

خطر الإرهاب السيبراني: تأثير ديناميكيات التهديد المترابط للظاهرة العابرة للحدود على الأمن الموسع

The Danger of Cyberterrorism: The Impact of the Interconnected Threat Dynamics of Transnational Phenomenon on Extended Security

فاطمة حموته

كلية العلوم الإنسانية والاجتماعية – جامعة باتنة

fatimahmouta@gmail.com

تاريخ القبول: 2012/12/ 15

تاریخ الاستلام: 2012/09/10

© 2017 Pearson Education, Inc. or its affiliate(s). All rights reserved.

Abstract: Cyber terrorism is one of the most complex issues and phenomena that raise the concern of many countries. Indeed, the development of the Internet and other computer networks is revealing new vulnerabilities in our societies, because of the serious effects and repercussions it causes that threaten national security and the highest interests of states, in an era in which cyberattacks and terrorist activities practiced by many entities have increased. How to control cyber risks and limit the impact of cyber threats on people's lives is becoming a crucial question. On this basis, the aim of this article was to take a look at the dangers that cyberterrorism poses to broader security as a "transnational" phenomenon that transcends all kinds of borders.

Keywords: Security - cyberterrorism
- threat – technology

ملخص: يعتبر الإرهاب السيبراني من أعقد القضايا والظواهر التي تثير قلق الدول الكبرى المتقدمة تكنولوجيا قبل غيرها من دول العالم الأخرى الأقل تقدماً، وذلك لما تسببه من آثار وانعكاسات خطيرة تهدد أمنها القومي ومصالحها العليا، في عصر تزايدت فيه الهجمات عبر الانترنت، وتصاعدت النشاطات الإرهابية التي تمارسها جهات غير رسمية ووقعت خسائر كبيرة وسببت انقسامات سياسية ومشاكل داخلية خطيرة للدول المستهدفة. وعلى أساس ذلك، جاء هدف هذا المقال لإلقاء نظرة على الأخطار التي يشكلها الإرهاب السيبراني على الأمن الموسع باعتباره ظاهرة "عبر دولية" تتخطى حدود كل الدول، لأن لها من الديناميكية ما يجعلها لا تنحصر في حيز مكاني واحد، ولا في تهديد واحد، ولا في مستوى أمني واحد، وإنما كل مترابط ببعضه البعض ويعمل هذا النوع من الإرهاب بذلك على تخطي كل الحواجز التي تتميز بها الدولة (تراجع حواجز التمايز، انهيار حواجز الاتصال، تقلص حواجز الاختيار).

كلمات مفتاحية: الأمن – الإرهاب السيبراني- التهديد تكنولوجيا

* المؤلف المرسل

مقدمة:

لقد أدى تطور الشبكة الالكترونية العالمية إلى ثورة في الاتصالات وأصبح الحوار سهلا وممكنا بين شريحة كبيرة وواسعة من الجماهير ومن جميع أنحاء العالم، وهذه الشبكة متاحة لأغراض متنوعة إيجابية وسلبية، وعلى ذكر هذه الأخيرة نجد من بينها ارتكاب أعمال غير قانونية وهجومية خطيرة على الأفراد أو الدول أو المنظمات كالإرهاب السيبراني الذي يشن هجومات سيبرانية تؤثر على الأمن بمفهومه الواسع بشكل سلبي وخطير، وهذا كله ناتج عن الجودة والاستخدامات التقنية عالية التطور والتقدم، ما يجعل الدولة لا تقوى على كبح مثل هذه الهجمات، الأمر الذي يضطرها في نهاية المطاف إلى بذل جهود واسعة سواء كان ذلك على المستوى الوطني أو العالمي لإدارة مثل هذه القضية "عبر دولية" التي تتخطى الحدود وتتجاوزها بذلك منتهكة حقوق الإنسان وارتكاب جرائم تمس بشخص وكرامة الفرد وأمنه من حيث المبنى والمعنى، ما يدعونا إلى الوقوف لمعالجة هذا الموضوع عبر طرح إشكالية مفادها: كيف يمكن لديناميكية التهديدات المترابطة للإرهاب السيبراني كظاهرة "عبر دولية" أن تؤثر على الأمن الموسع وتشكل خطرا عليه؟ وكيف يمكن للمجتمع العالمي مواجهة ذلك؟

وذلك وفق عناصر البحث التالية:

أولاً: الأمن الموسع وعلاقته بالأمن السيبراني

ثانياً: مفهوم الإرهاب السيبراني بين دائرة التهديدات "عبر دولية" ونطاق الجرائم الدولية الماسة بقضايا البعد الإنساني

ثالثاً: ديناميكية تهديدات الإرهاب السيبراني وأخطارها على الأمن الموسع

رابعاً: نحو مواجهة خطر الإرهاب السيبراني: التعاون العالمي لدعم طابع الردع واستحداث طابع التحفيز

أولاً: الأمن الموسع وعلاقته بالأمن السيبراني

1/ ماهية الأمن الموسع

إن تطوير "باري بوزان" 1983 الذي أقر ولأول مرة أن "الأمن لم يعد من الممكن أن يعرف بأنه تهديد، تتم السيطرة عليه باستخدام القوات العسكرية" وبنيّ الدول،

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

فالأمن يتضمن القطاعات غير العسكرية والفواعل من غير الدول، والأجندة الأمنية، وبالتالي هذه النظرة التي ركزت على القطاعات الأخرى للأمن وتجاوز القضايا التقليدية مهدت¹ للأبعاد أمنية أكثر اتساعاً داخل النظام العالمي، و"نبذ السياسات الأمنية المفرطة في التمحور حول الذات".² أي لم يعد مفهوم الأمن يقتصر على المفهوم التقليدي بمعناه العسكري، وإنما له أبعاد أشمل من ذلك حسب التحولات الایتمولوجية والایستمولوجية التي عرفها، فهو من أصعب المفاهيم التي يتناولها حقل العلاقات الدولية بصفة خاصة، وحقل العلوم السياسية بصفة عامة. في حين أن أحدث تعريفات الأمن التي يمكن أن نأخذ بها والأكثر تداولاً في الأدبيات الأمنية المتخصصة هو تعريف "باري بوزان" ومفاده "الأمن هو العمل على التحرر من التهديد".³ ما يعني أن المعنى الاصطلاحي للأمن هو: ذلك الظرف الضروري لنمو الحياة الاجتماعية وازدهارها وهو الشرط الأساسي لنجاح أي وجه من أوجه النشاط البشري سياسياً، اجتماعياً، اقتصادياً عسكرياً... الخ بل أنه من ألزم الضروريات لحفظ كيان الدولة وتأكيد استقلاليتها.⁴

وعلى أساس ذلك، ارتقى مفهوم الأمن في عالم ما بعد الحرب الباردة وأصبح موسعاً، بحيث يمكن تفسيره في أحسن الحالات، بوصفه (أمنًا جماعياً ومتعدد الأبعاد للأملاك المشتركة بين مكونات البشرية)، وقد نشأ هذا المفهوم من التقارير المتتالية التي قدمتها كل من لجنة برانت، ولجنة برانتلاد ورامفال التي أوصت بإعادة صياغة مفهوم الأمن على أساس التعددية، لتتمكن الدول، والمنظمات الحكومية، وغير الحكومية، من

¹ Robin E Walker and Annette Seegers, "Securitisation: The case of post-9/11 United States Africa policy", *Scientia Militaria, South African Journal of Military Studies*, Vol.40, Nr. 2(2012), p.24.

² سليمان عبد الله الحربي، "مفهوم الأمن: مستوياته وصيغته وتهديداته (دراسة نظرية في المفاهيم والأطر)"، *المجلة العربية للعلوم السياسية*، بيروت-لبنان: مركز دراسات الوحدة العربية، ع.14 (2008)، ص.14.

³ عبد النور بن عتر، *البعد المتوسطي للأمن الجزائري: الجزائر، أوروبا والحلف الأطلسي (الروية-الجزائر)*: المكتبة العصرية للطباعة، النشر والتوزيع، (2005)، ص.13.

⁴ هایل عبد المولى طمشوش، *الأمن الوطني وعناصر قوة الدولة في ظل النظام العالمي الجديد (الأردن: دار المنهل، 2012)*، ص.18.

