مجلة جامعة بابل للعلوم الإنسانية، المجلد 27، العدد 4: 2019.
Journal of University of Babylon for Humanities, Vol.(27), No.(4): 2019.

The Transmission of Threats from Reality to the Virtual World

Bahaa Adnan Al-Saabri Imad Abdul Khudair Al-Zarafi
College of Political Science /University of Kufa
ealzurufi@yahoo.com

ARTICLE INFO
Submission date: 29/ 5/2019
Acceptance date: 25/6 /2019
Publication date: 13/12/2019

Abstract

Electronic threats are one of the most influential elements of international politics and economy, as a major part of the conflicts between the world's superpowers, the Internet and the digital world. Although the causes and source of threats on the Web cannot be categorically identified and whether they are supported by governments, they are mutually controversial

Since the transfer of mass media to the network in the 1990s and increasing demand on the Internet, whether in production, distribution, communication, finance, etc., most of the world's productive, services and information services have been fundamentally and fundamentally dependent on that network, because of the heavy reliance on them, and also increased the risk of cyber-attacks, which are growing in scope and expanding in a world where the Internet is fragile and easy to penetrate as a result of the development of software and computers, and increase the activity of "hackers" or "Hackers" Deep experience in the field of information technology.

Key words:- Threat transmission, Electronic threats, Causes of threats, Virtual world, Electronic space, International security, Technological progress, Electronic security

انتقال التهديدات من الواقع الى العالم الافتراضي

بهاء عدنان السعبري عماد عبد خضير الزرفي
كلية العلوم السياسية/ جامعة الكوفة
ealzurufi@yahoo.com

الخلاصة

تمثل التهديدات الالكترونية إحدى العناصر المؤثرة في السياسة والاقتصاد على الصعيد الدولي، نتيجة انتقال جزء كبير من الصراعات بين القوى العظمى في العالم، إلى شبكة الإنترنت والوسط الرقميوعلى الرغم من عدم إمكانية معرفة اسباب ومصدر التهديدات على الشبكة العنكبوتية، بصورة قاطعة، وما إذا كانت تدعمها حكومات، إلا أنها باتت تثير جدلا متبادلا بين الدول.

ومنذ انتقال وسائل التواصل الجماهيري إلى الشبكة العنبكوتية في التسعينيات، وزيادة الطلب على الإنترنت، سواءً في الإنتاج أو التوزيع أو الاتصال أو التمويل... إلخ، بات معظم خدمات العالم الإنتاجية والخدماتية والمعلوماتية يعتمد بصورة جوهرية وأساسية على تلك الشبكة، وهذا ما زاد المخاطر من جراء الاعتماد الكبير عليها، وزاد أيضا من مخاطر ما يمكن أن تتسبب به الهجمات الإلكترونية التي يتعاظم دورها ويتسع نطاقها في عالم أصبحت فيه شبكة الإنترنت هشة ويسهل اختراقها، نتيجة تطور البرمجيات والحواسيب، وزيادة نشاط "قراصنة المعلومات" أو "الهاكرز" الذين باتوا يمتلكون خبرةً عميقةً في ميدان تقنيات المعلومات.

الكلمات الدالة:– انتقال التهديدات، التهديدات الالكترونية، اسباب التهديدات، العالم الافتراضي، الفضاء الالكتروني، الامن الدولي، التقدم التكنولوجي، الامن الالكتروني

1- المقدمة

ان العالم الرقمي هو عباره عن شبكات الكمبيوتر والاتصالات الإلكترونية وعبارة عن شبكة كمبيوتر خيالية تحتوى على كم هائل من المعلومات التي يمكن الحصول عليها لتحقيق الثروة والسلطة، حيث تقترب العلاقة بين العالم المادي والعالم الواقعي بحيث يحصل مستخدمو الكمبيوتر على خبرات لا وجود لها يكتسبونها عن طريق هذا الاستخدام فتؤثر المكونات الرقمية على العالم المادي، وأصبحت قوة الكمبيوتر تتزايد مما جعل الناس يرون في الفضاء الإلكتروني أنه عالم موازٍ للواقع الذى نعيش فيه، والفضاء الإلكتروني شأنه شأن كلمة الفضاء التقليدية حيث يتألف من أربعة مكونات رئيسية هي المكان والمسافة والحجم والمسار ويتميز الفضاء الإلكتروني بغياب الحدود الجغرافية.

ويمكن القول ان تحليل تأثير نهاية الحرب الباردة واحداث الحادي عشر من ايلول على طبيعة التفاعلات الدولية، قد غير هيكلة وخارطة المخاطر والتهديدات الأمنية من نمط تقليدي إلى نمط جديد اصُطلح عليه في الكثير من الأحيان "بالتهديدات اللاتماثليةAsymmetric Threats "، وبصورة أحدث" التهديدات الهجينة Hybrids Threats" كتعبير عن زيادة التعقيد والحركية والتطور المستمر الذي يمس الظاهرة الأمنية في العلاقات الدولية انطلاقاً من تفاعلها بما يحصل على أرض الواقع خاصة فيما يتعلق بالتطور التكنولوجي والمعرفي والتقني.

ويشهد العالم اليوم موجات من التغيرات والتطورات المتسارعة في شتى مجالات الحياة الاقتصادية، والاجتماعية، والسياسية والثقافية، والامنية، ويعود ذلك إلى التقدم الهائل في تكنولوجيا المعلومات ووسائل الاتصالات التي جعلت من العالم قرية واحدة، حيث غير التقدم الهائل الذي تم إحرازه في الميدان التكنولوجي من ظروف ممارسة العلاقات الدولية تغييرا عميقا إن لم يكن قد غير من طبيعة هذه العلاقات نفسها. بحيث أصبح الحديث اليوم وبشكل متزايد عن الصراعات غير المتناظرة تدار بوسائط وأدوات ليست بالضرورة عسكرية فقد تكون الكترونية أو وسائل مدنية أو حتى فيروسات معدية وغيرها.

1- 2اشكالية البحث: يوجه العالم اليوم مجموعة من التحديات والتهديدات الامنية المختلفة، اذ لم يعد نمط التهديد التقليدي وحده قادر على فرض على عدم الاستقرار، اذ اصبح العالم الافتراضي والفضاء الالكتروني احد ساحات التهديد التي يستخدمها الفواعل في صراعاتهم.

1-3 فرضية البحث: تستند فرضية البحث هنا على ان التهديدات اصبحت متعددة ومختلفة من حيث المصدر، وان التهديدات الالكترونية تعتمد على مميزات الفضاء الالكتروني لشن الهجمات ولذلك كلما زاد الاعتماد على العالم الافتراضي كلما زادت احتمالية التعرض للتهديد بسبب ميزات وخواص هذا العالم ولأثبات الفرضية يسعى البحث للأجابة على الاسئلة التالية:

1- لماذا اصبح هناك تغيير في نمط التهديد؟

2- ما اسباب هذا التغيير في التهديد؟

2- المطلب الاول: التغيير في التهديد:-

ان النظام الدولي قد يظهر في بعض الأحيان في حالة من التوازن شبه الاستاتيكي أو الديناميكي مثله في ذلك مثل أي نظام أخر لايبقى في حالة استقرار تام، أذ تحدث هذه التغيرات في البنية السياسية، والاجتماعية، والاقتصادية لكل وحدة دولية ومن ثم في بنية النظام الدولي بصورة عامة والتي تسهم في ظهور

تهديدات جديدة الى جانب التهديدات الموجودة اصلا ،أو ان تؤدي هذه التغيرات الى اختفاء التهديدات التقليدية مقابل صعود نمط جديد من التهديدات التي ترتبط بذلك التغيير. ما نريد توضيحه هنا ،هو علاقة التغيير بالتهديد ،أو اهمية التغيير في خلق التهديد أذ ان التغيرات التي تحدث من شانها أن تعود بالمكاسب لصالح بعض الاطراف أو الوحدات الدولية ،مقابل التسبب بالخسارة لأطراف أخرى وهذه الخسائر التي يمكن أن تنجم عن التغيير تشكل جوهر التهديد الذي تؤدي اليه التغيرات المختلفة[1].

