الجهود المصرية لمواجهة التحديات السيبرانية

إعدادالباحثة

جيهان أحمد عبد العال

إشراف

أ.د/ سلوي السعيد فراج **د رشا عطوة عبد الحكيم**

الملخص

تواجه مصر والدول العربية ومعها العديد من الدول فى منطقة الشرق الأوسط وشمال إفريقيا، تحديات حقيقية تتعلق بالمحافظة على السيادة في مجالات التكنولوجيات الحديثة التي أصبحت تفرضها الثورة الرقمية على الدول الوطنية وتدفعها إلى اعتماد منهجيات ومقاربات جديدة من أجل حماية أمنها القومي من الأخطار غير التقليدية التي يمثلها الواقع السيبرانى الذي استطاع أن يغير كل المفاهيم بشأن الزمان والمكان والمحيط الجيوسياسي للدول وأن يجعل الحدود الجغرافية تبدو فى غاية الضعف وقابلة للاختراق من قبل فاعلين افتراضيين يصعب تحديد هوياتهم والتعرف إلى القوى أو الدول التي تدعمهم وتوفر لهم الملاذ الآمن.

الكلمات المفتاحية:

الأمن السيبراني- الفضاء السيبراني- الاختراق الإلكتروني- شبكات التواصل الإجتماعي

Abstract:

Egypt and the Arab countries, along with many countries in the Middle East and North Africa region, are facing real challenges related to maintaining sovereignty in the areas of modern technologies that the digital revolution has imposed on national states and prompting them to adopt new methodologies

and approaches in order to protect their national security from the non-traditional dangers that it poses. The cyber reality that was able to change all concepts about time, place and the geopolitical environment of countries and make the geographical borders appear very weak and penetrable by virtual actors whose identities are difficult to identify and to identify the forces or countries that support them and provide them with a safe haven.

المقدمة:

إن مفهوم السيادة الرقمية، لم يعد قاصر على القوى الكبرى في العالم ولكن دول الشرق الاوسط بدأت تتنبه لأهمية الأمن والسيادة في المجال الرقمي، وخاصة بعد انطلاق ما سمي الربيع **(العربي)**، والتي جعلت دول المنطقة تقتنع بأن هناك من يتدخل في مسار الأحداث من خلال التحكم فى المعلومة ويعمل على نشر الإشاعة للتأثير في النقاشات التي كانت تحدث فى منصات التواصل الاجتماعي، كما اكتشفت هذه الدول أن معظمها دخل الفضاء السيبرانى المفتوح دون أن يمتلك القدرات والكفاءات التي تسمح لها بالتصدي للاختراقات التي تقوم بها القوى الأجنبية لأمنها وسيادتها الرقمية، وخاصة إن منصات التواصل الاجتماعي تطرح صعوبات كبرى تتعلق بإمكانية وأساليب تنظيم عملها ووضع ضوابط لها، حتى لا يتحول لنقاش في منصاتها إلى أداة يمكنها أن تهدد الوحدة الترابية واستقرار النسيج المجتمعي للدول.

وفى هذا الإطار يستعرض هذا البحث دور الفضاء السيبرانى فى عدم استقرار المنطقة العربية بشكل عام ومصر بشكل خاص، ثم التطرق إلى أهم جهود الدولة المصرية واستعراض أهم السيناريوهات المستقبلية للحروب السيبرانية .

مشكلة الدراسة:

في ظل سعى الدولة إلى الاعتماد على الأنظمة الإلكترونية في كافة منشأتها "الحكومة الإلكترونية، يرى البعض ان هذا الاتجاه يجعل من تلك الانظمة هدفا هجوميا مما يؤدى إلى شلل هذه الانظمة وتدميرها وبالتالي يؤثر على تدفق المعلومات وارباك عمل البنية التحتية مما يؤدى إلى سخط المواطنين وبالتالي عدم الاستقرار السياسي.

أهداف الدراسة:

- التعرف على الاليات التي يمكن تفعيلها من قبل النظام السياسي المصري لحماية أمنها القومي.
- استشراف المستقبل من خلال توضيح السيناريوهات المستقبلية الخاصة للحروب السيبرانية

تساؤلات الدراسة:

تسعى الدراسة إلى محاولة الإجابة عن التساؤل الرئيسي وهو:

ما هو تأثير الحروب السيبرانية على الأمن القومي المصري ؟

ويتفرع من التساؤل الرئيس مجموعة من التساؤلات الفرعية

١. كيف يمكن مواجهه هذه الحروب أو الحد من تأثيرها ؟

٢. ما هي السيناريوهات المستقبلية لمدى اعتماد الدول والفاعلين الدوليين على الحروب السيبرانية وقدرة الدول على التصدي لها ؟

اولاً : دور الفضاء السيبرانى فى عدم استقرار المنطقة العربية :

لقد شهد المجال السيبرانى فى المنطقة العربية دوراً كبيراً في إحداث عدد من المتغيرات ذات الطبيعة السياسية والامنية وبخاصة بعد عام ٢٠١١، وهو ما كان له تأثيرات كبري على المجتمع وعلى علاقته بالدولة بل كان له تأثيراً مباشراً على

الدول العربية بإفشالها وانهيار مؤسساتها وخاصة فى تلك الدول التي شهدت تراجع فى الحداثة والتنمية مثل اليمن وليبيا، على الجانب الآخر اتجهت للعب دوراً سياسياً فى دول أخرى مثل مصر وتونس، والتي تتميز بتطور مرتكزات الدولة والطبيعة المدنية لشعوبها، كما تعرضت المنطقة عبر المجال السيبرانى الى حروب نفسية استهدفت التأثير على الكتلة الحرجة من الشباب عبر الشبكات الاجتماعية سواء من قبل فرقاء على اساس الاختلاف السياسي أو الديني والمذهبي، إلى جانب استخدام القوى الخارجية التدخل السيبرانى للتأثير على الأمن والاستقرار سواء عبر تغذية النزاعات الطائفية مثل الدور الذي تلعبه ايران في تغذية حسابات على شبكات التواصل الاجتماعي لدعم الشيعة في دول الخليج وتحريضهم سياسيا، أو عبر توظيف المجال السيبرانى لتعزيز الرقابة والتجسس على دول المنطقة من قبل قوى اقليمية مثل إسرائيل وإيران وتركيا أو عبر التجسس من قوى دولية اخرى [١].

