ISSN: 2519 – 6138 (Print)
E-ISSN: 2663 – 8983(On Line)

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

Tikrit University Journal for Rights
Journal Homepage : http://tujr.tu.edu.iq/index.php/t

كلية القانون
College of Law

Cyber war and the position of international humanitarian law

Dr. Hamid Mohammed Ali Al-Baldawi
Al-Imam University College / Balad, Department of Law, Salahaddin, Iraq
hamedali196666@gmail.com

Article info.

Article history:
- Received 15 May 2023
- Accepted 26 June 2023
- Available online 1 Sept 2023

Keywords:
- Cyber war.
- international humanitarian law.
- cyberspace.

Abstract: The last decade has witnessed rapid developments in the field of information technology, leading to far-reaching changes in almost all areas of life. Cybercrime has continued to grow over the years as new crimes have been introduced into the deep Internet. The trend in recent attacks around the world has shown how diverse the perpetrators are and what they can do. The impact on organizations around the world cannot be emphasized. Cyber laws have also been incorporated over the years to be implemented at various levels and jurisdiction. The trend has called for attacks and the growing need among culprits for concerns about what cybercrime laws have done to curb growing crime. In this research, we will look at cybercrime and cyber laws in order to be able to make laws more effective and apply them in preventing more cybercrime.

الحرب السبرانية وموقف القانون الدولي الانساني

م.د. حامد محمد علي البلداوي
كلية الامام الجامعة / بلد، قسم القانون، صلاح الدين، العراق
hamedali196666@gmail.com

معلومات البحث :

تواريخ البحث:
- الاستلام : ١٥ / ايار / ٢٠٢٣
- القبول : ٢٦ / حزيران / ٢٠٢٣
- النشر المباشر : ١ / ايلول /٢٠٢٣

الكلمات المفتاحية :
- الحرب السبرانية.
- القانون الدولي الإنساني.
- الفضاء السبراني.

الخلاصة: شهد العقد الأخير تطورات سريعة في مجال تكنولوجيا المعلومات مما أفضى الى متغيرات بعيدة المدى في جميع مجالات الحياة تقريباً. إذ إستمرت الجرائم السيبرانية في النمو على مر السنين حيث تم إدخال جرائم جديدة في الشبكة الدولية للمعلومات. وقد أظهر الإتجاه في الهجمات الأخيرة في جميع أنحاء العالم مدى تنوع مرتكبي الجرائم وما يستطيعون فعله. لا يمكن التأكيد على التأثير والأثر الواقع على المنظمات في جميع أنحاء العالم. كما تم دمج القوانين السيبرانية على مر السنين ليتم تنفيذها على مختلف المستويات والإختصاص القضائي. وقد دعا الاتجاه الهجمات والحاجة المتزايدة بين الجناة الى مخاوف بشأن ما قامت به القوانين السيبرانية المدمجة للحد من الجرائم المتنامية. سنتطرق في دراسة هذا البحث في جرائم الإنترنت والقوانين الإلكترونية من أجل أن تكون قادرة على جعل القوانين أكثر فاعلية وتطبيقها في منع المزيد من الجرائم السيبرانية.

المقدمة :

الجرائم السيبرانية (cyber crime) أي الجرائم الإفتراضية الواقعة في فضاء إلكتروني منبثق من (cyber space) أي الفضاء التخيلي أو الإفتراضي، ويعد عالم الرياضيات نوربرت وينر (Norbert wiener)، هو أول من إستخدم مصطلح السيبرانية وذلك في عام ١٩٤٨م ، وفي الوقت نفسه هناك أضرار حدثت خلال السنوات الأخيرة وباتت هذه الجرائم من أخطر أنواع جرائم العصر إنتقل مرتكبيها بالجرائم من صورها التقليدية الى جريمة أخرى إلكترونية. إذ تعد مكافحة الجرائم السيبرانية ضمان لتعزيز للأمن الدولي.

أهمية البحث: تستمد أهمية الموضوع في توعية الأفراد من كافة المجتمعات والدول في الوسائل والطرق التي تلجأ إليها التنظيمات الإرهابية لغايات استقطاب وتجنيد هؤلاء الأفراد، كما يستمد هذا الموضوع أهميته إدراكاً من الواقع بأنَّ ظاهرة الجرائم المستحدثة ومنها الجرائم السيبرانية ,وكذلك الهدف من البحث هو تزايد اللجوء الى الهجمات السيبرانية وتزايد مشاركة المدنيين بصورة مباشرة وغير مباشرة في العمليات العدائية.

إشكالية البحث: تكمن إشكالية البحث بالحرب السيبرانية في مدى كفاية الحماية القانونية الدولية لمكافحة الجرائم التي تحصل نتيجة الحرب السيبرانية؟ وما هي إلتزامات الدول الأساسية بشأن مكافحة اللجوء الى الحرب السيبرانية ومدى امكانية الدول بالحد من الآثار الضارة لهذه الهجمات؟

فرضية البحث: تتمثلُ فرضية البحث بأنَّ الجرائم السيبرانية هي جريمة دولية إلكترونية (معلوماتية) ذات طبيعة خاصة. إذ يناقش البحث فرضيتين هما اولا: الاضرار التي تحصل نتيجة الحرب السيبرانية, ثانيا: هل تستطيع التشريعات والمحاكم القضائية بوسائلها وإجراءاتها الورقية أن تواجه غموض وتحديات جرائم العصر الحديثة.

منهجية البحث: حيث ستعتمدُ الدراسة في معالجتها لهذا الموضوع على المنهج الوصفي و التحليلي بإعتبارهما الأنسب بحكمِ التطرق إلى مختلف الجرائم التي تحصل ومعالجتها بنصوص القوانين.

خطة البحث: سنقسم دراسة هذا البحث على مبحثين، وهما ما يأتي:

المبحث الأول: مفهوم الجرائم السيبرانية:

المطلب الأول: تعريف الجرائم السيبرانية وخصائصها.

المطلب الثاني: التحديات التي يمثلها الأمن السيبراني للدول العظمى.

المبحث الثاني: آليات مكافحة الجرائم السيبرانية:

المطلب الأول: جهود المنظات الدولية لمكافحة الجرائم السيبرانية.

المطلب الثاني: التعاون الدولي لمكافحة الجرائم السيبرانية.

المبحث الأول

مفهوم الجرائم السيبرانية

إذ لم تكن الجرائم السيبرانية معروفة إلا في وقت قريب، ما يشكل إحدى أهم التحديات الراهنة التي يواجهها المختصون في القانون الدولي العام، وبالخصوص في تحديد طبيعتها وعناصرها، فضلاً عن نطاق هذه الجرائم في ضوء القانون الدولي الإنساني وما يترتب عليها من تبعات المسؤولية الدولية الجنائية كانت أم مدنية. وما يزيد في إتساع التحدي الذي يواجهه المختصون في القانون الدولي العام، والإنساني على وجه الخصوص، إنما يتجسد في الغموض التي إكتنفت مفهوم الجرائم السيبرانية وعدم الاتفاق على تعريف محدد، يمكن الإستدلال في ضوئه لتنظيم إستخدامها بالحظر أو التقييد لمواجهة عواقبها الخطرة على الصعيد الإنسان[١].

1- Oona' A.Hathway, Rebecca Crootof, Philip Levtiz, aley Nix, Aileen Nowlan, William perdue and Julia Spiegel, "The Law of Cyber- Attack", California Law Review, 2012,p.7.

ومن أجل الوقوف على تعريف الجرائم السيبرانية سنتناول دراسة هذا المبحث على مطلبين، وهما ما يأتي:

المطلب الأول: تعريف الجرائم السيبرانية وخصائصها

المطلب الثاني: التحديات التي يمثلها الأمن السيبراني وما هي العلاقة بينه وبين الدول العظمى

المطلب الأول / تعريف الجرائم السيبرانية وخصائصها

يشهد العالم في الفترة الأخيرة نوعاً جديداً من سباق التسليح لا على غرار المعروفة منها في حقل الأسلحة التقليدية وغير التقليدية، ويقوم هذا السباق على إستحداث أو تطوير برامج إلكترونية معدة لأغراض عسكرية تعرف إختصاراً بالسايبر (Cyber). لقد أعادت بعض الدول الى الأذهان نظرية توازن الرعب [١]، ولكن بصورة مختلفة نوعاً ما، وذلك بإستخدام تقنيات إلكترونية في نطاق أعمال عدائية [٢].

وعليه ومما تقدم سنقسم دراسة هذا المطلب على فرعين، وهما ما يأتي:

الفرع الأول: تعريف الجرائم السيبرانية

الفرع الثاني: خصائص الجرائم السيبرانية

الفرع الأول / تعريف الجرائم السيبرانية

تشير المراجع العلمية أن عالم الرياضيات نوربرت وينر (Norbert wiener)، هو أول من إستخدم مصطلح السيبرانية في عام ١٩٤٨، أثناء دراسته لموضوع القيادة والسيطرة والإتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكية [٣].