إن هيمنة التنافس والصراع بين القطبين على النظام الدولي في الفترة الممتدة من 1945 إلى1989 خلقت نوعا من التجانس والانسجام فبالنسبة للغرب العدوّ واضح محدّد وواحد هو الاتحاد السوفياتي وحلفاؤه (الشيوعية) كذلك الأمر بالنسبة للشرق العدو واضح محدد هو الولايات المتحدة وحلفاؤها (الامبريالية)، وبالنظرإلى التهديدات والأخطار التي يمثلها كل طرف على الآخر تم بناء استراتيجيات الحرب الباردة التي تميزت باحترام قواعد الردع النووي المتبادل[2]، بيد أن نهاية الحرب الباردة والتحولات التي أعقبتها أدخلت العالم في حالة" فوضى معممة"[3]، ترتب عنها حصول قناعة مفادها أن التهديدات الأمنية الراهنة أصبحت أكثر اتساعا وانتشارا وفتكا، حيث التهديد أقل وطنيةفي تعريفهوأكثر عالميةفي مداه بشكل أدى حسب "بريجنسكي" إلى نهاية عصر " الأمن المطلق" فلم " يعد بمقدور أي دولة مهما بلغت قوتها أن تحمى نفسها من التهديدات الأمنية الراهنة".[3، 4 – 15]، كما إن الأمر أصبح يطرح تحديا حتى بالنسبة للهيئات الأممية ذات الطابع العالمي كهيئة الأمم المتحدة التي كان تأسيسها من " أجل إنقاذ الأجيال القادمة من الحروب"[4] ، ولكن في ظل تهديدات تمتد إلى ما هو أبعد من دول تشن حربا عدوانية أصبح الحديث عن دور مثل هذه الهيئات في رصد وتحييد التهديدات الأمنية يتم على نطاق واسع فالتهديدات اليوم تُعرّض أمن الإنسانية كافة للخطر علاوة على أمن الدول[5].

إن الوضع الجديد الذي أفضت إليه نهاية الحرب الباردة جعل التهديدات الأمنية متعددة الاتجاهات والاشكال وغالبا ما يصعب توقعها كما أنها تختلف من حيث الشكل والمضمون عن تلك التي سادت أثناء الصراع القطبي فتهديد الحرب النووية الفاصلة انحسر ليفسح المجال لظهور تهديدات غير محددة المعالم، كما أن القوة العسكرية وحدها لم تعد قادرة على مواجهتها فتهديدات من قبيل الجريمة المنظمة، الإرهاب، الهجرة السرية، التهديدات الالكترونية غير متعلقة أساسا بزيادة الإنفاق العسكري على التسلح وتعزيز القدرات العسكرية الدفاعيةذلك أنها تتسم بالشمولية والقوة و تعتمدها جماعات منظمة عابرة للقوميات ومن ثم لم يعد بالمقدور التحكم فيها باعتماد الوسائل العسكرية باعتبارها تعرف بطبيعتها غير العسكرية فهي عابرة للحدود ولا تستثني أي دولة مهما كانت قوتها أو موقعها[6]

فالأمن اليوم في عالم يموج بتغيرات سريعة لم يعد مرتبطا فقط بتأمين سلامة الدول من مغبة الوقوع تحت سيطرة القوات العسكرية لدولة أجنبية فقد زُعزع هذا المفهوم على نحو أبرز التساؤل حول مدى اطلاقيته وفعاليته في إدراك التهديدات المحدقة بالأمن فالعدو لم يعد محددا والتهديدات لم تعد عسكرية بطبيعتها وحتى الدول لم تعد هي صاحبة الحل والربط في هذا المجال فنحن اليوم إذن نعيش " عصر علامات الاستفهام" حول ثنائية تهديد أمن حسب تعبير كين بوث Ken Booth (منظر العلاقات الدولية البريطانية والاستاذ في قسم السياسة الدولية بجامعة ابيريستويث)والذي يبرر هذا الحكم بقوله" التنامي المقلق لـــ: اللاأمن في بعده العالمي[7]. وبناءً على ما تقدم فإن حالة "اللانظام العالمي الجديد"أو ما يفضل أن يسميه سمير أمين" إمبراطورية الفوضى" أو "حالة الفوضى المعممة" جعلت العالم كله خاضعا لمنطق توزيع المخاطر[8] كما أنه

قد أصبح" ضال الوجهة ومحروم الإحساس بالتوجه" فهذا العالم يعرض علينا بصورة مكدرة ومحزنة فوضى شنيعة[9] نجم عنها أن حدّة وتعدد مستويات اللاأمن أصبحت سمة الحاضر والمستقبل المنظور فالمجتمع الإنساني يواجه تحديات متعددة الاتجاهاتلم يسبق له عبر تاريخه أن واجهها فالسياسة العالمية اليوم تواجه بأنماط من التهديدات لم تعد مقتصرة على الصراعات التقليدية الداخليةولكن مهددة باستراتيجيات مبتكرة وخطرة لفواعل من غير الدول.

كما أنها في مجملها ذات طبيعة غير عسكرية، كما أنها تفتقد لقاعدة أرضية خاصة (لإمكانية التهديد/ نهاية الجغرافيا) وبالتالي لا يمكن التعاطي معها ولا الضغط عليها فالخطر المحدق بالأمن هو اللايقين[10]، فالعدو هو ذلك المجهول والخوف والتهديد يأتي من ذلك التغير السريع الوتيرة ومن " عدوّ" لا تستطيع أن تراه أو تلمسه أو تحسه.

وفي السياق ذاته يذكر أورد "هيلد"Held وآخرون في كتابGlobalisation Transformation سبع فرضيات أساسية حول تأثير العولمة في قضايا الأمن التقليدية نذكرها هنا على أن نستدل بآخرها لما لها من علاقة ارتباطيه مباشرة بما تقدم ذكره[11].

– إن انتشار التقنيات العسكرية في جميع أنحاء العالم تعني انه بينما يطور المجددون ويستخدمون حدودا فاصلة في الأسلحة المتطورة، فان دولا أخرى تضطر للحصول على أحدث المعلومات والأنظمة أو أن تدفع ثمن تخلفها في قوتها العسكرية وفي أمنها[12].

– لم يعد يحتاج خوض حرب في عصر المعلومات إلى تحريك المجتمع فيزيائيا، بل يحتاج إلى سياسة علاقات عامة فعالة تستخدم فيها وسائل الإعلام بمهارة لإعلام الرأي العام. تحتاج معظم الحروب الآن إلى الهدوء السياسي لأنها الآن رأسمال شديد وإمكانات محددة أكثر.

– العالم يمارس ثورة جديدة في التكنولوجيا العسكريةMTR، فتقنيات المعلومات، تحول القدرات العسكرية الموجودة، وإدارة الحروب، والقدرة على إظهار القوة العسكرية من مسافات بعيدة بدقة عظيمة.

– تجعل أنظمة الاتصالات الآنية إدارة الحروب أسهل، لأن القادة يستطيعون الإشراف والتدخل بالعمليات العسكرية الميدانية إلى درجة لم تكن ممكنة من قبل[13].

– العولمة المتزايدة في قطاعات الصناعات المدنية التي تعمل في الإنتاج الدفاعي الالكترونيات أو البصريات، تتساهل في السيادة التقليدية للقدرات الدفاعية القومية، لأنها تجعل الحصول على الأسلحة واستخدامها خاضعا لقرارات إعمال سلطات أخرى.

– تصبح تهديدات أمن الدول، أكثر انتشارا ولم تعد عسكرية بطبيعتها

– تفرض العولمة تغييرات جذرية في الدول وتسلط الضوء على عجز الحكومات القومية عن ضبط أمن مواطنيها وسعادتهم

ويتوصل غراهام آليسون[*] في إطار محاولة تبيانه لأثر المتغيرات الجديدة في الأمن القومي والعالمي إلى أنه لا يمكن حل المشكلات عبر الأممية بما فيها المشكلات الاقتصادية والبيئية والإرهابية والثقافية والإجرامية

[*] غراهام تيليت أليسون، أستاذ العلوم السياسية الأمريكية وأستاذ في كلية جون ف. كينيدي في جامعة هارفارد. وهو مشهور بمساهمته في أواخر الستينيات وأوائل السبعينيات من القرن الماضي للتحليل البيروقراطي لصنع القرار، خاصة في أوقات الأزمات

والتهديدات الأخرى للأمن القومي بوسائل قومية فقط، لأنها تحتاج إلى حلول تعتمد آليات إقليمية وعالمية من التعاون والتنسيق حيث أن هذه التهديدات تخلق طلبا على الحكم فوق القومي ما دام يتعذر على القادة السياسيين– كمسؤولين عن مشاكل أضيق (المشاكل المرتبطة بالمجال الداخلي للدولة) معالجة ذلك[14].