كما أثر المجال السيبرانى كذلك على العلاقات البينية بين الدول العربية حيث شهدت العلاقة بين قطر وجيرانها توتراً أثر تصريحات نسبت الى أمير قطر، وادعاء قطر بإن موقع وكالة الابناء القطرية تم اختراقه في مايو ٢٠١٧، وهو ما كان من شأنه اتهام قطر من قبل الأمارات بالوقوف خلف القرصنة بينما نفت الاخيرة تلك الاتهامات ،واتجهت قطر لتعزيز أمنها الإلكتروني بالتعاون مع امريكا وتركيا، وكان لتلك الأزمة انعكاس في تطور الازمة بين قطر ودول الرباعي العربي وهى مصر والسعودية والامارات والبحرين بفرض مقاطعه ، وكان من ضمن آلياتها حجب المواقع الالكترونية الممولة والموجهة من قبل قطر والداعمة للإرهاب.

بالإضافة إلى ذلك شهدت المنطقة ما يعرف بنمو ظاهرة الجيوش الالكترونية والتي لا تعنى ان لها اية ابعاد عسكرية بل أنها عبارة عن كتائب تحاول التأثير في الجانب الأخر عبر توظيف الفضاء السيبرانى فى الصراع بين الفاعلين، الى جانب تزايد تعرض المنطقة الى الهجمات والقرصنة الالكترونية وبخاصة فى الخليج العربي، وهو الامر الذي دفع تلك الدول الى زيادة الانفاق والاستثمار في الأمن

السيبرانى، وبتشكيل هيئات وطنية للأمن السيبرانى مثل ما قامت به السعودية فى ٢٠١٧، ناهيك عن وجود المركز الإقليمي للأمن السيبرانى فى سلطنة عمان بدعم من الاتحاد الدولي للاتصالات[٢].

وفى هذا السياق سيتم التعرض لأهم اليات الفضاء السيبرانى

ثانياً: أليات الفضاء السيبرانى فى تعبئة الحشود فى المجتمع الافتراضي "بالتطبيق على مصر":

لقد تعددت أليات الحشود فى المجتمع الافتراضي، حيث يستخدم فالفضاء السيبرانى كسلاح دون مواجهة مباشرة، حيث يتسلل العدو فى هدوء ويحدث أثره الذى عادة ما يعطل خدمة حيوية أو يستهدف منشأة هامة، وأحيانا يسرب معلومات تؤدى لحالة واسعة من البلبلة وعدم الاستقرار، ولا يقتصر استعمال الهجمات السيبرانية على البلدان وأجهزتها الدفاعية التابعة عادة لقواتها المسلحة، بل هي سلاح يستطيع أي تقنى ماهر ممن يطلق عليهم لقب **(هاكر)** استخدامه ويحقق ما يرجوه من أهداف، كما تعتبر مسألة تسريب المعلومات من أخطر أنواع الهجمات السيبرانية، ولعل من أشهرها تبعات تسريبات **(جوليان أسانج)**عن طريق موقعه **(ويكيليكس)**، وتسريبات**(إدوارد سنودن)** الموظف السابق فى وكالة الأمن القومي الأمريكية وهما من أشهر الأمثلة لما يستطيع الفرد القيام به فى عالم الهجمات السيبرانية.

أ. <u>تسريبات ويكيليكس:</u>

ان استخدام التكنولوجية في وسائل الاتصال قد يكون لها دوافع سياسية ممثلة فى التهديد باختراق الدولة والوصول الى عقول أبناء شعوبها في محاولة لتغيير ادراكهم للأمور، أو تغيير النظم السياسية أو الإطاحة بالحكومات المختلفة وذلك من خلال غرس أفكار معينة فى أذهان الناس ومن ثم امكانية التأثير على سلوكهم، وهذا الدور قامت به تسريبات **(ويكيليكس)**، والتي تعد أكبر إصدار على الإطلاق لمواد سرية، حصل موقع **(ويكيليكس)** على ٩٠ ألف ثم ٤٠٠ ألف وثيقة ومستند ووزعتها خمس صحف في جميع أنحاء العالم [٣]، وهى الجارديان ونيويورك تايمز وإل باييس ولوموند ودير شبيجل وكان الشخص المسؤول عن إطلاق هذه البرقيات هو**(برادلي مانينغ)** ،

جندي في الجيش الأمريكي، اعترف **(مانينيغ)** بذلك في محادثات مع متسلل سابق **(أدريام لامو)** وفي ٢٦ مايو، ألقى القبض على **(مانينغ)**، بينما كان هناك تركيز متزايد على تأثير **(ويكيليكس)** على الانتفاضة التونسية، حيث أنها لعبت دورا بارزا فى توضيح الفساد والإسراف فى نظام بن على.

ب. شبكات التواصل الاجتماعي :

حيث كان لمواقع **(تويتر وفيسبوك)** تأثيرهما الكبير فى السياسة الداخلية المصرية، وذلك من خلال دوره فى إضراب ٦ أبريل، والتأثير الكبير الذى أحدثته تأسيس صفحة كلنا خالد سعيد، ومن الملاحظ أن هناك الألاف من الصفحات التي تشكلت أثناء تلك الفترة والتي أخذت تعلى من سقف طموحات المتظاهرين ، فى الواقع ، كانت السهولة التي تمكن بها المتظاهرون من تنظيم الأمور مدعومة بسرعة تويتر والسيولة التي عززتها وظيفة الهاش تاج، ومن ثم أتضح مدى قدرة وسائل التواصل الاجتماعي على نشر الاحتجاجات من العام الافتراضي إلى الواقع، ولكن نتيجة للوعى بالأخطار التي يمكن أن يتسبب فيها وسائل التواصل الاجتماعي، علق الموظف السابق فى الاستخبارات الأمريكية **(إدوارد سنودن)**، على انقطاع عمل الفيسبوك، بأن العالم أصبح أكثر صحة بعد العطل فى عمل **(فيسبوك)** وغيرها من منصات التواصل الاجتماعي .