مواجهة الأخطار الجديدة بشكل جماعي.⁵ ويتضمن هذا المفهوم أشكال أمن الدول (العسكري، والسياسي، والمجتمعي، والاقتصادي) كلها، إضافة إلى الأمن البشري (البيئي، والغذائي، والصحي، والتكنولوجي، والعلمي)، في مسعى يجب أن يكون تضامنيا وتعاونيا، لكن يبقى تفعيله شديد التعقيد، إذ ثمة احتمال قوي أن تختزل رؤيته بالأمن الموسع للممثل الفردي، للدولة أو لمجموعة من الدول، الذي يمكن أن يفهم بوصفه أمنا ينطوي على عدة مخاطر.⁶

بالإضافة إل ذلك فالأمن ذو مستويات تتضح على شكل كواكب تخضع في الأساس لعلاقات ارتباطية، تربط بين التفاعلات التي تحدث في المستوى الوطني، الإقليمي، الدولي، العالمي، من هنا يمكننا الحديث عن مستويات الأمن وهي خمس مستويات رئيسية كما يلي:

(1) الأمن الفردي: يعتبر من مستويات الأمن إذ يمثل أمن الفرد ضد أية أخطار

تهدد حياته أو ممتلكاته أو أسرته، وهذا الركن المادي للأمن، أما الركن المعنوي فهو يعبر عن الحاجات النفسية للإنسان من الاعتراف بوجوده وفائدته للمجتمع الذي يعيش فيه، وأهمية نشاطه ودوره للجماعة والمجتمع ومنحه مركزا مميزا في المجتمع تقديرا له.⁷

(2) الأمن الوطني: ويعني أمن الوطن ضد أية أخطار خارجية وداخلية للدولة وهو

ما يعبر عنه بالأمن الوطني الذي يعد المستوى الأساسي للأمن، والذي تسعى الدول لتحقيقه على المستوى الداخلي والخارجي وتنتهج كل السبل والآليات لتحقيق ذلك، بما في ذلك استخدام القوة العسكرية للدفاع عنه.⁸

⁵ قاسم المقداد، دراسة في العلاقات الدولية: النظريات السياسية، الجزء الأول (سورية- دمشق: دار نينوى للدراسات والنشر والتوزيع، ص.82.

⁶ المرجع نفسه، ص.82، 83.

⁷ سرور جرمان سرور المطيري، تغيير مفهوم الأمن القومي الكويتي ودلالاته في الفترة 1990-2012 (القاهرة- مصر: المكتب العربي للمعارف، ص.10.

⁸ المكان نفسه.

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

(3) **الأمن الإقليمي:** ينطوي مفهوم الأمن الإقليمي على مضمون مركب جغرافي وسياسي في آن واحد، مضمون جغرافي بحكم اهتمامه بقضايا الأمن المتعلقة بإقليم جغرافي محدد الخصائص والعناصر، ومضمون سياسي بحكم اهتمامه بقضايا الأمن المتعلقة بهذا الإقليم من زاوية الدول أي الوحدات السياسية الاجتماعية القائمة على هذا الإقليم،⁹ ويجري ذلك ضمن دائرتين:¹⁰

أ- الدائرة الداخلية المتعلقة بالدول الموجودة في نطاق إقليم معين.

ب- الدائرة الخارجية المتعلقة بالدول الموجودة خارج نطاق إقليم معين.

(4) **الأمن الدولي:** ينطوي مفهوم الأمن الدولي على مضمون ذو دالتين سياسيتين في آن واحد:¹¹

- الدلالة الأولى: تشير إلى أمن الوحدات السياسية كلها في النظام الدولي، أي الدول فقط وتحديدا، ولأن المقصود هنا ليس دولة بعينها ولا دول إقليم بذاته، بل المقصود الدول كلها دون استثناء، فسيكون 'الأمن الدولي' المفهوم المناسب للتعبير عن ذلك.

- الدلالة الثانية: تشير إلى متغيرين قديم وجديد، فالمتغير القديم هو الأنظمة السياسية ذات الطبيعة الشاملة المتسعة، كالأنظمة الإمبراطورية التي تسيطر على أقاليم متعددة ومتباعدة منتشرة في أنحاء متعددة من العالم بما يجعل أمنها مرتبطا بكل الأقاليم التي تتكون منها تلك الأنظمة وتسيطر عليها، وهو ما يعني أنه 'أمن دولي'. أما المتغير الجديد فيظهر في صورتين، صورة النظام الرأسمالي وسياساته الاستعمارية أولا، وصورة نظام العولمة وسياساته العابرة

⁹ علي عباس مراد، الأمن والأمن القومي: مقاربات نظرية، ط1 (الجزائر: ابن النديم للنشر والتوزيع، بيروت-لبنان: دار الروافد الثقافية- ناشرون)، ص.57.

¹⁰ المرجع نفسه، ص ص.57، 58.

¹¹ المرجع نفسه، ص ص.59، 60.

للحدود ثانيا، بكل ما نتج وينتج عن هاتين الصورتين من تغير في مفاهيم العلاقات الدولية وأسسها ومصالحها، مما انعكس وينعكس في الحالتين في إضفاء أبعاد متسعة وشاملة على المطالب والمخاطر الأمنية، وهو ما استدعى ويستدعي اتساعا وشمولا مماثلين في المفاهيم الأمنية ومتطلباتها. لذلك شاع مفهوم الأمن الدولي واتسع استخدامه في ظروف أدركت فيها الدول كلها، اتساع وشمولية الشروط العملية لهذا المفهوم، وحاجتها إليه لاستيعاب تلك الشروط في إطاره واستخدامه للدلالة عليها.

(5) الأمن العالمي: وهو أحدث مفاهيم الأمن وأكثرها قربا من مفهوم الأمن الدولي واختلاطا به، ولكن الفارق الجوهرى بينهما، يكمن في اقتصار مفهوم الأمن الدولي في دلالاته على الوحدات السياسية الاجتماعية(الدول)، واتساع نطاق مفهوم الأمن العالمي ليشمل بدلالاته في آن واحد: الوحدات السياسية الاجتماعية (الدول)، فضلا عن الوحدات الجديدة في النظام الدولي من غير الدول والتي بدأت بالظهور منذ بدايات القرن العشرين، مثل المنظمات الإقليمية والدولية، العامة والمتخصصة، المجتمعية والحكومية، ثم أضيفت إليها الشركات والمصالح الاقتصادية العابرة للحدود أو القوميات.¹²

لذلك، بات مفهوما الأمن العالمي، والأمن الدولي يختلفان من حيث:¹³

- عدد وطبيعة أطراف كل مفهوم.
- نوعية المطالب الأمنية لأطراف كل مفهوم.
- نوعية الوسائل والأساليب المناسبة للمطالب الأمنية لأطراف كل مفهوم.
- نوعية ومستويات الاستجابة المناسبة للمطالب الأمنية لأطراف كل مفهوم.

¹² علي عباس مراد، المرجع السابق، ص.60.

¹³ المرجع نفسه، ص.61.

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

ويعني ذلك، أن قضايا الأمن العالمي، لم تعد قضايا ذات طبيعة سياسية فحسب، بل أصبحت أيضا قضايا مجتمعية كالديمقراطية وحقوق الإنسان ومكافحة الإرهاب والتلوث والتصحر والمخدرات... إلخ، لذلك فإن الأمن العالمي يشمل في نطاقه الأمن الدولي، ولكن الأمن الدولي لا يشمل الأمن العالمي.¹⁴ والجدول التالي يبين لنا ما يحويه الأمن الموسع:

الجدول (01): توسيع وتعميق مفهوم الأمن

مجال (توسعي) مستوى (تعمقي)	قضايا الأمن العسكري	القضايا الأمنية الجديدة أو غير العسكرية		
		سياسي	اقتصادي	مجتمعي
				بيئي
نظام	الأمن الدولي			
دولة	الأمن الوطني (داخلي وخارجي)			
تحت الدولة	الأمن المجتمعي			
فرد	الأمن الإنساني			

المصدر:

Heiner Hänggi, "Making Sense of Security Sector Governance", (Retrieved on: 22/02/2019).

<www.dcaf.ch/content/download/36563/.../Hanggi.pdf

2/ الأمن السيبراني أحد "أنواع/ودعائم" الأمن الموسع

بناء على الكلام أعلاه، يمكن أن نستشف ملاحظتين مهمتين هما:¹⁵

1) أن بعض الباحثين قسموا الأمن إلى نوعين أو شكلين هما: الأمن السليبي

والذي يعني قيام الإنسان باتقاء الشر وهو أمن الإنسان الناتج من الخوف من

العدوان والظلم والفقر والجهل والمرض. أما الجانب الآخر فهو الأمن الإيجابي:

والذي يتمثل في سعي المرء المستمر والمتواصل للحصول على حقوقه وتحسين

أحواله وتأمين مستقبله وضمان كل ذلك، على أن الشكليين متصلان اتصالا

¹⁴ المكان نفسه.

¹⁵ هایل عبد المولى طشطوش، المرجع السابق، ص. 19.

