الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية
"التحديات والافاق المستقبلية"

Algerian strategy in the face of cybercrime
"Challenges and future prospects"

الدكتور/جمال بوازدية
جامعة الجزائر 3، الجزائر
bouazdia.djamel@gmail.com

تاريخ الاستلام: 2018/11/26 تاريخ القبول للنشر: 2019/02/13

❖❖❖❖❖❖❖

ملخّص:

بالعودة إلى رأي الخبراء والمختصين، فإن التحولات الكبرى التي واكبت نهاية الحرب الباردة خاصة في المجال التكنولوجي أرست قاعدة جديدة للحياة اسمها(الفضاء السيبراني) بحيث أصبح في متناول الشعوب والأمم، التواصل والتخاطب مباشرة في عالم بلا حدود في جو من الأمن والأمان، لكن الاستخدام المفرط لتكنولوجيا الاتصالات وأمام التدفق السريع والمذهل للمعلومات(ثورة المعلومات)، بدأ توظيف هذا الفضاء في بعض المستويات (الدول وكبريات الشركات) لخدمة مصلحة ما، مما سمح لطرف ثالث (القراصنة) لدخول المنافسة باختراقه هذا الفضاء وتحويله إلى مسرح للجريمة السيبرانية بطريقة لا تخضع إلى حدود شرعية.

أمام هذه التحديات الخطيرة أصبح من الصعب جدا على الدول توفير الحماية لأنظمتها المعلوماتية خاصة وإن عملية الاستعمال المتزايد والمفرط لتكنولوجيات الاتصال والاعلام، فاقت كل التقديرات، فهذا العالم الغريب والمتجدد، جعل من القابلية للعطب إحدى الهواجس التي تعاني منها الدولة، التي وجدت نفسها في حالة حرب دائمة مع فواعل ممن يمتلكون المهارة والوسيلة المعلوماتية ولهم القدرة على توظيفها لاختراق كل الأنظمة الحساسة مهما كانت القدرات والاحتياطات الأمنية المتوفرة.

فالجرائم المستحدثة في الفضاء السيبراني من شأنها المساس بالأمن القومي إن لم تفعل اليقظة المعلوماتية وذلك عن طريق المراقبة المستمرة لهذا الميدان، حتى يتم الاستباق في وضع الآليات الكفيلة للتأقلم مع التحديات التي تفرزها التطورات التكنولوجية.

في هذا الإطار، توجهت الجزائر إلى طرح تصورات ورسم سياسة أمنية مزدوجة (الأمن السيبراني) للتحكم في انظمة المراقبة لحماية المنظومة المعلوماتية للمؤسسات والمواطنين من جهة، ومواجهة الأخطار

من جهة ثانية، ولتدارك النقائص تجتهد الجزائر في الجبهة الخارجية من خلال التعاون المتعدد التخصصات، للاستفادة من تجارب غيرها من الدول.

الكلمات المفتاحية: القراصنة؛ البرمجيات الخبيثة؛ ثورة المعلومات؛ الحروب الالكترونية.

Abstract:

According to specialists and experts in international relations, the major changes that followed the end of the Cold War, especially in the field of technology, established a new platform of life called (cyber space), in which people and nations are able to communicate and address each other directly in a borderless world within a secure and safe environment. However, the excessive use of communication technology and the rapid and astounding flow of information (the informational revolution) lead to the employment of this space at some levels (states and major corporations) to serve a certain interest, which allows a third party (pirates) to enter the competition by breaking into this space and transforming it into a cyber-crime scene in a way that is not subject to legal boundaries.

In the face of these dangerous challenges, it has become very difficult for countries to protect their information system, especially since the increased and excessive use of communication and information technologies surpassed all estimates. This strange and renewed world has made from "fragility" one of the obsessions that the country suffers from, as the country is constantly engaged in wars with different actors who have skills and informational tools and are able to use these tools to penetrate the country's sensitive systems regardless of the security capacities and precautions provided.

