.

الحرب السيبرانية التهديدات وسبل المواجهة

Cyber warfare: threats and ways to confront them

أ.رشيد رحومة الرعاش

محاضر - كلية القانون- جامعة صبراتة

ملخص

إن التطور الذي ظهر مؤخرا نسبياً من ثورة المعلومات، وظهور الإنترنت قد خلف بيئة جديدة خاصة في توسيع نطاق العمليات الحربية العسكرية لتشمل الفضاء السيبراني، أو ما يسمى (المجال الخامس للحرب بجانب البر، والبحر، والجو، والفضاء)، وعلى الرغم من عدم وجود خلاف عمومًا على أن ثورة المعلومات، وظهور الأنترنت أصبح شيء أساسي لنهوض العالم وفق الجانب الإيجابي، إلا انه أصبح هذا التطور يؤثر في النظام العالمي بين الدول خاصة بعد بروز شكل جديد من الحرب هي الحرب السيبرانية المستحدثة، مما جعل الفضاء السيبراني مجالا جديدا للصراع بين دول العالم، بل من أخطر التحديات الأمنية التي تواجه كافة مجتمعات العالم في مجال استخدام تقنية المعلومات، ومصدر خطورة على الأمن القومي، وعلى الأمن والسلم الدوليين ومن خلال هذه الورقة البحثية سأتناول إن شاء الله ماهية الجرائم السيبرانية، وأيضاً سأتطرق لتداعيات الحروب السيبرانية، ومظاهر استهداف الأمن القومي الذي يحدث بسبب التفاعلات والتغيرات السياسية الدولية، وأيضا إيضاح أمثلة واقعية ستحداث الجرائم السيبرانية وزيادة معدلاتها.

الكلمات المفتاحية : الانترنت ، الجريمة، السيبراني ، التهديد.

Abstract

The relatively recent development of the information revolution and the emergence of the Internet have created a new environment, especially in expanding the scope of military warfare operations to include cyberspace, or what is called (the fifth domain of war alongside land, sea, air, and space). Although there is no general disagreement that the information revolution and the emergence of the Internet have become ، It is essential for the world to rise in a positive direction, but this development has begun to affect the global system between countries, especially after the emergence of a new form of war, which is the newly developed cyber war, which has made cyberspace a new area of conflict between the countries of the world, and even one of the most dangerous security challenges facing all societies of the world in the field of using information technology, and a source of danger to national security, and to security and peace ، Internationally, through this research paper, I will address the nature of cybercrimes, and I will also address the repercussions of cyber wars, and the manifestations of targeting national security that occur due to international political interactions and changes, and also clarify real examples of the emergence of cybercrimes and the increase in their rates.

Keywords: Internet, crime, cyber, threat.

مقدمــة

مما لا شك فيه أن العالم أصبح يعانى من مشكلات عالمية أفرزتها البيئة الرقمية، بيد أن هذه المشكلات أصبحت مسار للبحث والدراسة لا سيما في مجال علم الاجتماع مثل الغزو الثقافي الرقمي، والجريمة السيبرانية، والابتزاز، والتنمر، الإلكترونيين... إلخ، وفى ضوء هذه البيئة المتغيرة، توجد حاجة ملحة لاتخاذ إجراءات – على الصعيدين المحلى والدولي – لحماية الاستهلاك والخصوصية، ومجابهة تقنية المعلومات ضد جميع أشكال الجريمة السيبرانية، وهذا ما دعا لإعداد البحث الراهن، ففي ظل ما يشهده العالم من تطور سريع ومتزايد في النظم الذكية والأجهزة الإلكترونية، وما صاحبهما من هجمات، وجرائم سيبرانية دعت ضرورة ملحة لنشر دعائم الأمن السيبراني، وتأمين سلامة الممارسة الإلكترونية.

كانت ثورة المعلومات وظهور الإنترنت إيذاء بزوغ العصر السيبراني، وخلق بيئة جديدة هي الفضاء السيبراني (الفضاء الخامس) إضافة إلى الأرض، والبحر، والجو، والفضاء الذي أصبح يؤثر في النظام الدولي، خاصة مع بروز شكل جديد من القوة هي القوة السيبرانية التي توزعت وانتشرت بين عدد أكبر من الفاعلين على المستوى الدولي والمحلي، ما جعل الفضاء السيبراني مجال جديداً للصراع بين الدول، وبالتالي حاولت من خلال هذه الورقة البحثية إظهار الانعكاسات التي أحدثها الفضاء السيبراني على التحولات في مفهوم القوة و الصراع، ومن خلال التحول من الصراع المادي إلى الصراع الافتراضي، وهو ما أدى باهتمام الدول إلى أمنة الفضاء السيبراني.

أولاً- أهمية البحث

تنبثق أهمية الدراسة من أهمية التحديات الأمنية، والتقنية، والقانونية المصاحبة لاستخدامات تقنية المعلومات والحاسب الآلي، والإنترنت ومن خطورة الوضع الراهن للجريمة الإلكترونية على البنيات التحتية لأنظمة تقنية المعلومات، والاتصالات، وتهديد الاختراقات، والهجمات المستمرة لكل المصالح على نطاق مؤسسات القطاع العام

والخاص والأفراد، مما حيتم ضرورة إيجاد المعالجات، والحلول العلمية والعملية للحماية من الجريمة ، والحد من ارتفاع معدلاتها وآثارها التي أكدتها كل الدراسات المتخصصة التي دقت ناقوس الخطر، وفى تصوري إن أي بحث أو دراسة في المجال السيبراني هي دراسة مهمة.