ويرى جوزيف ناي في كتابه (soft power) القوة الناعمة أن الجزء الاعظم من المشكلات والتهديدات التي تنتاب العالم اليوم تنبع من التغيرات التي شهدها العالم خلال الجزء الاخير من القرن العشرين، واهمها زيادة اتجاهات العولمة والتقدم التكنولوجي الاستثنائي الذي يمكن التعبير عنه بالثورة المعلوماتية. ويوضح ناي أن هذه المتغيرات وخاصة المتغير التكنولوجي أدت الى تراجع التهديدات المرتبطة بالقوة الصلبة لصالح ظهور التهديدات المرتبطة بالقوة الناعمة، والتي من بينها القوة الثقافية والفكرية والتي تعد الأهم ذلك أن هذا النوع من القوة أدى الى خلق تهديدات لا تتمتع فيها اي دولة بميزة مطلقة كونها تقع خارج سيطرة القوة العسكرية والبنى الأساسية الحكومية، والسيطرة المؤسسية[15]. ويضيف ناي قائلا "أن هذا النوع من التغيرات أدى الى خصخصة الحرب وما يرتبط بها من تهديدات فتحولت الحرب الى معارك افراد ضد دول وليس دول ضد دول كما كانت في الماضي، ويخلص الى أن مواجهة هذه التهديدات الجديدة تحتاج الى وسائل جديدة ،فإذا كان استخدام القوة العسكرية يمكن أن يحقق نتائج إيجابية في حالات محدودة من هذه التهديدات فأن المطلوب هو أشكال جديدة ومختلفة من القوة وفي مقدمتها القوة الناعمة[16].

ومع ما يشهده العالم اليوم م تطور تكنولوجي هائل والانتقال من الواقع الى العالم الافتراضي، أصبح للفضاء الإلكتروني[*]دور في حركة التفاعلات والتحولات البنيوية كمجال جديد في العلاقات الدولية وبدأ ينتقل تأثيره من تغييرات هيكلية وتحتية إلى إحداث تغييرات كيفية في النظام الدولي، الفضاء الإلكتروني عبارة عن مجال طبيعي ومادي ويرى آخرون أنه ذا طابع افتراضي حيث يرونه بأنه " تلك البيئة الافتراضية التي تعمل بها المعلومات الإلكترونية والتي تتصل عن طريق شبكات الكمبيوتر.

وأصبح يشهد العالم تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي مع الانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف، وأصبحت قضية أمن الفضاء الإلكتروني تلقى اهتماما متصاعدا على أجندة الأمن الدولي وذلك في محاولة لمواجهة تصاعد التهديدات الإلكترونية ودورها في التأثير على الطابع السلمي للفضاء الإلكتروني، وباتت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الاستراتيجية – ذات الطبيعة الإلكترونية – إلى أخطار إلكترونية ،وتهدد بتحول الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الأطراف ودورها في تغذية التوترات الدولية ،وهو ما يفرض تحديات تتعلق بإعادة تعريف الأمن والقوة والصراع، وهو ما يثير التساؤلات حول مدى علاقة الفضاء الإلكتروني بإحداث تغييرات في البيئة الأمنية الدولية؟

لقد ظهر تنام في إدراك أخطار الهجمات الجديدة، فيما يمكن تسميته بـــالحرب الباردة الالكترونية، والتي أصبحت تمثل اكبر تهديد امني لاستقرار العالم وأسواقه المالية وحتى للبنية التحتية المدنية إضافة إلى الجهود الرامية لاكتشافه في مجالاته الفضائية وموارده الأساسية، التي تشن على أجهزة الكمبيوتر في العالم مما ينذر بتحوله إلى اكبر تهديد امني،كما ظهرت اسلحة الكترونيةCyber weapon جديدة ومتعددة كالفيروسات وهجمات انكار الخدمة[17]، والاختراق وسرقة المعلومات والتشويش.

---

[*]* الفضاء الإلكتروني عبارة عن مجال طبيعي ومادي ويرى آخرون أنه ذا طابع افتراضي حيث يرونه بأنه "تلك البيئة الإفتراضية التي تعمل بها المعلومات الإلكترونية والتي تتصل عن طريق شبكات الكمبيوتر.

وتختبر أجهزة الاستخبارات الدولية شبكات الدول الأخرى بصورة دورية بحثا عن ثغرات وتزداد أساليبها تطورا باستمرار، وشهد العديد من الدول التعرض للهجمات كان من بينها الولايات المتحدة والهند وألمانيا وفرنسا وبريطانيا عام 2007 بالإضافة إلى الهجوم على استونيا في ايار 2007، وفي الحرب الجورجية الروسية في 2008 وتطورت الهجمات الالكترونية من مجرد عمليات بحث بدافع الفضول في البدء العمليات جيدة التمويل والتنظيم من التجسس السياسي والعسكري والاقتصادي والتقني.

وتم الكشف عن شبكة تجسس الكترونية تعمل في الصين تمكنت من اختراق1295 جهاز كمبيوتر في103 دوله وتعد الحادثة الاكبر في العالم من حيث عدد الدول التي تم اختراق شبكاتها واجهزتها منها وزارات الخارجية كل من ايران وبنجلاديش ولاتفيا واندونيسيا والفلبين وبروناي وتايلاند وبوتان. وتم اكتشاف اجهزة تنصت علي الكمبيوتر في سفارات كل من الهند وكوريا الجنوبية واندونيسيا وقبرص ومالطا وتايوان والبرتغال والمانيا وباكستان[18]. وهناك نحو 120 دولة تقوم بتطوير طرق لاستخدام الإنترنت كسلاح لاستهداف أسواق المال ونظم الكمبيوتر الخاصة بالخدمات الحكومية.

وتقوم أجهزة الاستخبارات الدولية بالفعل باختبار شبكات الدول الأخرى بصورة روتينية بحثاً عن ثغرات لتوظيفها عند الضرورة. كما أن هناك ما يشبه تشكيل قوات الكترونية[19]. وأدى تصاعد حجم الأخطار الالكترونية الى تغير في مضامين الامن القومي للدول، وأصبحت تبحث عن إعادة تعريف لأمنها القومي مع ظهور جبهة الفضاء الالكتروني كمهدد لأمن الدول، وهو ما دفع الدول إلى إدخاله ضمن استراتيجيات ألأمن القومي لديها، والبحث عن تطوير قدراتها في مجال الدفاع والحماية والهجوم وتحديث جيوشها للتعامل مع الحرب الالكترونية الجديدة؛ وهو ما أثر على العلاقات الدولية وبخاصة معبروز تهديدات من جانب منهم ليس وابدول وغير مخاطبين بالقانون الدولي، ولا تملك الدول السيطرة كاملة على أنشطة القراصنة أو جماعات الاحتجاج الالكتروني، حيث أثر الفضاء الالكتروني على التنافس بين الدول في مجال الاستحواذ على القوة الإلكترونية، وفي نفس الوقت فتح الباب أمام التعاون لمواجهة الأخطار المشتركة وخاصة أنها بطبيعتها عابرة للحدود.وأصبح الفضاء الإلكتروني يواجه بتهديدات متصاعدة نتيجة[20]:

أ-ارتباط العالم المتزايد بالفضاء الإلكتروني بما عمل على زيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية.

ب-استخدام الفاعلين من غير الدول للفضاء الالكتروني لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة.

ت–انسحاب الدولة من قطاعات استراتيجية لصالح القطاع الخاص وخاصة بالمنشات الحيوية. مما جعل ادارة هذه القطاعات وامنها بيد القطاعات الخاصة.