Crimes taking place in cyber-space could affect the national security, if the country's informational alertness did not ensure a continuous monitoring of this space. This alertness would enable the anticipation of the creation of mechanisms that adapt to the challenges posed by technological development.

In this context, Algeria proposes, through the national security policies, different views and strategies (cyber-security) to manage the control system in order to protect the informational system for institutions and citizens on the one hand, and face various dangers on the other hand. In order to address any shortcomings, Algeria strives, on the foreign front, to benefit from the experience of other states through interdisciplinary collaboration.

Keys words: *Pirates, malicious software, the informational revolution, cyber wars.*

مقـدّمـة:

تندرج هذه الدراسة في إطار إثراء البحث العلمي الذي تجتهد مختلف الجامعات الجزائرية من أجل تطويره وذلك من خلال تنظيم ورعاية الملتقيات، اللقاءات الأكاديمية والأيام الدراسية، وهذا بدوره سيسمح للطلبة الباحثين التواصل مع الأساتذة والخبراء لمناقشة المواضيع المتصلة بالتخصصات المطروحة للتقويم، من أجل توحيد الرؤى عبر مقاربات علمية لواقع الحال ومتطلبات بناء وارساء قواعد تسمح بمواكبة التحديات التي أفرزتها العولمة .لأن التحولات التي واكبت نهاية الحرب الباردة طرحت في الحقل المعرفي العديد من المفاهيم (نهاية التاريخ)،

صراع الحضارات، نهاية الايديولوجيات، الأمن المجتمعي والجماعي، الفضاء السيبراني)، مما استدعى تطورا في العلوم للتوافق مع هذا الطرح، لكن النقاشات الطويلة والعريضة بين المنظرين لتطوير هذه المفاهيم لبناء نظام عالمي جديد ومواكبة التحولات، انتهت في الاخير إلى جدل فكري مازال معلقا إلى اليوم، مما أحال دون تحديد مفهوم للعديد من المصطلحات التي لها علاقة مباشرة بالأمن (الارهاب، الجريمة السيبرانية) وأمام هذا الفراغ، تحولت العديد من مناحي الحياة إلى مسرح لكل الفواعل الاجرامية.

فالتطور التكنولوجي وإن أرسى قواعد جديدة (الفضاء السيبراني)[1] استطاعت من خلالها الدول، الهيئات والشعوب والأمم للتواصل والتخاطب مباشرة وفي جميع الميادين، إلا أن هذه القيمة المضافة خلفت في مستويات معينة من التوظيف بعض التجاوزات حولت هذا الفضاء إلى مخبر للجرائم السيبرانية التي حالت دون حماية حقوق المؤسسات والافراد للاستفادة من هذا الفضاء بكل حرية وفي إطار قانوني، فالاستخدام المفرط لتكنولوجيا الاتصالات والتدفق السريع والمذهل للمعلومات(ثورة المعلومات)، ضاعف من نسبة الاختراقات ووسائل التجسس، لتمس في بداية الامر أمن الاشخاص مما جعل حياة البشر وخصوصياتهم ملاذ للابتزاز بشكل لا يصدق، وكثرت عمليات المساومة، فلم يعد يسلم فرد من هذه العمليات القذرة، سواء كان مسئولا أو مواطنا ثم انتقلت الاختراقات بهدف التجسس والتخريب لتنال من الأجهزة الأمنية ووزارات الدفاع والمؤسسات الحكومية والشركات والبنوك في أكبر دول العالم.

أمام هذا الخطر الذي أصبح لا يعرف حدود وتنوع في تطبيقاته (جرائم الالكترونية، ارهابي إلكتروني وحروب إلكترونية)، توجه صناع القرار على المستوى الدولي إلى إطلاق صفرات الأنذار لإعادة بناء حواجز وجدران تقنية لمنع هذه الهجمات (الأمن السيبراني) خاصة وأن عمليات الابتزاز قد بلغت مستويات من شأنها المساس بالأمن الوطني، القومي والعالمي.