ج. الجزيرة:Al-Jazeera

من العوامل المهمة التي أثرت فى زعزعة الاستقرار فى مصر كانت قناة الجزيرة، حيث كشفت مذكرات دبلوماسية أمريكية سربها موقع **(ويكيليكس)** ونشرتها صحيفة ذي جارديان البريطانية ان قطر تستخدم **(قناة الجزيرة الفضائية)** كأداة مساومة، حيث كان عدد الأشخاص الذين لديهم وصول إلى **(Facebook)** بلغ حوالي ثلاثة ملايين في مصر .

الجدير بالذكر أن قناة الجزيرة تعمل كفرع للسياسة الخارجية القطرية، وبالتالي فإن أجندتها التحريرية تتوافق مع جدول أعمال الدوحة، الذى يعد داعما

قويا لجماعة الإخوان المسلمين **(الإرهابية)**، وعلى الرغم من حظرها ومن ثم غيابها إلى حد كبير عن الشاشات المصرية، إلا أنها حافظت على تركيزها على مصر، مما أدى إلى انتقادات قوية لأجندة الجزيرة، وقد صرح **(عارف حجاوي)**، مدير البرامج في قناة(**الجزيرة العربية)**، أن **(الجزيرة)** بثت عشرات الساعات من التوثيق عن مصر، أكثر مما أنتج في جميع البلدان العربية الأخرى مجتمعة، بهدف توجيه انتقادات لمصر بشكل مستمر.

د. رد فعل مصر :

في مواجهة التهديد المتزايد الذى يشكله انتشار المعلومات - سواء أخبار الأحداث الجارية أو المواد الموجودة في ويكيليكس - عبر التكنولوجيا ، كان أحد ردود فعل مصر هو حجب موقع التواصل الاجتماعي، كمحاولة تقييد الوصول إلى الإنترنت، حيث تم حظر أكبر مزودي خدمة الإنترنت ، وشهد هذا التقييد قطع(٨٨٪) من الإنترنت المصري وانخفض عدد الشبكات من **(٢٩٠٣)** شبكة مصرية، نشأت من**(٥٢ ISPS)** إلى **(٣٢٧)** شبكة بين عشية وضحاها، كما تم سحب ما يقرب من**(٣٥٠٠)** مسار **(BGP)** فردى ، مما لم يترك أي مسارات صالحة يمكن لبقية العالم من خلالها الاستمرار في تبادل حركة الإنترنت مع مزودي الخدمة فى مصر، اقترن هذا التقييد على الوصول إلى الإنترنت مع الوصول المقيد إلى شبكات الهاتف المحمول، حيث أصدرت شركة فودافون - أحدى شركات الاتصال المصرية - تعليمات لجميع مشغلي شبكات الهاتف المحمول فى مصر بتعليق الخدمات في مناطق محددة، بموجب التشريع المصري الذى يحق للسلطات إصدار مثل هذا الأمر، وكان الهدف من قطع الاتصال هو منع الجماعة الارهابية من الاتصال بعناصرهم التي تحضر بالأسلحة وللتمكن من إفشال المؤامرة التي تتعرض لها البلاد[٤].

- **التأثير على الجهات الخارجية:**

وما كان مفقوداً من مناقشة **(ويكيليكس)** هو النظر في تأثير إصدار هذه البرقيات على الجهات الفاعلة الخارجية، سواء الحكومية أو غير الحكومية وعلى

الرغم من ذلك، فى ٢٥ يناير ٢٠١١، صرحت وزيرة الخارجية الامريكية فى ذلك الوقت **(هيلاري كلينتون)** تقييمنا هو أن الحكومة المصرية مستقرة وتبحث عن طرق للاستجابة للمطالب المشروعة للشعب المصري[٥]، ويمكن أرجاع ذلك الموقف لأهمية مصر كحليف لها فى المنطقة، علاوة على ذلك، لان لها معاهدة سلام رسمية مع إسرائيل، ولقد خلص **(أوباما)** إلى أن استمرار الدعم لمصر أمر هام.

ومما سبق يتضح أن موقع **(ويكيليكس)** كان له تأثير لا يمكن إنكاره على تونس ووصف بأنه يلعب دورا أساسيا في الثورة التونسية، كما كان له تأثير كبير على مصر، وذلك على الرغم من ان المعلومات الواردة فى البرقيات الدبلوماسية الخاصة بمصر لم تكن جديدة ولا مفاجئة، لكن نشر هذه المعلومات زاد من شرعية الحركة الاحتجاجية داخليا وخارجيا، حيث وثق موقع **(ويكيليكس)** ونشر معلومات عن مصر كانت معروفة بالفعل خارج مصر بشكل عام، ولكن غالباً بشكل خافت .

على هذا النحو ، فإن أهمية هذه التسريبات ترجع إلى:

أولا: كان المتظاهرون داخل مصر متأثرين بالأحداث التي وقعت فى تونس، والتي كانت من ضمن أسبابها المعلومات الموجودة في برقيات ويكيليكس.

ثانيا : هذه البرقيات قدمت دليلا تاريخيا على القيود التي فرضها نظام مبارك على الفضاء السياسي داخل مصر ، فضلاً عن الاسلوب الأمني الشديد المستخدم للحفاظ على السلطة.

ثالثا: أعطت الأدلة الواردة في البرقيات شرعية متزايدة للحركات الاحتجاجية ، داخليا وخارجيا.

رابعا: وفرت البرقيات على الصعيد الدولي وعيا محايدا متزايدا بطبيعة حكم مبارك ، مما يعنى أن الحكومات التي قبلت ضمنيا سلوك النظام لم تكن قادرة فى النهاية على الاستمرار فى ذلك بسبب التكاليف السياسية.

خامسا: ساعدت الجهات الفاعلة غير الحكومية مثل(**Anonymous** و **Telecomix**)المتظاهرين من خلال توفير الوصول إلى الإنترنت عندما تم تقييد ذلك، ومع ذلك، فإن الإشارة إلى أن (**ويكيليكس أو فيسبوك أو تويتر أو A1 Jazeera**) كانت ذات أهمية قصوى للمتظاهرين فى مصر من شأنه أن يقلل من قوة ودور وكالة القوى الاجتماعية والحركات الاجتماعية على هذا النحو، بينما لا يمكن إنكار أن هذه العوامل كانت مهمة في مراحل مختلفة مما يطلق عليه الثورة[٦].