ثانيا- منهجية البحث

تعتمد الدراسة في الوصول إلى نتائجها على المنهج الوصفي التحليلي، من خلال تحليل وتحديد ماهية ظاهرة الجريمة الإلكترونية/ وطبيعتها، وأسبابها، واتجاهاتها، وآثارها وأفضل الوسائل والمعالجات لمواجهتها، وإيجاد الحلول لها وتسليط الضوء على تداعيات الحروب السيبرانية.

ثالثا- إشكالية البحث

تكمن مشكلة البحث في تفاقم الجريمة الإلكترونية وتعدد أنواعها وازدياد حجمها وأضرارها حيث أصبحت خسائرها مهددا لأمن المعلومات في كافة المجالات العامة والحيوية بالقطاع العام والخاص والأفراد، بل مصدر خطورة على الأمن القومي وعلى السلم والأمن الدوليين بسبب استخدام الإنترنت في النشاطات الإرهابية.

وتشكل العوامل التالية مشكلة البحث وتجعلها أكثر تعقيدا كالتالي: .

- تحديد مفهوم الحرب السيبرانية؟
- ما سبل وآليات المكافحة؟
- ما الأبعاد السياسية التي دعت لوجود الأمن السيبراني؟
- الاستيلاء على المعلومات المحفوظة في الحاسب الآلي أو المنقولة عبر شبكة الإنترنت أو تغييرها أو حذفها أو الغائها نهائيا من النظام؟
- صعوبة مكافحة الجرائم الإلكترونية على المستوى الوطني والدولي بسبب سهولة إخفاء معالم الجريمة وصعوبة الحصول على الدليل المادي؟

رابعا- خطة البحث

وفق هذا الموضوع قسمت دراستي وفق التقسيم الثنائي إلى مطلبين حيث في الفرع الأول ماهية الجرائم السيبرانية بينما تطرقت في المطلب الثاني لتداعيات الحروب السيبرانية على الأمن القومي وذلك وفقا للخطة الآتية: .

- المطلب الأول: ماهية الجرائم السيبرانية.
- الفرع الأول: مفهوم الجريمة السيبرانية.
- الفرع الثاني: أسباب ووسائل مكافحة الجريمة السيبرانية.
- المطلب الثاني: تداعيات الهجمات السيبرانية على الأمن القومي.
- الفرع الأول: المخاطر والتداعيات على تفاعلات السياسية الدولية.
- الفرع الثاني: أمثلة واقعية لاستحداث الجرائم السيبرانية وزيادة معدلاتها.

المطلب الأول

ماهية الجريمة السيبرانية

إن الجرائم السيبرانية من الجرائم التي تباينت تسميتها عبر المراحل الزمنية لتطورها، فكانت بداية من مصطلح إساءة استخدام الكمبيوتر، مروراً بمصطلح احتيال الكمبيوتر، والجريمة المعلوماتية، إلى مصطلح جرائم الكمبيوتر (جار الله عبد العزيز 2017م ص7)، إذا الجرائم المرتبطة بالكمبيوتر، وجرائم التقنية العالية، إلى جرائم الهاكرز، وجرائم الإنترنت، إلى آخره كلها مصطلحات تأتي تحت مسمى (الجرائم السيبرانية).

سنتناول في هذا المطلب مفهوم الجريمة السيبرانية كفرع أول لكي تسهل على كل قارئ معنى هذا المصطلح الحديث مع ذكر بعض المصطلحات المتعلقة بالموضوع، ونتطرق فيما بعد في الفرع الثاني الى أسباب ووسائل مكافحة الجريمة السيبرانية.

الفرع الأول: . مفهوم الجريمة السيبرانية

لم يتفق الفقه الجنائي على تسمية موحدة للجريمة السيبرانية، إذ يطلق عليها البعض بالجريمة السيبرانية، وهناك من يسميها بالجريمة المعلوماتية، ويذهب أخرون إلى تسميتها بجرائم إساءة استخدام تكنولوجيا المعلومات والاتصال، ويطلق عليها آخرون مسمى جرائم الكمبيوتر والإنترنت.

وبما ان إيجاد تعريف للجريمة السيبرانية كان محلا لاجتهادات الفقهاء فقد ذهبوا في ذلك مذاهب مختلفة، ووضعوا تعريفات شتى، وبالتالي فلا نجد تعريفا محددا للجريمة السيبرانية وهناك اختلاف بين الباحثين في تعريف الجريمة السيبرانية، فمنهم من يتناول التعريف من الجانب التقني فنياً، ومنهم من يتناوله من الزاوية القانونية، فالذين يتناولونه من الجانب التقني يذهبون إلى القول بأن الجريمة المعلوماتية ما هي إلا نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود (د. البشري محمد، 21 مايو 2005 ص6).

أما أنصار الاتجاه القانوني فيذهبون إلى أن تعريف الجرائم السيبرانية يتطلب تعريف المفردات الضرورية المتعلقة بارتكاب جرائم الحاسب الآلي وهي (الحاسب الآلي، برنامج الحاسب الآلي، البيانات، الممتلكات، الدخول، الخدمات الحيوية).

وفريق أخر من الفقهاء أيضا يعرف جريمة الحاسب الآلي أو الجريمة السيبرانية بانها الجريمة التي تقع بواسطة الحاسب الآلي، أو عليه، أو بواسطة شبكة الأنترنت (د. سلطان محمد، 2005 ص5).

وتعتبر مهمة ضبط المفاهيم والمصطلحات تحديا يواجه مختلف الباحثين والدارسين في مختلف التخصصات، وذلك لما يطرحه من إشكاليات تجعل من الصعوبة بإمكان الاتفاق على تعريفات واضحة وشاملة وموحدة بين أعضاء المجتمع العلمي، ويعد مصطلح السيبرانية واحداً من المفاهيم المعقدة المستحدثة التي قدمت لها العديد من

التعريفات المختلفة وعلى سبيل الذكر لا الحصر، وللتوضيح للقارئ بعض المصطلحات المتعلقة بالبحث كالتالي: .