وثيقا، فهما وجهان لعملة واحدة، وغايتهما واحدة وهي العيش بسعادة وأمن وسلام.

(2) أن الأمن يقسم من وجهة نظر موضوعية إلى قسمين هما:

(أ) الأمن العام: ويشمل كافة فروع ومناحي الحياة مثل الأمن الاقتصادي والاجتماعي والسياسي والثقافي والإعلامي والعسكري...الخ.

(ب) الأمن الخاص: وهو المعني بعلوم الأمن، ويشمل أمن الأفراد وأمن المعلومات وأمن المكان وأمن المؤتمرات...الخ.

وعلى ذكر هذا الأخير الذي يندرج فيه الأمن السيبراني، نرى أن العلاقة بين الأمن والتكنولوجيا تزايدت، خاصة مع إمكانية تعرض المصالح الإستراتيجية للدول إلى أخطار وتهديد الالكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي. وفرضت تلك التطورات إعادة التفكير في مفهوم "الأمن بحماية قيم المجتمع الأساسية، وإبعاد مصادر التهديد عنها، وغياب الخوف من خطر تعرض هذه القيم للهجوم".¹⁶

والأمن السيبراني أو أمن تكنولوجيا المعلومات هو حزمة عمليات وإجراءات تتوخى تأمين وحماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من الهجوم أو التلف أو السرقة والوصول غير المصرح به، وكذلك من التعطيل أو العرقلة في الخدمات التي تقدمها. وفي هذا السياق ذي العلاقة بمنظومات الحاسبات، يتمثل مفهوم الأمن في كل من الأمن السيبراني الالكتروني وكذلك الأمن المادي.¹⁷

يشمل الأمن السيبراني التحكم في الوصول الفعلي من قبل الأجهزة إلى الشبكة العنكبوتية والبيانات المتاحة فيها، فضلا عن حمايتها ضد الضرر الذي قد يحدث جراء ذلك النفاذ والوصول، كما يتسبب سوء تصرف المشغلين أحيانا إلى تعريض أمن

¹⁶ عادل عبد الصادق، "أنماط 'الحرب السيبرانية' وتداعياتها على الأمن العالمي"، السياسة الدولية،

<http://www.siyassa.org/News/12072.aspx>

¹⁷ حسين باسم عبد الأمير، "تحديات الأمن السيبراني"،

<http://kerbalacss.uokerbala.edu.iq/wp/blog/2018/05/17>

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

تكنولوجيا المعلومات للخداع وإلى الانحراف عن الإجراءات الآمنة من خلال أساليب متعددة.¹⁸

وبات توافر أمن الفضاء الإلكتروني يتحقق حال وجود إجراءات الحماية ضد التعرض للأعمال العدائية، والاستخدام والمعلومات. وعني ذلك الأمن الإلكتروني بعملية وضع المعايير والإجراءات المتخذة لمنع وصول المعلومات عبر الاتصالات، ولضمان أصالة وصحة هذه الاتصالات.¹⁹ فحماية الأمن السيبراني أحد ضمانات حماية الأمن الموسع، فأى مساس به سيؤدي إلى انهيار المجتمع والدولة معا وبشكل سريع غير متوقع.

3/التحول في مفهوم القوة والتهديد والصراع العالمي

إن القوة العالمية اليوم تتأسس على مصادر هي من قبيل القوة اللينة-soft power- (الجذب الثقافي والأيديولوجي، التحكم في المؤسسات الدولية...)، كما تقوم على مصادر ملموسة، القوة الصلبة أو العتادية-hard power.²⁰ وتعتبر درجة مأسسة القوة اليوم لاسيما في إطار تحكم العولمة الغربية تبتعد شيئا فشيئا عن مفهوم تأكيد القوة بالقوات المسلحة أو الغزو، وحلت محلها القوة الناعمة التي تفوق المقدرة الاقتصادية والعسكرية في إنجاز الأهداف عبر التأثير على طريقة تصرف الآخرين.²¹ الأمر الذي دفع بـ "جوزيف ناي" إلى طرح مفهومه عن القوة الناعمة والتي تعني "قدرة الدولة على التأثير في الدول الأخرى، استنادا إلى جاذبية نظامها الاجتماعي والثقافي ومنظومة قيمها ومؤسستها، بدلا من الاعتماد على الإكراه أو التهديد".²²

ولعل ما يهم أيضا في تطوير مفهوم القوة الناعمة هو تحولات مفهوم القوة نفسه، الذي صار موضع بحث ونظر مع التحولات الدولية التي بدأت إرهاصاتها في ظل

¹⁸ حسين باسم عبد الأمير، المرجع السابق.

¹⁹ عادل عبد الصادق، المرجع السابق.

²⁰ عبد النور بن عنتر، البعد المتوسطي للأمن الجزائري الجزائر، أوروبا والحلف الأطلسي (الجزائر: المكتبة العصرية للطباعة، النشر والتوزيع، 2005)، ص.34.

²¹ جوزيف ناي، "حدود القوة الأمريكية"، ترجمة: علي حسين باكير، في، علم السياسة والعلاقات الدولية: قراءات عالمية، مجلد 1: العدد 3 (شتاء 2005): ص.29-40.

²² محمد توفيق البحري، مترجما، القوة الناعمة وسيلة النجاح في السياسة الدولية، ط.1 (الإمارات العربية المتحدة: مكتبة العبيكان، 2007)، ص.181-184.

الحرب الباردة، وظهور رؤى نقدية للمفهوم البسيط للقوة كعلاقة بين طرفين، فقد بدأ الالتفات لذلك المفهوم كمتغير متطور في أبعاده، وجهود "ناي" وغيره تبني على جهد نظري سبق كتاب "ناي وكيوهان"، أبرزها ما كتبه "ستيفن لوكس" في مجال النظرية السياسية منذ العام 1974 في كتابه الشهير "القوة: رؤية راديكالية"، وذكر فيه القوة الناعمة باعتبارها القدرة على تحديد الأجندة، وتوجيه دفة العلاقة الدولية، والتأثير النهائي في صياغة الأطراف المختلفة لأهدافها.²³ ولا تعني القوة الناعمة أن أدوات القوة الصلبة تختفي، لكن القوة الناعمة لها لحظتها المناسبة، وهي في الغالب تعمل في إطار من التبادل والتوافق مع أدوات القوة الصلبة الاقتصادية والسياسية والعسكرية.²⁴

كما أن مفهوم القوة لم يعد حبيس هاتين الرؤيتين، وإنما الحديث عن الحروب الالكترونية ينقلنا مباشرة إل التركيز على التغير في أساسيات الحروب التقليدية، الذي يعتبر العامل الأساسي في تحليل الصراعات مهما كان نوعها فالانتقال من المجال المادي الملموس إلى المجال الافتراضي أفرز مفهوما جديدا للقوة يقترن بمجال الصراع الجديد (الفضاء الالكتروني) وهو القوة الالكترونية.²⁵ فقد لعب الفضاء السيبراني دورا أساسيا في تعظيم القوة، أو الاستحواذ على عناصرها الأساسية في العلاقات الدولية أين أصبح المجال عنصرا حيويا في تنفيذ عمليات ذات فاعلية في الأرض، والبحر، والجو، والفضاء، واعتماد القدرة القتالية في التحكم والسيطرة التكنولوجية.²⁶

ويعرف "جوزيف ناي" القوة السيبرانية بأنها "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الالكتروني، بمعنى القدرة على استخدام الفضاء الالكتروني لخلق مزايا، والتأثير بالأحداث المتعلقة بالبيئات

²³ هبة رءوف عزت، القوة الناعمة المهددة: أزمة النظام القوي والدولة الضعيفة بمصر، مركز دراسات الجزيرة، 2012.

²⁴ المرجع نفسه.

²⁵ عبلة مزوزي، "إستراتيجية الردع وانعكاساتها على الواقع الإقليمي والدولي بعد نهاية الحرب الباردة-دراسة حالة إيران-" (مذكرة مقدمة لنيل شهادة دكتوراه العلوم في العلوم السياسية تخصص: علاقات دولية، جامعة باتنة، 2017/2018)، ص.105.

²⁶ عادل عبد الصادق، المرجع السابق.

