القصور التشريعي في مواجهة الهجمات السيبرانية

أ.م.د رعد فجر الراوي

العراق/ جامعة الانبار/ كلية القانون والعلوم السياسية/ قسم القانون

الملخص

قد تتداخل المسؤولية الدولية الجنائية مع المسؤولية الوطنية، فإذا ما ورد نص في القانون الوطني يعالج جريمة دولية ويعاقب عليها القضاء الوطني أخذاً بمبدأ الاختصاص الجنائي العالمي (الشامل) في هذه الحالة فإن المسؤولية تقع بعد أن تجمع بين وصفين الأول هو اعتبارها مسؤولية جنائية وطنية تنتج عنها جريمة وطنية بالنظر الى النص عليها في القانون الوطني، والثاني اعتبارها مسؤولية دولية جنائية ينتج عنها جريمة دولية بالنظر الى النص عليها في القانون الدولي.

أن طبيعة المسؤولية الدولية الجنائية في الهجمات السيبرانية في القانون الدولي الجنائي ترجع أساسا ومباشرة إلى مصدرها وهو القانون الدولي العرفي ولو تضمنتها اتفاقية دولية. بينما المسؤولية الجنائية عن الهجمات السيبرانية ذات البعد الدولي فلها طبيعة وطنية يكون مصدر تجريمها هو القانون الوطني ولو كان هذا القانون تطبيقاً لاتفاقية دولية حتى ولو كانت هذه الاتفاقية تستند إلى عرف دولي.

الكلمات المفتاحية

الفضاء السيبرانة، التشريع، المسؤولية، القصور التشريعي، الهجمات السيبرانة

Abstract

The nature of international criminal responsibility in cyber attacks is return to its source which is the custom of international law, even though its included in international convention. Although, criminal responsibility for cyber attacks has international character, it is also has a national nature. The national law is considered the source of criminalization, even if this law is applying to international agreement based on international custom.

The question that needs to be answered in this research is: can the authority facing cyber attacks as criminal side? And considering the perpetrators have international responsibility? The authority can impose international criminal responsibility on the perpetrators of cyber crimes because these crimes establish an assault on the basic interests of the international community. The cyber attacks is an attack on the interests of the state, directly or indirectly, because the government is a member of the international community. National criminal responsibility for cyber crimes has a wide scope because cyber attacks occur outside the territorial scope of the state in most cases.

المقدمة

تنبعث المسؤولية الدولية الجنائية للهجمات السيبرانية بالمعنى الدقيق من القانون الدولي العرفي، لأنها تقع اعتداء على القيم الأساسية للمجتمع الدولي، استقلالاً عما تنص عليه المسؤولية لجنائية للهجمات السيبرانية في القوانين الداخلية. وبعض الهجمات السيبرانية تشكل جرائم دولية تستند في الأساس على العرف الدولي. كما في جريمة العدوان التي لم يتفق المجتمع الدولي على تعريفها فهل يمكن أن تشكل الهجمات السيبرانية جريمة عدوان، أم أن هذه الهجمات يمكن أن تشكل نوع من جرائم الإبادة الجماعية أم جرائم حرب أم جرائم الاعتداء على الإنسانية فنجد أن المسؤولية الدولية الجنائية قد تبنت العرف الدولي والاتفاقات الدولية معاً. والبعض الأخر من الهجمات السيبرانية يمكن أن يكون مصدرها الاتفاق الدولي وذلك من خلال حصول جرائم وطنية ذات البعد الدولي والمسماة بالجرائم العابرة للحدود والتي يمتد إليها نطاق قانون العقوبات من حيث المكان رغم وقوعها كلها أو بعضها خارج إقليم الدولة.

أهمية الموضوع تتمثل في البحث عن مفهوم الجريمة السبرانية وخصائصها وكيفية التحقيق فيها وبيان إلية التعاون الدولي في مكافحة الجريمة السبرانية حيث تناولنا هذه المواضيع وبشكل موجز وبسيط.

ولحل مشكلة مهمة تدور حول عدم وجود إي من التشريعات الوطنية أو العالمية قامة بتنظيم هذا النوع من الهجمات في نصوص تشريعية والتي تعد قصورا خطيرا لما تمسه هذه الهجمات من مصالح الأفراد والمجتمع ككل, خاصة مع التطور التقني لأساليب ارتكاب هذه الهجمات والتي ترتكب عبر الحاسوب ألإلي وكيف يمكن معه استخلاص الدليل الالكتروني وكيفية إجراء التحقيق في هذه الجرائم.

والسؤال الذي يحتاج إلى إجابة عليه في أطار بحثنا. هل يتم مواجهة الهجمات السيبرانية من الناحية الجنائية من خلال إيقاع مسؤولية دولية جنائية على مرتكبيها لما ينتجه عنها من اعتداء على المصالح والقيم

الأساسية للمجتمع الدولي والتي يصاغ بها النظام العام الدولي، أم إن ما ينشأ عن الهجمات هو اعتداء على مصالح الدولة سواء بطريق مباشر أو بطريق غير مباشر بوصفها عضواً في المجتمع الدولي. فينتج عن ذلك اتساع نطاق المسؤولية الجنائية الوطنية لان الهجمات السيبرانية تقع خارج النطاق الإقليمي للدولة في أغلب الأحيان. على اساس ذلك سنبحث التهديدات السبرانية في مبحث اول، اما المبحث الثاني فيتضمن التعاون الدولي في مكافحة الجريمة السيبرانية.

المبحث الاول

التعريف بالتهديدات السبرانية

إذا كانت القاعدة الدولية هي أداة الشرعية في التجريم الدولي، فإن مبدأ الشرعية لا يعد جزءاً من المسؤولية الجنائية فهو سابق عليها. كما أن الحكم الدولي الجنائي وأن كان لازماً للعقوبات الدولية الجنائية لكنه ليس جزء من المسؤولية الدولية الجنائية ولا يصح معياراً لها، بل هو لاحق على وقوعها. ولعل المعيار الموضوعي للمسؤولية الدولية الجنائية يبدأ في الإخلال بالنظام العام الدولي المشمول بالحماية الجنائية من الهجمات السيبرانية وذلك من خلال العقاب الدولي الجنائي.

هذا ولا يوجد اختلاف على ما ساهم به تطور التكنولوجيا والإعلام والاتصال وظهور الشبكة العالمية الانترنت من تقديم خدمات وأحداث أثار ايجابية في نمط حياة المجتمعات ومصالحها ومصالح الدول بأسرها. وعلى الرغم من هذه الايجابيات، إلا أن هذا التطور لم يمر على العالم بسلام لما يحمله معه من أثار سلبية، تتمثل بالتهديدات الالكترونية، فظهرت الهجمات السبرانية أول مرة في الدول المتقدمة ذات التكنلوجيا العالية ثم انتقلت الى دول أخرى[1]. لذا سنحاول في هذا المبحث التطرق إلى مفهوم الهجمات السبرانية وخصائصها كذلك ندرس التحقيق والتعاون الدولي في مجال الهجوم السبرانية من خلال مطلبين وعلى النحو التالي.

