الإرهاب الإلكترونى فى ظل أزمة فيروس كورونا :الأنماط...التداعيات

Cyber terrorism in the shadow of COVID-19 virus crisis: patterns ... implications

د.ياسمين أحمد صالح

مدرس العلوم السياسية –كلية السياسة والاقتصاد جامعة بني سويف

المستلخص:

فرضت جائحة كورونا التى عصفت بغالبية دول العالم تحدياً عالمياً يتعين على الدول مواجهته سواء على مدى زمنى قريب أوبعيد،فقد أثارت هذه الأزمة حالة من الارتباك وعدم اليقين بشأن سبل التعامل مع هذه العدوى وآليات الوقاية والعلاج ،فضلاً عن التداعيات الاقتصادية والاجتماعية لتلك الأزمة،الا أن ذلك لم يثن الدول والتنظيمات المتطرفة عن ممارسة الأعمال الارهابية ،فقد شهد العالم فى ظل هذه الجائحة تزايداً فى أعداد الهجمات الالكترونية مع بروز أنماط جديدة من الارهاب والتطرف تعتمد على توظيف التقنيات الحديثة فى بث خطابات الكراهية ، والترويج للأفكار الهدامة ، وذلك بهدف جذب أكبر عدد من المؤيدين لهذه الأفكار،وتقويض الثقة فى الحكومات بشكل يؤدى الى زعزعة أمن واستقرار البلاد.لذا جاءت هذه الدراسة لتسلط الضوء على تداعيات أزمة فيروس كورونا على ظاهرة الارهاب الالكترونى ،وذلك بالوقوف على تحديد مفهوم الارهاب الالكترونى ،وأهم الخصائص التى تميز هذه الظاهرة ،والتى انعكست على طبيعة الهجمات الالكترونية العابرة للحدود ،مع ابراز طبيعة الهجمات الالكترونية فى ظل الجائحة ،والتى شهدت تزايداً فى تلك الفترة بشكل يؤدى الى زيادة حدة الصراعات، ويهدد أمن واستقرار البلاد .الأمر الذى

يستوجب تأمين أنظمة المعلومات بمختلف الدول منعاً لاختراقها ،وتعاون الدول مع بعضها البعض لمواجهة هذه التهديدات الالكترونية .اذ أبرزت الدراسة حاجة المجتمع الدولى الى تكاتف وتضافر الجهود الجماعية لسن تشريعات دولية رادعة وقادرة على مواجهة جرائم الارهاب الالكترونى.

الكلمات المفتاحية:الارهاب ،الارهاب الالكترونى،جرائم الارهاب الالكترونى،التداعيات الاقتصادية ،والاجتماعية ،والأمنية.

Abstract:

The Corona pandemic, which struck most of the countries of the world, has imposed a global challenge that countries must face, whether over a short time or long ago, as this crisis has created a state of confusion and uncertainty about ways to deal with this infection, prevention and treatment mechanisms, as well as the economic and social repercussions of this crisis. This did not discourage countries and extremist organizations from practicing terrorist acts. In light of this pandemic, the world has witnessed an increase in the number of cyber attacks with the emergence of new types of terrorism and extremism that depend on employing modern technologies to broadcast hate speech and promote destructive ideas to attract the largest number of Supporters of these ideas and to undermine confidence in governments in a way that destabilizes the security and stability of the country. Therefore, this study came to shed

light on the repercussions of the Coronavirus crisis on the phenomenon of cyber-terrorism, by defining the concept of cyber terrorism, and the most important characteristics that distinguish this phenomenon, which was reflected on the nature of cross-border cyber attacks, while highlighting the nature of cyber attacks in light of the pandemic, which It witnessed an increase in that period in a way that leads to an increase in the intensity of conflicts and threatens the security and stability of the country. This requires securing information systems in various countries to prevent their penetration and countries cooperating with each other to confront these electronic threats. The study highlighted the need for the international community to join together and collective efforts to enact Deterrent international legislation capable of confronting cyber-terrorism crimes.

Key Words: terrorism, cyber terrorism, cyber terrorism crimes, economic, social, security implications.

مقدمة الدراسة :-

أضحت أزمة فيروس كورونا تحدياً عالمياً يتعين على جميع الدول مواجهته ، اذ خلقت نوع جديد من التهديدات تجسدت فى فيروسات سريعة الانتشار فى العالم،وعدم وجود أجهزة استخبارات قادرة على توقع ظهور فيروسات مماثلة ،مما فرض على العديد من الدول تغيير أولوياتها خاصةُ فى ظل تناقص الأدوية

والمخزن السلعى ، وأثار العديد من التساؤلات حول امكانية توافر مخزون استراتيجى من السلع ، وكوادر طبية للعمل خلال هذه الأزمة ، والقدرة على انتاج مستلزمات طبية وبالكميات المطلوبة .هذا بالاضافة الى البعد الاقتصادى للأزمة ، فقد ساهمت فى احداث نوع من الركود الاقتصادى عانت منه الكثير من دول العالم .الأمر الذى ترتب عليه احداث تغيير فى مفهوم الأمن القومى التقليدى ،فأصبحت قدرة الدول على توفير السلع والاحتياجات الأساسية،وتوفير المستلزمات الطبية والقدرة على انتاجها،بالاضافة الى قدرة اقتصاديات الدول على العمل خلال أزمات مماثلة احدى مكونات الأمن القومى.الا أن هذا لايعنى انتهاء التهديدات التقليدية مثل التهديدات النووية ، وكذا أيضا التهديدات الغير تقليدية مثل الارهاب الالكترونى ، والذى يُعد من أخطر الظواهر التى تشهدها المجتمعات فى العالم المعاصر لما لها من تأثير كبير على الأمن والسلم الدوليين ، وما يترتب عليه من دمار وهلاك للبشرية .

ففى ظل التقدم الهائل فى وسائل الاتصال والثورة العلمية فى مجال تكنولوجيا المعلومات والانترنت ،برز نوع جديد من التنافس بين الفاعليين الدوليين للاستفادة من هذه التقنيات الحديثة وتوظيفها فى تحقيق نمو اقتصادى سريع ، الا أن هناك من حاول الاستفادة من هذه التكنولوجيا واستخدامها فى الأغراض الغير سلمية.فقد حاول البعض استخدام هذه التقنيات الحديثة فى اختراق أنظمة المعلومات للدول ،وممارسة أعمال التجسس ، وتدمير البنى التحتية للدول ،فنشأ مايعرف باسم "الارهاب الالكترونى".كما سعت الجماعات الارهابية الى الاستفادة من التقدم الهائل فى وسائل الاتصال فى تحقيق أغراضها ،من خلال انشاء حسابات خاصة بالارهاب فى مواقع الانترنت لنشر التطرف والترويج لأفكار الجماعات الارهابية فى العالم بأسره ، والتواصل بين أعضائها لخرق المواقع الالكترونية ونشر الفيروسات والتجسس على الدول

لكشف أسرارها والحصول على أموال لتمويل نشاطها الارهابى ،وكذا أيضا جمع أكبر عدد من المؤيدين لأفكار هذه الجماعات الارهابية .

واليوم،وفى ظل أزمة فيروس كورونا ،والتى أودت بحياة نحو ٥٣٢ ألف انسان حول العالم ،سعت بعض الدول مثل ايران وروسيا وغيرها من الدول الى شن العديد من الهجمات الالكترونية والتى استهدفت منظمة الصحة العالمية وعدد من مراكز الأبحاث البريطانية والأمريكية التى تسعى لايجاد لقاحات لعلاج مرض "كوفيد-١٩" ، والناتج عن الاصابة بفيروس كورونا ، كما سعت الجماعات الارهابية الى استغلال فترة انشغال الدول على مستوى العالم فى مكافحة تفشى فيروس كورونا فى القيام بمزيد من العمليات الارهابية ، وبث خطابات الكراهية والآراء المتطرفة عبر شبكات الانترنت ،وذلك لجذب أكبر عدد من المؤيدين لأفكارهم المتطرفة ، وتقويض الثقة فى الحكومات بشكل يؤدى الى زعزعة أمن واستقرار البلاد .

لذا جاءت هذه الدراسة لتلقى الضوء على هذه الظاهرة "الارهاب الالكترونى " والتى تميزت باستحداث وتطوير الأدوات التى تعتمد عليها ، وكذا أيضا خطورتها وذلك من خلال التطرق الى مفهوم الارهاب الالكترونى ، وأهم الادوات التى يتم الاعتماد عليها فى تنفيذ الهجمات الالكترونية ، مع الاشارة الى تداعيات أزمة فيروس كورونا على ظاهرة الارهاب الالكترونى ،والجهود الدولية لمكافحة مثل هذا النوع من الارهاب.

أهداف الدراسة :

تهدف هذه الدراسة الى ابراز تداعيات أزمة فيروس كورونا على ظاهرة الارهاب الالكترونى ، وذلك بالاشارة الى مخاطر هذه الأزمة ، والوقوف على تحديد مفهوم الارهاب الالكترونى ، وأسبابه ،والأدوات التى يعتمد عليها المجرم الالكترونى فى تنفيذ مخططاته ، وكذا أيضا توضيح المقصود بجريمة الارهاب

الالكترونى ،وأنماط الهجمات الالكترونية فى ظل أزمة فيروس كورونا ،مع الاشارة الى الجهود الدولية لمكافحة جرائم الارهاب الالكترونى.