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

العملية الأخرى عبر أدوات الكترونية".²⁷ أما "دانيال كويل" فيرى أن القوة الالكترونية هي "القدرة على استخدام الانترنت لخلق مزايا، والتأثير في الأحداث البيئية التشغيلية كافة من خلال أدوات القوة". ما يعني أن القوة الافتراضية عي امتداد لكل من القوة الصلبة والناعمة في الوقت ذاته.²⁸

وصاحب هذا التغير في مفهوم القوة التغير في مفهوم التهديد، فالتهديد الذي كانت الأسلحة التقليدية والنووية تثيره تحول إلى تهديد أساسه العقل والمدرجات، والمعارف المتوفرة لدى الخصم الالكتروني بحيث يستطيع التحكم في بعض الصراعات الموجودة على أرض الواقع من خلال أنظمة معلومات العدو وحتى البنيات الأساسية للبرامج سواء العسكرية الدفاعية أو البنية التحتية الالكترونية أو غيرها ومن ثم إلحاق الضرر به.²⁹

وهذا يعني أن بروز الفضاء الالكتروني كمهدد، بسبب النزاعات التي تنشأ فيه بين الفاعلين المختلفين، تكنولوجيا الاتصال والمعلومات، وبرز "الصراع السيبراني" كحالة من التعارض في المصالح والقيم بين الفاعلين في الفضاء الالكتروني.³⁰

إذ بعد أحداث 11 سبتمبر 2001 بدأ التركيز على الفضاء الالكتروني كتهديد أمني جديد بفعل أحداث دولية، كان أبرزها استخدام تنظيم القاعدة له كمساحة قتال ضد الولايات المتحدة الأمريكية، وفي عام 2007 برز بوضوح دور الفضاء الالكتروني كمجال جديد في العمليات العدائية في الصراع بين استونيا وروسيا، وفي العام 2008 في الحرب بين روسيا وجورجيا،

وجاء الهجوم الإلكتروني بفيروس "ستاكسنت" على برنامج إيران النووي عام 2010 ليمثل نقلة مهمة بالتطور في مجال الأسلحة الالكترونية.³¹

²⁷ عبلة مزوزي، المرجع السابق، ص.105.

²⁸ المكان نفسه.

²⁹ المرجع نفسه، ص.106.

³⁰ عادل عبد الصادق، المرجع السابق.

³¹ عادل عبد الصادق، "أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني"،

http://accronline.com/article_detail.aspx?id=28924

وإذا كان الأمن القومي يعنى بالحماية وغياب التهديد لقيم المجتمع الأساسية وغياب الخوف من خطر تعرض هذه القيم للهجوم، فإن الفضاء الإلكتروني قد فرض إعادة التفكير في مفهوم الأمن، والذي يتعلق بتلك الدرجة التي تمكن الدولة من أن تصبح في مأمن من خطر التعرض للهجوم العسكري أو الإرهابي، وإجراءات الحماية ضد تعرض المنشآت الحيوية للبنية التحتية للأعمال العدائية من خلال الاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.³² وتعني كلمة الأمن في مجال الفضاء الإلكتروني: إجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات. ومن جهة أخرى فإن الأمن القومي يعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها وغياب الخوف من خطر تعرض هذه القيم للهجوم، وتشير كلمة الأمن إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات.³³

ثانيا: مفهوم الإرهاب السيبراني بين دائرة التهديدات "عبر دولية"/ونطاق الجرائم الدولية الماسة بقضايا البعد الإنساني

لقد تلاقت الجريمة مع البيئة الإلكترونية عند نقطة الارتكاز وفي حيز بسيط للغاية وهي لوحة المفاتيح. ففي ظل هذه البيئة تكمن المشكلة في معرفة من الذي يقف خلف لوحة المفاتيح، فمرونة تكنولوجيا المعلومات والحاسب والانترنت هي التي ساعدت الأصابع الخبيثة لكي تنشر العنف والخوف ولكي تخطط وتنفذ الهجمات الإرهابية.³⁴ فتكنولوجيا المعلومات تكون مفيدة للجماعات الإرهابية في ناحيتين:³⁵

- (1) يمكن لهم أن يستخدموا أجهزة الحاسب والانترنت بوصفها أداة مفيدة لتعزيز النشاط الإرهابي التقليدي مثل استخدام الانترنت في التجنيد والتدريب وتبادل المعلومات بين المنظمات الإرهابية المختلفة.

³² المكان نفسه.

³³ المكان نفسه.

³⁴ محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية (دار ناشري للنشر الإلكتروني، جانفي

2012)، ص.08.

³⁵ المرجع نفسه، ص.09.

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

(2) البنية التحتية للمعلومات يمكن أن تشكل هدفا جذابا للأعمال الإرهابية التي يمكن من خلالها التأثير على الرأي العام العالمي

وإذا كانت تكنولوجيا المعلومات والحاسب عوامل جذابة للإرهابيين فإن الانترنت أكثر مرونة وأكثر جاذبية لعوامل عدة منها:³⁶

- سهولة الوصول إلى شبكة الانترنت
- ضالة أو معدومة التنظيم والرقابة، وانعدام السيطرة الحكومية في أغلب الأحيان
- الانتشار الجماهيري الكبير من جميع أنحاء العالم
- سهولة استخدام الانترنت، وتوفير بيئة جيدة للوسائط المتعددة، فيسهل الجمع بين النصوص والرسوم وبين الصوت والفيديو، كما يسهل تحميل الأفلام والأغاني والكتب والملفات المتعددة.
- القدرة على التأثير عن طريق التغطية الإعلامية.

إذا، ساهم تطور الانترنت ضمن عالم معتمد على انفتاح نظم المعلومات وتربط الشبكات، في جعل العالم قرية كونية شاملة، يمكن كل فرد من أفرادها تبادل المعطيات واقتسامها، والنفاد إليها بكل حرية ويسر. إلا أن هذا التطور السريع لا يخلو من أخطار تمثلت في ظهور أعراض وآثار اجتماعية حادة غير متوقعة لهذه التكنولوجيات، تفرض على مجتمع المعرفة والمعلومات التهيؤ واليقظة لمواجهة المخاطر الجديدة، ولعل أخطر تجليات هذه المخاطر شهرة وانتشارا في العالم ظاهرة الإرهاب السيبراني.³⁷

³⁶ المرجع نفسه، ص.10.

³⁷ أحمد دلال وآخرون، الثورات العربية: عسر التحول الديمقراطي ومآلاته، ط.1 (بيروت: المركز العربي للأبحاث ودراسة السياسات).

فالإرهاب السيبراني مرتبط بالعنف من الناحية السوسولوجية، فهو تعبير اجتماعي افتراضي جديد يحاول أن يصوغ لغة خاصة، وأن يفتك مساحة من السلطة على حساب السلطة القائمة، ليشكل جزء من النسيج الاجتماعي المدني؛ ففيه نزعة نحو تقليص مساحة الهيمنة، ورد الاعتبار إلى كل من كان في الأمس في التخوم والأطراف؛ أي ما يسمى عادة "المهمش" أو "المقصى"، أو يصنف ضمن الأقليات؛ فالعنف والإرهاب السيبراني أنشأهما الضعيف ضد القوي، وهما تعبير اجتماعي احتجاجي مختنق ومكتوم من الذين تمارس تجاههم سلطة إكراهية، فاعلها الدولة أو السلطة المالية أو السلطة الدينية... الخ.³⁸

فالإرهاب السيبراني يندرج ضمن دائرة التهديدات "عبر دولية"، فهو يعتبر كظاهرة تمددت عبر حدود الدولة، أي: التحول نحو ما يطلق عليه بالفواعل اللاشرعية/أو الإجرامية، ذلك التحول الناشئ عن نمو ظاهرة الجماعات غير شرعية ذات الصفة العالمية، وهي (الجماعات) التي تضم عضويتها أعضاء من جنسيات مختلفة، وتعمل في إطار التخريب والتدمير متعدد الأطراف، أو عالمية الاتساع، وهي -بحكم أيديولوجيتها وأهدافها- لا تتجاوز حدود الدول، فقط بل تهدد أمنها القومي.

ومع بداية القرن الحادي والعشرين احتلت هذه الجريمة مكان الصدارة بين المشكلات الأمنية الأكثر خطورة في العالم، وذلك نتيجة للمتغيرات الكبيرة التي أفرزتها الظروف والمعطيات السياسية والاقتصادية والاجتماعية التي من أبرزها النمو الشامل والمتسارع للنشاطات التجارية والمالية والاقتصادية، وما صاحبها من تطور هائل في وسائل الاتصالات والنقل والتقدم التقني، وعولمة النظم الاقتصادية والمالية التي أسهمت في تحرير التجارة الدولية، وتجاوز الحدود الوطنية بين الدول، ولاسيما المجال المصرفي وتداول الأموال فضلا عن انهيار سلطة الدولة أو ضعفها في بعض الدول.³⁹

³⁸ المكان نفسه.