أولاً: تعريف الجرائم السيبرانية لغةً

يتضح أن مصدر كلمة سايبر (Cyber) في المعاجم اللغوية أنها يونانية الأصل وترجع الى مصطلح (kybernetes)، الذي ورد بداية في مؤلفات الخيال العلمي ويعني القيادة أو التحكم عن بُعد فيما عرف

---

[٢] – شاع إستعمال مصطلح "توازن الرعب" خلال فترة الحرب الباردة، ويشير ميتشل مارين (Micheal Marien)، بالقول: "إن الولايات المتحدة الأمريكية والإتحاد السوفيتي السابق تبنيا هذا المصطلح كأساس للتفاهم الثنائي بشأن سباق التسليح بإعتبارهما قوتان استأثرتا بـ ٩٦% من الأسلحة النووية الإستراتيجية، و٧٠% من مجموع الصادرات العالمية للأسلحة و٥٠% من الإنفاق العالمي على التسلح".

[٢] – د. أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨، ص٥,

[4-] Norbert wiener: Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.

قاموس مصطلحات الأمن المعلوماتي، مصطلح السيبرانية بالقول "هجوم عبر الفضاء الإلكتروني يهدف الى السيطرة على مواقع إلكترونية أو بنى تحتية محمية إلكترونياً لتعطيلها أو تدميرها أو الإضرار بها"[١].

أما في اللغة العربية وبالرجوع الى المختصين فيها، فنجد أن تحدياً واجهوه في إختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الإنكليزية، ولا أدل على ذلك من أن الترجمة العربية لعنوان إتفاقية مجلس أوربا المتعلقة بالجرائم السيبرانية كانت ترجمة غير صائبة، إذ تُرجمَ العنوان (Convention on Cybercrime) الى اللغة العربية بأنه (الاتفاقية المتعلقة بالجرائم الإلكترونية) ويعود السبب في ذلك الى عدم وجود مصطلح مناظر في اللغة العربية[٢].

ثانياً: تعريف الجرائم السيبرانية إصطلاحاً

في هذه الدراسة إستخدمنا مصطلح الجرائم السيبرانية(Cyber Crime)، على عكس ما درج عليه البعض من المختصين، فمنهم من تبنى مصطلح الفضاء السيبراني (Cyber Space)، بالإستناد الى المحيط الذي تجري فيه العمليات السيبرانية (Cyber Operations) الناشئة عن أداء أنظمة إلكترونية مهمتها متابعة وجمع المعلومات التي تعمل إلكترونياً وتحليلها ومن ثم إتخاذ إجراءات محددة لمهاجمتها عن طريق أنظمة إلكترونية أخرى مخصصة لهذا الغرض[٣] .

أما البعض الآخر فاختار مصطلح الهجمات السيبرانية (Cyber Attacks)، كوصف واقعي يجمع بين كل ما ذكر آنفاً ، فهو تصرف يدور في عالم إفتراضي قائم على إستخدام بيانات رقمية ووسائل إتصال تعمل إلكترونياً، ومن ثم تطور ليتضمن مفهوماً أوسع يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، جراء إختراق مواقع إلكترونية حساسة، عادةً ما تقوم بوظائف تصنف بأنها ذات أولوية، كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات ووسائل النقل الأخرى .

يمكن القول بالاستناد إلى طبيعة السلاح المستخدم، وبالتالي يمكن القول أن الحرب السيبرانية، هي الحرب التي تستخدم فيها الاسلحة غير التقليدية وفقاً للآثار المترتبة على استخدام هكذا نوع من الاسلحة والمتمثلة بالتدمير واسع النطاق.

أن مصطلح الحرب هو مصطلح غير محبذ في وقتنا الراهن على المستوى التنظيم القانوني الدولي ، فيكون مصطلح الهجمات السيبرانية أكثر قرباً للموضوع، ولاسيما أن تصرفات دولية عدة أشارت الى

1- Richard Kissel, "Glassory of Key Information Security Terms", National Institute of Stand ards and technology, U.S Department of Commerce, Revision, 2, May 2013, p.57.

٢- د. أحمد عبيس نعمة الفتلاوي: مصدر سابق، ص١٢.

3- James A. Lewis, "Sovereignty and the role of Government in Cyberspace", Center for Strategic and International Studies Journal, spring summer, vol. XVI, Issue II, 2010, p.56.

مصطلح الهجمات، وعدتها بمثابة التصرف الذي يوضع في الحسبان في أثناء النزاعات المسلحة، طبقاً للقانون الدولي الإنساني[١] .

الفرع الثاني / خصائص الجرائم السيبرانية

إنَّ للجريمة السيبرانية عدد من الخصائص والسمات التي تختلف فيها عن بقية الجرائم، وتحول دون إختلاطها بالجرائم العادية، حيث يمكننا إيراد أهم هذه الخصائص وهي كما يأتي:

اولا : الجرائم السيبرانية مستحدثة: هي من أبرز أنواع الجرائم المستحدثة التي تشكل خطراً جسيماً في ظل العولمة، فلا تعد هذه الجرائم من الغرابة سواءً التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في إرتكابها، إذ إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، إذْ يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها[٢].

ثانيا : جريمة عابرة للحدود: إذْ تتسم الجرائم السيبرانية بكونها جريمة إرهابية متجاوزه للحدود وعابره للدول وللقارات، إذ أنَّها غير خاضعة لنطاق إقليمي محدود، إذْ أعطى إنتشار أجهزة الحاسوب إمكانية لربط أعداد هائلة بشبكات الإنترنت والمرتبطة بالشبكة العنكبوتية من غير أنْ تخضع لحدود الزمان والمكان، وهنا تظهر الحاجة لوجود تنظيم قانوني دولي متلائم معه لمكافحة مثل هذا النوع من الجرائم وضبط مرتكبيها.

---

٣ – الفقرة (٢) من المادة (٥٤) من البروتوكول الإضافي الأول لعام ١٩٧٧، والتي نصت بأنه: "يحظر مهاجمة أو تدمير أو نقل أو تعطيل الأعيان والمواد التي لا غنى عنها لبقاء السكان المدنيين..." كذلك المادة (٥٦) من البروتوكول نفسه والتي نصت: "لا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة ألا وهي السدود والجسور والمحطات النووية لتوليد الطاقة الكهربائية محلاً للهجوم" كذلك الفقرة (٢) من المادة (١٣) من البروتوكول الإضافي الثاني، والتي نصت بأنه " لا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة ألا وهي السدود والجسور والمحطات النووية لتوليد الطاقة الكهربائية محلاً للهجوم حتى لو كانت أهدافاً عسكرية، إذا كان من شأن هذا الهجوم أن يتسبب في إنطلاق قوى خطرة ترتب خسائر فادحة بين السكان المدنيين". د. أحمد عبيس نعمة الفتلاوي: مصدر سابق، ص١٤–١٥,

١– د. مصطفى يوسف كافي: جرائم (الفساد، غسل الأموال، السياحة، الإرهاب الإلكتروني، المعلوماتية)، ط١، مكتبة المجتمع العربي للنشر والتوزيع، الأردن، ٢٠١٤، ص١٤٧؛ مصعب القطاونة: الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني الأردن الإلكتروني، ٢٠١٠، ص٥؛ د. عبد القادر الشيخلي: طبيعة الإرهاب الإلكتروني، بحث مقدم الى المؤتمر العالمي (مكافحة الإرهاب) المملكة العربية السعودية، بتاريخ ٢٢–٢٥/شباط/٢٠١٥، ص٧–٨,

ثالثا : وقوع الجرائم الإلكترونية أثناء المعالجة الآلية للبيانات: إنَّ من خصائص الجرائم الإلكترونية أنَّها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكومبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجرائم الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات، وذلك لأنَّ تخلُّف الشرط يعني إنتفاء الجرائم الإلكترونية، وذلك أنَّ الجرائم الإلكترونية تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواءً عند مرحلة إدخال البيانات، أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات[١].

رابعا : عولمة الجرائم السيبرانية تثير مشاكل حول القانون الواجب التطبيق.

خامسا : جاذبية الجرائم السيبرانية: نظراً لما تمثله سوق الكمبيوتر من ثروة كبيرة فقد غدت أكثر جاذبية بإستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول الى الشبكات وسرقة المعلومات[٢].