وفي هذه النقطة تحديدا، تتفق العديد من الدوائر العلمية، أن الجرائم السيبرانية ألغت عنصر الزمان والمكان وأفقدت الدول إمكانية التحالف لمواجهتها، فالدقة المتناهية في تنفيذ الاختراقات جعلت الأنتصار شبه محقق حتى على المؤسسات العسكرية.

بالعودة إلى الجزائر نجد أن موقعها الجغرافي جعل منها فضاء مفتوح مغاربيا، متوسطيا وأفريقيا لتلاقي وتقاطع التهديدات اللاتماثلية التي تركت أثارها على مسألة الأمن الوطني وإذا أضفنا إلى ذلك المخاطر السيبرانية، فإن الجزائر كغيرها من الدول أصبحت إحدى ضحايا هذه التحديات وأصبحت في حاجة إلى

تصميم وتطوير استراتيجية أمنية متعددة التخصصات (الجوانب التشريعية، التنظيمية، البشرية، المالية، التقنية، والمعلوماتية) حتى يتسنى لها تأمين الثورة الرقمية للأفراد والمؤسسات وبالتالي التصدي لخطر تشتكي منه اليوم الدول الكبرى[2] وعلى رأسها الولايات المتحدة الامريكية التي يعود لها الفضل في إنشاء أول شبكة للأنترنت سنة 1969[3].

بناء على ما تقدم في هذا الطرح، سوف نعالج الاشكالية من خلال السؤال المركزي " هل وفقت المقاربة الجزائرية في توفير الحماية للأنظمة المعلوماتية ومواجهة الجرائم المستحدثة"، أما الاجابة فسوف تنطلق من الاسئلة الفرعية:

- هل تم الاتفاق على تعريف الجريمة السيبرانية؟
- هل تم الاتفاق دوليا على تشريع لمكافحة الجريمة السيبرانية؟
- أين يقع الاشكال في عدم التحكم في هذه الجريمة؟
- ما هو موقف الجزائر من هذا الفضاء؟

المحاور الرئيسية للبحث:

المحور الأول: الإطار المفاهيمي للدراسة.

المحور الثاني: استراتيجية الجزائرية في مكافحة الجريمة السيبرانية.

المحور الأول

الإطار المفاهيمي للدراسة

التطور العلمي والمعرفي كثيرا ما يطرح إشكالية تحديد المصطلحات بالنسبة لأهل الاختصاص من المفكرون والباحثون الذين يتلقون صعوبات في الاتفاق على تعريفات دقيقة، واضحة، شاملة وموحدة تسهل في المرحلة القادمة وضع الإطار المنهجي لتفسير بعض الظواهر وتفعيل الحلول الملائمة، ويعتبر حقل العلاقات الدولية من بين التخصصات التي تعرف جدال كبير بين رجالات البحث العلمي لتحديد أكثر المصطلحات تداولا" الأمن"، وسوف نتعرض لهذا التحدي من خلال هذه الدراسة.

1- تعريف الفضاء السيبراني:

تتفق جميع الدراسات العلمية على أن هذا الفضاء[4] هو بيئة افتراضية تعتمد في بنيتها على التكنولوجية الحديثة في التعامل والتواصل بين العديد من الفواعل سواء كانوا أشخاص أو هيئات حكومية وغير حكومية من خلال شبكة إلكترونية (الحاسوب) لها استقلاليتها عن وسائل الاتصال، بمعنى أخر أن كل المعلومات والمعاملات المتداولة بقدر ما تسهل عملية الأندماج بين كل أجهزة الاتصالات والأقمار الصناعية، والفضاء الإلكتروني، بقدر ما تفتح المجال لعمليات الاختراق[5].