- **الفضاء السيبراني**

هو العالم المادي والمفاهيمي الذي توجد فيه جميع هذه الأنظمة (الحواسيب والمعلومات والبرامج والشبكات المفتوحة وغيرها) 3((حمدون توريه، 2011م ص12).

كما عرفته الوكالة الفرنسية لأمن أنظمة الإعلام التي تعد وكالة قطاعية للدولة مكلفة بالدفاع السيبراني الفرنسي بانه هو فضاء التواصل المشكل من خلال الربط البيني لمعدات المعالجة الآلية للمعطيات الرقمية (د. فرحات علاء الدين، 2019م ص 88).

فمسألة تحديد مفهوم الفضاء السيبراني هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل دولة لأمنها القومي.

وفق هذه التعريفات فان الفضاء السيبراني هو عالم جديد لا ينتمي الى علم الجغرافيا أو الى علم التاريخ وهو عالم دون حدود ودون ذاكرة ودون تراث انه العالم الذي تبنيه شبكات الاتصال المعلوماتية الإلكترونية.

- **الأمن السيبراني**

لغوياً: مكون من لفظين: (الأمن، السيبراني)

الأمن: هو نقيض الخوف، أي بمعنى السلام والأمن مصدر الفعل أمن أمنا وأمانا وأمنة: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن من الشر، أي سلم منه، (د. العمارات فارس وآخرون، 2022م ص13).

وقد عرفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يهدد القيم النادرة ويمكن من حيث المبدأ أن يكون الأمن مطلقا، وقد اعتبر الأمن تاريخيا قيمة جوهرية وهدفا أسمى لسلوك الدول (غراهام ايفانز وآخرون، 2004م ص 671).

هذا التعريف يشير إلى أن الأمن يتحقق عندما لا توجد تهديدات للقيم والاهتمامات المهمة مثل السلامة والاستقرار والحرية.

والسيبراني: هي مصطلح السيبرانية الآن، وهو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي وتشير المقاربة الإيتيمولوجية لكلمة "cyber" إلى أنها لفظة يونانية الأصل مشتقة من كلمة "Kubernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي Norbert wleners 1964-1994 " وذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسبرنيتيقية من خلال مؤلفه الشهير": Cybernetics or control and communication in" the Animal and the machine

وأشار في كتابه إلى أن السبرنتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان، والآلة ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب (د. العمارات فارس وآخرون، 2022م ص14).

أما صطلاحياً : هناك العديد من التعريفات التي قدمت لمفهوم الأمن السيبراني، حيث يُعرف بأنه: "مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية، ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة، وأيضا هو القدرة على الدفاع أو الحماية الفضاء السيبراني (الإلكتروني) من الهجمات السيبرانية (إبراهيم عبد الحكيم 2015م ص18).

- **الحرب السيبرانية**

لتعريف الحرب السيبرانية يجب أن نشير إلى معنى الحرب وأهدافها وأجيالها المتعددة، إن جوهر الحرب يدور حول إكراه الخصم على تنفيذ إرادتنا، وذلك عبر أعمال القوة والعنف، ولا شك في أن الهدف الأول للحرب هو هدفها السياسي والذي عادة ما يتحقق بإخضاع إرادة العدو السياسي (فيتز كارل، 1997م، ص 103).

هذه الإرادة التي تتولى الحرب إخضاعها عبر تحطيم الطاقات المادية والمعنوية للعدو المستهدف؛ فالطاقات المادية تتحطم في المعارك الحربية، أما الطاقات المعنوية فتتحطم عبر حرب نفسية تستكمل معارك الميدان الحربي(الخطاب محمود 1973 ص26)

تعريف أخر للحرب أخذ بعض المنظرين الاستراتيجيين إلى اقتراح تعريف آخر لهدف الصراع، وهو تصادم إرادات وقوى خصمين أو أكثر يكون فيه هدف كل طرف من الأطراف تليين إرادة الآخر حتى ينتهي الصراع بما يحقق الأهداف والأغراض الرئيسية للأطراف المتصارعة (هويدي أمين، 1982م، ص 14)، فصار الأمر تليين إرادة الخصم بدلاً من إخضاع إرادته إخضاعاً كاملاً.

وهناك من عرف الحرب السيبرانية بأنها قيام دولة أو فواعل من غير الدول بشن هجوم إلكتروني، يمثل أعمالا عدائية إلكترونية تستهدف البنية التحتية المعلوماتية للدول لتحقيق أغراض متداخلة سياسية واقتصادية وإجراميه وغيرها (عبد الواحد صلاح، 2021م، ص69)

وإن الحرب بمفهومها الحديث شهدت أطواراً عدة، وسموا كل طور منها جيلا بدءا باستخدام القوة البشرية المكثفة كجيل أول، إلى استخدام قوة النيران كجيل ثان، ثم استخدام (المناورات) في الجيل الثالث من الحرب وتجلت في الحرب العالمية الثانية، خاصة من قبل ألمانيا، وأخيرا جاء ما سمي بحروب الجيل الرابع القائمة على استخدام توليفة من الأدوات السياسية والاقتصادية والاجتماعية والنفسية لتحقيق أهداف الحرب (عبد الرحمن شريف 2016م، ص 16.. وانظر شرح مفصل ومطول من منظور آخر في خوري إميل ، 2016م ، ص 29 وما بعدها.).

وبالمواكبة مع هذا الجيل الرابع من الحرب، ظهر ما أطلق عليه الحرب السيبرانية، وهي حرب ولدت من رحم التحولات المتسارعة الناتجة عن الثورة العلمية، والصناعية في مجال الحاسوب، والتطبيقات الرقمية، والإنترنت.