ث–تأثير مواجهة الحرب الالكترونية على حرية استخدام الفضاء الإلكتروني.

ج-إشكالية تعامل الدول مع الشركات التكنولوجية متعددة الجنسيات، والتي أصبحت فائقة القدرات مثل مواقع الشبكات الاجتماعية كالفيس بوكوتويتر واليويتوب التي أصبح تفاعلة دوليًّا.

ومن خلال ما تقدم ، نستطيع أن نقول أن مدخل التغيير يدل على وجود ثمة علاقة بين التغيير وظهور التهديد، وأن ما يهمنا هنا في هذه العلاقة هو التغيير في نمط التهديدات، وتغيير أشكالها ،وتغيير الطريقة التي يحصل بها التهديد و قياس أثر التغيير في عنونة التهديد وتحديد طبيعته وذلك من خلال رصد معامل الارتباط بين التهديد والمتغيرات الاتية[21]:

1–عندما يحصل التغيير سواء كان داخليا او خارجيا فأن القوة الداخلية للدولة سوف لن تبقى مستمرة

2ــ أن هذا التغيير سيضيف مصادر قوة جديدة للخصم.
3ــ أن هذا التغيير سيؤدي الى تفاقم الضعف الداخلي للدولة.
4ــ في ضوء التغيير الحاصل فأن التهديدات الخارجية ستبدو اكثر خطورة.
5ــ تحت ظروف التغيير ستكون الفرص الخارجية اكثر قوة.
6ــ سيحدد التهديد فيما اذا أضاف ام اضعف من قدرة الدولة في مواجهة الخصم.
وبناءً على ما تم ذكره من افكار وفي ضوء المتغيرات المطروحة، نجد أن التغيير يمكن أن يشكل مدخلا لتوالد التهديدات وظهور معضلات امنية،ذلك لأنه عندما يحدث فأنه يمكن أن يؤثر بالسلب أو الايجاب على النواحي المتعلقة بقوة الدولة الداخلية منها والخارجية، وقدرتها على التصدي للتهديدات المتوالدة، فضلا عن خطورة تأثيره في الترتيبات الامنية المألوفة التي تعتمدها الدول للحفاظ على امنها وصيانته.

المطلب الثاني: اسباب التغيير في التهديدات الالكترونية:-

غالباً ما يعتبر يوم 11 ايلول عام 2001 هو اليوم الذي غير كل شيء. وقد يكون هذا المعنى غير منطبق على حياتنا اليومية، لكن من الناحية الأمنية، يعتبر هذا التاريخ بداية عهد جديد. ومع انهيار برجي التجارة العالمي، انهارت معهما المفاهيم التقليدية للتهديدات الأمنية. وتغير سيناريو الحرب الباردة الذي هيمن على العالم على مدار أكثر من 50 عاماً بشكل جذري وحاسم. وهو تهديد لم يكن لديه عنوان واضح حتى الآن ومن هي الجهة التي تقف خلفه. فالحدود الإقليمية لم تعد ذات قيمة وكذلك القواعد العسكرية الخاصة بالمكان والزمان. فاستخدام الطائرات المدنية كأدوات للهجمات الإرهابية أظهر أن كل شيء ممكن استخدامه كسلاح في أي وقت. وفجأة بات لايوجد مستحيل أو محال بعد الآن. وينطبق هذا الوصف تماماً على التهديدات الإلكترونية كجانب من التغيير في التهديد نتيجة لعدة اسباب منها.

اولا: الاسباب السياسية:-

ان ما يميز الفضاء الالكتروني عن غيره من المساحات التقليدية للصراعات السياسية هو صعوبة تحديد هوية المهاجم في اغلب الهجمات الالكترونية، وبخاصة اذا ما اتسمت بدرجة عالية من التعقيد. فكلما زادت درجة تعقيد الهجوم الالكتروني، زادت صعوبة تحديد هوية المهاجم، او اتباع مسار الهجوم، او توقيته، او تحديد الدوافع الكامنة وراءه. لذا نجد ان كافة الدول التي وجهت اليها اتهامات بشن هجمات الكترونية كروسيا في حالتي استونيا و جورجيا، و الولايات المتحدة واسرائيل في حالة ستاكنست، والصين وغيرها، قد نفت تماما اية صلة لها بتلك الهجمات في ظل عجز الدولة المتعرضة للهجوم عن تقديم ادلة قطعية الثبوت لإسناد الاتهامات الى دولة بعينها او تحميلها المسؤولية[22].

ونتيجة لذلك تستطيع الدول ان تحقق اهدافها السياسية باستخدام الاسلحة الالكترونية بدلا من القوى العسكرية دون الحاجة الى تحمل اية مسؤولية دولية تترتب على هذا الهجوم، ودون قدرة الهدف على اثبات قيامها به. مما يزيد من احتمالات قيام الخصم بالهجوم المضاد، فضلا عما ستتعرض له الدولة من ضغوطات وانتقادات من قبل الراي العام العالمي والمحلي، و خاصة اذا ما اتسع نطاق وفداحة الخسائر المترتبة على هذا الهجوم، او اذا ما جاء كفعل استباقي وليس الدفاع الشرعي عن النفس كما هو الحال في الحالات التالية والتي حدثت بدوافع سياسية.[23]، ففي عام 2009 تم استهداف مواقع البيت الأبيض، ووكالة الأمن القومي، والإدارة الاتحادية للطيران Federal Aviation administration، ووزارة الخارجية، والخدمة السرية

Secret Service، والخزانة.ولجنة التجارة الاتحادية Federal Trade Commission، فضلًا عن جهاز المخابرات الوطني في كوريا الجنوبية. من قبل كوريا الشمالية،بسبب الصراع السياسي بينها وبين الولايات المتحدة من جهة، وكوريا الجنوبية من جهة اخرى حول البرنامج النووي لكوريا الشمالية، لما يمثله من تهديد عالمي.

وكذلك الهجوم على شركة سوني بيكتشرز الأمريكية في عام 2014، بسبب فيلم من إنتاج هوليوود، عن زعيم كوريا الشمالية كيم يونغ أون[24]. واستخدم فيروس "ستكسنت" – سابقًا– لمهاجمة برنامج إيران النووي في نوفمبر 2007، ويُعتقد أنه من تطوير الولايات المتحدة وإسرائيل، وقد تم اكتشافه في عام 2010.

وفي تموز 2011، أعلن نائب وزير الدفاع ويليام لين أن أكثر من 24 ألف ملف من ملفات وزارة الدفاع قد سرق. قبل ذلك ببضعة أشهر، تم اختراق إحدى المختبرات العلمية الرئيسية التابعة لحكومة الولايات المتحدة، ولم تعلن الحكومة الأمريكية عن هوية مرتكبي الهجوم[25].

وفي عام 2012، تم تدمير 35 ألف جهاز كمبيوتر في شركة النفط السعودية "أرامكو"، لتخريب صادرات النفط. وألقت المخابرات الأمريكية اللوم على إيران. وفي عام 2016، هاجم القراصنة إحدى الوكالات الحكومية السعودية، بالإضافة إلى منظمات في قطاعات الطاقة والصناعة والنقل، والهيئة العامة للطيران المدني التي تنظم الطيران السعودي.

وشهد عام 2016، التسلل الروسي إلى خوادم البريد الإلكتروني للجنة الوطنية الديموقراطية، كما تم اختراق البريد الإلكتروني الخاص بجون بوديستا رئيس الحملة الانتخابية الرئاسية لهيلاري كلينتون. وقام وسطاء بتسريب رسائل إلكترونية إلي موقع ويكليكس، وعلى إثرها قامت الولايات المتحدة بطرد 35 دبلوماسيًا روسيا.

ويمكن القول في ضوء تلك الحالات، أنه رغم اختلاف غرض وهدف كل حالة من الحالات السابقة، إلا أنه من الواضح أن حجم الهجمات الالكترونية يتزايد بشكل حاد، ولذا يصعب تحديد حجمها الحقيقي وبخاصة أن عديد منها لا يتم التبليغ عنه[26]. وتتمثل القواسم المشتركة بين تلك الحالات في صعوبة تحديد مرتكبي تلك الهجمات على وجه الدقة، وغياب الرد المضاد، كنتيجة لها. والأهم أنها ليست حكرًا على الدول المتقدمة ذات أنظمة المعلومات الهائلة والمتطورة فحسب.