- **الفضاء السيبرانى وثورة ٣٠ يونيو ٢٠١٣**

١. وسائل التواصل: أداة من أدوات الحرب النفسية

منذ ثورة ٣٠ يونيو عام ٢٠١٣، تعرضت مصر بشدة للجيل الرابع من الحروب التي أهم ما يميزها أنها تبدأ بالشائعات، فكان لشبكات التواصل الاجتماعي دوراً بارزاً في هذه الحرب، حيث تم استخدام شبكات التواصل الاجتماعي لزعزعة الاستقرار في البلاد، من خلال استخدامها كمنصة لنشر الأكاذيب والشائعات لبعض الجماعات الإرهابية التي تسئ استغلالها، وأصبحت بمثابة منصات للترويج لأفكارها المتطرفة وأكاذيبها التي تهدف إلى النيل من عزيمة المصريين وبث اليأس والإحباط في نفوسهم، كما اعتادت مصر من وقت لأخر ، على استخدام الدول المعارضة لها والجماعة الارهابية شبكات التواصل الاجتماعي فى إثارة الفتن وذلك من خلال نشر العديد من الاخبار المفبركة منها على سبيل المثال:

نشر مظاهرات وهمية على شبكات التواصل الاجتماعي بهدف إثارة الفتن وزعزعة الاستقرار، فمنها على سبيل المثال، بثت(**وكالة الاناضول التركية**) فيديوهات وصورا تم التأكد من أنها مفبركة، حيث كان ناشروها على شبكات التواصل الاجتماعي، زعموا أنها من مظاهرات في عدة ميادين مصرية ضد الرئيس (**السيسي**) ، لكن الأمر سرعان ما انكشفت حقيقته، حيث إن التجمعات كانت لجماهير مصرية تحتفل بصعود فريق بلادها لكأس العالم عام٢٠١٧[٧] .

وفي واقعة أخرى حاولت الجماعة الارهابية **(الاخوان)** الترويج لشائعة مقتل شاب من محافظة الإسكندرية، يدعى **(أحمد أبو ليلة)** ، فى المظاهرات بمنطقة **(سيدي بشر)**، وروجت صفحاتهم بشكل كثيف هذه الأكذوبة، بهدف إثارة الفوضى فى الشارع المصري، إلا أن الشاب خرج بنفسه عبر حسابه على موقع التواصل الاجتماعي **(فيسبوك)**، ليؤكد أنه حي يرزق، نافياً ما تردد من شائعات حول خبر وفاته، مهاجما أكاذيب جماعة الإخوان الارهابية[٨].

كما تداولت اللجان الإلكترونية الإخوانية صورة لشاب آخر على أنه أيضا **(أحمد أبو ليلة)**، وأنه قتل فى مظاهرة فى الإسكندرية، وبعد البحث والتدقيق وراء الصورة وكشف حقيقة ما تروجه ا(لإخوان ولجانها)، تبين أن الشاب الذي يروج صورته **(تنظيم الإخوان)** قتل في ٢٠١٣، ويدعى **(خالد محمد صالح)**، وهو من منطقة شبرا، وتوفي في أحداث منطقة رمسيس في أكتوبر ٢٠١٣ [٩].

ووفقًا لتقرير شركة **(كاسبر سكاي لابس)** أن مصر واحدة من أكثر الدول الأفريقية ا عرضة لخطر الإرهاب الإلكتروني، حيث تعرضت العديد من الدول لسلسلة من الهجمات الإلكترونية بتاريخ ١٢ مايو ٢٠١٧، وقد وقع أكثر ٤٥(**ألف هجمة إلكترونية لأكثر من ٩٩ دولة)**، وذلك وفقا لخبراء في الأمن المعلوماتي، أن مصر من ضمن الدول التي تعرضت لذلك الهجوم من خلال "الفيروس العالمي الذي يطلق عليه **(انتزاع الفدية)**[١٠].

ويتضح ما سبق أن حروب الجيل الرابع تعد إحدى أبرز الأدوات التحريضية التي تستخدمها التنظيمات الإرهابية لمحاولة تدمير الدول، وتعتمد بشكل رئيسي على مواقع التواصل الاجتماعي في نشر الأكاذيب والشائعات ضد الدول، فهي تعد أخطر أنواع الحروب فتعطيل أو اختراق بيانات وزارات الدفاع على سبيل المثال قد يغير شيئا من الحرب، لكن نشر المعلومات الكاذبة قد يكون تأثيره أعظم، كما تعتبر تسريب وثائق ويكيليكس وغيرها اختراقاً كارثيا لأنه يؤثر على علاقة الدول بعضها البعض ويؤثر على مدى السلام الاجتماعي داخل الدولة الواحدة.

ثالثاً :الجهود المصرية فى مكافحة الحروب السيبرانية :

تتضمن الرؤية المصرية دفع عجلة التنمية والتوسع فى تطوير البنية التحتية طبقا للمعايير الدولية من خلال دمج أنظمة وتقنيات تكنولوجية فى إدارة وربط مكونات البنية التحتية، والذي يترتب عليه زيادة حجم التهديدات الإلكترونية التي قد تتعرض لها تلك المكونات من خلال استهدافها بهجمة أو عدة هجمات سيبرانية قد تؤدى إلى تعطيل وشلل تلك الخدمات .

لذا وضعت الدولة المصرية سياسات الهدف منها مكافحة الحروب السيبرانية ، والتى قسمتها إلى مجموعتين كالاتى :

أ. **الجهود القانونية :**

لقد كان حرص المشرع المصري كبيرا في مواكبة النهضة التكنولوجية وما يصاحبها من اخطار ، لذا أصدر العديد من التشريعات اللازمة لمواجهة هذه الأخطار أهمها :

- المادة ٣١ من الدستور المصري الصادر عام ٢٠١٤ والذي ينص على ان "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي ، وتلتزم الدولة باتخاذ التدابير الازمة للحفاظ عليه ،على النحو الذي ينظمه القانون"[١١].
- الموافقة على انضمام مصر للاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام ٢٠١٤ ، بهدف تعزيز التعاون بين الدول العربية لمكافحة الجرائم والحروب السيبرانية ، وذلك اقتناعا من الدول العربية بضرورة تبنى سياسة جنائيه مشتركة تهدف إلى حماية المجتمع العربي ضد الجرائم الإلكترونية[١٢].
- سنت الحكومة المصرية في عام ٢٠١٨ قانونين رئيسيين يتعلقان بجرائم الكمبيوتر، يستهدف التشريع خدمة التواصل الاجتماعي مثل(**Facebook وTwitter**)، حيث يجرم التشريع الأخبار الكاذبة والإرهاب، ويضع علما على الحسابات التي تضم أكثر من ٥٠٠٠ مشترك أو متابع[١٣].