أهمية الدراسة :

لقد أثارت جائحة كورونا والتى عصفت بغالبية دول العالم حالة من القلق والارتباك وعدم اليقين بشأن آليات التعامل مع هذهُ الأزمة وكيفية منع انتشار العدوى وايجاد علاج لهذا المرض"كوفيد-١٩".فضلاً عن التداعيات الاقتصادية والاجتماعية والأمنية لتلك الأزمة،الا أن ذلك لم يثن بعض الدول عن شن العديد من الهجمات الالكترونية ، وكذا أيضاً الجماعات الارهابية عن توظيف الانترنت فى بث خطابات الكراهية والآراء المتطرفة.لذا من الأهمية ابراز تداعيات أزمة فيروس كورونا على الارهاب الالكترونى ،وذلك بالوقوف على تحديد مفهوم الارهاب الالكترونى ،وأسبابه ، وأهم خصائصه ،والوسائل الذى يعتمد عليها فى تنفيذ هذه الهجمات الالكترونية ،مع الاشارة الى الأنماط الجديدة من الهجمات الالكترونية التى شنتها الدول والتنظيمات المتطرفة فى ظل أزمة فيروس كورونا ، والجهود الدولية لمكافحة جرائم الارهاب الالكترونى.

المشكلة البحثية :

تُعد أزمة فيروس كورونا من أبرز التحديات التى تواجه غالبية دول العالم ،لما لها من تداعيات خطيرة على كافة الأصعدة الاجتماعية والنفسية والاقتصادية .الا أن هذه الأزمة لم تثن بعض الدول والتنظيمات الارهابية عن شن العديد من الهجمات الالكترونية ذات الطابع الجديد، اذ تستهدف مراكز أبحاث تسعى لانتاج لقاح لعلاج مرض "كوفيد-١٩" ،وتبث خطابات الكراهية والاراء المتطرفة عن طريق شبكات الانترنت وذلك لتقويض الثقة بالحكومات وزعزعة أمن واستقرار البلاد.

لذا جاءت هذه الدراسة لتجيب على تساؤل هام ورئيسى :

–ماهى تداعيات جائحة كورونا على ظاهرة الارهاب الالكترونى؟

ويتفرع عن هذا التساؤل عدد من التساؤلات الفرعية :

- ماالمقصود بالارهاب الالكترونى وجرائم الارهاب الالكترونى ؟
- ماهى الأسباب المؤدية للارهاب الالكترونى ؟
- ماهى طبيعة الأخطار الناجمة عنه؟
- ماهى أبرز ملامح جرائم الارهاب الالكترونى التى شهدتها دول العالم قبل وبعد جائحة كورونا؟
- كيف استغلت التنظيمات الارهابية أزمة فيروس كورونا فى الترويج لأفكارها الكترونيا؟
- ماهى الجهود الدولية لمكافحة جرائم الارهاب الالكترونى ؟

مناهج الدراسة:

نظرا لطبيعة الظاهرة ،اعتمدنا فى هذه الدراسة على المناهج التالية:

١– المنهج الوصفى : اعتمدنا على هذا المنهج فى وصف الظاهرة"الارهاب الالكترونى" وتوضيح طبيعتها ، والأساليب والوسائل التى تلجأ اليها الدول والجماعات الارهابية فى تنفيذ جرائم الارهاب الالكترونى ، ومصادر التهديد المختلفة.

٢– منهج دراسة الحالة :تم الاعتماد على هذا المنهج فى جمع البيانات بوحدات التحليل (جماعة ، دولة ،.....) ، حيث تم تقديم نماذج للعديد من الدول التى قامت بشن هجمات الكترونية من شأنها أن تهدد السلم والأمن الدوليين وكذا أيضا جماعات متطرفة حاولت الاستفادة من التقنيات الحديثة وانشغال العالم

بجائحة كورونا فى بث خطابات الكراهية والآراء المتطرفة ،اذ تساعد دراسة الحالات المتعددة على فهم الاختلافات ،واستكشاف أوجه التشابه بين الحالات .

٣- المنهج المقارن :تم الاعتماد على هذا المنهج فى ابراز طبيعة الهجمات الالكترونية قبل وبعد المرور بجائحة كورونا وذلك لتوضيح تداعيات جائحة كورونا على ظاهرة الارهاب الالكترونى .

الدراسات السابقة :

هناك العديد من الدراسات التى تناولت مفهوم الارهاب والتطورات التى طرأت على هذا المفهوم ، والارهاب الالكترونى وجرائم الارهاب الالكترونى ،وتأثير الارهاب الالكترونى على أمن الدول،وتداعيات أزمة فيروس كورونا على ظاهرة الارهاب الالكترونى ويمكن تقسيم هذه الدراسات على خمس محاور رئيسية :

١- الدراسات التى تناولت الارهاب :

تتناول هذه الدراسات ظاهرة الارهاب والتى تُعد من أخطر القضايا التى يشهدها العالم الأن ، فقد حاولت تقديم تعريف للارهاب. وعلى الرغم من عدم تقديم تعريف محدد للارهاب ، الا أنه تم الاتفاق على عدد من الخصائص التى تميز هذه الظاهرة وهى استخدام القوة أو التهديد باستخدامها لترويع المدنيين وتخويفهم والمساس بأمن وسيادة الدولة كما اشتملت هذه الدراسات على التشريعات المختلفة لمكافحة الارهاب منها اتفاقية جنيف لمنع ومعاقبة الأعمال الإرهابية ١٩٣٧م، والاتفاقية الأوروبية لقمع الإرهاب ١٩٧٧م،والاتفاقية العربية لكافحة الارهاب لعام ١٩٩٨م [١].

٢- الدراسات التى تناولت الارهاب الالكترونى :

حرصت الكثير من الدراسات التى تناولت الارهاب الالكترونى على تقديم تعريف لهذا المفهوم وهو توظيف التكنولوجيا والتقنيات الحديثة ،واستغلال وسائل الاتصال والشبكات المعلوماتية فى ترويع الأخرين

والحاق الضرر بهم أو تهديدهم.فمن خلال مواقعهم يستطيعوا اختراق المواقع الالكترونية العسكرية والمدنية والحصول على المعلومات التى يريدونها. بالاضافة الى توظيف الانترنت فى التنسيق بين هذه الجماعات الارهابية على مستوى العالم ، **وكذا أيضا تجنيد العديد من المؤيدين لأفكار هذه الجماعات والتى لاتكتفى فقط باعلان الانضمام اليها ، وانما تأكيد تأييدهم لمثل هذه الأفكار.ونظرا لطبيعة هذه الظاهرة وماتتميز به من خصائص ، جعلت من الصعب بمكان ثبوت الجريمة** ،فقد يتم استخدام أحد المواقع الالكترونية لتنفيذ مثل هذه الجرائم ، ثم يختفى هذا الموقع ليعاود الظهور بشكل جديد وبعنوان الكترونى جديد وذلك بعد فترة قصيرة جدا .أما بالنسبة للتشريعات والقوانين اللازمة لمكافحة الارهاب الالكترونى ، فقد أوضحت هذه الدراسات بأنه حتى الأن لم يتم الاتفاق على قوانين دولية لمواجهة الارهاب الالكترونى ومكافحته، وانما هناك جهود فردية من قبل الدول [٢].

٣- الدراسات التى تناولت نماذج للجرائم الالكترونية وطرق مكافحتها :

حرصت هذه الدراسات على تقديم نماذج للجرائم الالكترونية ، وهى الجرائم التى تعتمد على استخدام الانترنت فى تنفيذ الهجمات الارهابية ، وتعد من أخطر الجرائم التى تهدد أمن الدولة وسلامتها الاقليمية وذلك نظرا لطبيعة هذه الجرائم كونها عابرة للحدود وتفوق القدرات الأمنية للدولة . هذا وقد تم توقيع العديد من الاتفاقيات والمعاهدات الدولية لمكافحة مثل هذا النوع من الجرائم ، وكذلك انعقاد العديد من المؤتمرات منها : المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات في البرازيل ١٩٨٤م، واتفاقية بودابست ٢٠٠١م لمكافحة الجرائم المعلوماتية، والقانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية[٣].

٤- الدراسات التى تناولت تأثير الارهاب الالكترونى على أمن الدولة :

ركزت هذه الدراسات على ابراز مدى تأثير الارهاب الالكترونى على أمن الدولة وسلامتها الاقليمية ،فظاهرة الارهاب الالكترونى من أخطر الظواهر التى يشهدها العالم المعاصر . نظرا لما تتسم به هذه الظاهرة من القدرة على توظيف الكمبيوتر والانترنت فى اختراق أنظمة المعلومات للدول ،وتدمير البنى التحتية والحيوية. هذا بالاضافة الى سعى الجماعات الارهابية للاستفادة من التقنيات الحديثة، واستخدام الشبكات المعلوماتية فى اختراق المواقع العسكرية والمدنية بالدولة ،وجذب أكبر عدد من المؤيدين لأفكار هذه الجماعات من خلال بث أفكارهم المتطرفة عبر هذه المواقع الالكترونية ، والتنسيق فيما بينهم أثناء القيام بالعمليات الارهابية ،وكذا أيضا انتحال شخصية علماء وسياسيين بارزين للتأثير فى الرأى العام ، ونظرا لخطورة هذه الجرائم والتى يصعب ملاحقة مرتكبيها ،تسعى العديد من الدول الى سن تشريعات وقوانين لمكافحة هذه الجرائم خاصة فى ظل عدم الاتفاق على قوانين دولية موحدة لمواجهة الارهاب الالكترونى[٤].