ومن الجانب الدولي لقد حاولت عدة أعمال أكاديمية ضمن اتفاقيات دولية تعريف الجريمة السيبرانية وفي هذا الصدد نذكر اتفاقية مجلس أوروبا للجريمة السيبرانية لعام 2001، تم التوقيع على هذه الاتفاقية 23 نوفمبر 2001 في بودابست وتضم في عضويتها 45 دولة أوربية و17 دولة من خارج أوربا حتى تاريخ 2014/10/5، وعرفت هذه الاتفاقية في الفصل الثاني جرائم الحاسب الآلي بأنها الجرائم ضد السرية، والنزاهة، وتوافر البيانات، وأنظمة الحاسب الآلي في المواد من 2 إلى 12 حيث تم بالترتيب كالتالي: .

أولاً: التعريف الدخول غير المشروع، الاعتراض غير القانوني التدخل في البيانات، التدخل في النظام، إساءة استخدام أجهزة.

ثانياء: الجرائم ذات الصلة بالحاسوب الجرائم المتعلقة بالتزوير، والجرائم المتعلقة بالغش.

ثالثاء: الجرائم المتعلقة بالمحتوى : الجرائم المتعلقة بالمواد الإباحية عند الأطفال.

رابعاً: الجرائم المتعلقة بانتهاك حقوق الطبع والحقوق المجاورة.

خامساً: المسؤولية الإضافية المحاولة، والعون، والتحريض، والمسؤولية المؤسسية في المادة 12 (اتفاقية مجلس أوروبا للجريمة السيبرانية2001 م).

وقد اهتمت الدول والمنظمات الدولية كالأمم المتحدة وغيرها بتعريف الجريمة السيبرانية باعتبارها تشمل طائفة واسعة من الجرائم المرتكبة بدافع مالي والجرائم المتصلة بالمحتوى الحاسوبي، فضلاً عن الأعمال التي تمس بسرية النظم الحاسوبية وسلامتها وقابلية النفاذ إليها بغرض إجرامي. (مكتب الأمم المتحدة المعني بالمخدرات والجرائم دراسة شاملة عن الجريمة السيبرانية مسودة نيويورك 2013م على الموقع https://www.unodc.org/).

الفرع الثاني: . أسباب ووسائل مكافحة الجريمة السيبرانية

لا شك أن مرتكبي الجريمة الإلكترونية يختلفون عن مرتكبي الجريمة التقليدية، ويرجع ذلك لاختلاف الأشخاص من حيث السن، والجنس، والمستوى التعليمي، وغير ذلك من المؤثرات الخارجية، كما أن الأسباب أو الدوافع التي تدفعهم لارتكاب الجريمة هي أيضا تختلف لذلك فان الجريمة الإلكترونية تختلف عن الجريمة التقليدية، تبعا لذلك فإن الأسباب والدوافع التي تدفع الجناة لارتكاب الفعل غير المشروع لها تختلف عن الأسباب والعوامل التي تدفع الجناة لارتكاب الفعل غير المشروع للجريمة التقليدية.

ويأتي في مقدمة أسباب ودوافع الجريمة الإلكترونية ثمة أسباب ودوافع تتمثل في الرغبة أو الولع بجمع المعلومات التي قد تكون محفوظة في أجهزة الحاسب الآلي، أو منقولة عبر الشبكة العالمية للمعلومات، كما قد تكون الأسباب والدوافع الرغبة في الأضرار بالغير من جهات معينة وأشخاص، وكذلك الرغبة في الربح، والكسب الذي قد يدفع إلى التعدي على الحواسيب ونظم المعلومات إضافة إلى دوافع الشخصية للجاني لإبراز الذات التي قد تكون سببا في ارتكاب الجريمة المعلوماتية (http//accronline.com/article-detail.aspx? Id=7509).

- ونذكر بعض من تلك الأسباب والدوافع فيما يلي: .

1. الرغبة في جمع المعلومات وتعلمها.
2. الاستيلاء على المعلومات.
3. قهر النظام وإثبات التفوق على تطور وسائل التقنية.
4. الحاق الأذى بأشخاص أو جهات.
5. تحقيق أرباح ومكاسب مادية.
6. تهديد الأمني القومي والعسكري.

- وسائل مكافحة الجريمة الإلكترونية

1. إصدار التشريعات المواكبة لتطورات الجريمة الإلكترونية، وانسجام التشريعات الوطنية مع الاتفاقيات، والقواعد الدولية، والقوانين المقارنة ذات الصلة لتمكين أجهزة العدالة الجنائية من أداء دورها على النطاق الوطني والإقليمي والدولي بالصورة التي تسهم بالمكافحة الفعالة للجريمة السيبرانية.
2. رفع كفاءة الأجهزة التقنية المختصة برصد التهديدات والمخاطر والتبليغ بالإنذار المبكر وتزويدها بأحدث المعدات.
3. تدريب وتأهيل الفنيين والمهندسين العاملين في مجال الأدلة الرقمية وترشيد وتطوير أدائهم.
4. تدريب وتأهيل المختصين بأجهزة العدالة الجنائية على كيفية التعامل مع الأدلة الرقمية.
5. اتباع كافة وسائل التوعية الأمنية للحد من مخاطر الجريمة الإلكترونية (د. جبور منى،2017 م، ص24).

المطلب الثاني

تداعيات الهجمات السيبرانية على الأمن القومي

قد تبنى البعض مصطلح الحرب السيبرانية بدلا من مصطلح الهجمات السيبرانية بالاستناد إلى أيدلوجية أمنية أو عسكرية تضع منهاجا لتحقيق الأهداف على الصعيد الأمني أو العسكري تجاه العدو المفترض. (د. العمارات فارس، وآخرون، 2022م ص14).