- قانون مكافحة جرائم تقنية المعلومات، يعد صدور قانون مكافحة تقنية المعلومات بمثابة خطوة مهمة في ضوء القانون المصري، حيث تضمن القانون المصري لأول مرة تجريم الممارسات الإلكترونية غير المشروعة لما لها من تداعيات خطيرة وتهديد على الأمن القومي للدولة، فعلى سبيل المثال إنشاء المواقع الإلكترونية التي تحث على الإرهاب، والتزوير الإلكتروني، ووفقا لهذا القانون تتحدد العقوبة وفقا لحجم وطبيعة الجريمة، ففي حالة جرائم تقنية المعلومات تعد العقوبة كبيرة، لما لها من تداعيات جسيمة على الأمن القومي للدولة علاوة على العقوبات الأخرى المتعلقة بجرائم الاختراق الإلكتروني والتزوير وغيرها[١٤].

ب. -الجهود التنفيذية :

من منطلق تعزيز الثقة في البنى التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها في شتي القطاعات الحيوية وتأمينها من أجل تحقيق بيئة رقمية أمنة وموثوقة للمجتمع المصري، تم انشاء الاتي :

- **المركز المصري للاستجابة لطوارئ الحاسب الآلي سيرت.**

من منطلق تعزيز الثقة في البنى التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها في شتي القطاعات الحيوية وتأمينها من أجل تحقيق بيئة رقمية أمنة وموثوقة للمجتمع المصري، قامت وزارة الاتصالات والمعلومات بإنشاء المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات **(CERT-EG)** فى ابريل عام ٢٠٠٩، من أجل مواجهة خطر الإرهاب الإلكتروني، ويختص المركز بتقديم الدعم للقطاع الحكومي والمالي، من خلال الدعم التقني والميداني وتقديم التقارير الفنية للجهات المختصة، حيث يعمل به فريق من ستة عشر متخصصا ، ويقدم المركز الدعم اللازم لحماية البنية التحتية القومية للمعلومات الهامة خاصة في قطاع تكنولوجيا المعلومات والاتصالات والقطاع المالي.

كما يقدم المركز منذ عام ٢٠١٢ الدعم لمختلف الجهات عبر قطاعات تكنولوجيا المعلومات والاتصالات، والخدمات المصرفية والحكومية من أجل مساعدتهم على مواجهة تهديدات الأمن السيبرانى بما في ذلك هجمات الحرمان من الخدمة[١٥] ويتكون المركز من أربع إدارات رئيسية، وهي مراقبة المخاطر والتعامل مع الحوادث السيبرانية، وتحليل الأدلة السيبرانية، وتحليل البرمجيات الخبيثة، وفحص الثغرات واختبارات الاختراق.

وتتمحور مهمة المركز المصري للاستجابة لطوارئ الإنترنت والحاسب حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الإلكترونية التي تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية،[١٦]، كما تتركز المهمة الرئيسية للمركز المصري للاستجابة للطوارئ المعلوماتية **(سيرت)** حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الالكترونية التي تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية، ومن أهداف المركز أيضاً وضع إطار تشريعي ملائم للأمن السيبرانى، بمشاركة القطاع الخاص والمجتمع المدني واسترشادا بالخبرة الدولية والمبادرات ذات الصلة، ووضع إطار تنظيمي مناسب لإنشاء نظام وطني للأمن السيبرانى ومراكز استجابة للطوارئ، وتأسيس البنية التحتية اللازمة لضمان الثقة في المعاملات الالكترونية وحماية الهوية الرقمية، مثل البنية التحتية للمفاتيح العامة ومكاتب الائتمان بمشاركة القطاع الخاص، وجمع المعلومات حول الحوادث الأمنية وتحليلها، والتنسيق والوساطة بين كافة الأطراف لحل مثل تلك الحوادث ، بالإضافة إلى التعاون الدولي مع مختلف الفرق الأخرى.

- **وضع الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٤-٢٠٢١)**

في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري، ومع تزايد التهديدات والتحديات المستقبلية فى المجال السيبرانى والمجتمع الرقمي ولرصد ومجابهة المخاطر والتهديدات المتزايدة، والتزاماً بالمادة ٣١ من الدستور المصري الصادر عام ٢٠١٤ الذى سبق ذكره، تم الدعوة الي انشاء **(المجلس**

الأعلى لتأمين البني التحتية للاتصالات والمعلومات "المجلس الأعلى للأمن السيبرانى) التابع لرئاسة مجلس الوزراء، برئاسة وزير الاتصالات وتكنولوجيا المعلومات، الذى تم اعدد الوثيقة الاستراتيجية الوطنية للأمن السيبرانى، وهى الاستراتيجية التي توضح توزيع الأدوار بين الجهات الحكومية والقطاع الخاص ومؤسسات الاعمال والمجتمع المدني وما ستقوم به الدولة من إجراءات للتقدم نحو تحقيق تلك الأهداف لمواجهه الاخطار السيبرانية.