٥- الدراسات التى توضح تأثير جائحة كورونا على ظاهرة الارهاب الالكترونى :

حرصت هذه الدراسات على ابراز تأثير أزمة فيروس كورونا على ظاهرة الارهاب الالكترونى ،حيث سعت بعض الدول مثل ايران وروسيا وغيرها الى شن هجمات الكترونية على منظمة الصحة العالمية وعدد من مراكز الأبحاث ،والتى تسعى لانتاج لقاح لعلاج مرض "كوفيد -١٩".هذا بالاضافة الى استغلال التنظيمات المتطرفة انشغال العالم بهذه الأزمة فى استخدام الانترنت لبث خطابات الكراهية والاراء المتطرف ،وزعزعة الثقة فى الاجراءات التى تتخذها حكومات الدول لمواجهة هذه الأزمة[٥] .

تقسيمات الدراسة :

تقُسم الدراسة إلى أربع محاور على النحو التالى :

المحور الأول:التأصيل النظرى لمفاهيم الدراسة ، والذى يتناول تعريف الارهاب الالكترونى وخصائصه والأساليب التى يعتمد عليها المجرمين فى تنفيذ هجماتهم الارهابية ، مع توضيح أركان جريمة الارهاب الالكترونى.

المحور الثانى : تأثير الارهاب الالكترونى على أمن الدول ،والذى يتم فيه الاشارة الى نماذج من الهجمات الالكترونية التى تعرضت لها الدول.

المحور الثالث:تداعيات أزمة فيروس كورونا على ظاهرة الارهاب الالكترونى ،ويتضمن الأنماط الجديدة من الهجمات الالكترونية التى شنتها الدول والتنظيمات المتطرفة فى ظل هذه الأزمة.

المحور الرابع:الجهود الدولية لمكافحة جرائم الارهاب الالكترونى،ويشتمل على الجهود الفردية التى مارستها الدول لمكافحة مثل هذا النوع من الارهاب.

المحور الأول: التأصيل النظرى لمفاهيم الدراسة

أولا: مفهوم الارهاب الالكترونى:-

من المهم والضرورى قبل الولوج الى تعريف الارهاب الالكترونى ،يتعين علينا أن نتطرق الى تعريف الارهاب بشىء من التفصيل .

- **تعريف الارهاب :**

على المستوى اللغوى :لم ترد كلمة الارهاب فى المصادر اللغوية القديمة فى اللغة العربية كالقاموس المحيط ولسان العرب وأساس البلاغة وغيرها.وذلك لأنها كلمة حديثة الاستعمال(٦). فقد أقر المجمع اللغوى كلمة الارهاب ككلمة حديثة فى اللغة العربية وأصلها بمعنى رهب أى خاف ،أما معجم مصطلحات العلوم الاجتماعية ،فقد عرف الارهاب بأنه "بث الرعب الذى يثير الخوف والفعل بأى طريقة تحاول بها جماعة منظمة أو حزب أن يحقق أهدافه عن طريق استخدام العنف ، وتوجه الأعمال الارهابية ضد الأشخاص سواء كانوا أفراداً أو ممثلين للسلطة مما يعارضون أهداف هذه الجماعة"(٧).

هذاوقد وردت كلمة ارهاب فى القاموس السياسى لتعنى :"نشر الذعر والفزع لأغراض سياسية، والارهاب وسيلة تستخدمهاحكومة استبدادية لارغام الشعب على الخضوع والاستسلام لها.."أما حسب قاموس أكسفود فيقصد به :"استخدام العنف والتخويف أو الارعاب(من الرعب)،خاصة فى الأغراض السياسية"(٨).

على مستوى الهيئات والاتفاقيات الدولية ،فقد عرفه مجلس الأمن الدولى على أنه" كل عمل اجرمى ضد المدنيين بقصد التسبب بالوفاة أو الجروح البليغة أو أخذ الرهائن من أجل اثارة الرعب بين الناس أو اكراه حكومة أو منظمة للدولية للقيام بعمل ما أو الامتناع عنه، وكل الأعمال الأخرى التى تشكل إساءات ضمن نطاق المعاهدات الدولية المتعلقة بالارهاب والتى لايمكن تبريرها بأى اعتبار سياسى أو فلسفى أو ايديولوجى أو عرقى أو دينى "(٩).

كما عرف القانون المصرى الارهاب بأنه (كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجأ اليه الجانى تنفيذاً لمشروع اجرامى فردى أو جماعى بهدف الاخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر اذا كان من شأن ذلك ايذاء الأشخاص أو القاء الرعب بينهم أو تعريض حياتهم أو حرياتهم

أو أمنهم للخطر أو الحاق الضرر بالبيئة أو بالاتصالات أو المواصلات أو بالأموال أو المبانى أو بالأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم لاعمالها أو تعطيل تطبيق الدستور أو القوانين أو اللوائح). هذا وقد بادرت اتفاقية جنيف لقمع ومحاربة الارهاب لعام ١٩٣٧ بتعريف الارهاب على أنه " تلك الأعمال الاجرامية الموجهة ضد دولة ما وتستهدف أو يقصد بها خلق حالة من الرعب فى أذهان أشخاص معينين ، أو مجموعة من الأشخاص ، أو عامة الجمهور[١٠] ....".

ثم جاءت الاتفاقية العربية لعام ١٩٩٨ ، وعرفت الارهاب على أنه " كل فعل من أفعال العنف أو التهديد أياً كانت بواعثه أو أغراضه ، يقع تنفيذاً لمشروع اجرامى فردى أو جماعى ، ويهدف الى افشاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو أمنهم للخطر ، أو الحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة ،أو احتلالها ،أو الاستيلاء عليها ، أو تعريض أحد الموارد الوطنية للخطر [١١]".

- **<u>الارهاب الالكترونى:</u>**

برز مفهوم الارهاب الالكترونى فى مطلع الثمانينات من القرن الماضى ، وذلك عقب الطفرة التكنولوجية التى حققتها تكنولوجيا المعلومات واستخدام الانترنت فى ادارة وتسيير معظم المجالات ، الا أن هذه الجماعات الارهابية حاولت توظيف التكنولوجيا الحديثة فى استخدام الانترنت فى الوصول الى الأهداف والغايات المنشودة . هذا وقد تعددت تعريفات الارهاب الالكترونى ،فحسب الموسوعة الالكترونية ، جرى تعريف الارهاب الالكترونى على أنه " استخدام التقنيات الرقمية لاخافة أو اخضاع الأخرين أو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أوعرقية أو دينية "[١٢].

أما مجمع الفقه الاسلامى ، فيعرف الارهاب الالكترونى على أنه " العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الالكترونية، ويكون صادراً عن الدول أوالجماعات أو الأفراد على الانسان أو دينه أو نفسه أو عرضه أو عقله أو ماله ، بغير حق بشتى صنوفه (العدوان) وصور الافساد فى الارض"(١٣).

كما عرفت اللجنة الدولية للصليب الأحمر الارهاب الالكترونى بأنه "عمليات تُشن ضد أو عبر حاسوب بواسطة تيار بيانات وتهدف الى تحقيق أغراض منها اختراق النظام المعلوماتى أو جمع أو نقل أو تشفير البيانات أو التلاعب بها من قبل منفذ عملية الاختراق ،واستخدام هذه الوسائل لتدمير أو تعطيل مجموعة متنوعة من الأهداف فى العالم الحقيقى كالصناعات والبنى الأساسية(١٤) ."

وتعرف منظمة الدفاع الأمريكية الارهاب الالكترونى بأنه:"عمل اجرامى يتم الاعداد له باستخدام الحاسبات ووسائل الاتصالات ينتج عنها عنف وتدمير أو بث الخوف تجاه تلقى الخدمات بما يسبب الارتباك وعدم اليقين بهدف التأثير على الحكومة أو السكان لكى تمتثل لأجندة سياسية أو اجتماعية أو فكرة معينة ".

أما جيمس لويس ،فيعرف الارهاب الالكترونى:هو استخدام أدوات الحاسوب فى تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل الطاقة والنقل والعمليات الحكومية ،أو بهدف ترهيب حكومة ما أو مدنيين "(١٥).

ويعرف بونتارا الارهاب الالكترونى بأنه :"من أشهر الجرائم الالكترونية متعلق بتعطيل الخوادم عن تقديم خدمة الانترنت لموقع ما عبر القرصنة والهجمات الالكترونية المنسقة ،بشكل يحرم الناس من تلبية احتياجاتهم الأساسية منها"(١٦).

ويتمثل الجانب الاجرائى فى مفهوم الارهاب الالكترونى بأنه هو "نشاط أو هجوم متعمد ذو دوافع سياسية بغرض التأثير على القرارات الحكومية أو الرأى العام باستخدام الفضاء الالكترونى كعامل مساعد ووسيط فى عملية التنفيذ للعمل الارهابى أو الحرب من خلال هجمات مباشرة بالقوة المسلحة على مقدرات البنية التحتية للمعلومات أو من خلال استخدام آليات الأسلحة الالكترونية الجديدة فى معارك تدور رحاها فى الفضاء الالكترونى والتى قد يقتصر تأثيرها على بعدها الرقمى أو قد تتعدى الى أهداف مادية تتعلق بالبنية التحتية الحيوية "(١٧).