المطلب الثاني / التحديات التي يمثلها الأمن السيبراني للدول العظمى

لقد أصبحت الهجمات السيبرانية واحدة من السبل والأساليب المؤثرة من دون تكاليف كبيرة، فبعد أن كان النظام التقليدي يعتمد على القوة العسكرية البشرية لمواجهة باقي الدول أو السيطرة عليها براً وجواً وبحرا ، الذي كان يكلف الدول الكثير من الخسائر البشرية والمادية ويتطلب الوقت والجهد ، فإن النظام الدولي المعلوماتي (السيبراني) يعتمد أساساً على الوسائل الإلكترونية , وأصبح بذلك أمام المستخدم الخارجي المسلح ببعض المعرفة وبعض الأهداف الخبيثة، طريقة جديدة للتسلل الى الأنظمة الداخلية، حالما يصبح هذا الدخيل داخل شبكة المؤسسة أو الشركة، يمكنه أن يتجول فيها.

ثم هل أن الهجوم السيبراني يؤدي الى خرق سيادة الدول المستهدفة؟ ، كيف تعامل المجتمع الدولي مع هذه الهجمات؟ ، هل الأنظمة القانونية الحالية تنطبق على الهجمات السيبرانية؟ ، فإن كانت كذلك فهل هي كافية لتنظيم كل أشكال الهجمات السيبرانية أو هناك حاجة الى وضع إتفاقية دولية سواء كانت ثنائية أم متعددة الأطراف لتنظيم إستخدامها؟ .

٢- مشتاق طالب وهيب: مفهوم الجرائم المعلوماتية ودور الحاسوب بإرتكابها، بحث منشور في مجلة العلوم القانونية والسياسية، جامعة ديالى، مج٣، ع١، ٢٠١٤، ص٣٤٣؛ محمد علي سالم، حسون عبيد هجيج: الجرائم المعلوماتية، بحث منشور في مجلة جامعة بابل للعلوم الإنسانية، مج١٤، ع٢، العراق، ٢٠٠٧، ص,٩٢

٣- كوثر حازم سلطان: موقف القانون والقضاء من الجريمة الإلكترونية [السيرانية] : دراسة مقارنة ، بحث منشور, مجلة الجامعة المستنصرية كلية التربية الأساسية ,٢٠١٦م, ص,٩٧٣

وعليه ومما تقدم سنقسم دراسة هذا المطلب على فرعين، وهما ما يأتي:

الفرع الأول: التحديات التي يمثلها الأمن السيبراني.

الفرع الثاني: الدول العظمى وموقفها من الهجمات السيبرانية.

الفرع الأول / التحديات التي يمثلها الأمن السيبراني

ومن التحديات الراهنة أمام سيادة الدولة ونطاقها، ظهور الهجمات السيبرانية فالتغييرات التكنولوجية الهائلة وتطورات إستخدام الحاسوب وشبكات الإتصال التي نعيشها في الوقت الحاضر والتي لا تعترف بالحدود الجغرافية، خلقت فضاء جديداً إلى جانب البر والبحر والجو والفضاء الخارجي، وهو الفضاء السيبراني(Cyber-space) [١] .

وهنا ظهر التحدي الحقيقي، إذ لا تستطيع الدولة فرض سيطرتها على مواطنيها في الفضاء السيبراني عن طريق الجنسية مثلاً، كما لا يقتصر الفضاء السيبراني على الإحاطة بالمفاهيم الجغرافية التقليدية بل يمتد ليشمل ظاهرة تغييب الهوية الوطنية [٢].

إن إنعدام الحدود الجغرافية في الفضاء السيبراني ، جعل البعض يرى بأن الفضاء السيبراني يخرج عن نطاق سيطرة وسيادة الدولة، ويؤدي إلى انعدام حكم القانون فيه ، إلا أن ذلك ليس صحيحاً إطلاقا لأسباب عديدة منها:

١- الفضاء السيبراني يتطلب أجهزة ومعدات مادية التي من دونها لا يستطيع -المستخدمون الحصول عليه ، وبما إن الهيكل المادي يقع ضمن أراضي الدولة فمن الطبيعي أن يقع ضمن اختصاص تلك الدولة، وبذلك تفرض الدولة سيادتها وسيطرتهاعليه, ومن جهة أخرى إن الفضاء السيبراني بحد ذاته يتطلب التنظيم والرقابة فيما يتعلق بأسماء المستخدمين و عناوينهم و نطاق إنطلاق إشارة الإتصال الإلكتروني[٣].

٢- إن القدرة على التسبب بالأضرار أو خلق الفوضى أو نشر خطابات العنف - أو الكراهية (Speech of Hate) من خلال الفضاء السيبراني، ودائماً ما تصور الدول بأن الفضاء

١- مصطفى عصام نعوس، سيادة الدولة في الفضاء الإلكتروني ، مجلة الشريعة و القانون ، جامعة الإمارات العربية المتحدة ، كلية القانون ، السنة السادسة و العشرون ، العدد ٥١ ، يوليو ٢٠١٢ ، ص ,١٢٨

٢- ينظر نبيل علي وفادية حجازي،الفجوة الرقمية رؤية عربية لمجتمع المعرفة،سلسلة عالم المعرفة،العدد٣١٨, الكويت، المجلس الوطني للثقافة والفنون والآداب، ٢٠٠٥,ص ,١٢

1- See Joshua E. Kastenberg, Non Intervention and Neutrality in cyberspace: An Emerging principle in the National Practice of International Law, 64 Air Force Law Review.

السيبراني من المسائل المتعلقة بسيادة الدول الأمر الذي يتطلب إيجاد الوسيلة الممكنة لفرض السيطرة والحد من مخاطره [١].

٣- المحتويات والمعلومات المرسلة من خلال الفضاء السيبراني لها أهميتها – في العالم الحقيقي، أي للدولة حق للسيطرة على المعلومات التي تتدفق عبر هذا الفضاء و بالذات في حماية مواطنيها من البيانات التشهيرية أو حماية النظام والآداب العامة من المواد الإباحية، فإن هذه المعلومات يجب أن تخضع لقوانين الدولة التي تقع فيها لحماية مصالحها [٢].

٤- العلاقات المالية التي تنشأ من خلال الفضاء السيبراني تحتاج إلى قوانين – تنظمها ، والا أصبحت ضعيفة وغير موثوقة [٣].

إن الأسباب التي تم ذكرها تفند القول بأن الفضاء السيبراني، بمنأى عن سيادة الدول ولذلك شرعت الدول القوانين الداخلية بمعالجة مشاكل السيادة ، لتلافي المخاطر المستقبلية نتيجة إستخدام الفضاء السيبراني ، سواء على الصعيد الوطني أم الدولي. فقامت أغلبيتها بتطوير تشريعاتها القانونية لإستيعاب هذه الجرائم .

الفرع الثاني / الدول العظمى وموقفها من الهجمات السيبرانية

أصبحت الهجمات السيبرانية في هذا الزمن معقدة وخطيرة ولها أنواع متعددة وهي على نحو متزايد، وعندما وصلت أهدافها لمحاولة تدمير البنية التحتية لدول بأكملها، أصبح تطويرها في مقدمة أهداف الدول، فهي تعتبر قدرة ثانية لا تقل أهمية عن القدرة العسكرية وحتى النووية، إذ إن القدرة السيبرانية يمكنها اختراق المنشأت والقاذفات النووية والقواعد العسكرية وتعطيلها أو التحكم بها.

لذلك علينا البحث في جهود الدول من أجل التصدي و مكافحة هذه التهديدات سواء على الصعيد الداخلي للدول أو على الصعيد الدولي، لاسيما الدول العظمى لفهم مدى خطورة هذه الهجمات وماهو موقف الدول من مسألة تنظيم الهجمات السيبرانية ضمن إتفاقيات دولية, إن التفوق الذي تتميز به بعض الدول كالولايات المتحدة وروسيا الإتحادية في حقل الأنظمة الإلكترونية العسكرية والهيمنة على الساحة

2- Patrick W. Franzese, Sovereignty in Cyberspace: can it exist? University of Pennsylvania Law 20/6/2014 available at: http://www.law.upenn.edu/live/files/3473-Franzese-p-sovereignty-in cyberspacecan-it-exist. (last visit at 29/8/2016).-

3-See Jack L. Goldsmith & Tim Wu, Who controls the internet? Illusions of a borderless world, (Oxford Univ. Press, 2006).

4--See Jack L. Goldsmith & Tim Wu, Who controls the internet? Illusions of a borderless world, op.cit, P. 147-61.

الدولية، أدخل موضوع الهجمات السيبرانية ضمن دائرة الصراع التقليدي الذي كان دائراً بين هاتين القوتين في أثناء لحرب الباردة (Cold War) ، أي الهيمنة من أجل النفوذ وتحقيق المكاسب [١] .

اولا: الولايات المتحدة الامريكية : قبل مايقارب اربعة عقود، انشأت وزارة الدفاع الأمريكية شبكة الإنترنيت واليوم تظل الولايات المتحدة بأغلب المقاييس هي الدولة الرائدة في هذا المجال من حيث إستخداماتها العسكرية والمدنية، إلا إن فرط الإعتماد على أجهزة الحواسيب المرتبطة بشبكة واحدة ومستويات إتصالات متعددة، يجعل الولايات المتحدة أكثر عرضة للهجمات من أي دولة أخرى. وقد أصبح الفضاء الإلكتروني مصدراً رئيسياً لإنعدام الأمن حيث بات جانب الهجوم يتمتع بالغلبة على جانب الدفاع في هذه المرحلة من التطور التكنولوجي [٢] .