أما البعض الآخر ونحن من أنصاره فأختار مصطلح الهجمات السيبرانية كوصف واقعي فهو كما نعلم تصرف يدور في عالم افتراضي قائم على استخدام بيانات رقمية، ووسائل اتصال كل ما ذكر أنها تعمل إلكترونيا، ومن ثم تطور ليتضمن مفهوما أوسع،

يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، جراء اختراق لمواقع الإلكترونية حساسة عادةً ما تقوم بوظائف تصنف بأنها ذات أولوية كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات، ووسائل النقل الأخرى.

ولأن مصطلح الحرب هو مصطلح غير محبذ في وقتنا الراهن على مستوى التنظيم القانوني الدولي فيكون مصطلح الهجمات السيبرانية أكثر قربا للموضوع الذي تتناوله هذه الدراسة، ولا سيما أن تصرفات دولية عدة أشارت إلى مصطلح الهجمات، وعدتها بمثابة التصرف الذي يوضع في الحسبان في أثناء النزاعات المسلحة، طبقاً للقانون الدولي الإنساني.

ولكي نتعرف على تداعيات الهجمات السيبرانية على الأمن القومي وآثاره نقسم هذا المطلب الثاني إلى فرعين حيث سنخصص الفرع الأول المخاطر والتداعيات على تفاعلات السياسية الدولية، والفرع الثاني سنبني من خلاله على أمثله واقعية لاستحداث الجرائم السيبرانية وزيادة معدلاتها.

الفرع الأول: . المخاطر والتداعيات على التفاعلات السياسية الدولية

سببت الحروب السيبرانية جملة من المخاطر والتداعيات على تفاعلات السياسة الدولية وتكمن هذه الخطورة في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء السيبراني، لا سيما في البنى التحتية المعلوماتية، ولا شك أن ازدياد الهجمات السيبرانية يعني إمكانية تطورها لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل (WWW.Alkhanadeq.com) يمكن طرح أبرزها على النحو الآتي: .

1. تصاعد المخاطر الإلكترونية، خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم، الأمر الذي يؤثر في وظائف تلك المنشآت، وبالتالي فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة استراتيجية.

2. تعزيز القوة وانتشارها، عمل الفضاء السيبراني على إعادة تشكيل قدرة الأطراف المؤثرة، وأدى إلى عملية انتشار القوة بين فاعلين متعددين.
3. عسكرة الفضاء السيبراني، حيث برز في هذا الإطار عدة اتجاهات، مثل التطور في مجال سياسات الدفاع والأمن السيبراني، وتصاعد القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن في الدول، وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.
4. إدماج الفضاء الإلكتروني ضمن الأمن القومي للدول، وذلك عبر تحديث الجيوش، وتدشين وحدات متخصصة في الحروب السيبرانية، وإقامة هيئات وطنية للأمن والدفاع الإلكتروني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات الإلكترونية.
5. الاستعداد لحروب المستقبل، حيث تبني العديد من الدول استراتيجية حرب المعلومات باعتبارها حربا للمستقبل، حيث تري الدول الكبرى أن من يحدد مصير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على شل القوة، والتشويش على المعلومة.
6. إصدار التشريعات المواكبة لتطورات الجريمة الإلكترونية وانسجام التشريعات الوطنية مع الاتفاقيات والقواعد الدولية والقوانين المقارنة ذات الصلة لتمكين أجهزة العدالة الجنائية من أداء دورها على النطاق الوطني والإقليمي والدولي بالصورة التي تسهم بالمكافحة الفعالة للجريمة الإلكترونية.
7. رفع كفاءة الأجهزة التقنية المختصة برصد التهديدات والمخاطر والتبليغ بالإنذار المبكر وتزويدها بأحدث المعدات.
8. تدريب وتأهيل الفنيين والمهندسين العاملين في مجال الأدلة الرقمية وترشيد وتطوير ادائهم.
9. تدريب وتأهيل المختصين بأجهزة العدالة الجنائية على كيفية التعامل مع الأدلة الرقمية.

10. اتباع كافة وسائل التوعية الأمنية للحد من مخاطر الجريمة الإلكترونية (د.مختار محمد ،2015 ، ص6- 5).

ومن جانب اخر لقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي العالم، إذ تزداد المخاطر السيبرانية في غالب الأحيان كلما زادت هيمنة تكنولوجيا المعلومات، والاتصالات على النسق العام، فأصبحنا أمام جرائم حقيقية ومتكاملة الأركان تتم عن طريق شبكات الأنترنت، وأجهزة الحاسوب بأشكال كثيرة، كسرقة الأموال، النصب، والاحتيال، التخطيط لعمليات إرهابية، ترويج في العالم الرقمي الأخبار الكاذبة، وكذلك القرصنة باعتبارها الجريمة الأكثر شيوعا، وفي هذا السياق، فإن البحث في قضايا التهديدات السيبرانية والتحديات الأمنية يقتضي الغوص في حيثيات العصر الرقمي الجديد وتوصيف بيئة هذه التحديات.

وثمة تطور ظهر مؤخرًا نسبيًا هو توسيع نطاق العمليات العسكرية لتشمل الفضاء السيبراني، فيما يسمى (المجال الخامس للحرب) بجانب البر، والبحر، والجو، والفضاء، وعلى الرغم من عدم وجود خلاف عمومًا على أن القانون الدولي الإنساني ينطبق على العمليات السيبرانية المنفذة في إطار نزاع مسلح قائم، فمن غير الواضح ما إذا كانت العمليات السيبرانية في حد ذاتها يمكن أن تؤدي إلى نزاع مسلح، ومن ثم تؤدي إلى انطباق القانون الدولي الإنساني.