١. <u>تشكيل المجلس الأعلى للأمن السيبرانى فى مصر عام ٢٠١٤</u>

i. تم تشكيل المجلس الأعلى للأمن السيبرانى في مصر، بقرار من رئيس الوزراء السابق المهندس إبراهيم محلب، في ديسمبر ٢٠١٤، و يهدف إلى حماية المعلومات والبيانات لدى الجهات مع الاهتمام بإدارات المعلومات والاتصالات في الوزارات والجهات المختلفة، والتأكد من توافر التمويل اللازم لضمان تنفيذ منظومة الأمن السيبرانى، مع ضرورة وضوح الإطار التشريعي الخاص به، ويضم تشكيله وزير الإنصات وتكنولوجيا المعلومات رئيسا للمجلس، وعضوية ممثلين عن وزارات: الدفاع، والخارجية، والداخلية، والبترول والثروة المعدنية، والكهرباء، والصحة، والموارد المائية والري، والتموين، والاتصالات، وجهاز المخابرات العامة، والبنك المركزي، و٣ أعضاء من ذوي الخبرة، وفى يناير ٢٠١٥ أصدر المهندس إبراهيم محلب، قرارا بضم ممثل عن وزارة المالية، وممثل عن وزارة التخطيط والمتابعة والإصلاح الإداري، لعضوية المجلس ، كما أصدر المهندس شريف إسماعيل رئيس الوزراء السابق فى ١٩ يناير ٢٠١٦، قراراً بتعيين ممثل عن رئاسة الجمهورية عضواً بالمجلس يتولى وضع استراتيجية لمواجهة الأخطار السيبرانية والإشراف على تنفيذها[١٧]، وتتضمن الاستراتيجية عددا من البرامج التي تدعم الأهداف الاستراتيجية للأمم المتحدة منها:

برنامج تطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبرانى وتأمين البنى التحتية للاتصالات وتكنولوجيا المعلومات:

وذلك بإعداد وتفعيل ما يعرف بفرق مواجهة حوادث أمن الحواسيب في القطاعات الحيوية على المستوى الوطني، كون هذه الفرق مسئولة عن أعمال المتابعة الامنية لشبكات الاتصالات والمعلومات الوطنية والحواسب المتصلة بها وعن التعامل مع أية أخطار سيبرانية تهددها أو هجمات سيبرانية توجه اليها، وعن التوعية والاعداد لمواجهتها[١٨].

- **برنامج لحماية الهوية الرقمية ، وتفعيل البنى التحتية اللازمة لدعم الثقة فى التعاملات الالكترونية بوجه عام وفي الخدمات الحكومية الالكترونية بوجه خاص.**

مثل بنية المفتاح المعلن **(Public Key Infrastructure) (PKI)**، التي يعتمد عليها التوقيع الإلكتروني وتنظمها وتشرف عليها هيئة تنمية صناعة تكنولوجيا المعلومات، مهمتها إعداد رؤية استراتيجية على المستوي القومي للمواطنة الرقمية وخطة عمل لتحويل مفهوم المواطنة الرقمية الي واقع ملموس وإطلاق مشروعات قومية تستهدف تطبيقات موسعة تسهم فى تيسير وتأمين التعاملات الالكترونية، اعتمادا علي البنية التحتية التي تم انشاؤها[١٩].

- **برنامج إعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبرانى في مختلف القطاعات** .

وذلك بالتعاون والشراكة بين الجهات الحكومية والقطاع الخاص والجامعات ومؤسسات المجتمع المدني .

- **برنامج لدعم البحث العلمي والتطوير وتنمية صناعة الأمن السيبرانى**

من خلال دعم برامج ومشروعات التعاون بين الجهات البحثية والشركات الوطنية، وخاصة فى مجال تحليل البرمجيات الخبيثة المتقدمة ومجال تحليل الأدلة الرقمية، وفي مجال حماية وتأمين نظم التحكم الصناعية[٢٠].

- **برنامج للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية**

سواء بالنسبة للأفراد والمؤسسات والجهات الحكومية، وبأهمية الأمن السيبرانى لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها كما أجريت مصر أجتماعاً عالي المستوى يوم ٢٩ مارس ٢٠٢١ ، حيث وجه الرئيس السيسي بإيلاء موضوع الأمن السيبرانى الأولوية أن البنية التحتية للعاصمة الإدارية الجديدة تستند على الاتصالات والبنية الإلكترونية بصورة غير مسبوقة فى العمل الحكومي فى مصر، ومن اللافت للانتباه ان ذلك الاجتماع جاء ذلك بعد أيام من حادثة الهجوم السيبرانى على البرلمان الأسترالي.

وبعد اعلان شركة **(Trend Micro)** المتخصصة فى أمن المعلومات بانه تم معالجه أكثر من**(١٢ مليون)** تهديد إلكتروني فى مصر فى النصف الاول من عام ٢٠٢٠ وأشارت إلى أنه تم اكتشاف أكثر من ٢٣٥ ألف هجوم برمجيات خبيثة في مصر، وتم العثور على أكثر من **(٦.٨ مليون)** تطبيق خبيث للهواتف المحمولة.

كما أسهمت **(تريدن مايكرو)** في تحديد وإيقاف أكثر من**(٧٤٠,٠٠٠)** هجمة عبر البرامج الضارة، وكذلك صد وإيقاف أكثر من **(١٦٠٠)**هجمة عبر البرامج الضارة التي استهدفت مواقع بنكية ومصرفية، بالإضافة إلى ذلك أظهر التقرير تحولا فى الاستراتيجيات التي يستخدمها مجرمو الإنترنت، الذين حولوا تركيزهم خلال النصف الأول من عام ٢٠٢٠ نحو استغلال آثار فيروس كورونا الجديد **(COVID-19)**، تفاقمت المخاطر التي تتعرض لها الشركات بسبب الثغرات الأمنية الناتجة عن العمل عن بعد[٢١]، ومن ثم أصبحت الشبكات المنزلية في مصر المصدر الرئيسي

لاستقطاب مجرمي الإنترنت الذين يستهدفون الأنظمة والأجهزة والشبكات، فعلى امتداد البلاد، تمكنت **(تريدن مايكرو)** من خلال حل(**Smart Home Network**) من إيقاف أكثر من ١٨,٠٠٠ هجمة داخلية وخارجية ، بالإضافة إلى منع حدوث أكثر من ٣٠ مليون واقعة يمكن للمتسللين استهدافها أو السيطرة على أجهزة المنزل من خلال البرامج الضارة ، أو الحصول على معلومات حساسة ومهمة، أو اعتراض الاتصالات، أو شن هجمات خارجية.