³⁹ مايا خاطر، "الجريمة المنظمة العابرة للحدود الوطنية وسبل مكافحتها"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مجلد 27، ع.3(2011)، ص.510.

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

هذا من جهة، ومن جهة أخرى فالإرهاب السيبراني من الجرائم الدولية التي تمس بأحد قضايا البعد الإنساني التي تخص الأمن الموسع الذي يهدف إلى تحقيق أمن وسلامة الفرد ويمكن القول بأنه ذلك الذي يعني "كل ما يحقق الاستقلال السياسي للدولة وسلامة أراضيها، وضمان الاستقرار السياسي والاقتصادي والاجتماعي لأفرادها. فهو يشمل تحقيق الأمن الخشن- المتميز بالطابع العسكري للأمن (الأمن التقليدي)- والناعم(الجذب الثقافي، الدبلوماسية، القوة الإعلامية...) في الوقت ذاته، وبعديه الداخلي والخارجي، أي تأمين كيان الدولة داخليا وخارجيا، وتحقيق الاستقرار السياسي والاجتماعي والاقتصادي، وتحقيق الرضا التام لأفراد المجتمع".⁴⁰

بمعنى آخر، هناك من الآثار المحتملة للإرهاب السيبراني على حقوق الإنسان أحد قضايا البعد الإنساني، إذ يتعلق بالفضاء السيبراني اثنان من الحقوق التي أوردتها العهد الدولي للحقوق المدنية والسياسية (الذي صادقت عليه الولايات المتحدة الأمريكية في سبتمبر 1992). قد تكون المادة 17 (حماية الخصوصية والسمعة) ذات صلة بالعمليات السيبرانية التي يقصد بها الإضرار بسمعة فرد ما، أو الكشف عن معلومات خاصة عن فرد(قد تشكل استفزازا قبل نشوب نزاع إذا كان شخصا بارزا أو ذا نفوذ سياسي). وقد تكون المادة 19 (حماية الحق في طلب المعلومات) ذات صلة بالهجمات السيبرانية التي تهدف إلى منع الأفراد من الحصول على خدمات عن طريق شبكة الانترنت أو وسائل تواصل أخرى. وقد يتعلق الأمر أيضا بعدد من الحقوق الأخرى مثل الحق في الحياة والرعاية الصحية والغذاء، وذلك تبعا لطبيعة الهجوم السيبراني وأهدافه. وقد يشير احترام هذه الحقوق الأخرى على سبيل المثال إلى أن هجوما سيبرانيا بقصد فرض عقوبات اقتصادية يجب مع ذلك أن يسمح بإجراء معاملات متصلة بالحصول على الغذاء والدواء.⁴¹

⁴⁰ سليمان عبد الله الحربي، المرجع السابق، ص 10-12.

⁴¹ إيزابيل روبنسون وإيلين نول، "النزاع السيبراني والقانون الدولي الإنساني"، المجلة الدولية للصليب الأحمر، مجلد 94 (صيف 2012)، ص. 527.

وقد أعلن عدد من الدول أن الوصول إلى شبكة الانترنت حق أساسي من حقوق مجتمعاتهم (حتى أوت 2011، كان من بين هذه الدول استونيا وفرنسا واسبانيا وفنلندا).وعليه، إذا كان الوصول إلى الانترنت حقا من حقوق الإنسان، فإن الأعمال التي تقلص الوصول إلى الانترنت أو تمنعه تعد انتهاكا لذلك الحق.⁴²

وعلاوة على ذلك، ثمة نقطة مهمة مثار جدل في قانون حقوق الإنسان هي مدى انطباقه أثناء نزاع مسلح أو عمليات عدائية، ويذهب مثلا موقف الحكومة الأمريكية إلى أن ضرورات التقليل قدر الإمكان من المعاناة الإنسانية التي لا داعي لها يتم الوفاء بها من خلال متطلبات قانون النزاعات المسلحة، ومن ثم يجب أن لا يضع قانون حقوق الإنسان قيودا إضافية على تصرفات قواتها المسلحة.على النقيض من ذلك، عدد من الهيئات الدولية مثل المحكمة الجنائية الدولية، ولجنة حقوق الإنسان، ترى أن قانون حقوق الإنسان يجوز بل ويجب أن ينطبق مثل قانون النزاعات المسلحة على الأعمال العدائية.⁴³

ثالثا: ديناميكية التهديدات المترابطة للإرهاب السيبراني وأخطارها على الأمن الموسع

مع تطور الوسائط الالكترونية، وتعدد نوعية الخدمات التي تقدمها، ازداد عدد المواقع الالكترونية التي تديرها "المنظمات الإرهابية" على شبكة الانترنت في العالم، وهذا الأمر يعقد، من دون شك، عمليات التتبع والاصطياد والتحليل لمكونات "الوحش الالكتروني" الجديد الذي يعتقد بعضهم أن ما من حل له سوى مرافقته، والتعايش معه، بوصفه سيفاً ذو حدين؛ ذلك أنه يعد، بصرف النظر عن مخاطره وتهديده الأمن والسلامة، وسيلة للاسترشاد، ومصدرا للمعلومات في كل عملية تواصل بين الجماعات والأفراد والمنظمات الإرهابية.ثم إنه كلما منع الإرهابيون الإلكترونيون من استخدام شبكة الانترنت واستئصال مواقعهم، ظهرت مواقع جديدة باستراتيجيات جديدة ومتفرقة ومتنوعة ومراوغة؛ إذ هي تختفي فترة لتظهر مرة أخرى بصيغ وعناوين

⁴² المكان نفسه.

⁴³ المرجع نفسه، ص ص. 527، 528.

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

الكثرونية مغيرة تعكس الحركة المتواصلة التي يشهدها المجتمع في العالم الافتراضي، والمجتمعات العربية، أيضا بعد الثورة.⁴⁴

في سياق صراع الإرهاب الشبكي السيبراني، تستهدف بعض الجماعات والمنظمات خصومها على الانترنت، استناد إلى عوامل عدة، مثل الصراعات الاجتماعية-السياسية والصراعات الإثنية والعرقية. وتتميز حروب المواقع بين هذه الفئات بالتدمير المتبادل والاحتلال المؤقت من أحد الخصوم لموقع الآخر، ونشر الدعاوى السياسية (البروباغندا) المعادية له.⁴⁵

وفقا لما تحدث كل من Zanini & Edwards عام 2001 هناك ثلاثة أنواع من الأنشطة الهجومية يمكن للإرهاب السيبراني استخدامها:⁴⁶

أولا: يمكن للإرهابيين أن يستخدموا تكنولوجيا المعلومات لغرض الدعاية

ثانيا: استخدام شبكة الانترنت لشن هجمات تخريبية

ثالثا: يمكن استخدام هذه الشبكات لأغراض تدميرية

أما ما تحدث عنه Ballard فالإرهاب السيبراني يقوم بما يلي:⁴⁷

- هجومات المعلومات: يركز الإرهابيون من خلال هذا النوع على تغيير أو تدمير محتوى الملفات الالكترونية، وأنظمة الحاسب، أو أي مواد أخرى متصلة بالبيئة الالكترونية.

- هجمات البنية التحتية: هي الهجمات التي تستهدف تعطيل أو تدمير الأجهزة الفعلية، أو أنظمة التشغيل، أو البرمجيات، في بيئة محسوبة مما يؤدي إلى تدمير أو تعطيل البنية التحتية للمعلومات.

⁴⁴ أحمد دلال وآخرون، المرجع السابق.

⁴⁵ المكان نفسه.

⁴⁶ محمد سيد سلطان، المرجع السابق، ص 32، 33.

⁴⁷ المرجع نفسه، ص 33، 34.

- تيسير التكنولوجيا: يتم من خلالها استخدام الحاسب وأنظمة الاتصالات على التخطيط للهجمات الإرهابية، والتحريض عليها، أو تسهيل الإرهاب التقليدي.
- جمع التبرعات والترويج: يستخدم الإرهابيون شبكة الانترنت لجمع التبرعات من أجل قضية سياسية معينة، أو لجلب المساعدات، أو لتعزيز أيديولوجية بديلة في التوجيه.

فهذه التهديدات مترابطة ببعضها البعض سواء تمت على المستوى الداخلي أو المستوى الخارجي، فلها من الحركية ما يمكنها من القيام بتحركات، تشكل تهديدا على أمن الدولة ومصالحها والمنظمات والشركات، وعلى الأفراد وأمنهم الشخصي والخاص. ما يعني أن الإرهاب السيبراني أنواع يندرج ضمن ثلاث فئات رئيسية وهي:⁴⁸

- (1) بسيطة: تتكون من هجمات أساسية بما في ذلك اختراق نظام فردي
- (2) متقدمة: وهي هجمات أكثر تعقيدا وقد تتضمن اختراق أنظمة أو شبكات متعددة

(3) معقدة: وهي هجمات منسقة يمكن أن يكون لها تأثير واسع النطاق والاستفادة من الأدوات المتطورة.