المطلب الأول

مفهوم الهجمات السبرانية وخصائصها

لا يوجد أجماع على تعريف الهجمات السيبرانية من حيث كيف تعرف أو ما هي التهديدات التي تتضمنها الجريمة الالكترونية فهناك غياب لتعريف عام وإطار نظري منسق في هذا الحقل من الهجمات. لذا سنتكلم في هذا المطلب وعلى فرعين في الأول تعريف التهديد السيبراني وتمييزه عن السلوك التقليدية لطبيعة الاعتداء، وفي الفرع الثاني ندرس خصائص الهجوم السيبراني وطبيعة القائم بهذا الهجوم أي المجرم ألمعلوماتي وسماته ودوافعه.

([1]) عبد الله عبد الكريم عبد الله: جرائم المعلومات والإنترنيت (الجرائم الالكترونية)، ط1، منشورات الحلبي الحقوقية، لبنان، 2007، ص15.

الفرع الأول

تعريف الهجوم السبرانية وتميزه عن السلوك التقليدية

يمكن تعريف الهجوم السبيراني من حيث وسيلة استخدامها بأنه: (نشاط إجرامي تستخدم فيه التقنية الالكترونية الحاسوب ألإلي وشبكة الانترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الاعتداء الإجرامي المستهدف)[1]. كما يعرف التهديد السيبراني على أساس شخصي بأنه: (أية سلوك ينسب لفاعلها معرفة فنية بتقنية الحاسبات يمكن من ارتكابها)[2].

ويتشابه السلوك السبراني مع السلوك التقليدية الذي يقوم به فاعله من حيث القائم بهذا الهجوم فهناك مجرم له دافع للقيام بالهجوم، وضحية قد تكون شخص طبيعي أو معنوي. إما الاختلاف الحقيقي فيظهر في أداة الهجوم ومكان الهجوم ففي الهجوم السبراني الأداة تكون ذات تقنية عالية، وأيضا المكان الذي انطلق منه الهجوم لا يتطلب انتقال فاعله انتقال جسمانيا لأنه يتم عن بعد بواسطة خطوط وشبكات الاتصال بين المهاجم ومكان الهجوم.

إما تعريفنا للهجوم السبراني فيمكن أن نعرفه على انه (سلوك غير مشروع وغير أخلاقي من المجرم ألمعلوماتي يقع ضحيته أشخاص طبيعية أو معنوية يتخذ من الحاسوب والمعلوماتية وسيله لتحقيق أغراضه الإجرامية).

الفرع الثاني

خصائص الهجوم السبرانية (الالكترونية)

تحديد القواعد الدولية الجنائية المسؤولية عن الفعل بانه يأتي من خلال إيضاح الإخلال بالنظام العام الدولي وبيان أرادة مرتكب الهجوم وعلمه، ومن ثم بعد ذلك تحدد العقوبة اللازمة لهذا الهجوم. وما دام وقوع المسؤولية يأتي من خلال تحديد أركان الجريمة إلا أن المساس بالنظام الدولي عن طريق الهجمات السيبرانية يبدو هو الجوهر وهو الذي يميز وقوع المسؤولية من الناحية الموضوعية وبالتالي يؤثر في الطابع الدولي المنشئ للنص في التجريم الدولي. وفيما يأتي بيان لأهم الخصائص التي تتميز بها الهجمات السيبرانية.

([1]) محمد عبيد الكعبي: الجرائم الناشئة عن استخدام الغير مشروع لشبكة الانترنيت، دار النهضة العربية، القاهرة، بدون سنة نشر، ص34.

([2]) عبد الله عبد الكريم عبد الله: مرجع سابق، ص16.

أولا: صعوبة اكتشاف الهجوم السبراني.

أن الهجمات السيبرانية تتميز بأنها من الهجمات الخفية التي لا يلاحظها الضحية رغم أنها تقع أثناء وجوده على الشبكة والسبب في ذلك تمتع فاعل الهجوم بقدرات فنية عالية تجعله ينفذ هجومه بدقه مثلا عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها من الهجمات.

ثانيا: الهجمات السبرانية تتم باشتراك أكثر من شخص (تعدد الجناة).

تتميز الهجمات السبرانية بأنها تقع بتعاون أكثر من شخص على ارتكابها إضرار بالجهة المجني عليها، فالهجوم السبراني يخرج إلى حيز الوجود من قبل شخص متخصص في تقنيات الحاسوب وشخص أخر يغطي عملية التلاعب وتحويل المكاسب اليه، وقد يكون الاشتراك سلبي من خلال الصمت من جانب من يعلم بوقوع الهجوم في محاولة منه لتسهيلها وإتمامها؛ وقد يكون الاشتراك ايجابيا يتمثل في تقديم المساعدة الفنية والمادية[1].

ثالثا: الهجمات السبرانية عابرة للحدود.

لم تعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات بين الدول، وذلك لما تتمتع به الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وعليه فان أماكن متعددة في دول مختلفة قد تتأثر بهجمة الكترونية فقد يكون الفاعل في دولة والهجوم يقع في دولة أخرى.

رابعا: صعوبة أثبات الهجوم السبراني.

أن بيئة الهجوم السبراني بيئة غير تقليدية فهي تقع خارج الإطار الواقعي المادي الملموس فالهجوم يقوم في بيئة الحاسوب والشبكات مما يجعل الأمر معقدا على الأجهزة الأمنية والسلطات بالتحقيق فيها والملاحقة[2].

فإذا نظرنا في تقارير الخبراء كدليل من أدلة الإثبات نرى بأنه ولكثرة المسائل الفنية الدقيقة التي سوف تفرزها تطبيقات ثورة الاتصالات عن بعد، أن دور الخبرة يزداد في المسائل الجنائية، بالنظر إلى أن الكثير من الجرائم التي ترتكب كنتيجة لهذه الثورة ستقع على مسائل الكترونية ذات طبيعة فنية معقدة. أو قد تستخدم هذه الوسائل في ارتكابها ونتيجة لتطور مجالات الخبرة فانه سوف تتسع مجالات اللجوء أليها.

وفيما يخص الإثبات في الأدلة المادية نلاحظ ونتيجة لتطور التقنيات العلمية أن هذا التطور ساهم في صنع الدليل بحيث يتمتع بقوة علمية يصعب أثبات عكسها وذلك من خلال الإثبات بالبصمة الوراثية وبصمة الصوت وبصمة العين وبصمة الإذن والشفاه.

([1]) نهلا عبد القادر المؤمني: الجرائم المعلوماتية، ط2، دار الثقافية للنشر والتوزيع، لبنان، 2001، ص58.

([2]) د. هلالي عبد الاله احمد: جرائم الحاسب والانترنيت بين التجريم الجنائي واليات المواجهة، دار النهضة العربية، القاهرة، 2016، ص177.

خامسا: أسلوب ارتكاب الهجوم السبراني.