وهكذا يتضح لنا أن الارهاب الالكترونى برز وتنامى ظهوره بشكل واضح وجلى مع التقدم التكنولوجى فى وسائل الاتصال ، واستخدام الانترنت والكمبيوتر فى شتى المجالات ،فقد سعت الجماعات الارهابية الى توظيف هذه التقنيات الحديثة فى الوصول الى أهدافها .فأصبحت الحرب أكثر سهولة ، وأشد ضراوة فالأسلحة أصبحت أكثر فتكاً لأن مثل هذه الجرائم تتخطى حدود الدول ، مع الصعوبة البالغة فى الرقابة عليها ، اضافة الى سهولة تنفيذ مثل هذه الجرائم التى لاتتطلب سوى القدرة على اختراق الحواجز الالكترونية عن طريق جهاز كمبيوتر متصل بالشبكة المعلوماتية .

<u>خصائص الارهاب الالكترونى ،وأسبابه:</u>

يتميز الارهاب الالكترونى بعدد من الخصائص التى تجعله يتميز عن الارهاب بمفهومه التقليدى ، من أبرز هذه الخصائص:

١- يعتمد الارهاب الالكترونى على أسلحة غير تقليدية وغير مكلفة كالكمبيوتر وشبكات الانترنت ، فمثل هذا النوع من الارهاب لايحتاج الى وسائل أكثر من الشبكة العنكبوتية لاتمام جرائمه، ونشر أفكارهم المتطرفة واستقطاب أكبر عدد من المؤيدين لأفكارهم.

٢- جريمة عابرة للحدود ، فالمجرم يرتكب جريمته فى دولة ما ولكن تمتد اثارها الى العديد من الدول.

٣- جريمة يصعب اكتشاف مرتكبيها وملاحقتهم ، فقد يقوم مرتكب الجريمة بإنشاء موقع الكترونى يُمارس من خلاله جرائمه ، وفور ارتكاب هذه الجريمة يقوم بإغلاق هذا الموقع وانشاء حساب جديد له، الأمر الذى يُضفى على الظاهرة المزيد من التعقيد.

٤-يتمتع مرتكب مثل هذا النوع من الجرائم بالخبرة الكافية التى تمكنه من التعامل مع شبكة الانترنت بسهولة ويسر وكذا أيضا اختراق البريد الالكترونى وانتحال شخصيات سياسيين بارزيين ، والوصول الى أكبر عدد من الأفراد عبر مواقع التواصل الاجتماعى والدردشة الالكترونية(١٨).

أسباب الارهاب الالكترونى :

للارهاب الالكترونى مجموعة من الأسباب والدوافع التى تتباين فى درجة أهميتها وتأثيرها ، من أبرزها :

ضعف الشبكة المعلوماتية وسهولة اختراقها ،فشبكة المعلومات ليس عليها أية قيود أو حواجز أمنية لجذب أكبر عدد من المستخدمين ، مما دفع التنظيمات الارهابية الى الاستفادة من هذه المزايا وتوظيفها فى الهجمات الارهابية.هذا بالاضافة الى غياب الرقابة على الشبكة المعلوماتية ، وسهولة استخدامها ، وغياب التشريعات والقوانين العالمية التى تُجرم هذه الأعمال الارهابية ، وانتشار البطالة وديكتاتورية الأنظمة السياسية(١٩) .

أهداف جريمة الارهاب الالكترونى :

****يهدف الارهاب الالكترونى الى تحقيق مجموعة من الأهداف الغير مشروعة منها:**

١- نشر الخوف والرعب وعدم الطمأنينة بين الأشخاص والدول والشعوب المختلفة .

٢- الاخلال بالنظام والأمن العام.

٣- اثارة الرأى العام .

٤- تجنيد العديد من الشباب المؤيدين لأفكار هذه الجماعات الارهابية.

٥- تدمير البنى التحتية ، والاضرار بوسائل الاتصال وتقنية المعلومات .

٦- المساس بسيادة الدولة ، وتهديد أمنها .

ثانياً: أركان جريمة الارهاب الالكترونى:-

لجريمة الارهاب الالكترونى ركنان : ركن مادى ،وركن معنوى . هذا الى جانب الركن الخاص الذى يُميز هذه الظاهرة عن غيرها ، والمتمثل فى وسيلة ارتكاب الجريمة ،حيث يتم استخدام شبكة المعلومات الدولية فى ارتكاب مثل هذا النوع من الجرائم.

١ - الركن المادى:

يتمثل الركن المادى فى السلوك الذى يلجأ اليه الجانى عند ارتكاب الجريمة أى الأعمال الارهابية التى يقوم بها مرتكب الجريمة كتدمير البنى المعلوماتية التحية للدولة ،استهداف المنشأت العسكرية ، بث الرعب والخوف بين أفراد المجتمع ،اثارة الفتن الطائفية ،والترويج لعدد من الأفكار المتطرفة .

٢ -الركن المعنوى:

يتمثل الركن المعنوى فى قصد الجانى ارتكاب أفعال تُعد من الجرائم الارهابية أى قصد الجانى اثارة الرعب والخوف بين أفراد المجتمع ، وتدمير البنى المعلوماتية التحتية للدولة ، واستهداف المنشأت العسكرية والمدنية وغيرها من الأعمال الارهابية ، ويتحقق ذلك بتوفر علم الجانى بأن هذه الأفعال تُعد من الأعمال الارهابية ، والتى يترتب عليها المساس بأمن وسيادة الدولة ، وانصراف ارادته الى ذلك[٢٠] .

المحور الثانى : تأثير الارهاب الالكترونى على أمن الدول

يأخذ هذا النوع من الارهاب شكل "إرهاب الدول"،فهو يصدر عن دولة وموجه الى دولة أخرى،ونظراً لخطورة هذه الظاهرة،ومايترتب عليها من خسائر فى الأرواح وتدمير لكافة البنى المعلوماتية التحتية ،والمنشآت العسكرية والاقتصادية ،تزايد الاهتمام بهذا النوع من الارهاب من قبل الأجهزة الأمنية والاستخبارية فى العالم ،وتعد الصين الشعبية ،روسيا الاتحادية ،وكوريا الشمالية من أكثر الدول المتهمة بممارسة هذا النوع من الارهاب ضد الولايات المتحدة أو بعض الأعداء الاقليميين لها من خلال جمع المعلومات الاستخباراتية ،وسرقة البرامج ،وادارة ادراك العدو .هذا بالاضافة إلى العديد من النماذج تم استخدام فيها الحرب الالكترونية ،وهى روسيا والشيشان عام ١٩٩٤،وتدخل الناتو فى حرب كوسوفا عام ١٩٩٩[٢١]،والحرب الالكترونية فى الشرق الأوسط عام ٢٠٠٠،والصراع الأمريكى الصينى والذى هاجمت فيه الصين مواقع الكترونية للولايات المتحدة عام ٢٠٠١، حيث تعرض مايقرب من ١٢٠٠ موقع أمريكى لهجمات من قراصنة صينيين ،وقد شملت تلك الهجمات مواقع البيت الأبيض ،والقوات الجوية الأمريكية ،ووزارة الطاقة الأمريكية[٢٢]،وكذا أيضاً الهجمات الروسية ضد الحملة الانتخابية للولايات المتحدة فى عام ٢٠١٦،فقد اتهم مكتب التحقيقات الفيدرالى الأمريكى"اف بى آى"١٣ مواطناً روسياً بالتدخل فى الانتخابات الأمريكية التى جرت عام ٢٠١٦،ووفقاً لشبكة "إن بى سى " أكدت جانيت مانفيرا مسئولة الأمن السيبرانى بوزارة الأمن الداخلى أن القراصنة الروس استهدفوا ٢١ دائرة تسجيل للناخبين،وأن عدداً منها قد تم اختراقه بالفعل[٢٣]،والحرب الالكترونية الروسية ضد استونيا عام ٢٠٠٧،والتى تُعد أول حرب الكترونية تم استخدام فيها الفضاء الالكترونى لتدمير قطاعات حيوية والتى استمرت ثلاثة أسابيع،ونتج عنها تدمير لكثير من المواقع الرسمية والحزبية فى استونيا[٢٤]،وتوقف العمليات البنكية والمصرفية.هذا بالاضافة الى استخدام