وحسب مؤتمر الاستثمار الاستراتيجي لوزارة الاقتصاد الأمريكية في جويلية 2017، حسب المشاركون الذين أقرروا بأن الهجمات الإرهابية السيبرانية لا تشابه مع القرصنة والبيانات الاستهلاكية، مثلما حدث في خرق بيانات Equifax، فهم يهدفون بدلا من ذلك إلى إحداث حالة من الذعر العالمي أو فقدان عدد كبير من الأرواح عن طريق اختراق البنية التحتية الحيوية، مثل شبكات الطاقة، ومنظمات التداول، وأنظمة الرعاية الصحية.⁴⁹

⁴⁸ مركز سميت للدراسات، "الإرهاب السيبراني..الوجه التكنولوجي للتطرف"،

<<http://smtcenter.net/archives/slider>>

⁴⁹ المكان نفسه.

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

ويلجأ للإرهاب السيبراني، حسب "لوك ديمبوسكي"، نائب مساعد المدعي العام السابق للأمن القومي في وزارة العدل الأمريكية، تتبع التطورات في مجال الإرهاب السيبراني، وأوضح على نحو متزايد، على مدار السنوات القليلة الماضية، أن دولا مارقة مثل كوريا الشمالية تتورط في هجمات سيبرانية مدمرة، مثل تلك التي وقعت على Sony في عام 2014، بالإضافة إلى وجود أدلة على أن دولا مثل إيران تدخل في ضوابط نظام السدود في راي، نيويورك، الذي تم قطع الاتصال به لحسن الحظ لأغراض الصيانة.⁵⁰

ومثل هذا التهديد وضعنا، مباشرة، في مواجهة الجانب المتعلق بالدولة؛ والاهتزاز الحاصل في "حواجزها"، والمتمثلة في تراجع "حواجز التمايز، انهيار حواجز الاتصال، تقلص حواجز الاختيار".⁵¹ بحيث أصبحت الدولة حاليا في النقطة الأولى عاجزة عن السيطرة على ظواهر مثل الشركات الكونية، والبورصات، والأقمار الصناعية، والمشكلات البيئية الكونية، وحركة رؤوس الأموال، والأسواق المالية العالمية، وغيرها، ناهيك عن شبكة المعلومات الخاصة بالحاسب الآلي، أو خطوات الانترنت، أو المكالمات الهاتفية، وحتى الإرهاب السيبراني تلك التي لا تتوقف عند نقاط 'تفتيش' حدودية.⁵² في حين تظهر لنا النقطة الثانية: انكشاف ما بداخل الدول أمام تقنية المعلومات والاتصالات المرئية، وحتى خارج الدولة،⁵³ إذ من الصعب تحكم الدولة في وسائل الإعلام والاتصال وما يحدث في الفضاء السيبراني الذي أسقط أقتعة السلطة، وفتح بابا لممارسة العنف والإرهاب وكل الجرائم الالكترونية.

أما فيما يخص النقطة الثالثة المتعلقة بتقلص حواجز الاختيار؛ فالدولة لم تعد حرة سياسيا واقتصاديا في فرض توجهاتها، فبغير شبكات الاتصال العالمية، ومنظمات حقوق الإنسان الرسمية (من خلال الأمم المتحدة)، وغير الرسمية (الجماعات الأهلية)، صندوق النقد الدولي والأسواق العالمية وغيره كثير، فما يخص دولة بعينها أصبح أمرا يخص

⁵⁰ المكان نفسه.

⁵¹ حسين معلوم، المرجع السابق، ص. 9-13.

⁵² حسين معلوم، المرجع السابق، ص. 10.

⁵³ المرجع نفسه، ص. 11.

العالم بأسره.⁵⁴ إذ باستطاعة الإرهاب السيبراني فرض نظام سياسي واقتصادي معين على الدولة يخدم توجهاته أكثر مما يخدم مصلحة الدولة والمجتمع.

ويمكن أن نلخص ديناميكية التهديدات المترابطة للإرهاب السيبراني التي تفتك بالأمن بشكل واسع في أربع مسارات⁵⁵ متصلة ببعضها البعض وهي:

المسار الأول: يتعلق بعملية الانتقال للأحداث من أرض الواقع إلى الفضاء السيبراني إما لتصفية الصراعات أو استخدامه كوسيلة إعلام في التحريض أو العنف أو بث الكراهية مثل حالة انتقال الصراع بين الكوريتين إلى الفضاء الإلكتروني أو ما بين الصين وتايوان أو ما بين تنظيم القاعدة والولايات المتحدة الأمريكية.

المسار الثاني: فيتعلق بانتقال وتصدير الفضاء السيبراني لعناصر تهديد إلى أرض الواقع عن طريق ما يتم الاستجابة له من نشر معلومات أو صور أو فيديو من طرف إرهابيين مجهولي الهوية وهو ما يكون له تأثير في تكسير شبكة العلاقات القائمة ونشر شائعات تضر بالسلام من خلال ما ينشر من خطابات والتضليل بالمعلومات.

المسار الثالث: فتعلق بدور الفضاء السيبراني كوسيلة إعلام يتم استخدامها من طرف الإرهابيين كنشاط مواز للحوادث على أرض الواقع مثل أحداث القتل أو التدمير أو الحروب بما يساهم في خلق ردود أفعال عالمية رسمية وغير رسمية، مؤيدة ومعارضة.

المسار الرابع: فاستعمال الفضاء السيبراني من طرف الإرهاب هدفه التأثير على المصالح الإلكترونية من خلال إطلاق فيروسات، قرصنة، سرقة معلومات أو التجسس وغيرها كثير.

رابعا نحو مواجهة خطر الإرهاب السيبراني: التعاون العالمي لدعم طابع الردع واستحداث طابع التحفيز

إن الخطر المتزايد من جرائم الإرهاب السيبراني ضد نظم وأمن المعلومات، يمثل تحدي كبير أمام حكومات الدول. فهذه الأخيرة وجدت نفسها مُطَالَبَةً بالتصدي للجريمة

⁵⁴ المرجع نفسه، ص. 12.

⁵⁵ نورة شلوش، "القرصنة الإلكترونية في الفضاء السيبراني 'التهديد المتصاعد لأمن الدول' "مجلة مركز بابل للدراسات الإنساني، المجلد 8، ع. 2 (ص. 200، 201).

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

التي تعتبر من أكثر جرائم العصر صعوبة من حيث مكافحتها أو ملاحقة مرتكبيها. وبإجماع الخبراء يمكن للحكومات حماية البيئة الالكترونية من خلال العمل على وضع سد منيع وحاجز قوي من القوانين والتشريعات الوطنية، والعمل على مكافحتها، فالقوانين الحالية قد تكون غير قابلة للتنفيذ لمكافحة مثل هذه الجرائم.⁵⁶

وهذا أحدث نقلة نوعية في مفهوم القوة التي امتدت للحديث عن الردع الالكتروني والذي يعرفه "إميليو اسيليو" Emilio Iasiello بأنه "الإستراتيجية التي تحاول من خلالها الدولة المدافعة للحفاظ على الوضع الراهن عبر التلويح بإمكانية ردع الهجمات الالكترونية المعادية والتأثير على جهاز صنع القرار الخاص بالخصم".⁵⁷ في حين يمكن تعريف الردع السيبراني على أنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء وأصول التي تدعم العمليات الفضائية".⁵⁸ ويرتكز الردع السيبراني على:

(1) إستراتيجية الدفاع السيبراني وتتمثل في ثلاثة ركائز أساسية هي:⁵⁹

الركيزة الأولى: مصداقية الدفاع؛ يتطلب الدفاع عن أنظمة المعلومات، وردع أي محاولة لاختراقها، بالإضافة إلى توافر أنظمة نسخ احتياطية على أن أنه الحل العملي الأكثر فعالية.

الركيزة الثانية: القدرة على الانتقام؛ لابد أن يتكبد المهاجم ضررا يفوق ما وقع على المدافع من أضرار، ولكن هذا يتطلب القدرة على الانتقام وتنفيذ هجمة سيبرانية على الهجوم الأصلي، بعد التعرف عليه وهو صعب التحقق.

الركيزة الثالثة: الرغبة في الانتقام؛ فعلى المدافع أو من تعرض للهجوم أن يعلن عن رغبته في الانتقام من المهاجم، ذلك أن امتلاك القدرة على الانتقام لا تكفي بمفردها.