ومن بين العلماء الذي يعتبره الباحثون بمثابة الاب الروحي والمؤسس لهذا الفضاء، عالم الرياضيات الأمريكي الاستاذ (Norbert Wiener's) الذي استطاع وضع تعريف دقيق لهذا الفضاء،" علم التحكم والتواصل عند الحيوان والآلة، لنقل الرسائل بين الأنسان والآلة، أو بين الآلة والآلة كما يعتبره علم القيادة أو التحكم في كل منهما[6]".

بعد الحرب العالمية الثانية، أحدث التطور التكنولوجي خاصة مع ظهور الأنترنت، مجموعة من المفاهيم التي أصبحت تعبر على هذا الفضاء، الفضاء الرقمي، الدفاع الالكتروني، الهجوم الالكتروني، الجريمة الالكترونية، وحل الكمبيوتر محل الالة التي تكلم عليها نوربير وينر.

كما عبر عن هذه الوضعية بصورة دقيقة كل من الاستاذ ألأن فريدمان، الباحث في معهد الأمن السيبراني (الولايات المتحدة الامريكية) وبيتر سيبنجر المتخصص في السياسة الخارجية في مركز بروكينجز، بالقول أن هذا الفضاء الجديد بقدر ما يطرح من المرونة والسهولة في التواصل بين المجتمعات في جميع أنحاء العالم وفي جميع المجالات، بقدر ما يخلق صعوبات من الناحية الأمنية لمواجهة الخروقات[7].

2- تعريف الأمن السيبراني:

ما تضمنه الفضاء السيبراني من عمليات الدخول والخروج، لمختلف مواقع تداول وتخزين المعلومات والبيانات، يستوجب بالضرورة خلق قواعد وأليات تثبيت أصول الأمن لحماية هذه المواقع وأنظمتها المعلوماتية، لذا يتبادر لأذهان كل ممتهن أو مستخدم لهذا الفضاء طرح السؤال التالي: ما هو الأمن السيبراني؟

مختلف الإجابات الواردة من الدوائر الفكرية أو الرسمية، لم تنجح في وضع تعريف دقيق لهذا المصطلح، ومازالت هذه الاشكالية مطروحة بحدة لحد الأن، وهذا بدوره طرح إشكالا آخر يتمثل في عدم نجاعة اليات مواجهة الجرائم السيبرانية وعدم فعالية التعاون الخارجي بالتالي ضمان الأمن.

من خلال التعاريف التي سأذكرها على سبيل المثال، سيتضح للقارئ أن هناك اختلافا في الطرح، بين من يعتمد على الخبرة التقنية والميدانية لتفسير الظاهرة (الباحثون) ، وبين من يركز على الجوانب التنظيمية والقانونية (الدوائر الحكومية.)

بالنسبة للاكاديميين، يعرف كل من Martti Lehto,Pekka Neittaanmäki الأمن السيبراني" على أنه مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها ويتضمن تنفيذ التدابير المضادة المطلوبة"[8]، أما أستاذ الاتصالات في جامعة كاليفورنيا ريتشارد كمرر Richard A.Kemmerer، فيعتبر الأمن السيبراني "مجموعة وسائل دفاعية من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة"، وقد أيده في الطرح واحد من أهم المختصين في الميدان ؛ الأستاذ إدوارد أموروزو Edward Amoroso، الذي عرفه" بأنه تلك الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة. إلخ."

بالنسبة للدوائر الحكومية، ركزنا على إحدى أهم الفواعل في المجال (الدولة) ونخص بالذكر الولايات المتحدة الأمريكية المستهدف رقم 1 من طرف المجرمين، فمن جهة تعرف وزارة الدفاع الامريكية الأمن السيبراني على"أنه مجموعة الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها(الإلكترونية والمادية)، من مختلف الجرائم، الهجمات، التخريب، التجسس والحوادث. أما وكالة الأمن الرقمي الاوروبية (أول من أصدرت تشريع في هذا المجال) فعرفته بأنه" قدرة النظام المعلوماتي على

مقاومة محاولات الاختراق أو الحوادث غير المتوقعة، التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي (أول اتفاقية في الموضوع صدرت في بودابست 2001).