وبعد أحداث ١١ ايلول ٢٠٠١ م بدأ التركيز على الفضاء السيبراني كتهديد أمني جديد بفعل أحداث دولية كان أبرزها إستخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة [٣] , حيث تمحور إهتمام القيادة الأمريكية بعد ٢٠٠١ م فيما يتعلق بمخاطر الإنترنيت و محاولة التصدي لأي هجوم سيبراني قد يعمل على الإضرار ببعض مكونات البنية التحتية الأمريكية, وهناك مناورة سنوية يتم إجراءها في الولايات المتحدة الأمريكية، تحت عنوان العاصفة السيبرانية (cyber Storm) والهدف منها إختبار جاهزية الولايات المتحدة لمواجهة أي هجوم الكتروني معادي ، يشارك فيها ١١٢ جهازً أمني اً أمريكي[٤] , و إنها عملت على تطوير أسلحة وأدوات الحرب الإلكترونية تشمل فايروسات قادرة على تخريب شبكات العدو الحساسة، لتحسين درجات الإستعداد لحرب الكمبيوتر.

أما على صعيد التنظيم الدولي، فإن الولايات المتحدة ترغب في إبرام إتفاقية تقيد إستخدام المنظومات والتقنيات الإلكترونية في نطاق العمليات العسكرية والأمنية، اي: إنها لا تؤيد الحظرالتام لإستخدام تلك التقنيات ,ويمكن الوصول الى هذا التوجه الأمريكي عن طريق ما أبداه مدير وكالة (US cybercom) بالقول: "نحن ماضون في تبني قواعد بشأن الحرب السيبرانية لأجل تبني قواعد تحدد آلية

١- ينظر احمد عبيس نعمة الفتلاوي، مصدر سابق، ص ٣١.

٢- جوزيف س.ناي، الحرب والسلام في الفضاء الالكتروني، كمبريدج، ٢٠١٢ متوفر على الموقع,أخر زيارة بتاريخ ٢٠ / ١٢/ ٢٠٢٢م . http://alghad.com/prints/617907 .

٣- عادل عبد الصادق، الفضاء الإلكتروني وأسلحة الإنتشار الشامل بين الردع وسباق التسلح، مصدر سابق ص,٢٤

4- Ellen Nakashima, list of cyber weapons developed by pentagon to streamline computer warfare, the Washington post, published June 1, 2011 http://www.washington.post.com/national/list-of-cyber…/2021/8/16.

تعامل الحكومات مع الحرب السيبرانية مع تأكيد إن نجاح أي إتفاقية إنما يقوم على تحديد آليات ملزمة للدول الاطراف" [١].

يبين ذلك إن الولايات المتحدة، لا ترغب في حظر إستخدام الأسلحة الإلكترونية بشكل تام، وذلك خدمة لمصالحها، ولتسوي إستخدامها للنشاطات السيبرا نية في مواجهة أعدائها.

ثانيا: دولة روسيا الإ تحادية(الاتحاد السوفيتي السابق): منذ منتصف القرن الماضي ، بدأت معظم الدول ذات الجيوش الحديثة في تكوين وحدات فرعية خاصة مهمتها الأعمال الإلكترونية المضادة في بعض فروعها الرئيسية كالقوات الجوية و البحرية، ومن هذه الدول الإتحاد السوفيتي السابق ، الذي ظل حتى عام ١٩٧٠ م من الدول القلة التي لديها تنظيم عام للحرب الإلكترونية [٢].

ومنذ عام ١٩٩٩م أصبح أمن المعلومات و البرمجيات في روسيا الإتحادية، مسألة لها الأولوية في حزمة إهتمامات الأجهزة الأمنية والمخابراتية. فلم تخف الحكومة الروسية نشاطها في مجال الحرب الإلكترونية حينما أعلنت عن برنامج ما يسمى ب "أسلحة المعلومات". و انصرفت الجهود الحكومية الى تأمين الفضاء الإلكتروني عن طريق تخصيص إدارة مسؤولة عن أمن المعلومات تتصل بوكالة الأمن الروسي(FSB) لتطوير نظم المعلومات وحماية البيانات في عام ٢٠٠٢م , قامت وزارة الدفاع الروسية بالتعاون مع بعض شركات البرامجيات والأوساط الأكاديمية بوضع عقيدة "الحرب الإلكترونية" التي إنطوت على سلسلة من التدابير الهجومية والدفاعية لضمان نجاحها[٣],على الصعيد الداخلي إنتهجت روسيا منهجاً متشددا فيما يخص مراقبة الإنترنيت، إذ أسست جهازاً ضخماً للمراقبة يحمل إسم ستورم (storm) ، ويقوم هذا الجهاز بنسخ كل بايت مهما صغر حجمه يدخل أو يخرج من روسيا الى كمبيوترات تخزين مركزية في موسكو تحت سيطرة خدمة الأمن الإتحادية [٤] .

1- Transcript of Remarks by Gen. K. Alexander at the center for strategic and International Studies ,Washington ,D.C.(June3,2010) at 11,available at http://www.nsa.gov/public.

٢- دور الحرب الإلكترونية في الحروب الحقيقية ، مقال منشور بتاريخ ٢٤ /مارس/ ٢٠١٠م . على الموقع الالكتروني, أخر زيارة بتاريخ ٢٨ / ١ / ٢٠٢٣ , http://defense- arab.com/vb/threads/276111

٣- سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي (رؤية مستقبلية)، بحث منشور في مجلة رسالة الحقوق،جامعة كربلاء، السنة السابعة العدد الثاني ٢٠١٥م . ص ٩٥ .متوفر على الموقع:اخر زيارة بتاريخ ٢٠٢٣/٢/١٠م. http://law.uokerbala,edu.iq/index/php/law-magazine/100

٤- الإنترنيت والسيطرة الخفية... التمهيد لحرب غير مسبوقة، مقال منشور بتاريخ ٥ /نوفمبر/ ٢٠١٠ متاح على الموقع الإلكتروني :) آخر زيارة : ١٢ / ١٢ / ٢٠٢٢م. http://anbaa.info/spip.php?article

أما على صعيد التنظيم الدولي فإن روسيا الاتحادية، تعد من أقوى دول العالم التي يمكنها إدارة الحروب الإلكترونية على مستوى العالم، و لكن خلافاً للولايات المتحدة فإنها ترى إن السبيل لمنع الكوارث والنزاعات الناشئة عن الهجمات السيبرانية يكمن في الحظر التام لإستخدام النشاطات الإلكترونية في العمليات العسكرية، لا فقط تقييد إستخدامها على مستوى القانون الدولي [١] .

وفي استمرار تطورالتقدم التكلونوجي والمعلومات والإتصالات في سياق الأمن الدولي قدمت روسيا عدة إقتراحات الى الأمم المتحدة منها:

١- في عام – ١٩٩٨م قدمت إقتراحاً للجمعية العامة لأمم المتحدة طالبت فيه بوضع مسودة قرار يتعلق بأمن المعلومات وحمل المقترح مسمى "التطورات في مجال المعلومات والإتصالات في سياق الأمن الدولي"، وقد تبنت الجمعية العامة للامم المتحدة هذا الإقتراح بالإجماع [٢] .

٢- قدمت إقتراحاً في عام٢٠٠٠ م يدعو الى تحديد المفاهيم الدولية المرتبطة بأمن المعلومات.

٣- أيضاً قامت بتقديم مسودة قرار للجمعية العامة تسعى الى تطوير إتفاقيات – الحد من التسلح، لكي تشمل عمليات شبكات المعلومات و أشارت مسودة القرار الروسي في الدورة (٧٠ / ٥٣) للجمعية العامة لأمم المتحدة [٣].

ويتبين من ماتقدم ان روسيا الاتحادية تحاول ان تضع حدا للهجمات السبرانية بصورة شاملة وتقنين عمل التقنية السبرانية دوليا من خلال المقترحات التي قدمتها للجمعية العامة للامم المتحدة على عكس ما تعمل عليه الولايات المتحدة الامريكية .

المبحث الثاني

آليات مكافحة الجرائم السيبرانية

رغم أن الجهود التي بذلتها بعض المنظمات الدولية والإقليمية كالأمم المتحدة وحلف الشمال الأطلسي و المجلس الأوربي بشأن تنظيم الهجمات السيبرانية تبرهن على وجود إهتمام متزايد لمعالجة هذه الهجمات من خلال أطر قانونية مشتركة، إلا إنها أخفقت حتى الآن في تأسيس إطار قانوني صارم يحكم بفاعلية كل الهجمات السيبرانية، وذلك بسبب المصالح الدولية في الإحتكار والهيمنة على قطاع

5- ينظر: احمد عبيس نعمة الفتلاوي، مصدر سابق. ص ٣٧.