ثانيا: الاسباب الاقتصادية:-

تحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية دائرة، ويكون تعبيرًا عن حدَّة الصراع القائم بين الأطراف، وقد يكون مقدمة لعمل عسكري. وتدور حرب عبر الفضاء الإلكتروني عن طريق اختراق المواقع وقصفها وشنِّ حرب نفسية وغيرها. ويستمد ذلك الصراع قوته من قوة أطرافه وارتباطه بعمل عسكري تقليدي. وبخاصة مع تكلفه 4% من تكلفة الآلة العسكرية، بما يمكِّن من تمويل حملة حربية كاملة عبر الإنترنت بتكلفة دبابة. كما أنَّها لا تستغرق إلا وقتًا بسيطًا. فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب يعني أنّه ليس هناك حاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة جدا كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا وحقيقيا على دولة مثل الولايات المتّحدة الأمريكية على سبيل المثال ويتم استخدام الفضاء الإلكتروني في الصراع بطريقة موازية للحرب التقليدية. وتاريخيًّا تم استخدامه في هجمات حلف الناتو عام 1999 على يوغسلافيا، وتستهدف الهجمات شبكات الاتصالات ويعطلها، ما يؤدي تلقائيًّا لتوقف شبكات الجيش[27] . وتم استخدام هذا النمط من الهجمات

في الحرب بين حزب الله وإسرائيل في عام 2006، وتم استخدام الهجمات الإلكترونية في حالة الحرب الجورجية–الروسية في أغسطس من العام 2008. وتم ذلك في المواجهات بين حماس وإسرائيل في عام 2009 وفي نوفمبر 2012.

وعلى الرغم من ان العالم لم يشهد حربا الكترونيا منفردة ودون العمل العسكري التقليدي الا ان هناك ما يشير الى تحول ذلك في المستقبل. ويتميز هذا النمط من الصراع على سيطرة البعد التكنولوجي على إدارة العمليات الحربية حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، ويتم استخدام الروبوتات الآلية في الحروب والتي يتم إدارتها عن بعد فضلاً عن الطائرات بدون طيار، ويتم تطوير القدرات في مجال الدفاع والهجوم الإلكتروني والاستحواذ على القوة الإلكترونية، ويتم استخدام الفضاء الإلكتروني في الاستعداد لحرب المستقبل والقيام بتدريبات على توجيه ضربة أولى لحواسب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية والبنية التحتية المعلوماتية. ولعل الهدف من وراء ذلك؛ تحقيق "الهيمنة الإلكترونية الواسعة" بشكل أسرع وكلفة اقل بكثير مما تنتجه الصراعات التقليدية في حالة نشوب صراع. ويتم التقدم في مجال استخدام كافة أنواع الأسلحة الإلكترونية مثل أسلحة الميكروويف عالية القدرة، وتم توجيه هجمات إلكترونية باستخدام عدد من الفيروسات مثل قيام اسرائيل بشن هجمات فيروس ستاكسنت في أكتوبر2010 ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة و تم تطويرها وتجربتها عام 2007 في إسرائيل[28].

لقد أدت علاقة الفضاء الإلكتروني بعمل المنشآت الحيوية سواء أكانت مدنية أو عسكرية لقابلية تعرضها لهجوم من خلاله إما يستهدفه كوسيط وحامل للخدمات أو بشل عمل أنظمتها المعلوماتية،ويكون من شأنه التأثير على القيام بوظيفتها ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ استراتيجية بالغة الأهمية سواء في زمن السلم أو الحرب[29].

وهناك امثلة كثيره على هجمات تعرضت لها منشآت وقطاعات حكومية وغير حكومية:

ففي تموز 2010، أعلنت ألمانيا أنّها واجهت عمليات تجسس شديدة التعقيد لكل من الصين وروسيا كانت تستهدف القطاعات الصناعية والبنى التحتية الحساسة في البلاد ومن بينها شبكة الكهرباء التي تغذي الدولة[30].

والاعتداء الالكتروني على شركتي توزيع الكهرباء في غرب أوكرانيا، بريكارباتياأوبلنيرغو وكييف اوبلنيرغو عام 2015 أدى إلى انقطاع كبير في الكهرباء بتعطيل 50 محطة فرعية من شبكات التوزيع. وأفادت التقارير أن المنطقة شهدت انقطاعا في الكهرباء لعدة ساعات، وأن الكثير من العملاء والمناطق الاخرى تعرضوا لانقطاع الكهرباء بدرجة أقل، وقد تأثر من جراء ذلك ما يزيد عن 220000 مستهلك[31].

العمليات التي قام بها القرصان المحترف إلكترونيًّا "كريس روبرت" لعشرات الرحلات الجوية، والذي اعتقلته السلطات الأمريكية في نيسان 2015،بعد "تغريدة" له نشرها لشرح خطوات قرصنته لطائرة "يونايتد إيرلاينز" التي كان مسافرًا على متنها إلى نيويورك. وفي التحقيقات التي تمت من قِبل مكتب التحقيقات الفيدرالي FBI، اعترف "كريس" بحقيقة ما ارتكبه، وأعطى شرحًا كاملا لعملية قرصنة الطائرات من خلال "الإيثرنت"؛ وهي تكنولوجيا تم اعتمادها كأساس في تنفيذ عمليات المراسلة في الكثير من الشبكات المحلية[32].

وفي شباط 2016 تعرض النظام المصرفي الدولي للقرصنة في محاولة لسرقة مبلغ 951 مليون دولار من البنك المركزي في بنغلاديش، فقد اعطى المهاجم خلال هذه العملية تعليمات زائفة بسحب اموال من حساب

البنك المركزي في بنغلاديش لدى البنك الاحتياطي الفيدرالي في نيويورك باستخدام شبكة سويفت المصرفية لاستكمال التحويل، ونجحت عملية القرصنة بسحب مبلغ 101 مليون دولار قبل ان يوقفها البنك الاحتياطي الفيدرالي في نيويورك[33].

وشهد المجتمع الدولي اتجاهات التحول في قضية التعامل مع تهديدات الالكتروني وامكانية تحول المجال الالكتروني نحو العسكرة وبرز ذلك في عدة اتجاهات لعل اهما، تصاعد الهجمات الالكترونية ومخاطرها على امن الفضاء الالكتروني ،والتطور في مجال سياسات الدفاع والأمن الالكتروني، وتصاعد القدرات في سباق التسلح الالكتروني عبر الفضاء الإلكتروني وتبني سياسات دفاعية الالكترونية لدي الاجهزة المعنية بالدفاع والامن ،وتصاعد حجم الاستثمار في مجال تطوير ادوات الحرب الالكترونية داخل الجيوش الحديثة.

إن التطور التكنولوجي في مجال المعلومات والاتصالات ساعد على تزايد درجة الاندماج والارتباط بين الدول والمجتمعات وظهور الشركات الكبرى متعددة الجنسيات وتحرير التجارة الدولية وإزالة العوائق أمام تدفقات رءوس الأموال المصرفية والاستثمارات الدولية؛ وإلغاء الحدود الإقليمية فالأقمار الصناعية وشبكة المعلومات الدولية جعلت العالم اليوم يمثل مجتمعا واحداً حيث الانتقال السريع للمعلومات وسهولة انتقال الأموال والأشخاص كل هذه الظروف هيأت مناخاً جديداً مشجعاً لارتكاب الجريمة المنظمة عبر الحدود الوطنية سواء ارتكبت في دولة بناء على تخطيط وتنفيذ جماعة إجرامية منظمة تمارس أنشطة إجرامية في أكثر من دولة، أو تم التخطيط لها في دولة، وتنفيذ ما خطط له في دولة أخرى، أو ارتكبت في دولة واحدة ولكن ترتب عليها آثار شديدة في دولة أو دول أخرى[34].