الهجوم السبراني يتميز بأسلوب خاص به عند ارتكابها يختلف عن أسلوب الاعتداء التقليدية التي تحتاج نوعا ما الأسلوب العضلي الذي يكون في صورة كسر أو تقليد كما هو الحال في جريمة السرقة[1]. إما الاعتداء السبراني فيحتاج إلى حواسيب وشبكات معلومات الانترنت مع وجود شخص ذو خبره وقدرات على التعامل مع الشبكة للقيام بهجمات مختلفة.

سادساً: مرتكب الهجوم السبراني.

يطلق خبراء امن المعلومات السبرانية مصطلح هاكرز وهي جمع لكلمة هاكر، على الشخص الذي يقوم بعمليات الاختراق والتخريب والتجسس عبر الفضاء السبراني، كما يطلقون مصطلح كراكرز وهي جمع لكلمة كراكر على المختصين في فك أو كسر شفرات البرامج أو كلمات السر وليس تخريب الشبكات، فهم نوع من الهاكرز المتخصص. واستنادا على هذا التحديد يصبح المرتكب الهجوم هو الشخص الذي ينتمي إلى احد هذين النوعين، وبالتالي يمكن تعريف الشخص الذي يقوم بالهجوم بأنه (ذلك الشخص الذي لدية دراية ومهارات تقنية في مجال الحاسبات وأمن المعلومات تمكنه من القيام بعمليات الاختراق والتخريب والتجسس عبر الفضاء السبراني، أو القيام بفك أو كسر شفرات البرامج أو كلمات السر لتغيير معلومات أو تعطيلها أو لتقليد البرامج واستغلالها، أو للتحويل من حسابات الغير والاستيلاء عليها، أو للسيطرة على الحاسب أو تشغيله دون وجه حق، وذلك عن طريق استخدام نظام معلوماتي معين)[2]. وعليه يمكن أن نحدد بعض سمات أو خصائص مرتكب الهجوم السبراني على نحو التالي:

1. انه شخص لديه دراية وخبرة تقنية عالية في مجال الحاسبات وامن المعلومات، تمكنه من اختراق الفضاء السبراني والشبكات الالكترونية وكسر كلمات المرور والشفرات، والتغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الحاسبات والشبكات، كما في حالة البنوك والمؤسسات العسكرية، مما يساعده على التخصص في هذه النوعية من الهجمات السبرانية دون غيرها من وسائل الاعتداء التقليدية أو النمطية.
2. مرتكب الهجوم السبراني دائماً ما يتميز بالذكاء إذ يمتلك من المهارات ما يؤهله أن يقوم بتعديل أو تطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع هجماته من خلال الشبكات أو داخل أجهزة الحواسيب. فهو يتميز بأنه يقوم بتوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير مصرح به مرات ومرات فهو يعتاد على القيام بالهجمات لمرات متعددة ولا يكتفي على القيام بهجمة واحدة فقط.

([1]) د. ماهر عبد شويش الدرة: شرح قانون العقوبات القسم الخاص، دار أبن الأثير، الموصل، 1988،ص276.

([2]) د. علي جبار الحسيناوي: جرائم الحاسوب والانترنيت، دار اليازوري العلمية للنشر، عمان، 2009، ص93.

يحركه في ذلك دوافع وبواعث تدفعه لارتكاب جرائمه تتمثل في الكسب المالي السريع والثراء العاجل على حساب الغير، وذلك عن طريق جرائم السرقة والنصب والاستيلاء على أرقام بطاقة الائتمان وأرقام الحسابات التي يتمكنون من تحقيقها عبر شبكة الانترنت. كما يمكن أن يكون لإثبات الذات ووضع المهارات التقنية والفنية في مجال الحاسبات وامن المعلومات موضع التنفيذ دافع في ذلك، كذلك فأن التنافس بين الأفراد والجماعات والدول والرغبة في تجميع اكبر قدر من المعلومات عن الطرق المنافسة. والرغبة في الانتقام التي تنتاب من تم فصلهم أو الاستغناء عنهم من بعض المؤسسات أو الشركات الدافع في ارتكاب الهجوم السيبراني.

المطلب الثاني

التحقيق والتعاون الدولي في مجال الهجوم السبرانية

لتحديد المسؤولية الجنائية الدولية لابد من القيام بإجراء التحقيقات والتي يراد منها الدفاع عن مصالح المجتمع من الهجمات السبرانية التي وقعت وذلك بعرض مرتكبيها وتقديمهم للمحاكمة وإقامة الدعوى الجزائية ضدهم. والمقصود بالتحقيق هو (تمحيص الأدلة التي جمعت في مرحلة جع الأدلة والتحري والمعلومات وتقديرها بغية أحالة الدعوى الجزائية إلى المحكمة المختصة من عدمها)[1]. إما التعاون الدولي فهو يشتمل التعاون القضائي بين الدول و التعاون الفني في مجال مكافحة الهجمات السبرانية والجهود الدولية المبذولة في سبيل ذلك. وهذا ما سنتناوله في هذا المطلب إذ يتضمن الفرع الأول منه التحقيق في الهجمات السبرانية، أما الفرع الثاني فيتضمن التعاون الدولي في مجال الهجمات السبرانية وعلى النحو التالي.

الفرع الأول

التحقيق في الهجمات السبرانية

بالرغم من وجود تشابه كبير بين التحقيق في الهجمات السبرانية والاعتداءات الأخرى من حيث الإجراءات مثل المعاينة والتفتيش والمراقبة والتحريات والاستجواب كما أنها تشترك في الإجابة عن الأسئلة، إلا أن هناك اختلافات جوهرية ببعض الجوانب. الأمر الذي يتطلب توافر بعض المهارات اللازمة لدى المحقق كون هذه الهجمات تشكل جرائم من نوع الجرائم المستحدثة فمن الطبيعي أن يتسم أسلوب المحقق بالحداثة أيضا ولعل من ابرز المهارات التي يجب أن يتصف المحقق تتمثل بالتعرف على المكونات المادية للحاسبة ومعرفة الأساسيات لعمل شبكة الحاسبة الآلي ومعرفة الأدوات والأساليب المستخدمة في ارتكاب الهجمات السبرانية. كذلك معرفة

([1]) سعيد حسب الله سعد الله: شرح قانون أصول المحاكمات الجزائية، دار أبن الاثير، الموصل، 2008، ص123.

تقنيات الحاسوب وطريقة عمل أدواتها من خلال الاطلاع على بعض الهجمات المرتكبة عن طريق الفضاء السبراني[1].

الأعمال التي يقوم بها المحقق والإجراءات التي يتبعها في التحقيق لإثبات المسؤولية الجنائية الدولية على مرتكب الهجوم السبراني تشمل مجموعة من الأعمال من ضمنها أن المحقق هو أول من يتلقى الشكوى أو الأخبار عن وقوع هجوم سبراني أو إنها على وشك الوقوع باعتباره هو السلطة المختصة عن القيام بالتحقيق, كما ان المخبر عن وقوع اعتداء سبراني يجب أن يكون على معرفة مقبولة بالحاسب الالي حتى يتمكن من وصف المعلومات المتعلقة بالحادث بشكل جيد بحيث يستطيع المحقق معها من معرفة التفاصيل التي تساعده في عمله.