1-General Assembly, Developments in the field of information and Telecommunication in the context of international security, UN document A/RES/53/70, 4 January 1999.

2- General Assembly , A/RES/61/54, 19 Dec 2006.

البرامج الإلكتر ونية لأغراض العسكرية دون إبرام اتفاقيات دولية تحظر إستخدام الهجمات السيبرانية أو تقييدها.

وعليه ومما تقدم سنتناول دراسة هذا المبحث على مطلبين، وهما مايأتي:

المطلب الأول: جهود المنظمات الدولية في مكافحة الجرائم السيبرانية.

المطلب الثاني: التعاون الدولي في مكافحة الجرائم السيبرانية.

المطلب الأول / جهود المنظمات الدولية في مكافحة الجرائم السيبرانية

من المعلوم أن أحد الأهداف الرئيسية لمنظمة الأمم المتحدة هو حفظ السلم والأمن الدولي، حيث تغيرت الطرق التي تجري فيها النزاعات المسلحة في السنوات الأخيرة، إذ إنتقلت المعارك من المجال المادي الى مجال إفتراضي يسمى بالفضاء السيابر والحروب السيبرانية.

في هذا المطلب سنحاول تسليط الضوء على الجهود الدولية الرامية بالاساس إلى تنظيم موضوع الهجمات السيبرانية وفقا لما استقر عليه في القانون الدولي العرفي وعلى النحو الآتي:

الفرع الاول / دور منظمة الامم المتحدة

بالرغم من كون ميثاق منظمة الأمم المتحدة لم ينصْ صراحةً على تجريم استخدام المعلومات كأداة إرهابية ضمن إطار ما يعرف بـالإرهاب السيبراني، إلّا أنَّ روح الميثاق يتفق مع تجريم استخدامه بوصفه إنتهاك لما ورد في الميثاق بخصوص "التهديد أو استخدام القوة ضد السلامة الإقليمية أو الإستقلال السياسي لأي دولة"، ومع الأخذ في الإعتبار أنَّ الميثاق جاء لمكافحة النزاعات المسلحة، على اعتبار إن الجرائم السيبرانية واستخدام حرب المعلومات يقعان ضمن العدوان، حيث إن هذا النوع من الإرهاب لا يتفق مع السيادة الدولية، لأنه يهدد العلاقات الدولية باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الإستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد منظمة الأمم المتحدة[١].

وتبذل منظمة الأمم المتحدة جهوداً فاعلة لا يستهان بها في مجال مكافحة الجرائم السيبرانية الدولية ,وقد أقرت الأمم المتحدة عدة قرارات بشأن التطورات في مجال المعلومات والإتصالات في سياق الأمن الدولي ،وأكدت من خلالها على ما يلي : "قد تستخدم هذه التقنيات لأغراض تتعارض مع السلم و الأمن الدولي" و أيضا على "إن إنتشار البيانات و إستعمال التقنيات و الأساليب المعلوماتية قد أثرت على

1- د. سامر مؤيد عبد اللطيف، د. نوري رشيد الشافعي: دور المنظمات الدولية في مكافحة الإرهاب الرقمي، جامعة كربلاء، ٢٠١٦، ص١٥، بحث منشور عبر الرابط الآتي:
http://elearning.uokerbala.edu.iq/mod/resource/view.php?id=12861، (آخر زيارة للموقع في ٢٠٢٣/٢/٢م).

مصالح المجتمع الدولي" ,إلا إن هذه القرارات جاءت غامضة ولا تتطلب أية إجراءات محددة من قبل أعضاء الأمم المتحدة ومن أمثلة القرارات الصادرة عن الجمعية العامة يمكن الإشارة إلى القرار المتعلق بـ "إنشاء ثقافة عالمية بشأن الأمن السيبراني وحماية البنية التحتية الأساسية للمعلومات" ,وكذلك القرار المتعلق ب "إنشاء ثقافة عالمية بشأن الأمن السيبراني و الإستفادة من الجهود الوطنية لحماية البنى التحتية الأساسية للمعلومات" [١] .

وعند متابعة قرارات الجمعية العامة نجدها غالباً ما تدعو إلى المزيد من المباحثات والمناقشات بشأن "الأمن المعلوماتي" وقضايا الأمن المعلوماتي الدولي من دون تحديد إجراءات واضحة . و هو مايمكن بيانه في مؤتمر القمة العالمي بشأن الأمن المعلوماتي الذي عقد على مرحلتين في عامي ٢٠٠٣م و ٢٠٠٥م إذ جاء من دون نتائج ملموسة تذكر [٢] .

أما في عام ٢٠١٠ فقد إتخذت الأمم المتحدة خطوة جريئة وذلك نتيجة التوصيات التي قدمها خبراء الأمن السيبراني من خمس عشرة دولة بما فيهم القوى السيبرانية العظمى كالولايات المتحدة و روسيا الإتحادية والصين الى مجلس الأمن التابع لأمم المتحدة، وتعد هذه خطوة مبدئية نحو بناء إطار دولي لأمن والإستقرار الذي تتطلبه التقنيات الحديثة، وقد دعت هذه التوصيات إلى:

١- المزيد من الحوارات بين الدول.

٢- بناء الثقة والإستقرار وتدابير الحد من المخاطر بما فيها تبادل وجهات النظر الوطنية بشأن إستخدام تكنولوجيا المعلومات والإتصالات في أثناء النزاع.

٣- تبادل المعلومات بشأن التشريعات الوطنية وتكنولوجيا المعلومات – والإتصالات، الإستراتيجيات والتكنولوجيا السياسية والأمنية.

٤- تحديد التدابير بهدف دعم بناء القدرات في الدول النامية.

٥- إيجاد الإمكانيات لوضع المصطلحات والتعاريف المشتركة [٣].

إن السؤال الذي يطرح هنا : ما السبب في عدم مبادرة الأمم المتحدة إلى طرح مشروع إتفاقية دولية لحد الآن ، بشأن حظر أو تقييد إستخدام الهجمات السيبرا نية على غرار إتفاقية حظر إنتشار الأسلحة النووية ، ولماذا إقتصر دورها على المناقشات وتبادل المعلومات .

1- GA. Res. 64/211, U. N. Doc. No, A/RES/64/211 (March., 17, 2010).

2- World summit on the information society: Geneva 2003-Tunis 2005.

3-- U. N. Secretary General , Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, 4, U. N. Doc. A/65/20 (July. 30, 2010) .

للأجابة لابد من القول بأن التفوق الذي تتميز به بعض الدول كالولايات المتحدة وروسيا الإتحادية في حقل الأنظمة الإلكترونية العسكرية والمهيمنة على الساحة الدولية، أدخل موضوع الهجمات السيبرانية ضمن دائرة الصراع التقليدي الذي كان دائراً بينها أثناء الحرب الباردة [١].

إن التعاون الدولي هذا يوحي بإمكانية عقد معاهدة متعددة الأطراف في المستقبل تحت رعاية الأمم المتحدة والتي تعد روسيا من أهم المنادين بها وبالفعل هناك محادثات بشأن كيفية عمل معاهدة تنظم الهجمات السيبرانية بين الولايات المتحدة وروسيا. وان كانت هذه المحادثات في مراحلها الأولية إلا إنها مشجعة [٢].

الفرع الثاني / مبادرات منظمة شنغهاي للتعاون (sco)

منظمة شانغهاي للتعاون هي منظمة دولية سياسية واقتصادية وأمنية. تأسست في ٢٠٠١ م في شانغهاي، على يد قادة ستة دول آسيوية؛ هي الصين، وكازاخستان،وقيرغيزستان، وروسيا، وطاجيكستان، وأوزبكستان. وقع ميثاق منظمة شانغهاي للتعاون في ٢٠٠٢ م، ودخلت حيز التنفيذ في ١٩ /٩/ ٢٠٠٣ م. كانت هذه البلدان باستثناء أوزبكستان أعضاء في «مجموعة شانغهاي الخماسية» التي تأسست في ٢٦ /٤/ ١٩٩٦م في شانغهاي.

اتخذت منظمة شنغهاي للتعاون ,خطوات أولية مهمة نحو التعاون في مجال الأمن السيبراني كما يلي:

١- عام ٢٠٠٦م وقع رؤساء الدول الأعضاء إعلاناً حول أمن المعلومات الدولية .