الولايات المتحدة الأمريكية قوتها الالكترونية فى شن هجمات على منشآت ايران النووية ،وذلك رداً على الهجمات الالكترونية التى شنتها ايران على مؤسسات مالية وأنظمة حكومية وشبكات للطاقة الأمريكية ،فقد كشفت شركة "كاسبرسكى لاب"الروسية المتخصصة فى حلول وتطبيقات الأمن والحماية من خلال ماتقول أنه أدلة دامغة عن وجود تعاون فى مرحلة واحدة على الأقل بين برمجية فيروس "ستاكسنت"(stuxnet)،والبرمجية الخبيثة لفيروس "فليم"(flame)،والذى يُعتقد أن الولايات المتحدة الأمريكية واسرائيل قد استخدمتهما لمواجهة منشآت نووية ايرانية ،وبعد شهر واحد،أعلنت ايران وقف انتشار فيروس يمحو بيانات خوادم أجهزة الكمبيوتر فى قطاعاها النفطى.فهناك مجموعات من الفصائل والمليشيات الرقمية الايرانية التى تعمل فى الفضاء الالكترونى وتم تجهيزها وتطويرها وفق رؤى وأهداف وضعت من قبل رؤوس النظام الايرانى أطلق عليها"جيش فضاء إيران الالكترونى"،وذلك لشن هجمات الكترونية على المعارضة والدول الكبرى التى تقف عائقاً أمام البرنامج النووى الايرانى ،حيث يصنف مركز خبير لتقنية المعلومات الذى أنشىء عام ٢٠١١ ضمن قائمة الميلشيات الرقمية ،والذى أوكلت اليه شن هجمات معلوماتية ضد وحدات انتاج الطاقة الكهربائية ،وادارة تشغيل السدود بالولايات المتحدة الأمريكية ،وشن هجمات ضد مصارف بالسعودية، ففى عام٢٠١١، قام الجيش الرقمى بشن هجمات الكترونية على موقع صوت أمريكا (VOA)،وفى عام ٢٠١٢،أطلقت ايران فيروس أطلق عليه"شمعون" والذى عطل عشرات الآلاف من أجهزة الكمبيوتر بشركة أرامكو السعودية[٢٥] ،وفى عام ٢٠١٣،تم انشاء معهد المبنى، والذى يُعد ضمن تصنيف"الميلشيات "الايرانية، وذلك لوضع برنامج مسئول عن سرقة المعلومات التقنية والبيانات من المعاهد والجامعات العالمية للاستفادة منها فى دعم النهوض التقنى والعلمى لتعزيز قدرات ترسانة ايران العسكرية، ووضع أسس قوية لبرنامجها النووى . كما أكد التقرير

الصادر عن شركة "cloud flare"الأمريكية لأمن الشركات أن الهجمات الالكترونية التى شنتها ايران ضد مواقع عالمية قد تضاعفت ٣ مرات بعد مقتل قائد فيلق القدس التابع للحرس الثورى الايرانى قاسم سليمانى .هذا وقد تعرضت أيضاً مصر والسعودية لعدد من الهجمات الالكترونية،فقد أعلنت شركة " كاسبرسكاى لابس" Kaspersky Labs، أن مصر من الدول التى تعرضت لهجوم الكترونى من خلال "الفيروس العالمى الذى يُطلق عليه انتزاع الفدية"،والذى قد تعرضت له العديد من الدول مثل(بريطانيا ،ألمانيا ،تركيا،اليابان ،الهند،الصين ،فرنسا ،إسبانيا،المكسيك،روسيا ،الفلبين).أما السعودية،فقد تعرضت شركة أرامكو السعودية لهجوم الكترونى،حيث أصيب ٣٠ ألف كمبيوتر بفيروس مدمر فى شهر أغسطس ٢٠١٢،والذى ترتب عليه تدمير بيانات ومسح أقراصاً صلبة فى أجهزة الكمبيوتر،وذلك بهدف وقف إنتاج البترول ، وفى مايو ٢٠١٣،قام الجيش الالكترونى السورى بشن هجوم الكترونى على عدة مواقع حكومية سعودية على الانترنت كالهجمات التى تعرضت لها الحواسيب الخاصة بالشرطة الوطنية ،وفى عام ٢٠١٦،تعرضت العديد من الهيئات الحكومية وشركات القطاع الخاص لهجمات الكترونية استهدفت البنى التحتية،ومن بين تلك الهجمات:الهجوم الالكترونى على هيئة الطيران السعودية باستخدام برمجيات ازالة البيانات(٢٦) .

وهكذا يتضح لنا بعد استعراض النماذج المختلفة للهجمات الالكترونية التى تعرضت لها البلاد ،إلى أى مدى تختلف طبيعة جرائم الارهاب الالكترونى عن جرائم الارهاب التقليدى ،فجرائم الارهاب الالكترونى عابرة للحدود ، وتعتمد على **استخدام الانترنت فى تنفيذ مثل هذه الهجمات .هذا بالإضافة إلى صعوبة تحديد مرتكب هذه الجريمة على عكس جرائم الارهاب التقليدى ،والتى تعتمد على استخدام الأسلحة التقليدية كالقنابل والصواريخ وغيرها .**

المحور الثالث :تداعيات أزمة "فيروس كورونا" على ظاهرة الارهاب الالكترونى

فرض وباء كورونا الذى اجتاح العديد من دول العالم تحدياً أمنياً مرتبط بالأمن السيبرانى ،فقد شهدت العديد من دول العالم هجمات الكترونية شكلت تهديداً لأمن واستقرار الدول ،كما قامت العديد من التنظيمات المتطرفة باستغلال انشغال العالم بوقف انتشار العدوى وايجاد علاج لهذا المرض "كوفيد-١٩"فى استخدام الانترنت فى بث خطابات الكراهية ونشر الآراء المتطرفة .لذا سعت الباحثة الى طرح العديد من نماذج الدول التى قامت بشن هجمات الكترونية على دول أخرى ،وكذا أيضا تنظيمات متطرفة استطاعت استغلال هذه الأزمة فى نشر أفكارها الهدامة ، وذلك لابراز التغيرات التى طرأت على طبيعة الهجمات الالكترونية بعد جائحة كورونا.ففى ايران ،قامت مجاميع للقرصنة بشن العديد من الهجمات الالكترونية على منظمة الصحة العالمية ،ومراكز أبحاث بريطانية وأمريكية تسعى لانتاج لقاحات لعلاج فيروس كورونا.فقد نقلت وكالة رويترز للأنباء عن مصادر متخصصة فى الأمن السيبرانى أنه فى ابريل الماضى قام قراصنة الكترونيين يعملون لصالح الحكومة الايرانية باختراق حسابات البريد الالكترونى الشخصية لموظفين من منظمة الصحة العالمية.هذا بالاضافة الى قيام ايران بشن هجوم الكترونى على مرافق مياه الشرب والصرف الصحى فى ٢٤ أبريل الماضى ،والتى تسببت فى توقف مضخة في شبكة مياه بلدية في منطقة شارون عن العمل.كمانشرت استشارية المركز الوطنى للأمن السيبرانى(NCSC) فى المملكة المتحدة تفاصيل حول نشاط مجموعة تعرف باسم"APT29"تستهدف العديد من مراكز الأبحاث فى المملكة المتحدة وكندا والولايات المتحدة،وتعمل بشكل شبه مؤكد كجزء من خدمات المخابرات الروسية ،كما تعتمد على مجموعة من الأدوات منها البرامج الضارة المخصصة المعروفة باسم WellMess وWellMail،وذلك فقًا للتصريحات الصادرة عن المركز الوطنى للأمن السيبرانى(NCSC) ،مستندةً فى

ذلك على تقارير صادرة من قبل شركاء في المؤسسة الكندية لأمن الاتصالات (CSE) ووزارة الأمن الداخلي الأمريكية (DHS) ووكالة أمن البنية التحتية للأمن السيبراني (CISA) ووكالة الأمن القومي الأمريكية.هذا بالاضافة الى ماتعرضت له وكالة الصحة الأمريكية فى السادس عشر من مارس الماضى لهجوم سيبرانى أدى الى تعطل شبكاتها الداخلية[٢٧]،وكذا أيضا العديد من مراكز الأبحاث الاسرائيلية،والتى تسعى لانتاج لقاح لفيروس كورونا سبق وأن تعرضت لهجمات الكترونية حاولت اتلاف عملية تطوير اللقاح ،لكنها لم تنجح فى ذلك،وذلك وفق مانشرته صحيفة"جيروزالم بوست"الاسرائيلية، وفى الثالث عشر من مارس من

العام الجارى ،أفاد مستشفى برنو الجامعى فى جمهورية التشيك أنه تعرض لهجوم سيبرانى (برمجيات الفدية)ترتب عليه الغاء العديد من العمليات الجراحية وتحويل المرضى الجدد الى مستشفيات قريبة،وبالتالى احداث خسائر مادية[٢٨].هذا وقد استغلت أيضاً العديد من التنظيمات الارهابية وعلى رأسهم "داعش" انشغال العالم بهذه الأزمة"أزمة فيروس كورونا" فى بث خطابات الكراهية والآراء المتطرفة عبر مواقع التواصل الاجتماعى ،فقد سعى تنظيم "داعش" الى توظيف هذه الأزمة بشكل دينى ،مدعياً أن هذا الفيروس يمثل عقاباً من الله ،وأن السبيل الوحيد للخلاص منه هو تنفيذ العديد من العمليات الارهابية ، وكذا أيضاً تنظيم القاعدة ، والذى سار على نفس نهج تنظيم "داعش"من حيث اعتبار الجائحة نصراً الهياً من الضرورى استغلاله بتكثيف العمليات الارهابية ،وذلك وفقاً للتقرير الصادر عن مرصد الأزهر لمكافحة التطرف فى الخامس والعشرين من شهر مارس الماضى ، والذى كشف عن تزايد العمليات الارهابية التى قام بها تنظيم القاعدة فى دولتى الصومال وكينيا لتصل الى ١٣٧ عملية[٢٩].كما سعت جماعة (الاخوان) وفق ما أعلن عنه مرصد الفتاوى التكفيرية والآراء المتشددة التابع لدار الافتاء المصرية فى الواحد

والعشرين من شهر سبتمبر الجارى الى استحداث كيانات الكترونية ، وذلك بهدف نشر الأفكار المتطرفة والدعوة للتظاهر وتجنيد عناصر جدد،وذلك من خلال استغلال تواجد الشباب فى المنازل ،وقضاء المزيد من الأوقات فى تصفح الانترنت ومواقع التواصل الاجتماعى .هذا بالاضافة الى ماقامت به هذه الجماعة من انشاء قنوات مغلقة عبر تطبيق التليجرام وذلك بهدف تكليف الأفراد بأدوار محددة لنشر الفوضى وتقويض قدرة الدولة على البناء والتنمية [٣٠].