وفي ضوء هذه الاحداث يمكن القول، ان الهجمات سابقة الذكر لها اثار اقتصادية و امنية سواء على مستوى الفرد او على مستوى الشركات، مما تؤدي الى نتائج يكون منها :

1- أضعاف ثقة المواطن فيها

2- تدفع هذه الشركات الى تكاليف اضافية لتأمين الحماية اللازمة

3- احتمالية وقوع مثل هذه المؤسسات الاقتصادية بيد المهاجمين وهذا ما يخلق اثر اقتصادي على الدول

4- خلق نوع من التنافس الاقتصادي بين الشركات(ابل و سامسونج).

ثالثا: الاسباب التكنولوجية:-

ان تطور وسائل الاتصال وشبكات المعلومات ومختلف الامكانيات العلمية والتقنية، جعل استغلالها في تنفيذ العمليات الارهابية أكثر سهولة خاصة وأنها تتميز بالدقة والسرعة والخطورة، حيث يمكن تنفيذها على الأهداف الحكومية بدقة كبيرة تقل فيها نسبة الخطأ، وذلك بفضل التوجيه والتحكم في وسائل نقل المتفجرات والاتصال بين العناصر الارهابية أثناء عملية التنفيذ بوسائل اتصال جد متطورة، كما أن استهداف تدمير وتخريب البنية التحتية لشبكة المعلومات الحكومية أو العامة للمؤسسات الاقتصادية والشركات، قد يتم بسرعة فائقة ويكلف خسائر كبيرة جدا تتجاوز الخسائر التي تكون نتيجة العمليات الارهابية بالشكل التقليدي، والأخطر من كل ذلك أن الجماعات الارهابية قد تنفذ هذه العمليات وهي في أماكن بعيدة وآمنة فقد أصبحت فواعل الى جانب الدول فبإمكانها تهديد أمن الدول وتغيير مجرى الأحداث الدولية، فهذه الأخيرة لم تعد اللاعب الوحيد في العلاقات الدولية، ومنهلم تعد تتمتع بالسيادة المطلقة مثل ما كان تسابقا[35].

لقد أصبحت التنظيمات الارهابية في السنوات الأخيرة تمتلك قدرات كبيرة في توظيف الوسائل التكنولوجية، حتى أصبح استخدام مصطلح" الارهاب التكنولوجي " موضوعي االى أبعد الحدود، كما توضح

الدراسة التي نشرها– مركز الأبحاث لدراسات الصراع والارهاب في لندن بعنوان" :التكنولوجيا والارهاب : التهديد الجديد للألفية الجديدة "والتي كتبها كل من ستيفن أرباورز– وكمبرلياً ركيز، حيث أكدت هذه الدراسة أن التنظيمات الارهابية أصبح بإمكانها حاليا الحصول على كل ما تريد من معلومات عبر الاستخدام المقنن للكمبيوتر، ومن خلال استغلال ثغرات شبكات المعلومات أو باللجوء الى عمليات القرصنة المعلوماتية والدخول الى بنوك المعلومات العسكرية والأمنية للدول، واستغلالها في التخطيط للعمليات الارهابية، كما يمكنها ايضا الدخول الى شبكات البورصة والأسواق المالية وتدميرها بقصد المساس بالقوة الاقتصادية للدول المستهدفة. وهذا يعني سهولة الحصول على التكنولوجيا من اجل الهجوم او التهديد[36].

لقد ألغت التكنولوجيا عموماً والأنترنت خصوصاً الفارق الزماني والمكاني، فالجريمة الإلكترونية الافتراضية لا تترك دليل ملموس؛ بل ويُمكن في أي لحظة إتلاف الدلائل فيها كما أن الضحية والمجرم في الجريمة الإلكترونية غير متكافئين في القوى فالأنترنت تجسد بفعالية مبادئ الصراع غير التناظري أيأن اطراف الصراع فيها ليست بالضرورة من نفس الطبيعة أو من نفس الحجم، يُمكن أن تكون دولة، مؤسسة، مجموعة من اضلين أو فرد منعزل.

فمثلاً يُمكن لعامل غير راضً أن يُهدد المؤسسة التي يعمل بها. ففي عام 2016 تعرض نظام معلومات مستشفى فيولاية لوس أنجلوس الأمريكية إلى اعتداء إلكتروني طالب من خلاله المعتدي فدية ب15000 دولار مقابل فك تشفير ملفات المستشفى الذي أدى إلى تعطيل الاتصال بين الأطباء وكافة طاقم المستشفى[37].

ان تكنولوجيا المعلومات والاتصال أخذت الجريمة الإلكترونية كما يرى ARPAGIAN.N نحو العولمة ومكنت من القيام بأعمال اجرامية عبر الأنترنت حيث يقوم منتجو الخدمات التكنولوجية بعرض منتجاته محول العالم ويستغلون في ذلك الاختلافات الإقليمية في القوانين التي تعطي حصانة لمرتكب الجريمة .ففي الفترة ما بين12أيار2017و14أيار2017أصابت الموجة الأولى من هجوم "WannaCry" 200000 ألفضحية في150 دولة على الأقل بما في ذلك شركات عالمية كبيرة مثل :شركة Kaspersky Lab ألتي علنت أن أنها رصدت نحو 45 ألف هجمة ببرنامج "WannaCry" واعلنت ان روسيا كانت من أكثر البلدان تضررا من هذه الاعتداءات الإلكترونية حيث تعرضت أنظمة أحد أكبر البنوك الروسية لهجمة مماثلة زُعم أنها لم تؤثر في خدماته بسبب نظام الحماية الذي يعتمد عليه، كما أصيبت خوادم وزارة الداخلية الروسية وذكرت وسائل إعلام روسية أن شركة الهواتف الخلوية الروسية أغلقت عددا من خوادم شبكتها بسبب الهجمات الإلكترونية. كما تعرض النظام الإلكتروني لمنظومة الصحة الوطنية البريطانية لاختراق منظم تسبب في مشاكل تقنية كبيرة حيث صار تعدّة عيادات ومستشفيات في مدن ومقاطعات في بريطانيا عاجزة عنده ولقاعدة البيانات الشخصية الخاصة بالمرضى وتم تشفير كلبيانات المرضى من قبل قراصنة يطالب ونبد فعأم والمقابل ازالة نظام التشفير .وفي فرنسا كانت شركة السيارات Renault اكبر المتضررين حيث أنها أوقفت العمل في مصانعها بفرنسا وفي رومانيا محاولة منها للحد من انتشار هذه الهجمات، وتأثرت أيضا من هذه الهجمات شركة FedEx العالمية للبريد السريع إضافة إلى تضرر العديد من شركات الاتصال في البرتغال او لأرجنتين واسبانيا[28]، [39].

ان التسارع المثير للتكنولوجيا المكتشفة، والمطورة بصورة كثيفة لم يحصل من قبل، حتى أصبح الكثيرون يحذرون من هذا التسارع الذي أصبح يخيف البعض، فلا نخرج من اكتشاف أو تطوير تقنية ما حتى نصطدم بتقنية أخرى قد ظهرت لنا، فالجميع أصبحوا يتسابقون لاكتشاف ما هو جديد، أو تطوير ما هو موجود في هذا

المجال. ونتيجة لثورة الاتصالات المتسارعة يزداد خطر التقنيات التكنولوجية المستخدمة في التهديدات الالكترونية

رابعا: الاسباب القانونية

اظهرت الثورة التكنولوجية الفجوة بين القواعد القانونية التقليدية وبين التطور في النظام الدولي، حيث افضت الى تحديات غير تقليدية للمجتمع الدولي. وجاءت التغيرات التكنولوجية بأنشطة جديدة لايوجد تكييف قانوني واضح يلائمها في الاطر القانونية الحالية او انها كشفت عن التعارض مابين القوانين الدولية القائمة، فضلا عن بروز مشكلات تتعلق بوضعها القانوني[40]، ففرض بذلك الاستخدام السلبي لها تحديات في سبيل معالجة القانون الدولي، واصبح هناك تأثير متبادل بين التقدم التكنولوجي وما يفرزه من تحديات وقدرة القانون الدولي على التكيف معها[41]، مع عدم وجود اطار قانوني دولي واضح لتناول تلك الظاهرة المستحدثة، الامر الذي يوجد حاجة لقانون دولي جديد، او عقد اتفاقيات مكملة للاتفاقيات الدولية، او تفعيل اتفاقيات اخرى قائمة، الا انه وفي مقابل لا يمكن انكار وجود قواعد للقانون الدولي تنطبق مباشرة على انشطة الفضاء الالكتروني متمثلة بالمبادئ المعمول بها بين الامم ومبادئ القانون الدولي الناشئة عن القانون الدولي العرفي والمعاهدات، والمبادئ العامة التي استندت اليها الامم المتحضرة[42].