الفرع الثاني: . أمثلة واقعية لاستحداث الجرائم السيبرانية وزيادة معدلاتها

مع الاعتماد المتزايد في الحياة اليومية على الأنظمة المعلوماتية، والأجهزة المتصلة بالشبكة الدولية للمعلومات وتشعب طبيعة هذه الأجهزة من هواتف خلوية، وأجهزة حوسبة شخصية يزداد عدد المتصلين بالفضاء السيبراني، وتزداد احتمالات الاعتداءات والجريمة، وتسهل سبل التجسس الاقتصادي، وتؤثر على عمليات الحكومة مثل الفيروسات، وهجمات منع الخدمة، وسرقة البيانات والرسائل الاقتحامية، والتدليس وكلها تقوض مصداقية تكنولوجيا المعلومات، والاتصالات وقدرة المجتمعات على العمل، وقد أشار تقرير صادر عن

مؤسسة ماكينزي إلى توقع زيادة المعلومات الرقمية بمعدل 44% خلال الأعوام الممتدة من 2009م إلى 2020م (Mckinsey noted in its July 2011 report).

ومع الصعيد الأخر قد تزايدت العلاقة بين الأمن والتكنولوجيا، ومعها تزايدت إمكانية تعرض المصالح الاستراتيجية للدولة للتهديدات السيبرانية، وتهدد بتحول الفضاء السيبراني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف.

بعد أحداث 11 سبتمبر بدأ التركيز على الفضاء السيبراني كتهديد أمني جديد، خاصة مع استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة الأمريكية، وفي 2007م و 2008م على التوالي، كان الأمن القومي لكل من إستونيا وجورجيا مهددا من طرف روسيا، حيث استعملت هجمات الحرمان من الخدمة لتقويض العمل في الإدارات والمؤسسات الحكومية لكلا الدولتين، وأصبح الفضاء السيبراني للدولتين مجالا للعمليات، وجاء الهجوم السيبراني بفيروس" ستاكسنت "على أجهزة الطرد المركزي الإيرانية، من أجل تعطيل برنامج ايران النووي، ليمثل نقلة نوعية مهمة في تطوير واستخدام الأسلحة السيبرانية (د. بسيوني حمد ، على الرابط: http://newsabah.com/newspaper/138116 2017 – 10 - 30 :) هذا إضافة إلى الدور الكبير الذي لعبته شبكات التواصل الاجتماعي في حالة الثورات العربية في بداية 2011م حيث مثلت نقطة هامة في زيادة الاهتمام الدولي بأمن الفضاء السيبراني، وبرزت محاولات للسيطرة عليه بعد تصاعد الاحتجاجات حتى في الدول الأكثر ديموقراطية كبريطاني، والولايات المتحدة الأمريكية.

كما عثر المتخصصون على برامج تسمى (Wiper ماسح) وهو برامج ضار يمكنه حذف الكثير من البيانات من دون ملاحظة ذلك، مثل هذا الهجوم الروسي حدث في عام 2017م على أوكرانيا ببرنامج ماسح (NotPetya) ما تسبب بأضرار اقتصادية كبيرة.

وكذلك من أبرز التهديدات السيبرانية المحتمل تزايدها في السنوات القادمة، هجوم الفدية الذي وصفته وزارة العدل الأمريكية بأنه (نموذج عمل جديد للجريمة

الإلكترونية، وقدر مكتب التحقيقات الفدرالي الأمريكي أن المبلغ الإجمالي من مدفوعات الفدية تقترب من مليار دولار سنويا، حيث أن الشركات التجارية سوف تقع ضحية لهجوم الفدية كل ١٤ ثانية في 2023م.

وتشير التقارير الدولية إلى أن فيروس الفدية تسبب في خسائر مالية تفوق الخمسة مليارات دولار أثناء عام 2017م، وهو معدل مرتفع جدا خلال عام واحد، ومن أمثلة الهجوم الإلكتروني ما أصاب شبكة الكهرباء الأوكرانية، والذي تسبب في بقاء أوكرانيا لساعات في الظلام، وبذلك، تخطت الحروب الإلكترونية والهجمات السيبرانية حاجز البيانات والمعلومات، والمواقع الإلكترونية لتصل للبنية التحتية، والأنظمة الحيوية مثل المفاعلات النووية وأنظمة الكهرباء والأنظمة الطبية والنقل، وغيرها من القطاعات التي تعد ركائز أساسية للدول، مما يرفع مستوى الخطورة على الدول (د. العجمي حسن، 2018، ص16).

ومن أشهر الاختراقات ما حدث من سرقة حسابات شركة ياهو (Yahoo) حيث بلغ عدد الحسابات المسروقة ثلاثة مليارات حساب، وكذلك اختراق إكيفاكس (Equifax) في عام 2017م، حيث تأثر، خمس مليون عميل، وذلك يتطلب بشكل ملح إفساح المجال وبشدة للأمن السيبرانى تقنيا، وتشريعا، وتنظيما، ونشر ثقافة المواطنة الرقمية لزيادة سلامة التعامل السيبرانى (د. الغامدي عبد الله، 2018، ص9).

ولذا حذر القائمون على مؤتمر أمن المعلومات السنوي بمنطقة الشرق الأوسط وشمال أفريقيا 2017م من أن المنطقة تواجه تحديات شديدة الأهمية تتعلق بتأمين المعلومات والبنية التحتية من الهجمات الإلكترونية التي يرتكبها القراصنة كالتخريب أو الابتزاز أو الاحتيال على ضحاياهم وتشير التقارير إلى توالى حوادث اختراق الأنظمة وسرقة البيانات وتسربها، كاختراق أنظمة معلومات سوني، التي نتج عنها تسرب بيانات مليون مستخدم (د. ريان محمد، 2018، ص28).