وهكذا يتضح لنا بعد استعراض الأنماط الجديدة من الهجمات الالكترونية فى ظل أزمة فيروس كورونا الى أى مدى ساهمت هذه الأزمة فى تغيير طبيعة هذه الهجمات ،وزيادة أعدادها،وخلق بيئة مناسبة لتنامى التطرف وتصاعد خطر الارهاب فى المنطقة والعالم.فمن المتوقع أن تزيد حدة الصراعات بين الدول .فقد سعت الدول الى شن العديد من الهجمات الالكترونية وذلك بهدف الترهيب أو التأثير فى الدول المستهدفة ،والقضاء على بنيتها التحيتية ومؤسساتها الحيوية ، وكذا أيضا الضغط على قادة حكومات الدول، كما قد تضطر الدول الى خفض انفاقها الأمنى خاصةً فى ظل بروز مفهوم جديد للأمن القومى ، والذى أصبح يتضمن عناصر ومكونات جديدة تتمثل فى توفير مخزون سلعى ومنشأت طبية مزودة بآلالات وكودار طبية قادرة على التعامل مع الأزمة ، مع تفعيل دور القطاع الخاص ليشارك حكومات الدول فى النهوض باقتصاديات الدول.موجهةً مواردها الى معالجة المشكلات الاجتماعية والاقتصادية والأمنية التى تواجهها، وذلك باستثمار هذه الموارد فى القطاعات الحيوية كالصحة ومراكز الأبحاث ومؤسسات الأمن السيبرانى ،وغيرها من القطاعات التى تعتبر بمثابة خط الصد الأول فى مواجهة هذا الوباء ، فقد ضاعف انتشار وباء فيروس كورونا أهمية أمن الفضاء السيبرانى ، والذى أصبح من أهم الأدوات التى تعتمد عليها الدول فى مواجهة تداعيات هذا الفيروس ،حيث قام مكتب الاتصالات الحكومية البريطانية بالتعاون مع دوائر

الاستخبارات البريطانية فى تأمين التطبيقات الرقمية لمؤسسات الصحة العامة،وبينما تمكنت عدد من حكومات دول مثل الولايات المتحدة الأمريكية والمملكة المتحدة والصين وروسيا واليابان وكندا وغيرها من الدول من أن تمتلك بنية تحتية جيدة ، وأن تضع خططاً طارئة لحماية فضاءاتها الرقمية ضد التهديدات المحتملة.هناك دول ماتزال تفتقر الى بنية تحتية وكوادر مدربة قادرة على مواجهة التهديدات المصاحبة لأزمة فيروس كورونا(٣١).

كما أتاحت التداعيات التى ترتبت على هذه الجائحة"كوفيد –١٩" فى العديد من دول العالم من تعليق الأنشطة الثقافية والترفيهية ،واغلاق المدارس ،والتعليم عن بعد فرصاً للتنظيمات المتطرفة لنشر أفكارها الهدامة من خلال استغلال تواجد الشباب فى المنازل ،وقضاء المزيد من الأوقات فى تصفح الانترنت ومواقع التواصل الاجتماعى ، والبحث عن فئات جديدة واقناعها بأفكار هذه الجماعات ،خاصة فى المجتمعات الغربية التى كانت الأكثر تضرراً من هذا الوباء.ففى الفلبين على سبيل المثال ،استغل تنظيم داعش الاغلاق التام للبلاد لاحتواء تفشى هذا الوباء ،لنشر الأفكار الهدامة وتجنيد أعضاء جدد ،خاصةً فى المناطق الريفية الأكثر تضرراً من عمليات الاغلاق(٣٢).

الأمر الذى يستوجب تعاون الدول وتكاتفها مع بعضها البعض لمواجهة هذه الأزمة، فقد كشفت هذه الأزمة عن هشاشة وضعف التحالفات والتنظيمات الاقليمية .فمثل هذه التحالفات تنهض على فكرة التعاون والتضامن بين الدول ،الا أنه مع تفشى فيروس كورونا أخذت هذه التحالفات ومنها الاتحاد الأوروبى سلوكاً مغايراً،فقد قامت الدول الأوروبية باغلاق الحدود فيما بينها ،وأخذت تتنافس على الحصول على المساعدات الطبية من الصين ،فقد استولت التشيك على كمامات قادمة من الصين، كما رفضت الدول الأعضاء تقديم مساعدات لايطاليا ،الأمر الذى أثار امتعاض المواطنيين الايطاليين من أسلوب تعامل

الدول الأوروبية مع ايطاليا خلال هذه الأزمة [٣٣].لذا شكلت هذه الأزمة تحدياً عالمياً يقتضى تضافر الجهود بين الدول ،وكذا أيضا التعاون بين كافة القطاعات داخل الدولة الواحدة لمواجهة هذه الأزمة والتغلب عليها.

المحور الرابع: الجهود الدولية فى مكافحة الارهاب الالكترونى

مع بداية التسعينات ،شهد العالم ثورة فى مجال الاتصالات ، وبدأ الجميع يسعون الى توظيف مثل هذه التقنيات الحديثة فى الكثير من المجالات السياسية والاقتصادية والاجتماعية ، كما بدأت الجماعات الارهابية وبعض الدول والفاعلين من غير الدول فى توظيف واستخدام هذه الأدوات التكنولوجية الحديثة ولكن بشكل سيء، الأمر الذى ترتب عليه تهديد للسلم والأمن الدوليين، وفرض العديد من التحديات التى أصبحت تواجه المجتمع الدولى ، منها طبيعة الجرائم الالكترونية والتى تتميز بأنها جرائم عابرة للحدود تعتمد على استخدام الكمبيوتر والانترنت بدلاً من استخدام الأسلحة التقليدية كالقنابل والصواريخ فى اختراق قواعد البيانات وتدمير البنى التحتية والمنشآت الحيوية للدول .هذا بالاضافة الى صعوبة تعقب مرتكبى الجريمة ، وعدم وجود تشريعات قانونية تُجرم مثل هذه الأعمال الغير مشروعة ،فقد ناقش الانتربول الدولى عام ١٩٨١ امكانية وضع تشريع قانونى لمواجهة الهجمات الالكترونية الأن التشريعات القانونية الصادرة لمواجهة مثل هذه الهجمات جاءت لتعبر عن جهود فردية وليست جهود جماعية ،فقد سعت الدول التى واجهت العديد من الأخطار الالكترونية الى سن تشريعات قانونية لمواجهة الهجمات الالكترونية ،هذا بالاضافة الى اجراءات الحماية التى اتخذتها لمنع اختراق أنظمة المعلومات الخاصة بها،ففى عام ١٩٩٧ ،قامت مجموعة الثمانى الصناعية بإنشاء مجموعة فرعية للجريمة بتقنيات عالية ،وأصبح الهدف هو منع الجرائم الالكترونية على مستوى العالم ، وبعد أحداث الحادى عشر من سبتمبر ،

قام البنتاجون بوضع خطة بعنوان " خريطة طريق لعمليات المعلومات" والتى تهدف الى مراقبة الانترنت ، وفى أكتوبر عام ٢٠٠١،قام الرئيس بوش بتعيين ريتشارد كلارك مستشار للأمن الرقمى ، كما تم انشاء مكتب الأمن للفضاء الالكترونى .وفى عام ٢٠٠٢،قامت الولايات المتحدة بإنشاء المركز القومى لحماية البنية التحتية NIPC ، ومركز تحليل وتبادل المعلومات ISACs[٣٤]،وفى عام ٢٠١٤، أعلنت الولايات المتحدة عن خطة للتحالف المعلوماتى مع الدول العربية والغربية لمواجهة جرائم الارهاب الالكترونى .هذا وقد قامت السعودية فى مارس ٢٠٠٧ بإصدار قانون خاص بمكافحة جرائم الارهاب الالكترونى، كما انضمت الى الاتفاقية العربية لمكافحة مثل هذا النوع من الجرائم ، والتى تهدف الى تكاتف الدول العربية مع بعضها البعض من أجل مكافجة الجرائم الالكترونية ،بالاضافة الى الجهود المبذولة من قبل وزارات الدولة ، فقد اقترحت وزارة الاتصالات السعودية الاستراتيجية الوطنية لأمن المعلومات الخاصة بالمملكة العربية السعودية فى عام٢٠١١،والتى تهدف الى تأمين أنظمة المعلومات منعاً لاختراقها ودعم البنية التحتية وخدمات الحكومة الالكترونية بالمملكة ،كما سعت وزارة الداخلية ووزارة العدل وغيرها من الوزارات الأخرى الى بذل المزيد من الجهود للتصدى لهذه الجرائم الالكترونية .الا أن الأمر لم يقتصر فقط على الجهود الحكومية ،بل لعبت مؤسسات المجتمع المدنى دوراً هاماً فى مكافحة الجريمة من خلال العديد من الشركات المتخصصة فى مجال البرمجيات الخبيثة كشركة سيسكو،وشركة سيمانتك.