أدت تداعيات الهجمات التي استهدفت البنية التحتية الرقمية لإستونيا إلى إنشاء مركز التميز للدفاع الإلكترونية التعاوني، وهو عبارة عن مبادرة أطلقها حلف «الناتو» لإجراء بحوث في مجال الأمن الالكتروني ودراسة إمكانية وضع إجراءات معيارية للرد على الهجمات الالكترونية. وقد تم إنشاء المركز في خضم الهجمات الالكترونية ضد جورجيا في 2008. وفي الفترة ما بين سنتي 2009 و2012، وبطلب من مركز التميز للدفاع الالكترونية التعاوني، قامت مجموعة من الخبراء والباحثين القانونيين بتقييم إمكانية تطبيق المبادئ القانونية على الهجمات الالكترونية. وتم تتويج هذه الجهود بنشر "دليل تالين" الذي يبحث إمكانية تطبيق القانون الدولي على الفضاء الالكتروني.

وبالرغم من أن "**دليل تالين**"[*] عبارة عن وثيقة غير ملزمة قانونياً، إلا أنه يتناول عدداً من المفاهيم مثل الحصار الالكتروني والهجمات المصطحبة باستخدام القوة ويقدم تعريفات لـــ"الخسارة" و"الضرر" في سياق الفضاء الالكتروني، كما أنه يعد مبادرة رائدة. ورغم التحديات التي يعرفها وضع إطارات قانونية للعمليات المسلحة وعدم ضمان امتثال الدول دائماً، فإن هذه المفاهيم تخضع للقانون الدولي سواء تم تطبيقها في البر أو الجو أو البحر.

دليل تالين (Manuel de Talinn) هو وثيقة قانونية تتضمن قواعد القانون الدولي المطبقة اثناء الحروب الالكترونية يتكون الاصدار الاول عام 2013 من 95 قاعدة قانونية ويتكون الاصدار الثاني عام 2017 من 154 قاعدة قانونية.ومثلاً، يحدد مجلس الأمن التابع للأمم المتحدة ما إذا تم شن هجوم عدواني على أعضائها (المادة 39) والإجراءات المؤقتة التي سيتم اتخاذها (المادة 40) والنهج المتبع لإعادة إحلال السلام (المادتان 41–42). لكن ميثاق الأمم المتحدة لا يعتبر العمليات "الالكترونية" بمثابة هجمات مسلحة بالمعنى الملموس للكلمة.

[*]دليل تالين (Manuel de Talinn) هو وثيقة قانونية تتضمن قواعد القانون الدولي المطبقة اثناء الحروب الالكترونية يتكـــون الاصدار الاول عام 2013 من 95 قاعدة قانونية ويتكون الاصدار الثاني عام 2017 من 154 قاعدة قانونية.

ولا يزال القانون الدولي القابل للتطبيق على الفضاء الالكتروني في طور الإعداد. وبينما يسعى "دليل تالين" لإرساء مبادئ قانونية في هذا الصدد مستنداً في ذلك إلى القوانين القائمة، فإنه يركز بالأساس على الجهات الحكومية. ولكي يتم تطبيق المبادئ القانونية، يجب أن يتم اعتبار الأعمال العدوانية.

إما صراعاً مسلحاً دولياً أو غير دولي. غير أن غالبية الحوادث الالكترونية التي تقع يومياً لا تندرج ضمن هذين التصنيفين. لذلك، فإن الدليل لا يتطرق لها، وهذا يبعث على التساؤل حول إمكانية سريان أحكام القانون الدولي الحالية على النشاط الالكتروني[43].

ولكي يتم تدويل الصراعات وتطبيق القانون الدولي، يجب أن تتوفر الشروط الواردة في المادة 8 من تقرير لجنة القانون الدولي، الذي تم تقديمه الى الجمعية العامة للأمم المتحدة في دورتها الثالثة والخمسين، حيث حددت مسؤولية الدولة بشكل واضح. لكن لم تلاحظ أية أمثلة للصراعات الدولية الالكترونية المسلحة إلى يومنا هذا. وصحيح أن النسخة الثانية من دليل تالين ستتطرق لهذه الإشكالات، لكن نسخته الحالية لا تأخذ بعين الاعتبار أنشطة الجهات غير الحكومية. وحتى لو طبقت المبادئ القانونية على الفضاء الالكتروني، فإنه لا توجد آليات تضمن امتثال الدول للقانون الدولي.

عوضاً عن ذلك، ركزت المحادثات على تطوير معايير للسلوك للحد من الصراعات في الفضاء الالكتروني وتشجيع الحوار بين الحكومات والأوساط الأكاديمية والمجتمع المدني. وترى بعض الحكومات أن هذا الحوار هو أفضل وسيلة على المدى القصير، على الأقل، للوصول إلى فهم مشترك للسلوك الالكتروني. غير أن وضع هذه المعايير لا زال في طور الإعداد، شأنه في ذلك شأن القانون الدولي. وأثناء لقاء المجموعة الأممية للخبراء الحكوميين حول التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي، قامت الجهات الحكومية خاصة الأمريكية والروسية والصينية بالاتفاق حول أهمية تطوير معايير في مجال الفضاء الالكتروني، بغض النظر عن التعاريف المتضاربة للقواعد وعدم الاتفاق حول كيفية النهوض بها. أما على مستوى القطاع الخاص، أصدرت شركة «مايكروسوفت» جملة من المبادئ التوجيهية لتعزيز النهوض بتطبيق المعايير الخاصة بهذا المجال[44] .

ونتيجة لضعف المتابعة القانونية، فأن اللجوء الى التهديدات الالكترونية يكون عامل مساعد للأطراف او الدول لشن هجمات، ادراكا منها بأنها سوف لن تواجه عقوبات قانونية.

الخاتمة:-

اصبح المجال الافتراضي بمنزلة ساحة قتال جديدة تشكل تهديدا يضاف الى قائمة التهديدات التي تواجه العالم، وتتجاوز في ابعادها واثارها الحدود الجغرافية والسياسية، وتلقي بتداعياتها على مستقبل الامن القومي والحيوي للدول.

وهذا ما كان واضحا في تأثير نهاية الحرب الباردة واحداث الحادي عشر من ايلول على طبيعة التفاعلات الدولية، حيث غيرت طبيعة التفاعلات الدولية هيكلة وخارطة المخاطر والتهديدات الأمنية من نمط تقليدي إلى نمط جديد اصُطلح عليه في الكثير من الأحيان "بالتهديدات اللاتماثلية، وبصورة أحدث "التهديدات الهجينة كتعبير عن زيادة التعقيد والحركية والتطور المستمر الذي يمس الظاهرة الأمنية في العلاقات الدولية انطلاقاً من تفاعلها بما يحصل على أرض الواقع خاصة فيما يتعلق بالتطور التكنولوجي والمعرفي والتقني. وكذلك نتيجة لوجود اسباب عديدة دفعت الى انتقال التهديدات من الواقع الى العالم الافتراضي. منها اسباب سياسية و اقتصادية وامنية وتكنولوجية

وفي ضوء ما شهد العالم من موجات التغيرات والتطورات المتسارعة في شتى مجالات الحياة الاقتصادية، والاجتماعية، والسياسية والثقافية، والامنية، نتيجة التقدم الهائل في تكنولوجيا المعلومات ووسائل الاتصالات التي جعلت من العالم قرية واحدة، حيث غير التقدم الهائل الذي تم إحرازه في الميدان التكنولوجي من ظروف ممارسة العلاقات الدولية تغييرا عميقا إن لم يكن قد غير من طبيعة هذه العلاقات نفسها. بحيث أصبح الحديث اليوم وبشكل متزايد عن الصراعات غير المتماثلة والتي تدار بوسائط وأدوات ليست بالضرورة عسكرية فقد تكون الكترونية أو وسائل مدنية أو حتى فيروسات معدية وغيرها.