وأيضا ما تعرضت له (روسيا من اتهام بالقرصنة الإلكترونية في الانتخابات الأمريكية لدعم المرشح الجمهوري دونالد ترامب في مواجهة منافسته الديمقراطية هيلاري كلنتون) (افادات وكالة الاستخبارات الأمريكية بتدخل روسيا في الانتخابات الرئاسية الأمريكية لدعم) دونالد ترامب (، وان روسيا وراء الهجمات الإلكترونية والقرصنة المعلوماتية التي طالت حسابات البريد الإلكتروني لمرشحة الحزب الديمقراطي هيلاري كلنتون 2018/8/10، موقع الكتروني.www.SaSapost.com)

وهناك نمط آخر من الحروب السيبرانية يتمثل في تحويل الصراع عبر الفضاء الإلكتروني كساحة موازية أو مرافقة أو مرتبطة لحرب تقليدية دائرة على الأرض، ومنها ما تعرضت له سوريا في 2007/12/6م لهجمة سيبرانية على دفاعاتها الجوية في إحدى المنشئات التي يشتبه في انها منشأة نووية في مدينة دير الزور من قبل إسرائيل، مما أدى إلى تعطيل هذه الدفاعات لتمكين الطائرات الإسرائيلية من قصف هذا الموقع دون أن يتم الكشف عن الهجوم.

ونمط ثالث يعبر عنه في نشوء حروب في الفضاء الإلكتروني بصورة منفردة، واذا لم يشهد العالم هكذا نوع من الحروب وفقاً لأثارها المدمرة من خلال اختراق العمليات العسكرية عالية التقنية أو استهداف الحياة المدنية والبنية التحتية بالشكل الذي يمكن تصوره إلا أن هناك نماذج لتلك الحروب تتمثل على شكل رسائل تهديد مصحوبة بآثار محدودة جراء تلك الهجمات، ومنها ما تعرضت له جمهورية إستونيا عام 2007م من هجوم سيبراني مستقل بذاته موجه من روسيا الاتحادية وذلك عن طريق إغراق المواقع الإلكترونية بسيل من البيانات غير اللازمة، حيث وجهت ما يقارب من مليون حاسبة من عدة نقاط في العالم، واستهدفت المواقع الحكومية والصحف والجامعات والمستشفيات (والمصارف وخدمات الإطفاء و والإسعاف وذلك بهدف اسقاط وشل الحكومة الإستونية (د. احمد سراب، ص83 –84).

الخاتمة

على ضوء ما تبين أن الأمن السيبراني أصبح على رأس أوليات قضايا الأمن القومي، حيث قامت معظم الدول بإعادة صياغة عقيدتها الأمنية لتتلاءم مع المتغير الجديد، وهذا في محاولة مواجهة التهديدات السيبرانية التي تزداد وتتطور بسرعة، فالجريمة والإرهاب والحرب في الفضاء السيبراني تعد من بين التحديات الأمنية الجديدة أمام الدول وبعد الاستدلال بهذا البحث وما تم عرضه نتناول بعض النتائج والتوصيات:

أولا- النتائج

1. لم يتفق الفقه الجنائي على تسمية موحدة للجريمة السيبرانية كان محلا لإجتهادات الفقهاء فقد ذهبوا في ذلك مذاهب مختلفة، ووضعوا تعريفات شتى.
2. مرتكبي الجريمة الإلكترونية يختلفون عن مرتكبي الجريمة التقليدية، ويرجع ذلك لاختلاف الأشخاص من حيث السن، والجنس، والمستوى التعليمي، وأيضا كما ان الأسباب أو الدوافع التي تدفعهم لارتكاب الجريمة عواملها تختلف كل من الجريمتين التي سبق ذكرهم.
3. فمسألة تحديد مفهوم الفضاء السيبراني هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل دولة لأمنها القومي.
4. جملة المخاطر والتداعيات على تفاعلات السياسة الدولية والصراعات والحروب هي التي جعلت العالم يعتمد على الحروب بالمنظور الجديد الحرب السيبرانية.
5. هيأ المجتمع الدولي في مجال الأمن السيبراني حدودا في التعامل السيبراني بعيدا عن الإجرام والتطرف والعنف والتنمر والمساس بالأمن وفي نفس الوقت هيأ آليات لتيسير الفعل من خلال سبل الحماية وتشريعات المكافحة.
6. جاء في خطاب الفاعلين للأمن السيبرانى أن ليبيا في مراحل متقدمة في هذا المجال ما جعلها تحتل المركز ١٤ عربيا والمركز 105 عالميا حسبITU التقرير النهائي 2017م.

7. الجريمة السيبرانية جزء من الحرب الهجينة ويمكن أن يكون لها تأثير في الحرب الفعلية على الأرض، فتعطيل أو اختراق بيانات وزارات الدفاع قد يغير شيئا من الحرب، لكن نشر المعلومات الكاذبة قد يكون تأثيره أعظم بحسب خبراء.

ثانيا- التوصيات

1. أوصي بزيادة التعمق في الفضاء السيبراني في مجال علم الاجتماع الرقمي وخاصة نحن الدولة الليبية لابد أن نسعى لرفع مستوى الحماية، والاستعداد للأمن السيبراني وفق ما جاء في خطاب الفاعلين للأمن السيبرانى أن ليبيا في مراحل تعتبر مقبولة في هذا المجال ما جعلها تحتل المركز 14 عربيا والمركز 105 عالميا حسبITU التقرير النهائي 2017م.
2. ويعتبر تأمين المعلومات والشبكات أكثر الطرق فعالية للحماية من الهجمات الإلكترونية ويجب تطبيق التحديثات الأمنية على كافة الأنظمة بما فيها تلك التي لا تعتبر حساسة وذلك لان أي ثغرة في النظام يمكن استغلالها لشن هجمات.
3. لاهتمام بوضع آليات وسن تشريعات لمجابهة التدهور الأخلاقي والقيمي المستخدم في الفضاء السيبرانى كالتنمر الإلكتروني والبغاء الإلكتروني والتطرف الفكري والدينى... إلخ.