⁵⁶ محمد سيد سلطان، المرجع السابق، ص.37.

⁵⁷ عبلة مزوزي، المرجع السابق، ص.106.

⁵⁸ رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات"، المركز العربي لأبحاث الفضاء للالكتروني،

<http://accronline.com/article_detail.aspx?id=28706>

⁵⁹ المكان نفسه.

(2) متطلبات الردع: الردع السيبراني صعب التنفيذ كما أن هناك العديد من العوامل التي يجب أن تحدث لضمان تحقيق النتائج المرجوة منه، منها: تطبيق طرق ووسائل جديدة، وإعادة تكييف مفاهيم الردع التقليدية لتناسب مع هذا المجال الجديد، فلا يمكن معرفة الهدف دون معرفة الخصم وهدفه، لا يمكن للردع أن ينجح، قد تتكرر مثل هذه الأفعال الإرهابية الإجرامية مستقبلا، ودون الرد على ذلك الهجوم لن يكون الردع ممكنا لتآكل مصداقيته ولذلك تتعدد الخيارات للردع، ولعل منها ما يلي:⁶⁰

الخيار الأول: الردع السلبي: وهو الأقل تعقيدا، لكنه ليس واقعيًا، إذ يتمثل في عدم الرد على الخصم، ولكن مع الاعتراف بأن الأمن السيبراني، وكافة الإجراءات المتعلقة بالأنظمة الأمنية بشكل مستمر. فمن شأن أي تحسن في تدابير الأمن السيبراني أو الردع السلبي أن يرفع أي تكاليف أي هجوم سيبراني في المستقبل، مما يقلل من فرص حرص المهاجم وأن هذا الرد بمثابة دعوة لمواصلة الأنشطة السيبرانية على نطاق أوسع.

الخيار الثاني: الاحتجاجات الدبلوماسية: يمكن طرد مسئول الدولة التي يشتبه في شنّها الهجوم أو مشاركتها في مثل هذه الأعمال الإرهابية. حتى لا يتسبب ذلك أضراراً وهجمات مستقبلية.

الخيار الثالث: التدابير القانونية: بمعنى اتخاذ إجراءات قانونية ضد المشتبه فيه شن الهجوم، ومع ذلك، فهذه التدابير تبقى ذات طبيعة رمزية، وتنطوي على خطر إقامة دعوى قضائية تضطر فيها الدول لكشف معلومات استخباراتية حساسة، ليسبب ذلك ضرراً أكثر مما يستحق.

الخيار الرابع: العقوبات الاقتصادية: بعد اتهام الولايات المتحدة الأمريكية إيران والعراق وكوريا وتصنيفها ضمن قائمة الدول المارقة والإرهابية تم تعزيز

⁶⁰ المكان نفسه.

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

العقوبات الاقتصادية على كل من كوريا وإيران، والحرب والعدوان العسكري على العراق.

الخيار الخامس: الانتقام في الفضاء الافتراضي: لطالما كان التهديد بالانتقام رادعا فعلا يردع الاختراقات السيبرانية المستقبلية، فمن شأن الإرهابيين أن يزيدوا من خطر التصعيد في العمل على سرقة ونشر المعلومات الخاصة بالبنية التحتية.

الخيار السادس: الانتقام العسكري؛ وهو خيار غير واقعي، لأنه سيسفر عن رد عسكري مضاد، ويمكن أن يبدأ عملية خطيرة من التصعيد.

(3) بلورة إستراتيجية متكاملة للردع: الحديث عن الردع السيبراني بات أكثر مرونة، وباقتربات مختلفة، وتلك المرونة يمكن تداولها بطريقتين مختلفتين هما:⁶¹

الأولى: الأنظمة البديلة؛ إن اعتماد دولة ما على نظام واحد، وتم اختراقه، سيسفر عن عواقب وخيمة؛ وبخاصة إذا تعلق هذا النظام بالبنية التحتية الرئيسية للدولة، أنظمة بديلة لتكون في حوزة الدولة نفسها أو الدول الصديقة، وفي حالة الهجوم السيبراني يمكن الاستعانة بتلك الأنظمة البديلة أو الاحتياطية.

الثانية: إعادة التأسيس؛ فإذا أمكن للدولة التغلب على الهجوم الذي تعرضت له بسرعة، وإعادة تشغيل النظام، ستكون الآثار هامشية، ولكن الطريقة الوحيدة لتجنب الكوارث على الجميع، ورغم كونه السبيل الأفضل للردع، إلا أنه يكتنفه مسائل قانونية عدة.

هذا من ناحية دعم طابع الردع، أما من ناحية أخرى فيمكن استحداث منظومة تحفيزية تحفز الأشخاص عن التراجع عن هذه الجريمة ومكافأة من يبلغ عن هؤلاء المجرمين، لأن التحفيز يعتبر "شكلا من أشكال تشجيع الشخص الذي يعمل للحد من العمل السلبي لذا يجب أن تكون قيمة المنحة مهمة ومعتبرة لكي تشجع الشخص

⁶¹ رغدة البيبي، المرجع السابق.

على الحد من هذا العمل السلبي، وإلا فضل ذلك الشخص التخلي عن هذه المنحة بدلا من الالتزام بالأضرار⁶² السيبرانية والحد منها" ويكون وفق الطرق التالية:

1) المقاربة النفسية:

يتم هذا عبر المقاربة النفسية التي تعتمد في تحقيق ذلك على تخفيف التناقضات والخلافات بين الإرهاب السيبراني والأشخاص أو الدولة عبر الفضاء الإلكتروني وحتى في وسائل الإعلام الأخرى، ببناء إطار سيكولوجي بإثارة للبناء الاجتماعي والتفاعل الرمزي بالابتعاد عن المنهات والاستفزازات السلبية، وإنما استحضار البُنى التي تتشكل من خلال الانضمام مع الآخرين والتفاعل معهم، من المعتقدات، القيم، التجارب التاريخية الإيجابية، تصورات الهوية... الخ، التي تشكل مجتمعة الوعي الإداري الجماعي للفرد حتى يتسنى استمالتهم عن طريق العواطف والإدراكات الجيدة.

أي هنا نكون أمام استعداد نفسي لتسوية العلاقة بين هؤلاء المجرمين والمجتمع، وهو ما أسماه "شارلز أوسقود" "التخفيض التدريجي للتوتر والعنف".⁶³

2) تحقيق الاحتياجات الإنسانية:

يقترح "جون بيرتون" (John burton) حل لمثل مشاكل من قبيل الإجرام والعنف بحيث يقر بأن هؤلاء الذين يقومون بمثل هذه الأعمال لهم احتياجات مشروعة يجب الوفاء بها من أجل التوصل إلى حل، فحسبه إدارة قضية الإرهاب السيبراني على أساس سن قوانين ردعية، إلقاء القبض عليهم وسجنهم وما إلى ذلك لا تنجح إلا بحصول هؤلاء على شيء ملموس يشبع حاجاتهم الأساسية وتمكينهم أمنيا.

لأن حل مثل هذه القضية يكون عن طريق إزالة مصادرها، فإذا كانت الظروف الاجتماعية هي المشكلة فإن حلها والوقاية منها ممكنا، بتحقيق المعايير الاجتماعية وفقا

⁶² صافية زيد المال، "حماية البيئة في إطار التنمية المستدامة على ضوء أحكام القانون الدولي" (رسالة دكتوراه العلوم في

القانون الدولي، قسم الحقوق، جامعة تيزي وزو، 2012)، ص. 433.

⁶³ محمد السيد سليم، تحليل السياسة الخارجية (القاهرة: مكتبة النهضة المصرية، 1998)، ص. 327.

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

لاحتياجات هؤلاء الإرهابيين والمتمثلة في الغذاء، المأوى، الأمن، الهوية، الاعتراف والمشاركة التي هي أساس التنمية والأمن الفردي في المجتمع. ففي مثل هذه الحالة المدروسة-الإرهاب السيبراني- فإن المؤسسات والقواعد في الدول النامية على الخصوص من يحبط احتياجات الأفراد لذا يسعون إلى الهجوم والعنف والتخريب كسبيل لتحقيق ذلك، لذلك جاء "بيرتون" بالاستباقية "Prevention" والتي تعني بدلا من علاج الأمراض التي تصاحب الإرهاب السيبراني ينبغي معالجة أسبابها من خلال الاهتمام بتحقيق حاجات هؤلاء المهاجمين، بتحليل عميق للظاهرة بكل أبعادها لمعرفة الحاجات التي تستوجب الاستيفاء واكتشاف الخيارات لتحقيقها كوسيلة ليس فقط لحل مسألة بل التنبؤ بها وإزالة مصادرها.