وعلى المستوى العالمي ، تم حظر(٢٧.٨) مليار تهديد إلكتروني في النصف الأول من عام ٢٠٢٠ ، مع حدوث ما يقرب من ٩٣٪ من هذه التهديدات عبر البريد الإلكتروني.

- **إستراتيجية الوطنية للأمن السيبرانى (٢٠٢٢-٢٠٢٦)**

تهدف الاستراتيجية الوطنية للأمن السيبرانى إلى مكافحة التحديات والمخاطر العالمية الناجمة عن التهديدات السيبرانية وذلك من خلال مجموعة من الخطوات التى تدعم لجهود الدولة لدعم الأمن القومي، وتنمية المجتمع المصري تم اصدار الاستراتيجية الوطنية للأمن السيبرانى التي تهدف إلى مكافحة الاخطار السيبرانية وذلك من خلال رصد ومواجهة التهديدات والتحديات المستقبلية فى مجال الأمن السيبرانى والمجتمع الرقمي بما يسهم فى تحقيق تنمية اجتماعية واقتصادية شاملة، وحماية الموطنين من المخاطر فى الفضاء السيبرانى، والحفاظ على مصالح الدولة العليا، وهذا ما أكده الدكتور**(عمرو طلعت)** وزير الاتصالات وتكنولوجيا المعلومات على ضرورة مواكبة الإستراتيجية الوطنية للأمن السيبرانى (٢٠٢٢ - ٢٠٢٦) لكافة المستجدات وأحدث التكنولوجيات والتقنيات فى مجال الأمن السيبرانى حتى تصبح قادرة على التصدي للتحديات والمخاطر العالمية الناجمة عن التهديدات السيبرانية، على النحو الذي يدعم جهود الدولة فى بناء مصر الرقمية والتي يتم من خلالها رقمنه الخدمات الحكومية وتبنى المعاملات الرقمية[٢٢١].

١

- **أليات التعاون الدولي**:

حيث تحرص مصر على المشاركة الدولية والإقليمية والتعاون الدولي من أجل تعزيز الأمن السيبرانى، فعلى سبيل المثال مشاركتها في المحافل الدولية والإقليمية، علاوة على اتفاقيات التعاون الدولي من خلال مركز **(السيرت)** المصري في مجالات تعاون الأمن السيبرانى.

رابعاً : السيناريوهات المستقبلية للحروب السيبرانية :

أ. **السيناريو الأول :**

وهو أن الفضاء السيبرانى سيظل أمن إلى حد كبير للأعمال والتواصل مع الأخرين، وفى نفس الوقت سيتم توظيفها فى حروب سيبرانية لسرقة البيانات الشخصية للأفراد أو الحرمان من الخدمة وستعمل الدول على تعزيز قدرتها على الحد من الهجمات السيبرانية .

ب. **السيناريو الثانى :**

وضع الأمان الجزئي : بمعنى أن الفضاء السيبرانى سيصبح مجال صراع فى الجو والبحر والفضاء ، ومع ذلك سيظل مكان أمن للأعمال والتواصل بين الأفراد، مع عدم قدرة بعض الدول على مواجهة تحديات الحروب السيبرانية .

ج. **السيناريو الثالث :**

وضع الأمان الواسع، أي أن الفضاء السيبرانى سيصبح أكثر أمنا وهذا يتطلب جهدا كبير فى مجال أمن المعلومات ، من خلال استحداث برامج تكنولوجية عالية فى مجال الدفاع

د. **السيناريو الرابع :**

توجه الدول نحو بناء حدود داخل الفضاء السيبرانى، أي التخلي عن وجود شبكة دولية واحدة، ولكن ستتعدد الشبكات، ومن ثم حرية تناول المعلومات .

ه. **السيناريو الخامس :**

وهو أكثر السيناريوهات خطورة، وفيه أن القراصنة وجماعات الجريمة المنظمة والجيوش الالكترونية تستطيع احداث تأثير على نطاق واسع على البنية التحية للدول ، قد تتسبب فى انهيار الشبكة الكهربائية والتأثير على امدادات الطاقة ، مما قد يؤدى إلى توقف المستشفيات والقطارات والطائرات والنظام المالي ،أو الهجمات على السدود التي تؤدى إلى فتح بوابات السدود ومن ثم لم يصبح الفضاء مكان أمن للاتصالات والأعمال وبالتالي ستتصاعد حدة الصراعات بين الدول .

ويلاحظ أن السيناريو الأخير يحتاج إلى قدرات سيبرانية متطورة وهو الذي تمتلكه بالفعل العديد من الفواعل ، سواء من الدول أو جماعات الجريمة المنظمة للقدرات السيبرانية المتطورة التي تؤهلها لشن هجمات سيبرانية تخترق نظم التحكم الصناعي مما يعد عاملا محفز لشن المزيد من الهجمات وزيادة للصراعات بين الدول .

النتائج :

إن المعارك المستقبلية قد تدور في الأساس حول البنيه التحتية للأنترنت بما في ذلك انظمة العملات المشفرة وانظمة الأمن السيبرانى والمعايير الفنية ، ولتجنب هذه المعارك المستقبلية هناك بعض المقترحات من بعض الدول للحفاظ على السيادة الفضاء السيبرانى حيث تعددت هذه المقترحات المتعلقة بسيادة البيانات فقد تم تنفيذ بعضها من بعض البلدان لمنع السيطرة على البنيه التحتية وخدمات الانترنت الأمريكية وتشمل هذه المقترحات :البريد الالكتروني الوطني والتوجيه المحلي لحركة المرور على الانترنت وكابلات الالياف البصرية تحت البحر ومركز البيانات المحلي

وللسيطرة على سيادة البيانات لكل دولة يجب تكييف مفهوم السيادة التقليدية مع الفضاء السيبرانى بنهج علمي يحظى بقبول المجتمع الدولي .

وفيما يتعلق بالدولة المصرية ، نجد انه الرغم من أن الحروب السيبرانية هي تعد مصطلح حديث نسبيا، إلا أن الدولة المصرية أولت لها أهمية كبيرة منذ فترة طويلة ، وأسست مجلسا أعلى للأمن السيبرانى وما زالت تواصل جهودها لتحصين الجهات الحكومية ضد تلك النوعية الحديثة من الحروب .