ومما تجدر الإشارة إليه أن هذه المحادثة تكون قصيرة الهدف منها تمكين المحقق من وضع تصور أولي عن الحادث قبل الانتقال إلى محل الحادث، وكلما كانت المعلومات دقيقة كلما كانت مهمة وتساعد المحقق في التحقيق مثل تحضير قائمة بأسماء الموظفين في المؤسسة أو من لهم علاقة بالأجهزة المتضررة وتجهيز النسخ الاحتياطية من البيانات للأجهزة المتضررة والتأكيد على عدم إبلاغ احد إلا من كانت الضرورة تقتضي ابلاغه. وبعد ذلك على القائم بالتحقيق في الهجمات السبرانية أن يقوم بتكوين فريق عمل للإجراء التحقيق لان العمل في التحقيق بالهجمات السبرانية عادة ما يكون ليس بمقدور الشخص الواحد أن يتولاه بمفرده إذ يجب أن يسانده أشخاص آخرين ويتعاونوا فيما بينهم من اجل الحصول على الحقيقة الكاملة, فيجب أن يكون لدى الفريق حاسوب محمول ومتصل بالشبكة وتوجد به بطاقة شبكة لكي يأخذوا نسخ احتياطية من محتويات الأجهزة التي وقع من خلالها الهجوم ولعل أهم الأشخاص اللذين يجب أن يتكون منهم فريق العمل هم قاضي التحقيق والخبراء في مجال كشف الهجمات السبرانية[2].

الغاية من عمل المحقق والخبير هو الوصول إلى الدليل الالكتروني ويقصد به (المعلومات ذات القيمة المحتملة والمخزونة والمنقولة في صورة رقمية) [3]. هذا وان الأدلة الإلكترونية تكون على نوعين فهي أما أدلة مادية وتشمل" جهاز الحاسب الآلي وملحقاته، جهاز الهاتف النقال، الطابعات، المودم، الفلاش". أو أدلة ورقية وتشمل " الأوراق الخطية للإدخال في الحاسبة، أوراق أصلية تحفظ بالأرشيف الورقي، المستندات بأنواعها القانونية والإدارية، الأوراق التالفة في سلة المهملات". هذا وان أماكن وجود هذه الأدلة مهم جدا ويجب توجيه فريق التفتيش إلى هذه الأماكن بحثا عن الأدلة ومن أهم هذه الأماكن هي " شاشة الحاسوب، حافظة النقود، المفكرة الالكترونية، جيوب المتهم".

([1]) محمد امين الشوابكة: جرائم الحاسوب والانترنيت الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، 2009، ص147.

([2]) محمد حجازي: جرائم الحاسبة والانترنيت (الجرائم المعلوماتية)، بلا مكان نشر، 2005، ص18.

([3]) حسب ما عرفته المنظمة العالمية لدليل الكمبيوتر IOCE في أكتوبر 2001. مصطفى محمد موسى: التحقيق الجنائي في الجرائم الالكترونية، ط1، دار الثقافة للنشر والتوزيع، عمان، 2009، ص213.

تجدر الإشارة إلى أن المجرم ألمعلوماتي في كثير من الأحيان لا يترك أي أدلة تقود إليه وهذا لطبيعة الجريمة التي يكون مسرحها الشبكة العنكبوتية وهي عالم افتراضي فقد لا يتم الكشف عن الجريمة إلا بعد فوات الأوان وزوال الأثر. كذلك عدم ظهور الدليل المادي ورؤيته وذكاء مرتكبي الجرائم وضعف طرق الاستدلال والتعقيد الذي يتميز به عالم الانترنت كل هذه الصعوبات تشكل معوقا بطريق كشف الجريمة وصعوبة تحصيل الدليل الذي يمكن القاضي من بناء قناعته عند تسبيب الحكم.

الفرع الثاني

إجراءات التحقيق في مجال الجرائم السبرانية

تتميز الجرائم السبرانية او المتعلقة بالحاسب الالي بالخصوصية الامر الذي يتطلب تطوير اسلوب التحقيق الجنائي واجراءاته بصورة تتلاءم مع هذه الخصوصية وبنفس الوقت يتمكن المحقق من كشف الجريمة والتعرف على مرتكبها الامر الذي يتطلب الأمور التالية :-

اولا :- تدريب الكوادر والاستعانة بالخبرة الفنية.

يجب ان يتم تدريب فريق التحقيق تدريباً تاماً على كل ما يتعلق بالحاسب الالي، ويجب ان يشتمل التدريب على كيفية تشغيل الحاسوب ومهارات تتعلق بالبرمجة والمعالجة الالكترونية للبيانات والجرائم مع دراسة الحالات التطبيقية؛ هذا وفي كثير من بلدان العالم تعقد الدورات التدريبية لرجال الشرطة كما هو الحال في امريكا وانكلترا وكندا[1]. ولتحقيق كفاءة افضل في العمل حبذا لو تم انشاء قوات شرطة متخصصه في هذا المجال نظرا لاتساع نطاق هذه الجرائم وحداثة عصرنا الحالي الذي يتقدم بالمعرفة التكنولوجية تقدما مخيفا مما يؤدي في كثير من الاحيان الى عدم اللحاق بها.

هذا وان الاستعانة بالخبرة الفنية المطلوبة امر مهم جدا في هذا المجال؛ على عكس الاستعانة بالخبرة في الجرائم الاعتيادية اذ هي امر جوازي وليس وجوبي، الا ان في هذه الجرائم يجب الاستعانة بالخبرة الفنية المطلوبة لان الحكم بهذه الجرائم دون الاستعانة بالخبرة الفنية يكون معيب ويستوجب نقضه.

تظهر اهمية الاستعانة بالخبرة انه عند غيابها تعجز الشرطة عن كشف الجريمة او قد تدمر الدليل او تمحوه بسبب الاهمال او عدم معرفة التعامل معه والخبير لا يشترط فيه كفاءة علمية عالية في مجال التخصص فحسب بل ويجب ان تكون لديه خبرة سنوات في هذا المجال .

([1]) حسين طاهر داود: جرائم نظم المعلومات، ط1، اكاديمية نايف العربية للعلوم الامنية، الرياض، 200، ص225.

ثانيا : المعاينة.

يقصد بالمعاينة مشاهدة واثبات الاثار المادية التي خلفها ارتكاب الجريمة بهدف الحفاظ عليها. وهي اجراءات التحقيق الابتدائي ويجوز اللجوء اليها متى ما دعت الحاجة الى ذلك. فتتم المعاينة عن طريق تصوير الحاسوب والاجهزة الطرفية المتصلة، ويجب تسجيل وقت ومكان التقاط كل صورة , كذلك يجب ملاحظة الكابلات والتوصيلات والاسلاك وعدم نقل اي مادة من مسرح الجريمة دون اتخاذ كافة الاحتياطات لحمايتها من التلف والتحفظ على المستندات الورقية لما قد يوجد عليها من بصمات[1].

ثالثا :- التفتيش والضبط.

