؤتمر الإقليمي الثامن للأمن السيبراني، المركز العربي الإقليمي للأمن السيبراني ARCC، مسقط، سلطنة عمان، خلال الفترة 31/27 أكتوبر 2019، متوفر على الموقع www.arcc.om

مواقع الانترنت

-بالة صباح، التهديدات الأمنية، الموسوعة السياسية، 2020، متوفر على الموقع political.encyclopedia.org

-تعريف التهديدات الأمنية والمصطلحات المشابهة، موقع العلاقات الدولية، 2019/11/24، متوفر على الموقع www.elsiyasa-online.com

-نوران شفيق، أشكال التهديدات الإلكترونية ومصادرها، المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات ECC، ألمانيا، 2020/01/29، متوفر على الموقع www.europarabct.com

-نانسي البنا، الأمن السيبراني...بيئة تكنولوجية أكثر أمناً، 2018/01/20، متوفر على الموقع <http://boutiqueceena325/ezez/rdoc329.er>

- فارس قره، الأمن السيبراني، الموسوعة السياسية، 2015، متوفر على الموقع
political.encyclopedia.org
- أنواع التهديدات السيبرانية ومجالاتها، مجلة رواد الأعمال، جوان 2020، متوفر على الموقع-
rowadalaamal-com.cdn.ampproject.org
- حسين باسم عبد الأمير، تحديات الأمن السيبراني، مركز الدراسات الاستراتيجية CSS ، جامعة كربلاء،
العراق، أيار 2018، متوفر على الموقع kerbalacss.uokerbala.edu.iq/wp/blog
- عمر حامد شكري، المجال الخامس-الفضاء الإلكتروني، المعهد المصري للدراسات، 2019، متوفر على
الموقع eipss -eg-org.cdn.ampproject.org
- رانيا سليمان وآخرون، سياسة مكافحة الإرهاب الإلكتروني...مصر والسعودية نموذجا، المركز العربي
للبحوث والدراسات، 2020/02/02، متوفر على الموقع www.acrseg.org/41483
- الحرب الإلكترونية، موسوعة مقاتل من الصحراء، 2020، متوفر على الموقع www.muqatel.com
- التجسس الإلكتروني، موقع موسوعة ويكيبيديا، 2019/09/24، متوفر على الموقع :
www.ar.m.wikipedia.org
- عادل عبد الصادق، الهجمات السيبرانية-أنماط وتحديات جديدة للأمن العالمي، المركز العربي لأبحاث
الفضاء الإلكتروني ACCR، 11/03/2018، متوفر على الموقع accronline.com
- عادل عبد الصادق، الهجمات السيبرانية-انماط وتحديات جديدة للأمن العالمي، الموسوعة الجزائرية
للدراسات السياسية والاستراتيجية، 2019/11/27، متوفر على الموقع www.politics-dz.com
- حسن مظفر الرزوي، النزاعات والمواجهات السيبرانية في فضاء منطقة الخليج العربي، مركز الجزيرة
للدراسات، 2019/09/15، متوفر على الموقع studies.aljazeera.net/ar/reports
- التهديدات السيبرانية تواكب التطور التكنولوجي، صحيفة الرؤية، 02 أبريل 2019، متوفر على الموقع
www.alroeya-com.cdn.ampproject.org
- ترتيب الدول العربية في الأمن السيبراني، موقع قناة الحرة، 2019/03/29، متوفر على الموقع
www.alhurra.com
- عمر حرز الله، الحرب الإلكترونية...صراع في العالم الافتراضي، صحيفة البيان، 2012/03/04، متوفر
على الموقع www-albayan-ae.cdn.ampproject.org
- أحمد ناصر أبو السعود، الإرهاب الإلكتروني، الموسوعة السياسية، متوفر على الموقع
political.encyclopedia.org