إن الفضاء السيبرانى أصبح جزءاً من التفاعلات الدولية التي تبذل الأمم المتحدة والمجتمع الدولي الجهود لضبط مجالات المسئوليات فيه، لأن معدلات التهديدات وفرص الحروب السيبرانية تتوسع بشكل كبير. وبزيادة عدد الأطراف في هذا المجال، صار الصراع ذا طبيعة سياسية، لكنه يتخذ شكلاً عسكرياً -إن صح التعبير- من حيث طبيعة الأضرار وتدمير الثروة المعلوماتية في البنية التحتية للدولة لأهداف سياسية. فخط التقسيم الجديد للعالم لن يكون بين عالم الشمال والجنوب، والعالم المتقدم والمتخلف، بل على أسس جديدة أولها من يملكون القوة السيبرانية والقدرة على صناعتها وإدارتها، وعلى الجانب الآخر المحرومين منها وإن كان يُسمح لهم باستخدامها.

المراجع :

[١] وليد زكى، من التعبئة الافتراضية إلى الثورة، مجلة الديمقراطية، القاهرة ،العدد ٤٢، أبريل ٢٠١١ ، ص٧٢.

[٢] وليد رشاد، المتغيرات الفاعلة فى المجال العام الافتراضي وتحليل السيسيولوجى، المؤتمر السنوي والعشرون للبحوث السياسية : تنامى الصراع ومستقبل التوافق الاجتماعي، مركز البحوث السياسية، كلية الاقتصاد والعلوم السياسية، القاهرة،٢٠٠٤ ، ص ٢١٠.

[٣] رنا أبو عمرة ، ويكيليكس نموذج لواقع إعلامي جديد، مجلة السياسة الدولية ، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة ، العدد ١٨٣، يناير ٢٠١١، ص ١٨٢.

[٤] عمرو الشوبكي، الحركات الاحتجاجية فى الوطن العربي، المستقبل العربي، مركز دراسات الوحدة العربية ، بيروت ، فبراير ٢٠١١، ص ١٠٥،متاح على الرابط:

https://gulfpolicies.org/2019-05-18-07-14-32/92-2019-06-25-12-45-40/694-2019-06-26-06-19-09

[٥] إبراهيم فريحات، ما تتغاضى عنه وزيرة الخارجية هيلاري كلينتون في موجة الاحتجاجات المصرية ضد النظام، مركز بر وكنجز، الدوحة، يناير ٢٠١١، متاح على الرابط :

https://www.brookings.edu/ar/opinions

[٦] المرجع السابق

[٧] المرجع السابق

[٨] رانيا سليمان وآخرون، سياسات مكافحة الإرهاب الالكتروني مصر والسعودية نموذجاً، المركز العربي للدراسات والبحوث، القاهرة، فبراير ٢٠٢٠، متاح على الرابط:

http://www.acrseg.org/41483

[٩] المرجع السابق

[١٠] المرجع السابق.

[١١] وثيقة الدستور المصري ٢٠١٤، متاح على الرابط:

https://www.constituteproject.org/constitution/Egypt_2014.pdf?lang=ar

[١٢] وثيقة الموافقة على انضمام مصر إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الجريدة الرسمية لجمهورية مصر العربية، ٢٠١٤، متاح على الرابط :

https://manshurat.org/sites/default/files/docs/pdf/002600.pdf

[١٣] رشدي على، الجرائم المعلوماتية دوليا خطر دولي مواجهة جرائم الإنترنت بين اتفاقية بودابست والتشريعات الوطنية، يوليو ٢٠١٦، العدد ٤٧٣٣١، تاريخ الدخول ١٥ /٢/ ٢٠٢٠، متاح على الرابط :

https://gate.ahram.org.eg/daily/News/191955/107/536569/

[١٤] غادة عامر ، جهود الدول فى مكافحة الإرهاب التكنولوجي ، مجلة السياسة الدولية ، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، العدد ٢٢٧، يناير ٢٠٢٢، ص ٢٥٧ .

[١٥] هاشم شريف، نحو استراتيجية وطنية للأمن السيبرانى، رئاسة مجلس الوزراء، المجلس الأعلى للأمن السيبرانى، الجهاز القومي لتنظيم الاتصالات، القاهرة، فبراير ٢٠١٩، ص ٨، متاح على الرابط:

https://www.eces.org.eg/cms/NewsUploads/Pdf/2019_12_4-02019.pdf

[١٦] وثيقة الاستراتيجية الوطنية للأمن السيبرانى "٢٠١٧- ٢٠٢١ "، تاريخ الدخول ٢٠٢١/١٢/٤ ، متاح على الرابط :

https://www.mcit.gov.eg/Upcont/Documents/Publications_12122018000_ar_AR_National_Cybersecurity_Strategy_2017_2021.pdf

[١٧] المرجع السابق .

[١٨] وزير الاتصالات يترأس اجتماع المجلس الأعلى للأمن السيبرانى، الموقع الرسمي لوزارة الاتصالات وتكنلوجيا المعلومات المصرية ، القاهرة، ديسمبر ٢٠٢٠ ، تاريخ الدخول ٢١ فبراير ٢٠٢٢، متاح على الرابط

https://mcit.gov.eg/ar/Media_Center/Press_Room/Press_Releases/64851

[١٩] الاستراتيجية الوطنية للأمن السيبرانى "٢٠١٧- ٢٠٢١ "، مرجع سابق.

[٢٠] المجلس الأعلى للأمن السيبرانى ستعرض برامج عمل الاستراتيجية الوطنية،٢٥ الهيئة العامة للاستعلامات، القاهرة، ديسمبر ٢٠١٨ ، تاريخ الدخول ٢٥ ابريل ٢٠٢١، متاح على الرابط :

https://sis.gov.eg/Story/181171/%D8%A7% B3-%D8D9%89-

[٢١] المرجع السابق .

[٢٢] فاطمة سويري، وزير الاتصالات: مواكبة الإستراتيجية الوطنية للأمن السيبرانى لأحدث تقنيات بناء مصر الرقمية، بوابة الاهرام، القاهرة، ديسمبر ٢٠٢١، متاح على الرابط :

https://gate.ahram.org.eg/News/3187514.aspx