المصادر والمراجع

أولا- . الكتب

1. د. أمين هويدي، الأمن العربي المستباح دار الموقف العربي، القاهرة، 1982م.
2. د. إميل خوري، صراعات الجيل الخامس، شركة المطبوعات للتوزيع والنشر، بيروت، الطبعة الأولى 2016م.
3. د. حمدون توريه، الفضاء السيبراني وتهديد الحرب السيبرانية كتاب صادر عن مركز الاتحاد الدولي للاتصالات 2011م.

4. د. فارس محمد العمارات، إبراهيم محمد الحمامصه، الأمن السيبراني المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، الأردن، عمان، الطبعة الأولى، 2022م.
5. د. شريف عبد الرحمن، حروب الجيل الرابع بين الرواية الأمريكية والرواية المصرية، دار البشير، الطبعة الأولى، القاهرة 2016م.
6. د. عبد العزيز بن غرام الله آل جار الله، جرائم الإنترنت وعقوبتها وفق نظام مكافحة الجرائم المعلوماتية، السعودية، دراسة مقارنة الطبعة الأولى، دار الكتاب الجامعي الرياض 2017م.
7. د. غراهام ايفانز، وجيفري نوينهام، قاموس بنغوين للعلاقات الدولية، ترجمة عبد العزيز بن عثمان بن صقر، مركز الخليج للأبحاث، الطبعة الأولى، 2004م.
8. د. كارل فون كلاوز فيتز، عن الحرب، ترجمة سليم شاكر الإمامي، في المؤسسة العربية للدراسات والنشر، الطبعة الأولى، بيروت، 1997م
9. د. محمود شيت الخطاب، إرادة القتال في الجهاد الإسلامي، دار الفكر القاهرة الطبعة الثانية، 1973م.

ثانيا- . المجلات والدوريات البحوث والدراسات والمقالات

1. د. حسن بن على العجمي، الثورة الصناعية الرابعة وتغيرات الحياة الإنسانية، الرياض، السعودية، المجلة العربية: الأمن السيبرانى حروب الأرقام الصماء، 498، 2018.
2. د. عبد الحكيم مولاي إبراهيم، الجرائم الإلكترونية مجلة الحقوق والعلوم الإنسانية جامعة، زيان عاشور بالجفلة، الجزائر، العدد ،23، 2015م.
3. د. عبد الله شرف الغامدي، الجرائم السيبرانية والتحديات المستقبلية، المجلة العربية: الأمن السيبرانى حروب الأرقام الصماء، ع 498، 2018.
4. د. علاء الدين فرحات الفضاء السيبراني تشكل ساحة المعركة في القرن الحادي والعشرون مجلة العلوم القانونية والسياسية المجلد 10 العدد 3 2019م).

5. د. محمد الأمين البشري، التحقيق في الجرائم الحاسب الآلي، بحث مقدم إلى مؤتمرات القانون والكمبيوتر والأنترنت كلية الحقوق والشريعة، جامعة الإمارات 21 مايو 2005.
6. د. محمد سيد ريان، الأمن السيبراني وثقافتنا الرقمية في مصر، الرياض، السعودية، المجلة العربية: الأمن السيبراني حروب الأرقام الصماء، ع 498، 2018.
7. د. محمد عبد الرحيم سلطان العلماء، جرائم الإنترنت والاحتساب عليها، بحث مقدم لمؤتمر القانون والكمبيوتر والأنترنت جامعة الإمارات مايو 2005.
8. د. محمد مختار، هل يمكن للدول أن تتجنب مخاطر الهجمات الإلكترونية؟ مفاهيم المستقبل، العدد6 ، مركز المستقبل للأبحاث والتطوير،2015 .
9. د. منى الأشقر جبور، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والقضائية، بيروت،2017 .

ثالثا- الرسائل العلمية

1. أ. صلاح حيدر عبد الواحد، حروب الفضاء الإلكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة ماجستير في العلوم السياسية كلية الآداب والعلوم، بجامعة الشرق الأوسط، عمان، يونيو 2021م.

رابعا- الاتفاقيات والمواثيق والدساتير والإعلانات الدولية:

1. اتفاقية مجلس أوروبا للجريمة السيبرانية 2001م.

خامسا- الشبكة العالمية للمعلومات (الأنترنت)

1. إفادات وكالة الاستخبارات الأمريكية بتدخل روسيا في الانتخابات الرئاسية الأمريكية لدعم) دونالد ترامب (، وان روسيا وراء الهجمات الإلكترونية والقرصنة المعلوماتية التي طالت حسابات البريد الإلكتروني لمرشحة الحزب الديمقراطي) هيلاري كلنتون 2018/8/10، موقع الإلكتروني.www.SaSapost.com

2. د. حمد بسيوني، دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية، جريدة الصباح الجديد، على الرابط http://newsabah.com/newspaper/138116
3. http//accronline.com/article-detail.aspx? Id=7509
4. الحرب الإلكترونية والحرب السيبرانية WWW.Alkhanadeq.com
5. Mckinsey noted in its July 2011 report
6. مكتب الأمم المتحدة المعني بالمخدرات والجرائم دراسة شاملة عن الجريمة السيبرانية مسودة نيويورك 2013م على الموقع https://www.unodc.org