٢- عام ٢٠٠٩م تم صدور "إعلان يكاترينبورغ" والك في قمة منظمة شنغهاي للتعاون التي عقدت في يكهاترينبورغ في روسيا وقد أظهرت المنظمة من خلاله التعاون والالتزام بهدف منع الحروب والهجمهات السيبرانية ,والحاجة الملحة للرد على التهديدات السيبرانية واعتبر أمن المعلومات على نفس أهمية السيادة الوطنية، والأمن الوطني، والاستقرار الاجتماعي والاقتصادي. حيث جاء في الفقرة السابعة : "تؤكد الدول الأعضاء في منظمة شنغهاي للتعاون على أهمية ضمان أمن المعلومات الدولي كأحد العناصر الرئيسية للنظام العام للأمن الدولي" [٣].

٤- أحمد عبيس نعمة الفتلاوي، مشكلة الأسلحة التقليدية بين جهود المجتمع الدولي والقانون الدولي العام، مكتبة زين الحقوقية والأدبية، الطبعة الأولى، بيروت، ٢٠١٣ ، ص ,٣١

1-Markoff J. & Kramer A. E., in shift U.S. talks to Russia Internet Security, New York Times, Dec., 12, 2009.

2- Shanghai Cooperation Organization, Yekaterinburg Declaration of The Heads of The Member States of The Shanghai Cooperation Organization, Consulate General of=

٣- عام ٢٠١١ تقدمت دول منظمة شنغهاي للتعاون بمشروع قرار للجمعية العامة للأمم المتحدة بشأن أمن المعلومات.

خلاصة القول، إن الجهود الدولية وإن كانت لا ترقى إلى مستوى تنظيمي دولي شامل، إلا أنها تظهر مدى الاهتمام الدولي المتزايد لوضع أطر تنظيمية للتصدي للهجمات السيبرانية.

المطلب الثاني / التعاون الدولي في مكافحة الجرائم السيبرانية

تكمن أهمية التعاون الأمني الدولي بضرورة شعور المجتمع الدولي بمخاطر الجرائم السيبرانية وما يمكن أن تحدثهُ من آثار سلبية على مصالح المجتمع الدولي المشتركة، وإدراكه للنمو السريع والمتزايد لهذا النمط المستجد والخطر من الجرائم الإرهابية الإلكترونية، وهذا التعاون يكون بين أجهزة الشرطة الدولية المتخصصة لمكافحه الجرائم السيبرانية عن طريق إنشاء مكاتب متخصصه لجمع المعلومات عن مرتكبي هذه الجرائم وتعميمها، فينبغي أن يكون هناك تعاون بين أجهزة الشرطة المختلفة في الدول، والتنسيق فيما بينهم لضبط المجرمين ومكافحه هذه الجرائم التي تتجاوز حدود الدولة[١].

وفي ضوء ما تقدم سنتناول دراسة هذا المطلب على ثلاثة فروع، هي ما يأتي:

الفرع الاول / صور التعاون الأمني الدولي لمكافحة الإرهاب الإلكتروني

ومن أهم هذه الصور هي ما يأتي:

اولا- ربط شبكات الإتصال والمعلومات: تحتاج الأجهزة الشرطية إلى وسائل للإتصال تحقق السرعة الممكنة في أجهزة العدالة الجزائية من خلال التواصل بين سلطات التحقيق والملاحقة المختلفة، وهذا ما عمدت له الدول والمنظمات الدولية بتطوير الإتصال وتبادل المعلومات فيما بينها[٢].

ثانيا- القيام ببعض العمليات الشرطية والأمنية المشتركة: تشترك الدول فيما بينها للقيام بعمليات شرطية وأمنية بما يؤدي إلى صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم ووضع حدٍ لها، وذلك من خلال تعقب المجرم وتعقب الأدلة الرقمية وضبطها، والقيام بعمليه التفتيش العابرة للحدود

=Uzbekistan In New York City (July 9, 2009), Available at: http://eng.sectsco.org/load/198293

1-أحمد سعد محمد الحسيني: الجوانب الإجرائية للجرائم الناشئة عن إستخدام الشبكات الإلكترونية، إطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ٢٠١٢، ص٢٧٨؛ د. جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٢، ص٧٥.

2-د. عادل عبد العال إبراهيم خراشي: إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، ٢٠١٥، ص٢٤-٢٥.

لمكونات الحاسوب الآلي والأنظمة المعلوماتية وشبكات الإتصال بحثاً عما قد تحويه من أدلة وبراهين على إرتكاب الجرائم الإرهابية الإلكترونية، فالقيام بهذه الأمور يستدعي هكذا عمليات[١].

الفرع الثاني / التعاون الأمني وجهود المنظمة الدولية للشرطة الجنائية (الإنتربول) في مكافحة الجرائم السيبرانية الدولية: أُنشأت منظمة الإنتربول عام (١٩٢٣)، وهي أكبر منظمة دولية مقرها الرئيسي في مدينة ليون بفرنسا، وقد أنشأت هذه المنظمة وحدة تحليل المعلومات الجنائية والتي تقضي بإستخلاص المعلومات الهامة عن المنظمات الإجرامية وتبويبها، وذلك بهدف وضع تلك المعلومات في متناول هيئة الشرطة، أو الدول الأعضاء في الإنتربول، حيث تعمل هذه المنظمة على تأكيد وتشجيع التعاون بين سلطات البوليس[٢].

كذلك قد أنشأت هذه المنظمة خلال عام (٢٠٠٤ م) وحدات خاصه لمكافحة جرائم التكنولوجيا، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى (G-8)[٣] بوضع إستراتيجيات لمواجهة هذا النوع من الجرائم، وأبرزها إنشاء مركز إتصالات أمني عبر الشبكة المعلوماتية يعمل على مدار (٢٤ ساعة) على مستوى الشرطة في الدول الأطراف [٤].

الفرع الثالث / تبادل التعاون لمواجهة الكوارث والأزمات والمواقف الحرجة

يمثل عنصر الوقت دوراً أساسياً في المواقف الحرجة، ومن الأمور الحاسمة في مواجهة الأمر الذي يحتاج إلى تكثيف الجهود الخاصة والخبرات والإمكانيات بشكل يصعب تحقيقه إلا بتظافر الجهود الدولية، وهذا التعاون الأمني يمثل أهم الصور لمكافحة الجرائم السيبرانية الدولية، سيما وأن أجهزة العدالة الجزائية ليست بنفس المستوى والجاهزية في جميع الدول، وإنما هناك تفاوت فيما بينها، فبعض

1- د. سليمان أحمد محمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، ٢٠١٣، ص٤١٥-٤١٦.

2- نسرين عبد الحميد نبيه: الجرائم الدولية والإنتربول، المكتب الجامعي الحديث، مصر، ٢٠١١، ص٢٥٤.

3- مجموعة الثمانية أو مجموعة الدول الصناعية الثمانية تضم الدول الصناعية الكبرى في العالم أعضائها هم: الولايات ألمانيا، روسيا الاتحادية، إيطاليا، المملكة المتحدة، فرنسا، وكندا، ويمثل مجموع اقتصاد المتحدة الأمريكية، اليابان، القوة العسكرية تحتل ٧ من ٨ مراكز الأكثر أنفاقاً على التسلح) وأغلبية هذه الدول الثمانية ٦٥% من إقتصاد العالم وتقريباً كل الأسلحة النووية عالمياً)، وأنشطة المجموعة تتضمن مؤتمرات على مدار السنة ومراكز بحث سياسية مخرجاتها تتجمع في القمة السنوية التي يحضرها زعماء الدول الأعضاء.

4- نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ٢٠٠٧، ص١٥٣؛ محمد أمين الرومي: جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية،٢٠٠٣، ص١٣٦.

الدول المتقدمة تقنياً وتكنولوجياً لها دور كبير في مواجهة مثل هذه الجرائم تشريعياً وفنياً، والبعض الأخر تفتقد لذلك، ومن هنا كان لابد من التعاون بين الدول[١].

إذ يتضح مما تقدم ضرورة التعاون الدولي للحد من مخاطر الجرائم السيبرانية بإعتباره أحد الأخطار الحالية والمستقبلية، إذ أن التعاون بين جميع الدول في جميع المجالات يقلل من نسبة خطورة هذه الجرائم.

الخاتمة :

الاستنتاجات :

١- الهجمات السيبرانية من المفاهيم الحديثة التي لا يوجد اتفاق دولي على تعريفها حتى يومنا هذا، ويمكن الاستناد في ذلك إلى المادة ٣٦ من البروتوكول الإضافي الأول لعام ١٩٧٧م وأيضاً لآراء وقرارات محكمة العدل الدولية كرايها بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها .

٢- إنَّ للجرائم السيبرانية الدولية خصائص وأهداف وأشكال تميزها عن بقية الجرائم الإعتيادية والسياسية، فالجرائم السيبرانية تختلف عن الجرائم العادية في إسلوب إرتكابها وشخص مرتكبها والوسيلة المستعملة في إرتكابها، وهي من الجرائم صعبة الإكتشاف كما أنَّها تحتاجُ إلى خبراءَ مختصين في التحقيق فيها.