التفتيش هو احد إجراءات التحقيق يهدف إلى البحث عن أشياء تتعلق بالجريمة وكل ما يفيد بصفة عامة في كشف الحقيقة. وان السلطة المختصة بالتفتيش هما قاضي التحقيق والمحقق. وللتفتيش شروط شكلية وهي :-

1- ان يكون الامر بالتفتيش مسببا .
2- حضور المتهم او من ينوب عنه .
3- تحرير محضر بالتفتيش .

التفتيش يكون بالبحث في الشبكات الالكترونية ومحل هذا التفتيش هو البرامج والكيانات المنطقية المسجلة في ذاكرة الحاسبة والسجلات الخاصة بعمليات الدخول إلى النظام وكل ما يتعلق بكلمات السر ومفاتيح فك الشفرة[2]. لكن هناك مشكلة تثور فيما أذا كان التفتيش عابر للحدود فلا يجوز إهمال هذا الأمر لأنه يعتبر تدخل في سيادة دولة أخرى لذا تظهر لنا أهمية التعاون الدولي والاتفاقيات المعقودة في هذا المجال[3].

أن الغاية من عملية التفتيش هو ضبط شيء يخص الجريمة, ويهدي في التحقيق فيها، وبالنظر لمحل الجريمة والمتمثل بالبيانات المعالجة، فقد اختلف الفقه في هذا الامر وانقسم إلى اتجاهين فالبعض يرى ان البيانات لا تصلح لان تكون محلا للضبط لانتقاء الكيان المادي لها ولا سبيل لضبطها[4], إما الاتجاه الثاني فيرى أن البيانات المعالجة ما هي إلا ذبذبات الكترونية تقبل التسجيل والحفظ والتخزين ولهذه الطريقة يمكن نقلها وبثها واستقبالها[5]. وتواجه عملية الضبط للبيانات صعوبات منها :-

---

([1]) د. براء منذر كمال عبد اللطيف: شرح قانون أصول المحاكمات الجزائية، ط2، مكتبة السنهوري، بغداد، 2012، ص206.

([2]) مصطفى محمد مرسي: التحقيق الجنائي في الجرائم الالكترونية، ط1، دار النهضة العربية، القاهرة، 2009، ص213.

([3]) بهاء المسرى: جرائم المحمول والانترنت، منشأة المعارف، الإسكندرية، 2017، ص267.

([4])

([5])

1- حجم الشبكة التي تحتوي على المعلومات والمطلوب ضبطها .
2- يمثل التفتيش والضبط اعتداء على حقوق الغير او حرمة حياته فيجب اتخاذ الضمانات الكافية لحماية هذه الحقوق .
3- وجود هذه البيانات في شبكات أو أجهزة تابعة لدولة أجنبية, وهنا يظهر لنا أهمية التعاون الدولي في مجال مكافحة الجرائم السبرانية.

المطلب الثاني

التعاون الدولي في مكافحة الجريمة السبرانية

تعد الجريمة السبرانية من الجرائم العابرة للحدود والتي لا تقف عند حدود الدولة بل تتعدى إلى دول أخرى, وقد يساهم أكثر من شخص في دول مختلفة في ارتكاب جريمة سبرانية واحدة يقع ضحيتها عدد من الأفراد يقيمون في بلدان متعددة الأمر الذي يتطلب معه وجوب التعاون بين الدول لمكافحة هذه الجريمة والتعاون المقصود هنا لا يقتصر على التعاون القضائي بين الدول بل يشمل التعاون الفني, إلا أن هذا التعاون ليس بالأمر اليسير بل تواجهه صعوبات وهذا ما سنحاول بيانه في الفرعين التاليين.

الفرع الأول

التعاون القضائي في مكافحة الجريمة السبرانية

يعد التعاون القضائي الآلية الرئيسية لمكافحة الجريمة السبرانية, ففاعلية التحقيق والملاحقة القضائية غالبا ما يقتضي المساعدة من السلطات في البلد الذي كان منشأ للجريمة أو من السلطات التي عبر من خلاله النشاط المجرم وهو في وصوله إلى الهدف الذي يبتغيه أو حيث قد توجد أدلة الجريمة, فقد يكون مرتكب الجريمة من جنسية دولة ما ويستعمل حواسيب في دولة أخرى وتقع أثار الجريمة في دولة ثالثة في هذه الحالة يقف مبدأ السيادة ومشاكل الحدود والولايات القضائية عقبه أمام اكتشاف هذه الجريمة ومعاقبة مرتكبيها ومن هنا تظهر أهمية التعاون القضائي بين الدول. والتعاون القضائي يأخذ عدة صور أهمها:

أولا: تبادل المعلومات.

لتبادل المعلومات بين الدول أهمية كبيرة بوصفه وسيلة لمكافحة الأجرام عموماً والجريمة السبرانية خصوصاً، وذلك لما توفره من معلومات صحيحة وموثوقة التي بدورها تساند الأجهزة التي تقوم بتنفيذ القانون وتشمل المعلومات والوثائق التي تطلبها سلطة أجنبية وهي بصدد النظر في جريمة معلوماتية معينه[1].

ثانياً: نقل الإجراءات.

يقصد بنقل الإجراءات قيام دولة بمقتضى معاهدة باتخاذ إجراءات جنائية وهي بصدد التحقق في جريمة سبرانية ارتكبت في دولة اخرى تنقل الإجراءات لمصلحتها[2]. ويشترط لنقل الإجراءات أن يكون الفعل المرتكب والذي يستند إليه الطلب مجرماً لدى الدولة المطلوب منها تقديم الإجراءات، وهذا ما جاء في معاهدة الأمم المتحدة النموذجية بشان نقل الإجراءات في المسائل الجنائية[3].

ثالثا: الإنابة القضائية الدولية.

يقصد بهذه الصورة من صور المساعدة القضائية (تكليف جهة قضائية في الدولة لجهة قضائية في دولة أخرى باتخاذ إجراء قضائي نيابة عنها طبقاً لمعاهدة آو اتفاق بين دولتين)[4]. فهذه الصورة تهدف إلى تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية والتي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى مثل سماع الشهود أو إجراء تفتيش وعادةً ما يتم طلب الإنابة القضائية عبر القنوات الدبلوماسية. إلا انه سعياً وراء الحد من الروتين والتعقيد والبطء التي تتميز بها الإجراءات الدبلوماسية فقد أبرمت اتفاقيات ساهمت في تقصير الوقت واختصار الإجراءات والتي نصت على الاتصال المباشر بين السلطات القضائية في الدول الاطراف منها اتفاقية الأمم المتحدة لمكافحة الفساد واتفاقية الرياض العربية للتعاون القضائي[5].

([1]) حسين بن سعيد بن سيف الغافري: الجهود الدولية في مواجهة جرائم الانترنيت, بحث منشور على الشبكة الدولية (الانترنيت) الموقع www.minshawi.com, ص5, تاريخ الزيارة 2017/12/15 .

([2]) حسين بن سعيد بن سيف الغافري: المرجع السابق, ص9.

([3]) المادة (2) معاهدة الأمم المتحدة النموذجية بشأن نقل ألإجراءات في المسائل الجنائية 1990.