(3) المكفآت المالية التشجيعية: وهي من الحوافز الايجابية التي تعكس تقديم مزايا مختلفة لهؤلاء الإرهابيين أو الذين يبلغون عنهم، ومنحهم قيمة ملموسة/مادية إذا ما نفذوا المطلوب منهم كالتراجع عن استعمال الفضاء السيبراني لتنفيذ الأعمال الإرهابية والهجومية على الأفراد أو الدول أو المنظمات والكشف عن هويتهم الحقيقية وتسليم أنفسهم، أو التبليغ من طرف أشخاص يعرفون من هؤلاء الإرهابيين الذين ينفذون هجمات سيبرانية.

ولن يتم الردع أو التحفيز إلا بالتعاون العالمي ويكون عن طريق التبادلية التي تكون بين "دولة-دولة"، وبين "الدولة-المواطن"، وبين "المواطن-المجتمع المدني" وبين "الدولة-القطاع الخاص"، فالاعتماد المتبادل والذي يعتبر أحد صور التشابكية وهو يعني وجود قنوات وأشخاص ومؤسسات تتفاعل عبر الحدود الدولية، وهو أحد المفاهيم التي أولتها المدرسة الليبرالية عناية خاصة، حيث تعتبر هذه المدرسة المنظمات الإقليمية آلية مهمة للتنسيق، وهي إحدى أهم قنوات المجتمع الدولي المترابط. كما يعني الاعتماد المتبادل المعقد على أن هناك قضايا متعددة التي تشكل جدول الأعمال الدولي، بحيث يوجد هناك نوع من الترابط بين تلك القضايا، ويجب أن يتوفر النزوع

الردعي لدى الدول بدعم طابع الردع واستحداث طابع التحفيز.⁶⁴ لأن العلاقات والروابط والمصالح المشتركة والمتبادلة بين الدول تتداخل إلى حد بعيد، ما يتم عليها في أحيان كثيرة اتخاذ توجهات وسياسات تشاركية، الأمر الذي يجعل من تلك التبادلات والاعتمادات ذات طبيعة متداخلة إلى درجة لا يمكن من خلالها أن تتخذ بشكل فردي حتى وإن كانت قرارات وطنية أو ذات سيادة، أو دون الأخذ بالاعتبار لانعكاسات وتأثير بعض التوجهات والسياسات على مصالحها المشتركة أو حتى مراعاة لمصالح الآخرين في المجتمع الإقليمي، كما أن للكثير من الاتفاقيات والمعاهدات الأمنية والسياسية والعسكرية الوطنية والإقليمية⁶⁵ والدولية والعالمية دور كبير وبارز في التصدي لمثل هذه الجرائم.

الخاتمة:

من خلال ما سبق، يمكن أن نصل إلى نتيجة مفادها أن الإرهاب السيبراني صار يعرقل الأمن بكل أنواعه وأبعاده ومسوياته، ويعسر على نحو يومي على تحقيقه، والسبب في ذلك تأثير العولمة التكنولوجية على المجتمعات الحديثة وما أحدثته من تحولات في مفهوم القوة وفي مفهوم التهديد، وحتى في مفهوم الصراع، والتحكم في مفاتيح المعرفة ومنها الثورة الرقمية.

حيث باستطاعة هذا الإرهاب التحكم في الأشخاص والدول، وحتى في العالم برمته، بفضل الفضاء السيبراني الذي أصبح مكان لانتشار العنف والجريمة، وانتهاكات حقوق الإنسان، وبالتالي كما هي المجتمعات اليوم مرتبطة ارتباطا وثيقا بتكنولوجيات المعلومات والاتصال، يجب أن ترتبط أكثر في تكثيف الجهود الردعية واستحداث منظومات تحفيزية لمكافحة الإرهاب السيبراني كظاهرة "عبر دولية" وتهديداتها الخطيرة على الأمن بشكله الموسع.

⁶⁴ جهاد عودة، مقدمة في العلاقات الدولية المتقدمة (القاهرة- مصر: المكتب العربي للمعارف، 2012)، ص ص.172،

173.

⁶⁵ محمد بن سعيد الفطيسي، "مبدأ التبادلية في العلاقات الدولية وتأثيره على مستقبل السياسات الأمنية والشؤون العسكرية"، مجلة جيل الدراسات السياسية والعلاقات الدولية، ع.18 (ماي 2018)، ص.18.

فاطمة حموته: خطر الإرهاب السيبراني: تأثير ديناميكية التهديدات المترابطة لظاهرة "عبر دولية" على الأمن الموسع

قائمة المراجع

- أحمد دلال وآخرون، الثورات العربية: عسر التحول الديمقراطي ومآلاته، ط.1. (بيروت: المركز العربي للأبحاث ودراسة السياسات).
- إيزابيل روبنسون وإيلين نول، "النزاع السيبراني والقانون الدولي الإنساني"، المجلة الدولية للصليب الأحمر، مجلد 94 (صيف 2012)،
- جهاد عودة، مقدمة في العلاقات الدولية المتقدمة (القاهرة- مصر: المكتب العربي للمعارف، 2012)،
- جوزيف ناي، "حدود القوة الأمريكية"، ترجمة: علي حسين باكير، في، علم السياسة والعلاقات الدولية: قراءات عالمية، مجلد 1: العدد 3 (شتاء 2005)
- رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات"، المركز العربي لأبحاث الفضاء الإلكتروني،
- سرور جرمان سرور المطيري، تغيير مفهوم الأمن القومي الكويتي ودلالاته في الفترة 1990-2013 (القاهرة- مصر: المكتب العربي للمعارف،
- سليمان عبد الله الحربي، "مفهوم الأمن: مستوياته وصيغته وتهديداته (دراسة نظرية في المفاهيم والأطر)"، المجلة العربية للعلوم السياسية، بيروت-لبنان: مركز دراسات الوحدة العربية، ع.14 (2008)
- صافية زيد المال، "حماية البيئة في إطار التنمية المستدامة على ضوء أحكام القانون الدولي" (رسالة دكتوراه العلوم في القانون الدولي، قسم الحقوق، جامعة تيزي وزو، 2012)،
- عادل عبد الصادق، "أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني"، عبد النور بن عنتر، البعد المتوسطي للأمن الجزائري الجزائر، أوروبا والحلف الأطلسي (الجزائر: المكتبة العصرية للطباعة، النشر والتوزيع، 2005)،
- عبد النور بن عنتر، البعد المتوسطي للأمن الجزائري: الجزائر، أوروبا والحلف الأطلسي (الروية-الجزائر: المكتبة العصرية للطباعة، النشر والتوزيع، 2005)
- علي عباس مراد، الأمن والأمن القومي: مقاربات نظرية، ط.1 (الجزائر: ابن النديم للنشر والتوزيع، بيروت-لبنان: دار الروافد الثقافية- ناشرون،

- قاسم المقداد، دراسة في العلاقات الدولية: النظريات السياسية، الجزء الأول سورية- دمشق: دار نينوى للدراسات والنشر والتوزيع،
- مايا خاطر، "الجريمة المنظمة العابرة للحدود الوطنية وسبل مكافحتها"، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مجلد 27، ع.3(2011)،
- محمد السيد سليم، تحليل السياسة الخارجية (القاهرة: مكتبة النهضة المصرية، 1998)
- محمد توفيق البحيري، مترجما، القوة الناعمة وسيلة النجاح في السياسة الدولية، ط.1 (الإمارات العربية المتحدة: مكتبة العبيكان، 2007)،
- محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية (دار ناشري للنشر الالكتروني، جانفي 2012)
- مركز سميت للدراسات، "الإرهاب السيبراني..الوجه التكنولوجي للتطرف"،
- نورة شلوش، "القرصنة الالكترونية في الفضاء السيبراني 'التهديد المتصاعد لأمن الدول' "مجلة مركز بابل للدراسات الإنساني، المجلد 8، ع.2
- هايل عبد المولى طشطوش، الأمن الوطني وعناصر قوة الدولة في ظل النظام العالمي الجديد (الأردن: دار المنهل، 2012)،
- هبة رءوف عزت، القوة الناعمة المهذرة: أزمة النظام القوي والدولة الضعيفة بمصر، مركز دراسات الجزيرة، 2012

Robin E Walker and Annette Seegers, "Securitisation: The case of post-9/11 United States Africa policy", *Scientia Militaria, South African Journal of Military Studies*, Vol.40, Nr. 2(2012)

http://accronline.com/article_detail.aspx?id=28706

http://accronline.com/article_detail.aspx?id=28924

<http://smtcenter.net/archives/slider>