٣- إن عملية وضع تنظيم شامل لهذه الظاهرة الخطيرة تتسم بصعوبات شتى وذلك لأن المصالح الدولية للقوى العظمى تقف حجر عثرة أمامها، كالصعوبات التي واجهت المجتمع الدولي عند وضع إتفاقية بشأن الأسلحة النووية والجدل حول تقييدها أو حظر إستخدامها كلياً .

٤- إنَّ منظمة الأمم المتحدة بذلتْ جهوداً كبيرةً لمكافحةِ الجرائم السيبرانية من خلال إصدار قرارات عن طريق مجلس الأمن والجمعية العامة للأمم المتحدة، ولكن مثل هذه الجرائم تتطلب المزيد من الجهود بسبب الحداثة والتطور الهائل.

٥- تكمن الميزة النسبية للهجمات السيبرانية في إنخفاض تكاليفها و سهولة اللجوء اليها إذ لا تتطلب حشود اً من المقاتلين ،بل يكفي لتنفيذها شخص أو مجموعة صغيرة ممن لديهم الخبرة و المهارة في التكنولوجيا السيبرانية وثغرات البرامج و الأنظمة الكمبيوترية لإستخدامها ضد دولة أو دول أخرى.

1- أحمد سعد محمد الحسيني: مصدر سابق، ص٢٧٩؛ د. عادل عبد العال إبراهيم خراشي: مصدر سابق، ص٢٨-٢٩.

المقترحات :

١- اعتماد تعريف جامع مانع للجرائم السيبرانية الدولية، من خلالِ عقد مؤتمر دولي بإشراف الأمم المتحدة، ويتم من خلاله تحديد تعريف للجرائم السيبرانية.

٢- ضرورة التعاون الدولي للحد من مخاطر الجرائم السيبرانية بإعتباره أحد الأخطار الحالية والمستقبلية، إذ أن التعاون بين جميع الدول في جميع المجالات يقلل من نسبة خطورة هذه الجرائم.

٣- يتوجب على الدول إتخاذ خطوات جدية لمكافحة الهجمات السيبرانية بإعتماد تدريس الفضاء السيبراني والمخاطر الناشئة عنه لا سيما على المستوى الدولي في المؤسسات الأكاديمية.

٤- فصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية وذلك لحماية السكان المدنيين من مخاطر الهجمات السيبرانية .

٥- هناك حاجة الى تطوير القانون الدولي والدولي الإنساني تزامناً مع تطور التكنولوجيات ووسائل الإتصال لإحتواء التحديات الحديثة بشكل أفضل .

المصادر :

اولا المصادر العربية :

١- أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨.

٢- أحمد عبيس نعمة الفتلاوي، مشكلة الأسلحة التقليدية بين جهود المجتمع الدولي والقانون الدولي العام، مكتبة زين الحقوقية والأدبية، الطبعة الأولى، بيروت، ٢٠١٣.

٣- جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٢.

٤- سليمان أحمد محمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، ٢٠١٣.

٥- عادل عبد العال إبراهيم خراشي: إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، ٢٠١٥.

٦- علاء الدين شحاته: التعاون في مجال مكافحة الجريمة، إتراك للنشر والتوزيع، القاهرة،٢٠٠٠.

٧- محمد أمين الرومي: جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٣.

٨- محمد نيازي حتاتة: حماية الأمن العام مكافحة الجريمة على المستوى الوطني والإقليمي والدولي، الضوابط الإجرائية الوطنية والعالمية وصكوك المبادئ الإرشادية العالمية والإتفاقيات الدولية، ج١، مطبعة كلية الشرطة، القاهرة، ١٩٩٥.

٩- مصطفى يوسف كافي: جرائم (الفساد، غسل الأموال، السياحة، الإرهاب الإلكتروني، المعلوماتية)، ط١، مكتبة المجتمع العربي للنشر والتوزيع، الأردن، ٢٠١٤.

١٠- نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ٢٠٠٧.

١١- نسرين عبد الحميد نبيه: الجرائم الدولية والإنتربول، المكتب الجامعي الحديث، مصر، ٢٠١١.

١٢- هناء إسماعيل إبراهيم الأسدي: الإرهاب وغسيل الأموال كأحد مصادر تمويلة، دراسة مقارنة، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٥.

ثانيا: الرسائل والاطاريح والبحوث.

١- أحمد سعد محمد الحسيني: الجوانب الإجرائية للجرائم الناشئة عن إستخدام الشبكات الإلكترونية، إطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ٢٠١٢.

٢- سراب ثامر احمد، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة دكتوراه في القانون العام، جامعة النهرين، كلية الحقوق، ٢٠١٥.

٣- عبد القادر الشيخلي: طبيعة الإرهاب الإلكتروني، بحث مقدم الى المؤتمر العالمي (مكافحة الإرهاب) المملكة العربية السعودية، بتاريخ ٢٢-٢٥/شباط/٢٠١٥.

٤- كوثر حازم سلطان: موقف القانون والقضاء من الجريمة الإلكترونية (السيبرانية)، دراسة مقارنة، بحث منشور في مجلة كلية التربية الأساسية، الجامعة المستنصرية، العراق، مج٢٢، ع٢٠١٦،٩٦.

٥- محمد علي سالم، حسون عبيد هجيج: الجرائم المعلوماتية، بحث منشور في مجلة جامعة بابل للعلوم الإنسانية، مج١٤، ع٢، العراق، ٢٠٠٧.

٦- مشتاق طالب وهيب: مفهوم الجرائم المعلوماتية ودور الحاسوب بإرتكابها، بحث منشور في مجلة العلوم القانونية والسياسية، جامعة ديالى، مج٣، ع١، ٢٠١٤.

٧- مصطفى عصام نعوس، سيادة الدولة في الفضاء الإلكتروني ، مجلة الشريعة و القانون ، جامعة الإمارات العربية المتحدة ، كلية القانون ، السنة السادسة و العشرون ، العدد ٥١ ، يوليو ٢٠١٢ .

٨- مصعب القطاونة: الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني الأردن الإلكتروني، ٢٠١٠.

ثالثا: المواقع الالكترونية:

١- جوزيف س.ناي، الحرب والسلام في الفضاء الالكتروني، كمبريدج، ٢٠١٢ متوفر على الموقع,أخر زيارة بتاريخ ٢٠ / ١٢ / ٢٠٢٢م . http://alghad.com/prints/617907 .

٢- شيماء ابراهيم، مخاوف عالمية من الهجمات الإلكترونية، مقال منشور بتاريخ ١٨ يوليو ٢٠١٦ . متوفر على الموقع الالكتروني: (أخر زيارة بتاريخ ١٥ /١٠/ ٢٠٢٢) , http://alghad.com/prints/617907

٣- دور الحرب الإلكترونية في الحروب الحقيقية ، مقال منشور بتاريخ ٢٤ /مارس/ ٢٠١٠م . على الموقع الالكتروني, أخر زيارة بتاريخ ٢٨ / ١ / ٢٠٢٣-p/t law.net/law/archive/indexph .28524.html

٤- الإنترنيت والسيطرة الخفية... التمهيد لحرب غير مسبوقة، مقال منشور بتاريخ ٥ /نوفمبر/ ٢٠١٠ متاح على الموقع الإلكتروني :) آخر زيارة : ١٢ / ٧ / ٢٠٢١م. http://anbaa.info/spip.php?article

٥- د. سامر مؤيد عبد اللطيف، د. نوري رشيد الشافعي: دور المنظمات الدولية في مكافحة الإرهاب الرقمي، جامعة كربلاء، ٢٠١٦، ص١٥، بحث منشور عبر الرابط الآتي:

1http://elearning.uokerbala.edu.iq/mod/resource/view.php?id=1286 ، (آخر زيارة للموقع في ٢/٢/٢٠٢٢م).

رابعا: المصادر الاجنبية :

1- Oona' A.Hathway, Rebecca Crootof, Philip Levtiz, aley Nix, Aileen Nowlan, William perdue and Julia Spiegel, "The Law of Cyber- Attack", California Law Review, 2012, p.7.

2- Norbert wiener: Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.

3- Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University press, 2010.

4- Richard Kissel, "Glassory of Key Information Security Terms", National Institute of Stand ards and technology, U.S Department of Commerce, Revision, 2, May 2013, p.57.

5- James A. Lewis, "Sovereignty and the role of Government in Cyberspace", Center for Strategic and International Studies Journal, spring summer, vol. XVI, Issue II, 2010, p.56.

6- K.saalbach, "Cyber War, Methods and practice", Version 9.0, University of Osnabruck-17 Jun 2014, p.6.

7- See Joshua E. Kastenberg, Non Intervention and Neutrality in cyberspace: An Emerging principle in the National Practice of International Law, 64 Air Force Law Review.