([4]) د0 رعد فجر الراوي: شرح قانون أصول المحاكمات الجزائية ,ج2, ط1, مكتب الهاشمي للكتاب إلجامعي ,بغداد ,2016, ص244 .

([5]) المادة (15) اتفاقية الرياض العربية للتعاون القضائي1983. (ف13 م46) اتفاقية الأمم المتحدة لمكافحة الفساد2003 .

رابعاَ: تسليم المجرمين.

يعتبر تسليم المجرمين شكلاً من أشكال التعاون الدولي في مكافحة الجريمة, وهذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات ومنها مجال الاتصالات وتقنية المعلومات, إذ أن الحدود القائمة بين الدول لم تعد تشكل حاجزاً أمام مرتكبيها, كما إن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل امتد إلى أكثر من إقليم, فقد يشرع في التحضير لارتكاب جريمته في دولة, ويشرف على تنفيذها في دولة أخرى, وقد يفر إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة, وبما انه لا يمكن لأي دولة تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين كان لابد من إيجاد إلية معينة للتعاون مع الدول التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها, وهذه الإلية تتمثل في تسليم المجرمين الفارين لها, وهذا الإجراء يقوم أساسا على إن الدولة التي يتواجد على إقليمها المتهم بارتكاب جريمة معلوماتية عليها أن تقوم بمحاكمته أذا كان تشريعها يسمح بذلك, وإلا كان عليها تسليمه لمحكمه أخرى مختصة[1].

يعرف تسليم المجرمين بأنه (نظام في علاقات الدول من مقتضاه أن تتخلى دولة عن شخص موجود على إقليمها لدولة أخرى بناء على طلبها لتتولى محاكمته عن جريمة منسوب إليه ارتكابها أو لتنفيذ حكم صادراً من محاكمها وذلك باعتبارها صاحبة الاختصاص)[2], وتسليم المجرمين قد ينظم باتفاقيات دولية أو اتفاقيات ثنائيه؛ مثل اتفاقية جامعة الدول العربية عام 1953، واتفاقية بودابست التي نظمت مسألة تسليم المجرم الالكتروني إذ اشترطت أن تكون الجريمة معاقب عليها بمقتضى قانون الطرفين بعقوبة سالبة للحرية لا تقل عن سنة[3].

الفرع الثاني

التعاون الفني في مكافحة الجريمة السبرانية

لا يقتصر التعاون الدولي لمكافحة الجريمة السبرانية على المساعدة القضائية المتبادلة فحسب وإنما يشمل كذلك المساعدة التقنية وتبادل الخبرات بين الدول, فالتقدم المتواصل بين الدول في تكنولوجيا المعلومات يفرض على الجهات القضائية والأمنية أن تسير في خطوات تواكب التطور السريع التي تشهدها هذه التقنيات والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذا التقدم، ومن ناحية اخرى فأن أعمال القانون في مواجهة الإجرام السبراني يستلزم اتخاذ إجراءات تتجاوز ما هو سائد في المدونة العقابية التقليدية, لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعه في التنفيذ وسهولها في إخفائها ومحو أثارها, وبالتالي فان ظهور هذه الأنماط

([1]) أمير فرج يوسف: مرجع سابق, ص476.

([2]) د. علي حسين الخلف, د. سلطان عبد القادر الشاوي: المبادئ العامة في قانون العقوبات, ط2,العاتك لصناعة الكتاب, القاهرة, 2010, ص120.

([3]) المادة (24) اتفاقية بودابست لمكافحة الجرائم الالكترونية عام 2001.

الجديدة من الجرائم أصبح يشكل عبئاً ثقيلاً على عاتق الأجهزة القضائية المختصة, الأمر الذي يجب معه أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والقدرة في التعامل مع الجريمة السبرانية, ولا يمكن تحقيق ذلك إلا عن طريق تدريب الكوادر القضائية من خلال الاستفادة من خبرات ومهارات الآخرين عن طريق أشخاص أكفاء ومؤهلين على نقل التجارب والمهارات بوسائل سهلة وميسره[1].

وبما إن كفاءة الدول تختلف فيما بينها وذلك بحسب تقدم الدولة ورقيها فأجهزة العدالة بالدول النامية ليست لديها الجاهزية لمواجهة الجرائم المتعلقة بشبكة الانترنيت لافتقارها الموارد الكافية البشرية والمادية الأمر الذي يدعو بالضرورة إلى وجود تعاون دولي في مجال التدريب وتبادل الخبرات. وهذا ما نجده في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود أذ نصت على انه: ((تعمل كل دولة طرف قدر الضرورة على أنشاء أو تطوير أو تحسين برنامج خاص للعاملين في أجهزتها المعنية بالنفاذ القانون ...))[2].

أما عن المنهج التدريبي فيجب أن يشمل على بيان المخاطر والتهديدات ونقاط الضعف وأماكن الاختراقات لشبكة المعلومات وأجهزة الحاسب الآلي وتحديد أنماط ونوعية الجريمة السبرانية, وبياناً لأهم الصفات التي يتميز بها المجرم ألمعلوماتي والدوافع وراء ارتكابه للجريمة، كذلك يشمل التدريب على إجراءات التحقيق وتجميع المعلومات وتحليلها وأساليب المواجهة والاستجواب, بالإضافة إلى ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على الأدلة [3].

من الاتفاقيات التي نصت على التعاون الدولي في مكافحة الجريمة السبرانية هي اتفاقية بودابست لمكافحة الجرائم الإكترونية عام 2001. والاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2012. والاتفاقية الأمريكية المتعلقة بجرائم الحاسب الآلي والانترنيت 1999. وعلى الرغم من وجود هذه الاتفاقيات التي تنص على ضرورة التعاون الدولي إلا أن هذا التعاون تواجهه صعوبات لابد من بيانها وهي:

أولا: عدم وجود نموذج موحد للنشاط الإجرامي.

أن الأنظمة في بلدان العالم لم تتفق على صورة محددة يندرج ضمنها ما يسمى إساءات استخدام النظم المعلوماتية, ولم تحدد النشاط الذي يعتبر جريمة فاختلاف التقاليد بين الدول والعادات والأديان جعلت ما يعتبر مباحاً في دولة ما لا يكون كذلك في دولة أخرى, وبالتالي فان اختلاف الدول في ذلك جعل من الصعوبة تحديد

([1]) امير فرج يوسف :مرجع سابق, ص438.

([2])المادة(29) اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الحدود عام 2000.

([3]) حسين بن سعيد بن سيف الغافري: مرجع سابق,ص41.

النشاط الذي يعتبر نشاطاً مُجَرماً في جميع دول العالم[1]. وهذا الأمر يقتضي تحديث التشريعات المحلية المعنية بالإجرام السبراني وإبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم.

ثانيا: اختلاف النظم القانونية والإجرائية.