أما مصر ، فقد اتخذت العديد من الاجراءات القانونية والخطوات التنفيذية لمكافحة الجرائم الالكترونية ، فعلى الصعيد القانونى ، نصت المادة ٣١ من الدستورالمصرى عام ٢٠١٤ على " أمن الفضاءالمعلوماتى جزء أساسى من منظومة الاقتصاد والأمن القومى وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذى ينظمه القانون"،كما انضمت مصر أيضاً الى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

.هذا بالاضافة الى القانون المصرى لمكافحة جرائم الارهاب الالكترونى ، والذى حدد العقوبة وفقا لطبيعة الجريمة وحجم تهديدها للأمن القومى للدولة[٣٥] .

كما نظمت دولة الامارات المؤتمر الدولى لتجريم الارهاب الالكترونى عام ٢٠١٧،وذلك بهدف تعزيز وترسيخ قيم التعاون بين الدول وذلك للتصدى لهذه الظاهرة . وفى الثانى والعشرين من شهر يوليو الماضى ،قامت دولتى اسرائيل والهند بتوقيع اتفاقية تعاون فى مجال الأمن السيبرانى لمواجهة أى هجوم الكترونى قد تتعرض له الدولتين ، اذ أعلنت اسرائيل استعدادها لتقديم خبراتها للهند فى هذا المجال ،ورغبتها فى الاستفادة من خبرات الهند فى التعامل مع التهديدات السيبرانية .

الا أن هذا الاتفاق ليس الاتفاق الأول الذى أبرمته اسرائيل فى ظل هذه الجائحة"جائحة كورونا" ، فقد سبق وأن أبرمت اسرائيل اتفاق مع رومانيا شهد تعاون بين البلدين فى مجال الأمن السيبرانى[٣٦] .

وهكذا يتضح لنا بعد استعراض الجهود الدولية المختلفة فى مكافحة جرائم الارهاب الالكنرونى أن التشريعات القانونية الصادرة لمواجهة مثل هذه الهجمات جاءت لتعبر عن جهود فردية وليست جهود جماعية ، ومن ثم فإن المجتمع الدولى فى حاجة الى تكاتف وتضافر الجهود الجماعية لسن تشريعات دولية رادعة وقادرة على مواجهة جرائم الارهاب الالكترونى.

خاتمة الدراسة :

تُعد أزمة فيروس كورونا من أبرز التحديات التى تواجه دول العالم الآن ،فقد خلقت هذه الأزمة نوع جديد من التهديدات تجسدت فى فيروسات سريعة الانتشار،كما فرضت حالة من الارتباك وعدم اليقين بشأن آليات التعامل مع هذه الأزمة ،وكيفية وقف انتشار العدوى وطرق الوقاية والعلاج .الا أن هذه الأزمة لم تثن بعض الدول عن شن العديد من الهجمات الالكترونية على مراكز الأبحاث التى تسعى لانتاج لقاح

لفيروس كورونا ، وكذا أيضا التنظيمات المتطرفة عن ممارسة أعمالها الارهابية.فقد استغلت هذه التنظيمات انشغال العالم بهذه الأزمة وقامت بنشر أفكارها الهدامة ،وبث خطابات الكراهية عبر مواقع التواصل الاجتماعى .الأمر الذى شكل تهديدا للسلم والأمن الدوليين ،ورسم تصوراً جديداً للبيئة الأمنية على المستويات المحلية والاقليمية والدولية.

لذا سعت الباحثة فى اطار هذه الدراسة الى تسليط الضوء على ظاهرة الارهاب الالكترونى نظرا لخطورة هذه الظاهرة ،ومالها من تداعيات على السلم والأمن الدوليين، وذلك من خلال تحديد المقصود بهذا المفهوم ،وأسبابه ،وخصائصه ،وطبيعة جرائم الارهاب الالكترونى ، والتى تأثرت بأزمة فيروس كورونا ،تلك الأزمة التى أودت بحياة الملايين من البشر،وساهمت فى بروز مفهوم جديد للأمن القومى يتضمن العديد من المكونات منها:توفير مخزون استراتيجى من السلع،ومنشأت طبية مزودة بكوادر طبية قادرة على التعامل مع هذه الأزمة ، فضلاً عن التداعيات الخطيرة لتلك الأزمة على تلك الأصعدة السياسية والاقتصادية والاجتماعية.الأمر الذى يؤكد على أهمية العمل الجماعى والتعاون الاقليمى والدولى لتعزيز قدرات الدول الأكثر تضرراً على تجاوز آثار هذه الجائحة.

- **وفى النهاية ، تخلص الدراسة الى عدد من النتائج :**

١- الارهاب الالكترونى من أخطر الظواهر التى تواجه المجتمع فى عالمنا المعاصر نظراً لما تتميز به هذه الظاهرة من خصائص ، من أهمها :سهولة التطبيق ، اذ يعتمد على استخدام الكمبيوتر والانترنت فى تنفيذ الهجمات الالكترونية ،وصعوبة تحديد مرتكب الجريمة بالاضافة الى طبيعة الجريمة الالكترونية العابرة للحدود .الأمر الذى يترتب عليه تهديد لأمن واستقلال الدول ، وتدخل فى شئونها الداخلية.

٢- تحول الفضاء الالكترونى الى ساحة للصراع تحركه دوافع سياسية ، ويتميز بنمطين:نمط عنيف توظف فيها القوة الغير تقليدية فى تنفيذ مثل هذا النوع من الهجمات الالكترونية والتى من شأنها أن تُحدث تدمير للبنى التحتية ، واختراق لأنظمة المعلومات ، ونمط آخر يتسم بطبيعته المرنة والتى تتمثل فى الصراع والتنافس حول الحصول عل المعلومات والترويج لأفكار متطرفة واثارة الفتن واحداث اضطرابات داخل الدول .اذ أصبح المصدر الرئيسى للقوة فى الحصول على أكبر قدر من المعلومات وامتلاك أحدث التقنيات فى مجال التكنولوجيا.

٣- تُعد أزمة فيروس كورونا من أبرز التحديات التى تواجه دول العالم الآن ، فقد خلقت نوع جديد من التهديدات تجسدت فى فيروسات سريعة الانتشار أودت بحياة الملايين من البشر ، وساهمت فى احداث نوع من الركود الاقتصادى عانت منه الكثير من دول العالم.

٤- لم تثن جائحة كورونا بعض الدول والتنظيمات المتطرفة عن ممارسة الأعمال الارهابية ،فقد قاموا بشن العديد من الهجمات الالكترونية بهدف التأثير فى الدول المستهدفة وتدمير بنيتها التحتية ومؤسساتها الحيوية ،ونشر الأفكار الهدامة ،وجذب أكبر عدد من المؤيدين لهذه الأفكار لنشر الفوضى وزعزعة أمن واستقرار البلاد.

٥- الجهود الدولية المبذولة لمكافحة جرائم الارهاب الالكترونى مازالت جهود فردية لم ترق الى جهود جماعية ،وبالتالى نحن فى حاجة الى تضافر الجهود والتأكيد على أهمية العمل الجماعى لسن تشريعات دولية رادعة وقادرة على مواجهة جرائم الارهاب الالكترونى.

هوامش الدراسة:

١) من هذه الدراسات :خليل حسن ،"ذرائع الارهاب الدولى وحروب الشرق الأوسط الجديد"،(لبنان:منشورات الحلبى الحقوقية ،٢٠١٢).د.شاكر ظريف،"اشكالية العلاقة بين ظاهرة الارهاب العابر للحدود والجريمة المنظمة":قراءة مقارنة فى الوسائل والأهداف"،مجلة الباحث للدراسات الأكاديمية،جامعة مستغانم، العدد الحادى عشر،٢٠١٧.فتوح أبو الدهب هيكل،"التدخل الدولى لمكافحة الارهاب وانعكاساته على السيادة الوطنية"،(الامارت العربية المتحدة:مركز الامارات للدراسات والبحوث الاستراتيجية،٢٠١٤).

٢) من هذه الدراسات: د.عادل عبد الصادق ،"الارهاب الالكترونى:القوة فى العلاقات الدولية – نمط جديد وتحديات مختلفة"،(القاهرة : مركز الدراسات السياسية والاستراتيجية ،٢٠٠٩).

-Matthew Lippman,"Terrorism &Counter terrorism":Theory, History and Contemporary Challenges",(Chicago: University of Illinois,2019).

٣) من هذه الدراسات: محمد أمين الشوابكة ،"جرائم الحاسوب والانترنت– الجريمة المعلوماتية "،(عمان:دار الثقافة للنشر والتوزيع،٢٠٠٧).

-توفيق مجاهد ،طاهر عباسه،"جريمة الارهاب الالكترونى فى ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠،مجلة العلوم القانونية والسياسية ،المجلد ٩ ،العدد ٣،ديسمبر ٢٠١٨،متاح على الرابط:- https://www.asjp.cerist.dz/en/article/72222

٤) من هذه الدراسات:

-أمين فرج يوسف،"الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت"،(الاسكندرية :مكتبة الوفاء القانونية ،٢٠١١).

-على عدنان الفيل،"الارهاب الالكترونى"، مجلة الجامعة الخليجية ،جامعة الموصل ،المجلد٢،العدد ٢،٢٠١٠.

-جيهان عبد السلام عوض،"أمريكا والربيع العربى:خفايا السياسة الأمريكية فى المنطقة العربية"،(القاهرة:العربى للنشر والتوزيع،٢٠١٩).