8- Patrick W. Franzese, Sovereignty in Cyberspace: can it exist? University of Pennsylvania Law 20/6/2014 available at: http://www.law.upenn.edu/live/files/3473-Franzese-p-sovereignty-in cyberspacecan-it-exist. (last visit at 29/8/2016).-

9-See Jack L. Goldsmith & Tim Wu, Who controls the internet? Illusions of a borderless world, (Oxford Univ. Press, 2006).

10-See Jack L. Goldsmith & Tim Wu, Who controls the internet? Illusions of a borderless world, op.cit, P. 147-61.

11- Ellen Nakashima, list of cyber weapons developed by pentagon to streamline computer warfare, the Washington post, published June 1, 2011 http://www.washington.post.com/national/list-of-cyber…/2021/8/16.

12- Transcript of Remarks by Gen. K. Alexander at the center for strategic and International Studies ,Washington ,D.C.(June3,2010) at 11,available at http://www.nsa.gov/public.

13-General Assembly, Developments in the field of information and Telecommunication in the context of international security, UN document A/RES/53/70, 4 January 1999.

14- World summit on the information society: Geneva 2003-Tunis 2005.

15-- U. N. Secretary General , Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, 4, U. N. Doc. A/65/20 (July. 30, 2010) .

16-Markoff J. & Kramer A. E., in shift U.S. talks to Russia Internet Security, New York Times, Dec., 12, 2009.

17- Shanghai Cooperation Organization, Yekaterinburg Declaration of The Heads of The Member States of The Shanghai Cooperation Organization, Consulate General of Uzbekistan In New York City (July 9, 2009), Available at: http://eng.sectsco.org/load/198293 .

Sources :

First, the Arabic sources:

1- Ahmed Abbes Nima Al-Fatlawi: Cyberattacks, an analytical legal study on the challenges of their contemporary regulation, 1st edition, Zain Legal Publications, Beirut, 2018.

2- Ahmed Abis Nima Al-Fatlawi, The Problem of Conventional Weapons between the Efforts of the International Community and Public International Law, Zain Legal and Literary Library, first edition, Beirut, 2013.

3- Jamil Abdel Baqi Al-Saghir: Procedural Aspects of Internet-Related Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 2002.

4- Suleiman Ahmed Muhammad Fadl: Legislative and security confrontation of crimes arising from the use of the international information network (the Internet), Dar Al-Nahda Al-Arabiya, Cairo, 2013.

5- Adel Abdel-Al Ibrahim Kharashi: Problems of international cooperation in combating information crimes and ways to overcome them, New University House, Alexandria, 2015.

6- Aladdin Shehata: Cooperation in the Field of Combating Crime, Etrak Publishing and Distribution, Cairo, 2000.

7- Muhammad Amin Al-Roumi: Computer and Internet crimes, University Press House, Alexandria, 2003.

8- Muhammad Niazi Hatata: Protecting public security and combating crime at the national, regional and international levels, national and global procedural controls and instruments of global guiding principles and international agreements, Part 1, Police College Press, Cairo, 1995.

9- Mustafa Youssef Kafi: Crimes (corruption, money laundering, tourism, electronic terrorism, information technology), 1st edition, Arab Society Library for Publishing and Distribution, Jordan, 2014.

10- Nabila Heba Harwal: Procedural aspects of cybercrimes in the evidence-gathering stage, a comparative study, Dar Al-Fikr Al-Jami'i, Alexandria, 2007.

11- Nisreen Abdel Hamid Nabih: International Crimes and Interpol, Modern University Office, Egypt, 2011.

12- Hana Ismail Ibrahim Al-Asadi: Terrorism and money laundering as one of its funding sources, a comparative study, 1st edition, Zain Legal Publications, Beirut, 2015.

Second: Theses, dissertations, and research.

1- Ahmed Saad Muhammad Al-Husseini: Procedural aspects of crimes arising from the use of electronic networks, doctoral thesis, Faculty of Law, Ain Shams University, Egypt, 2012.

2- Sarab Thamer Ahmed, Attacks on Computer Networks in International Humanitarian Law, doctoral thesis in public law, Al-Nahrain University, Faculty of Law, 2015.

3- Abdul Qader Al-Shaikhli: The nature of electronic terrorism, a paper presented to the World Conference (Combating Terrorism), Kingdom of Saudi Arabia, on February 22-25, 2015.

4- Kawthar Hazem Sultan: The position of the law and the judiciary on electronic (cyber)crime, a comparative study, research published in the Journal of the College of Basic Education, Al-Mustansiriya University, Iraq, vol. 22, no. 96, 2016.

5- Muhammad Ali Salem, Hassoun Ubaid Hajij: Information crimes, research published in the Journal of the University of Babylon for Human Sciences, Volume 14, No. 2, Iraq, 2007.

6- Mushtaq Talib Wahib: The concept of information crimes and the role of the computer in committing them, research published in the Journal of Legal and Political Sciences, University of Diyala, Volume 3, No. 1, 2014.

7- Mustafa Essam Naous, State Sovereignty in Cyberspace, Sharia and Law Journal, United Arab Emirates University, College of Law, Twenty-Sixth Year, Issue 51, July 2012.

8- Musab Al-Qatawneh: Special Criminal Procedures in Information Crimes, research submitted to the Jordan Electronic Legal Network, 2010.

Third: Websites:

1- Joseph S. Nye, War and Peace in Cyberspace, Cambridge, 2012, available on the website, last visit on 12/20/2022 AD. http://alghad.com/prints/617907.

2- Shaima Ibrahim, Global Fears of Cyber Attacks, article published on July 18, 2016. Available on the website: (last visit on 10/15/2022), http://alghad.com/prints/617907

3- The role of electronic warfare in real wars, an article published on March 24, 2010. On the website, last visit on 1/28/2023 law.net/law/archive/indexph p/t-28524.html.

4- The Internet and hidden control... the prelude to an unprecedented war, an article published on November 5, 2010, available on the website:) Last visit: 7/12/2021 AD. http://anbaa.info/spip.php?article

5- Dr. Samer Moayed Abdel Latif, Dr. Nouri Rashid Al-Shafi'i: The role of international organizations in combating digital terrorism, University of Karbala, 2016, p. 15, research published via the following link: http://elearning.uokerbala.edu.iq/mod/resource/view.php?id=1286 1, (last visit to the site on 2/2/2022 AD).

Fourth: Foreign sources:

1- Oona' A.Hathway, Rebecca Crootof, Philip Levtiz, Aley Nix, Aileen Nowlan, William Perdue and Julia Spiegel, "The Law of Cyber- Attack", California Law Review, 2012, p.7.

2- Norbert Wiener: Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.

3- Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University press, 2010.

4- Richard Kissel, "Glassory of Key Information Security Terms", National Institute of Standards and Technology, U.S. Department of Commerce, Revision, 2, May 2013, p.57.

5- James A. Lewis, "Sovereignty and the role of government in Cyberspace," Center for Strategic and International Studies Journal, spring summer, vol. XVI, Issue II, 2010, p.56.

6- K.saalbach, "Cyber War, methods and practice", Version 9.0, University of Osnabruck-17 Jun 2014, p.6.

7- See Joshua E. Kastenberg, Non Intervention and Neutrality in cyberspace: An Emerging principle in the National Practice of International Law, 64 Air Force Law Review.

8- Patrick W. Franzese, Sovereignty in Cyberspace: can it exist? Uni versity of Pennsylvania Law 6/20/2014 available at: http://www.law.upenn.edu/live/files/3473-Franzese-p-sovereignty-in cyberspacecan-it-exist. (last visit on 8/29/2016).

9-See Jack L. Goldsmith & Tim Wu, Who controls the internet? Illusions of a borderless world, (Oxford Univ. Press, 2006).

10-See Jack L. Goldsmith & Tim Wu, Who controls the internet? Illusions of a borderless world, op.cit, P. 147-61.

11- Ellen Nakashima, list of cyber weapons developed by Pentagon to streamline computer warfare, the Washington post, published June 1, 2011 http://www.washington.post.com/national/list-of-cyber…/2021/8 /16.

12- Transcript of Remarks by Gen. K. Alexander at the center for strategic and international studies, Washington, D.C. (June 3, 2010) at 11, available at http://www.nsa.gov/public.

13-General Assembly, Developments in the field of information and Telecommunication in the context of international security, UN document A/RES/53/70, 4 January 1999.

14- World summit on the information society: Geneva 2003-Tunis 2005.

15-- U.N. Secretary General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, 4, U.N. Doc. A/65/20 (July 30, 2010).

16-Markoff J. & Kramer A.E., in shift U.S. Talks to Russia Internet Security, New York Times, Dec., 12, 2009.

17- Shanghai Cooperation Organization, Yekaterinburg Declaration of The Heads of The Member States of The Shanghai Cooperation Organization, Consulate General of Uzbekistan In New York City (July 9, 2009), Available at: http://eng.sectsco.org/load /198293.