CONFLICT OF INTERESTS

There are no conflicts of interest

المصادر:-

1- روبرت جبلن، الحرب والتغيير في السياسة العالمية، ترجمة باسم مفتن، دار الشؤون الثقافية العامة، بغداد،2009، ص27.

2- أشرف سعيد العيسوي، "التغيرات الدولية الحديثة ومفهوم الأمن القومي، شبكة المعلومات الدولية .http://www.kk Maq.gov.sa/Detail.asp?

3- حسن الحاج علي أحمد، " حرب أفغانستان التحول من الجيوسياسي إلى الجيوثقافي". مجلة المستقبل العربي. العدد (276)، مركز دراسات الوحدة العربية، بيروت، 2002. ص13.

4- مصطفى بخوش، "التحول في مفهوم الأمن وانعكاسه على الترتيبات الأمنية في المتوسط ". العالم الاستراتيجي. العدد 3 ،مركز الشعب للدراسات الاستراتيجية، الجزائر، 2008. ص08.

5- سمير أمين، إمبراطورية الفوضى، دار الفارابي، بيروت 1991، ص19.

6- جوزيف ناي،" تأمين عالم أكثر أمانا، شبكة المعلومات الدولية : http://www.project.syndicate.orgcntribtor/422

7- بن صغير عبد العظيم،الحرب على الإرهاب وتأثيرها في الأمن الإنساني، العالم الاستراتيجي. العدد 3، مركز الشعب للدراسات الاستراتيجية، الجزائر، 2008، ص22.

8- غربي محمد، الدفاع والأمن إشكالية تحديد المفهومين من وجهة نظر جيو- استراتيجيه، العالم الاستراتيجي، العدد (3)، مركز الشعب للدراسات الاستراتيجية، الجزائر، 2008،ص13.

9- مصطفى بن شنان،" النظام أو اللانظام العالمي الجديد". قواسم دولية. المعهد الوطني للدراسات الاستراتيجية الشاملة، الجزائر، 2008،ص3.

10- موسى الزعبي، "نهاية الحرب الباردة وإعادة فحص الأمن" ،شبكة المعلومات الدولية http://www:dam.org/politic/03/ind frt001.html

11-Ken Booth;"Critcal Security and World Politics".Lynne Rienner,Boulder, CO, 2005, P47

12- غسان العزي،11 مابعد سبتمبر2001، مجلة شؤون الأوسط، العدد (105)، مركز الدراسات الاستراتيجية،بيروت، 2002. ص34

13- غراهام أليسون " أثر العولمة في الأمن القومي والعالمي" في الحكم في عالم يتجه نحو العولمة جوزيف ناي وجون د. دوناهيو تر: محمد شريف الطراح ، مكتبة العبيكات، الرياض،. 2002، ص 132-.

14-Joseph S.Nye; soft power the means to success in world politics , public Affairs 1st Ed, New York, 2004, P5.

15-John Markoff,, Vast Spy System Loots Computers in 103 Countries , New York Times,2009http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1&hpw

16- عادل عبد الصادق، " من قطع كابلات الانترنت عن الشرق الاوسط "،ملف الاهرام الاستراتيجي، جريدة الاهرام، العدد (160) ،مركز الدراسات السياسية والاستراتيجية،القاهرة، 2008 ص 45-46

17-عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، ، سلسلة اوراق العدد(23)، وحدة الدراسات المستقبلية مكتبة الاسكندرية،الاسكندرية، 2016، ص17

18-MorganeFouché, Robert Macrae and Jon Danielsson,. "Could a Cyber Attack Cause a Financial Crisis?", World Economic Forum, 2016, online e-article, https://www.weforum.org/agenda/2016/06/coulda-cyber-attack-cause-a-financial-crisis. -

19-David A. Wheeler & Gregory N. Larsen, Techniques for Cyber Attack Attribution, Institute for Defense Analysis,Alexandria, VA,2003,p2

20- نوران شفيق، نواران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في ابعاد الامن الالكتروني،المكتب العربي للمعارف ،القاهرة،2016، ص 168.

21-David A. Wheeler & Gregory N. Larsen, Techniques for Cyber Attack Attribution, Institute for Defense Analysis, Alexandria, VA,2003,p2

22- نوران شفيق، نواران شفيق ، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في ابعاد الامن الالكتروني ،المكتب العربي للمعارف ،القاهرة،2016، ص 168

23-David A. Wheeler & Gregory N. Larsen, Techniques for Cyber Attack Attribution, Institute for Defense Analysis, Alexandria, VA,2003,p2

24- نوران شفيق، نواران شفيق ، أثر التهديدات الالكترونية على العلاقات الدولية دراسة في ابعاد الامن الالكتروني ،المكتب العربي للمعارف ،القاهرة،2016، ص 168

25- Ryan T. Kaminski, Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions, Conference on Cyber Conflict Proceedings, Columbia University, New York, 2010, p.81

26- Jensen, Eric Talbot, Cyber Deterrence, Emory International Law Review, No. (26), Emory University School of Law,Atlanta, Georgia, 2012, pp. 1-52

27-Sico Van Der Meer, Deterrence as a Security Concept Against Cyber Threats, p. 38. Available at https://www.clingendael.nl/pub/2015/clingendael_monitor_2015_en/2_deterrence_as_a_security_concept_against_non_traditional_threats/pdf/appendix_2_cyber.pdf , Accessed at: 11/6/2018

28- Florian Bieber, "Cyberwar or Sideshow? The Internet and the Balkan Wars", Current History 99, no. (635) ,2000, 124-128, online article. http://search.proquest.com/docview/201851259?accountid=7180

29-Robert McMillan. "Was Stuxnet Built to Attack Iran's Nuclear Program?" PC World,https://www.pcworld.com/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.htm

30- عادل عبد الصادق، الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق، المكتبة الأكاديمية، القاهرة، 2016، ص 22-265.

31- Simon Tisdall, Cyber-warfare 'is growing threat', Guardian Newspaper February 2010, at: https://www.theguardian.com/technology/2010/feb/03/cyber-warfare-growing-threat

32- جون إس. ديفيس الثاني واخرون، تهديدات مجهولة المصدر نحو مساءلة دولية في الفضاء الالكتروني، معهد راند، كاليفورنيا، 2017، ص11.

33- محمد عزت هلال، تهديدات الامن الالكتروني في قطاع الطيران المدني، المستقبل للأبحاث والدراسات المتقدمة، شبكة المعلومات الدولية. https://futureuae.com/ar/Mainpage/Item/2827/

34- جون إس. ديفيس الثاني واخرون، تهديدات مجهولة، مصدر سبق ذكره، ص12

35- Thomas Quiggin, Seeing the Invisible National Security Intelligence in an Uncertain Age, London World Scientific Publishing, UK, 2007. p13

36- السيد محمود وهيب: ظاهرة العولمة وانعكاساتها الأمنية، مجلة الأمن العام، المجلة العربية لعلوم الشرطة، العدد(164)، مطابع الشرطة، القاهرة، 1999، ص225

37- Thomas Quiggin, Seeing the Invisible National Security Intelligence in an Uncertain Age, Op, Cit, P14

38- Nicolas Arpagian, « La Cybersécurité », PUF, Paris, 2010, P : 24.

39- عادل عبد الصادق، اسلحة الفضاء الالكتروني في ضوء القانون الدولي الانساني، سلسلة اوراق، العدد (23)، وحدة الدراسات المستقبلية، مكتبة الاسكندرية، الاسكندرية، 2016، ص81.

40- مصطفى سلامة حسين، التأثير المتبادل بين التقدم العلمي والتكنولوجي والقانون الدولي، دار النهضة العربي، مصر 1990، ص 78.

41-Tallinn Manual's Rule 30, North Atlantic Treaty Organization, Tallinn Manual on the International Law applicable to Cyber Warfare, NATO Cooperative Cyber Defense Centre of Excellence, Cambridge University Press, Cambridge, 2013, p. 106

42- Infosec Institute,The Attribution Problem in Cyber Attacks, posted in Hacking on Feb 1,2013 https://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/#gref