بسبب هذا الاختلاف قد تكون هناك طرق للتحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بأجرائها أصلا. كما هو الحال بالنسبة للمراقبة الالكترونية, فإذا ما اعتبرت أن طريقة ما من طرق جمع الأدلة أو التحقيق إنها قانونية في دولة معينة؛ قد تكون بذات الطريقة غير مشروعة في دولة أخرى, بالإضافة إلا إن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطريقة ترى هذه الدولة إنها غير مشروعة.

ثالثاً: عدم وجود قنوات اتصال.

إن أهم الأهداف المرجوة من التعاون الدولي في مجال الجريمة هي الحصول على المعلومات والبيانات المتعلقة بها, وللوصول إلى هذا الهدف لابد من وجود نظام اتصال يسمح للجهات القائمة بالتحقيق الاتصال بجهات أجنبية للحصول على المعلومات والبيانات, وان عدم وجود مثل هذا النظام يعني انعدام الفائدة من التعاون الدولي[2]. وللقضاء على هذه الصعوبة نرى انه من الضرورة أن تعقد اتفاقيات على الصعيد الدولي تنص على إنشاء قنوات اتصال بين دول العالم للحصول على المعلومات وتبادلها.

رابعاً: مشكلة الاختصاص في الجرائم السبرانية.

تعد الجرائم السبرانية من اكبر الجرائم التي تثير مسألة الاختصاص على المستوى الدولي, فقد يرتكب أجنبي جريمة من الجرائم السبرانية في إقليم دولة معينة, فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة صاحبة الإقليم استناداً إلى مبدأ الإقليمية, وتخضع إلى الاختصاص الجنائي لدولة الأجنبي على أساس الاختصاص الشخصي، كذلك قد تقع الجريمة السبرانية التي تهدد امن وسلامة الدول الأخرى في إقليم دولة معينة فتخضع لاختصاص الدولة التي مست الجريمة أمنها[3]. وللقضاء على هذه الصعوبة نرى انه لابد من عقد اتفاقيات دولية يتم فيها توحيد وجهات النظر فيما تتعلق بقواعد الاختصاص القضائي.

([1]) أمير فرج يوسف: مرجع سابق,ص435.

([2]) حسين بن سعيد بن سيف الغافري: مرجع سابق,ص53.

([3]) امير فرج يوسف: مرجع سابق, ص436.

خامساً: الصعوبات المتعلقة في مجال التدريب.

تتمثل في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لاعتقادهم بدوره السلبي في تطوير العمل من خلال ما تعلمه المتدربون واكتسبوه من معلومات في الدورات التدريبية, ومن الصعوبات التي تهدد التدريب أيضا ما يتعلق بالفوارق الفردية وتأثيرها على اكتساب المهارات, اذ يوجد بعض الأشخاص مما لا يعي شيء في هذا المجال, وبالمقابل يوجد أشخاص على درجة عالية من الثقافة والدراية في هذا المجال بالإضافة إلى إن نظرة المدرب إلى الدورات التدريبية على إنها مرحلة تدريبية أو عب لا طائل منه تهدد العملية التدريبية[1]. ونرى انه يجب أن تتوفر دورات تدريبية على مستوى العالم في هذا المجال وان تكون هذه الدورات متناسبة مع حجم التطور الذي تشهده التقنية الالكترونية.

سادساً: الصعوبات المتعلقة بالمساعدات القضائية.

إن الأصل بالنسبة لطلبات الإنابة القضائية الدولية والتي تعد من أهم صور المساعدة القضائية الدولية في المجال الجنائي أن تسلم بالطرق الدبلوماسية الأمر الذي يجعلها تتسم بعدم السرعة والتعقيد, والذي يتعارض مع طبيعة الانترنيت وما تتميز به من سرعة وهو الأمر الذي انعكس على الجرائم المتعلقة بالأنترنيت. وللقضاء على هذه الصعوبة لابد من وجود طرق تتسم بالسرعة تسلم من خلالها طلبات الإنابة كتعين سلطة مركزية[2].

سابعاً: التجريم المزدوج.

يعد التجريم المزدوج من أهم الشروط الخاصة بنظام تسليم المجرمين وبالرغم من أهميته إلا انه يشكل عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم السبرانية فقد لا يشكل الفعل جريمة في دولة معينة, ويكون كذلك في دولة أخرى الأمر الذي يعوق التعاون الدولي في مجال تسليم المجرمين[3].

ولأجل القضاء على هذه الصعوبات لابد من إدراج أحكام عامة في المعاهدات المعنية بتسليم المجرمين وذلك أما بسرد الأفعال التي تتطلب أن تُجرم كجرائم مهمة أو أفعال مخلة بمقتضى قانون الدولتين أو بمجرد السماح بالتسليم لأي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة [4].

([1]) أمير فرج يوسف: مرجع سابق,ص438.

([2]) علي حسين الطوالبه: التعاون القضائي في مجال مكافحة الجرائم الالكترونية, بحث منشور على الشبكة الدولية (الانترنيت),الموقع www.policemc.gv.bh, ص11 تاريخ الزيارة 2017/11/20.

([3]) امير فرج يوسف: مرجع سابق, ص437.

([4]) حسين بن سعيد بن سيف الغافري: مرجع سابق ص60.

الخاتمـــــة

يتطلب لتحقيق الحماية من الجريمة السبرانية وضع تشريعات داخلية تتناسب مع التطور في الظروف ومنها الظروف المتعلقة بالتطور العلمي والتكنلوجي. عليه حاولنا عرض أهم المشاكل القانونية التي يتعرض لها القصور التشريعي في مجال الجريمة السيبرانية ومعالجتها لضمان مستقبل افضل. لان الفضاء السيبراني يمكن ان يهدد المستقبل من خلال اساءة استخدامه بأفعال يمكن ان تشكل جريمة، فاذا لم تتوفر له الحماية القانونية اللازمة من خلال نصوص القانون الداخلي فان ذلك يشكل قصور تشريعي يجب ان تتحقق له المواجهة الجنائية لوضع حلول مستقبلية. وسنتناول في الخاتمة اهم النتائج والمقترحات.

اولا: النتائج:

1. يلاحظ على نصوص النظام الاساسي للمحكمة الدولية الجنائية انها اعطت قوة الزامية للجرائم الجسيمة التي تدخل في نطاق القانون الدولي الجنائي وذلك من خلال تحديد الجرائم الدولية التي تدخل في اختصاص هذه المحكمة وهي العدوان والابادة الجماعية والجرائم ضد الانسانية وجرائم الحرب، وبالعودة الى الهجمات السيبرانية نلاحظ انها يمكن ان تشكل جرائم تعتبر اشد جسامة من الجرائم التقليدية وعليه يجب ان تقع المسؤولية الدولية الجنائية نتيجة لهذه الهجمات.
2. تعتبر الجريمة السبرانية اكبر مشكلة تواجه رجال القانون في الدول التي لا تمتلك تشريع كافي لردعها والتي تكون مرتبطة بالتطور التكنولوجي الهائل الذي يتقدم يوما بعد يوم، وكذلك المجرم المعلوماتي الذي يختلف عن المجرم الاعتيادي من حيث ذكاءه وطرقه في الاحتيال، حيث يجب موازاة هذا الذكاء بمحققين يتميزون بنفس الدرجة من الذكاء.
3. لما كانت الجريمة السبرانية واقعا نعيشه الان وانتشرت بين افراد المجتمع ولأجل حماية مصالح الافراد والحفاظ على ممتلكاتهم وسرية معلوماتهم وبسبب غياب التشريعات اللازمة لردعها والحد من اثارها وجب التنويه على ماهية هذه الجرائم وبيان خصائصها وطرق التحقيق فيها ومجال التعاون الدولي.
4. الجريمة السيبرانية تتميز عن الجريمة التقليدية بعدة خصائص. منها أنها تعد جريمة عابره للحدود مما يؤدي إلى عدم قدرة القائمين عليها لمكافحتها. كما انها تعد مشكلة من المشكلات التي أفرزتها المعلوماتية فهذه الثورة على قدر ما قدمته من تسهيلات للأفراد والمجتمعات على حد سواء فإنها قد زعزعت سكينتهم. من خلال تميز المجرم الالكتروني عن المجرم العادي. وعدم أمكانية تطبيق أحكام الجرائم العادية على الجرائم الالكترونية وسبب ذلك اتخاذ هذه الجريمة من الحواسيب والشبكات بيئة لها. كما أن ضعف اغلب التشريعات في مجال مكافحة الظاهرة الإجرامية لما تمثله من مخاطر تهدد أفراد المجتمع ككل وبدون استثناء.

ثانيا: المقترحات.

1- ضرورة أعداد الكوادر الأمنية وسلطات تحقيق كفؤة من الناحية الفنية وهذا ما تفتقده اكثر البلاد العربية.
2- لتحقق المسؤولية الدولية الجنائية لابد من عد الهجمات السيبرانية من ضمن جرائم العدوان الجسيم لغرض تطبيق مبدأ التكامل بين المحكمة الدولية الجنائية والقضاء الوطني، والذي أخذ به النظام الاساسي والتي نصت عليه الفقرة الرابعة من ديباجته على ان معظم الجرائم الجسيمة والتي تهم المجتمع الدولي باسره الان تمر دون عقاب وأن المحاكمة الفعالة عنها يجب كفالتها على المستوى الوطني مع دعم من التعاون الدولي.
3- ضرورة تطوير التشريعات الحالية لقصورها في مجال الجرائم المستحدثة وخاصة السبرانية. وتشديد العقوبة التي تقع بهذه الوسيلة.
4- ضرورة التعاون بين الدول العربية في مجال مكافحة الظاهرة الاجرامية لما تمثله من مخاطر تهدد افراد المجتمع ككل وبدون استثناء .
5- عدم وجود اتفاقيات عربية مشتركة في هذا الصدد الامر الذي نوصي بعقد مثل هذه الاتفاقيات على غرار الدول الاوربية .
6- عقد ندوات ومؤتمرات لمكافحة الاجرام الالكتروني .
7- تأهيل المجرمين الإلكترونيين وجعلهم اعضاء صالحين في المجتمع واستغلال ذكائهم في تطوير الاجهزة الامنية وبنفس الوقت يتم توجيههم نحو فعل الخير.
8- ضرورة وجود قوات شرطة متخصصة في هذا النوع من الجرائم وتوجيه المواطنين باتخاذ كافة الاحتياطات الامنية للمحافظة على معلوماتهم.

المراجع

اولاً: الكتب القانونية.

1. امير فرج يوسف: الجريمة الالكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت.
2. د. براء منذر كمال عبد اللطيف: شرح قانون أصول المحاكمات الجزائية، ط2، مكتبة السنهوري، بغداد، 2012.
3. بهاء المسرى: جرائم المحمول والانترنت، منشاءه المعارف، مطبعة دار المعارف، الاسكندرية،2007.
4. د. حسين طاهر داود: جرائم نظم المعلومات، اكاديمية نايف للعلوم، ط1، الرياض، 2000.
5. حسين بن سعيد بن سيف الغافري: الجهود الدولية في مواجهة جرائم الانترنيت, بحث منشور على الشبكة الدولية (الانترنيت) الموقع www.minshawi.com.
6. د. رعد فجر الراوي: شرح قانون اصول المحاكمات الجزائية، ج1،ط1، مكتب الهاشمي للكتاب الجامعي، بغداد، 2016.
7. د. رعد فجر الراوي: شرح قانون اصول المحاكمات الجزائية، ج2، ط1، مكتب الهاشمي للكتاب الجامعي، بغداد،2016.
8. سعيد حسب الله سعد الله: شرح قانون أصول المحاكمات الجزائية، دار أبن الاثير، الموصل، 2008.
9. د. عبدالله عبدالكريم عبدالله: جرائم المعلوماتية والانترنت (الجرائم الالكترونية)، ط1، منشورات الحلبي الحقوقية، بيروت،2007.
10. د. علي جبار الحسناوي: جرائم الحاسوب والانترنت ، دار البازوري العلمية للنشر، عمان، 2009.
11. د. علي حسين الخلف ود. سلطان عبدالقادر الشاوي: المبادئ العامة في قانون العقوبات، مكتبة السنهوري، بغداد، 2015.
12. علي حسين الطوالبه: التعاون القضائي في مجال مكافحة الجرائم الالكترونية, بحث منشور على الشبكة الدولية (الانترنيت),الموقع www.policemc.gv.bh.
13. د. فخري عبدالرزاق صلبي الحديثي: شرح قانون العقوبات القسم العام ، ط2، العاتك للطباعة والنشر، القاهرة،2010.
14. د. ماهر عبد شويش الدرة: شرح قانون العقوبات القسم الخاص، دار أبن الأثير، الموصل، 1988.
15. محمد امين الشوابكة: جرائم الحاسوب والانترنت الجريمة المعلوماتية، دار الثقافة والنشر والتوزيع ، الاردن، 2009.

16. محمد عبيد الكعبي: الجرائم الناشئة عن استخدام الغير مشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، بدون سنة.
17. محمد حجازي: جرائم الحاسبة والانترنيت (الجرائم المعلوماتية)، بلا مكان نشر، 2005.
18. مصطفى محمد موسى: التحقيق الجنائي في الجرائم الالكترونية، ط1، دار النهضة العربية، القاهرة، 2009.
19. نهلا عبد القادر المومني: الجرائم المعلوماتية، ط2، دار الثقافة لنشر والتوزيع، الاردن، عمان، 2001.
20. هلالي عبد اللاه احمد: جرائم الحاسب والانترنت بين التجريم الجنائي واليات المواجهة ، دار النهضة العربية، القاهرة، 2016.

ثانياً: الاتفاقيات الدولية والقوانين.

1- اتفاقية الرياض العربية للتعاون القضائي.
2- اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الحدود.
3- اتفاقية الامم المتحدة لمكافحة الفساد.
4- اتفاقية بودابست لمكافحة الجرائم الالكترونية 2010.
5- قانون العقوبات رقم 111لسنة 1969.
6- قانون اصول المحاكمات الجزائية رقم 76 لسنة 1983.