٥) من هذه الدرسات:

-خالد عباس طاشكندى ،"الارهاب الالكترونى .. <<استراتيجية الملالى>> فى أزمة كورونا،٢٢مايو ٢٠٢٠ ،متاح على الرابط:

https://www.okaz.com.sa/news/politics/2025307-

-د.مروة نظير،"كيف تستغل الجماعات الارهابية جائحة كورونا؟"،٢٦-٤-٢٠٢٠،متاح على الرابط:

https://futureuae.com/arMainpage/Item/5543/%D9%85%D8%B3%D8%A7%D8%B1%D8%A7%D8%A

-بريطانيا تتهم روسيا بتدبير هجمات الكترونية لسرقة أبحاث لقاح فيروس كورونا،١٦-٧-٢٠٢٠، متاح على الرابط:

https://arabic.cnn.com/world/article/2020/07/16/russian-cyber-attackers-targeting-organizationsinvolved-in-coronavirus-vaccine.

٦) مسعد عبد الرحمن زيدان،"الارهاب فى ضوء القانون الدولى العام"،(بيروت:دار الكتاب القانونى ،٢٠٠٩)،ص٤١.
٧) حيدر على نورى،"الجريمة الارهابية:دراسة فى ضوء قانون مكافحة الارهاب"،(لبنان:مكتبة زين الحقوقية والأدبية،٢٠١٢)،ص٥٦.
٨) أحمد عطيه،"القاموس السياسى"،(القاهرة:دار النهضة العربية،١٩٧٥)،ص٤٥.
٩) سامر مؤيد عبد اللطيف ونورى رشيد الشافعى،"دور المنظمات الدولية فى مكافحة الارهاب الرقمى"،بحث مقدم بجامعة كربلاء،٢٠١٦، متاح على الرابط: http://www.elearning.uokerbala.edu.iq/mod/resource/view/php
١٠) –المادة الأولى من اتفاقية جنيف لقمع الارهاب لعام ١٩٣٧.
١١) المادة الأولى من الاتفاقية العربية لمكافحة الارهاب لعام ١٩٩٨.
١٢) سامر مؤيد عبد اللطيف ونورى رشيد الشافعى،المرجع نفسه ، ص ٤.
١٣) سامر بن عبد الرحمن بن عبد الله السند،"وسائل الارهاب الالكترونى حكمها فى الاسلام وطرق مكافحته، متاح على الرابط:
www.assakina.com/files/book/book8
١٤) سامر مؤيد عبد اللطيف ونورى رشيد الشافعى،المرجع نفسه ،صفحة ٤.
١٥) أحمد ناصر أبو السعود،مفهوم الارهاب الالكترونى،٢٠١٧/١٠/١٠،متاح على الرابط:
http://political-encyclopedia.org-
١٦) pontara,G."The concept of violence", Journal of peace research,vol15,No1,1978,pp19-32.
١٧) Stefan Soesanto," Cyber Terrorism. Why it exists, why it doesn't, and why it will",17-4-2020
i. Available at:- http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?,
١٨) شريخى توفيق،"الارهاب الالكترونى وتأثيره على أمن الدولة "،رسالة ماجستير، الجزائر،جامعة محمد بو ضياف مسيلة،٢٠١٨،ص ١٥. انظر أيضاً:
Gabriel Weimann,"Cyper terrorism :How Real is the Threat",Special Report 119,UNITED STATES INSTITUTE OF PEACE,December 2004,Available at:WWW.Usip.org.
Gabriel Weimann ," Terror on the Internet: The New Arena, the New Challenges",(Washington.: United States Institute of Peace Press,2006), pp. 37-38
١٩) أمين فرج يوسف،"الجريمة الالكترونية المعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت"،(الاسكندرية:مكتبة الوفاء القانونية ،٢٠١١)،ص٢٢٤.
٢٠) خالد المهيرى ،"جرائم الكمبيوتر والانترنت والتجارة الالكترونية "،(دبى : معهد القانون الدولى ،٢٠٠٤)،ص١٨٥-١٨٦.

٢١) Janet J. Prichard and Laurie E. MacDonald," Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks ", Journal of Information Technology Education,USA, Bryant University,Vol3,2004,pp280-281.

٢٢) ايهاب خليفه،"القوة الالكترونية...كيف يمكن أن تدير الدول شؤونها فى عصر الانترنت:الولايات المتحدة نموذجاً،(القاهرة:العربى للنشر والتوزيع،٢٠١٧)، ص ١٠-١٣.

٢٣) جيهان عبد السلام عوض،"أمريكا والربيع العربى:خفايا السياسة الأمريكية فى المنطقة العربية"،(القاهرة:العربى للنشروالتوزيع،٢٠١٩)،ص ٧١-٧٢.

i. Babak Akhgar,Hamid R.Arabnia,"Emerging Trends in ICT Security",(U.S.A: Morgan kaufmann,2013)Available at: https://www.sciencedirect.com/topics/computer-science/cyber-attack.

٢٤) TimothyL.Thomas," Nation – state Cyber strategies:Examples from china and Russia", Cyber power and National Security,(Washington D.C :National defense University,May2009),pp465-470.

٢٥) حسن مظفرالرزو،"مجاميع القرصنة والميلشيات الايرانية الرقمية"،(الرياض:المعهد الدولى للدراسات الايرانية،٢٠١٩)،ص ٢٢٠-٢٢٢.

٢٦) رانيا سليمان،فاتن فايز وآخرون ،سياسات مكافحة الإرهاب الإلكتروني .. مصر والسعودية نموذجاً،المركز العربى للبحوث والدراسات،٢ فبراير ٢٠٢٠ ،متاح على الرابط:
- http://www.acrseg.org/41483

انظر أيضا:

Madhian, B., & Majed, M. , "Saudi Arabia's counterterrorism methods: A case study on homeland security", (United States :Naval Postgraduate School Monterey,2017),P. 44.

Mitko Bogdanoski," Cyber terrorism –Global Security Threat", International Scientific Defence, Security and Peace JOURNAL,21-5-2014,Available at: file:///D:/Documents/Downloads/CYBERTERRORISMGLOBALSECURITYTHREAT.pdf

٢٧) بريطانيا تتهم روسيا بتدبير هجمات الكترونية لسرقة أبحاث لقاح فيروس كورونا ،١٦ يوليو ٢٠٢٠،متاح على الرابط:
https://arabic.cnn.com/world/article/2020/07/16/russian-cyber-attackers-targeting-organizations-involved-in-coronavirus-vaccine

انظر أيضا:

Naveen Goud," Cyber Attack on Britain Universities for COVID 19 Medicine and Vaccine – Avaliable at: https://www.cybersecurity-insiders.com,"documents

٢٨) د.عادل عبد الصادق،"كورونا ...فيروس الكترونى"،جريدة الخليج،١٦-٤-٢٠٢٠،متاح على الرابط:

http://www.alkhaleej.ae/supplements/page/4faa1df0-091e-4f50-8c03-cfb721dd1ca9

٢٩) د.مروة نظير،"كيف تستغل الجماعات الارهابية جائحة كورونا"،مركز المستقبل للأبحاث والدراسات المتقدمة ، ٢٦-٤-٢٠٢٠،متاح على الرابط:https://futureuae.com/ar-AE/Mainpage/Item/5543 .-

انظر أيضاً:

-وليد عبد الرحمن ،"مفردات خطاب تنظيمات الارهاب فى "زمن كورونا"..تحريض واستغلال للدين أملاً فى صعود كاذب"،الشرق الأوسط ،٧أبريل ٢٠٢٠،متاح على الرابط:

https://aawsat.com/home/article/2220516)

٣٠) مرصد الافتاء:جماعة الاخوان الارهابية تسعى لنشر الفوضى فى مصر عبر الارهاب الالكترونى،جريدة الرواق،٢٢ سبتمبر ٢٠٢٠،متاح على الرابط:

https://alruwaq.com/35875-

٣١) مهند سلوم،"الأمن الوطنى فى زمن جائحة فيروس كورونا"، المركز العربى للأبحاث ودراسة السياسات،١٣-٧-٢٠٢٠،متاح على الرابط:

.https://www.dohainstitute.org/ar/PoliticalStudies/Pages-

٣٢) د.أشرف العيسوى،"التنظيمات المتطرفة والتوظيف الدينى ل"كوفيد -١٩":الأبعاد والتداعيات المحتملة على الارهاب الدولى"،٦يوليو ٢٠٢٠ الرابط: متاح علىhttps://trendsresearch.org/ar/insight

٣٣) د.أشرف كشك،"أزمة كورونا..التداعيات والآليات التى انتهجتها الدول لادارة الأزمة"،تقريرصادر عن مركز البحرين للدراسات الاستراتيجية والدولية والطاقة ،أبريل ٢٠٢٠،متاح على الرابط:-http://www.akhbar alkhaleej.com/news/article/1206828

٣٤) عادل عبد الصادق ، مرجع سبق ذكره،ص ٣٤٧-٣٤٩.

٣٥) رانيا سليمان،فاتن فايز،نهى الدسوقى ،مرجع سبق ذكره.

36) -Jessica Haworth," Israel and India sign cybersecurity agreement to protect against Covid-19 cyber-attacks",The Daily Swig:Cyper securitynews and views,22-7-2020, Available at :- https://portswigger.net/daily-swig/israel-and-india-sign-cybersecurity-agreement-to-protect-against-covid-19-cyber-attacks.

****