في الاخير نذكر التعريف الذي جاء به الاتحاد الدولي للاتصالات الصادر في تقريره حول" اتجاهات الاصلاح في الاتصالات للعام 2010-2011"، والذي يعتبر بمثابة أرضية إجماع لمختلف التوجهات الفكرية والمهنية "هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات امنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين".

من هذا المنطلق، يمكننا إعطاء تعريف شامل بالقول" أن الأمن السيبراني أو الالكتروني هو مجمل القوانين، الأدوات، النصوص، المفاهيم والميكانيزمات الأمنية وطرق تسيير الأخطار والممارسات التقنية المتعلقة بتكنولوجيات المعلومات والاتصالات المستخدمة لحماية مصالح الدول والأشخاص .ليبقى الهدف في الاخير، هو قدرة هذه الادوات على مقاومة التهديدات المتعمدة من طرف قراصنة المعلومات أو غير المعتمدة من طرف المستخدمين (الخطأ البشري) للتعافي، وبالتالي التحرر من الأضرار الناجمة عن تعطيل أو سوء استخدام تكنولوجيا المعلومات والاتصالات.

للإشارة، فإن القراصنة سواء كانوا الهاكرز (الفضوليين أومن لهم هواية التعمق المعلوماتي)أو الكراكرز (المحترفين الأكثر خطورة في ارتكاب الجريمة الالكترونية) أو الطائفة الناقمة (التي تستهدف المنشآت للانتقام أو المنفعة)، وفي كلتا الحالتين تتميز هذه الفصيلة من المجرمين عن غيرهم، بما يكتسبونه من مهارات عالية في استخدام التكنولوجيا ومستويات علمية مذهلة مما يسمح لهم التعامل بكل سهولة مع كل شبكات التواصل الالكترونية والوصول إلى المعلومات السرية لتحقيق الأهداف المسطرة، وتتراوح أعمالهم بين:

أ- الحرمان من الخدمة :

ويتمثل في تخريب أو تعطيل الوسائط المستخدمة في تداول المعلومات سواء على مستوى المؤسسات العمومية أو على الحسابات الخاصة للأفراد.

ب- الجريمة:

وذلك من خلال الوصول إلى الأرقام السرية لبطاقات الائتمان الشخصية للحصول على الأموال من الحسابات البنكية أو اختراق البريد الإلكتروني للأشخاص، كبار الشخصيات السياسية للاطلاع على معلوماتهم وبياناتهم ثم القيام بإفشائها من أجل الابتزاز[9].

ج- التجسس:

وهي عمليات الاختراق الإلكتروني التي تتم عن طريق استعمال التقنيات العالية من طرف أجهزة الاستخبارات الأجنبية للوصول إلى المعلومات السرية المخزنة في المواقع الحيوية والاستراتيجية للدولة على شاكلة تسريبات ويكي ليكس، هذا الاختراق من اكثر الاعمال تأثيرا على العلاقات الديبلوماسية بين الدول.

د- الهجمات الاستراتيجية:

وتعتبر من أخطر الجرائم السيبرانية التي تلجأ إليها الجماعات المسلحة للمساس بالأمن الوطني للدول، لأنه يستهدف على الخصوص إلحاق الضرر بأنظمة الاتصالات، أو قطع شبكات الاتصال بين الوحدات القتالية والقيادات المركزية، كما تستهدف أنظمة التحكم الدفاع الجوي وقواعد إطلاق الصواريخ، ومن أخطر الهجمات التي تم حصرها، تفجير منشآت اقتصادية، نشر فيروسات لتدمير شبكات المعلومات والتجسس على الحسابات الخاصة للرؤساء لمعرفة مراسلاتهم ومخاطباتهم والاستفادة منها في عملياتهم الإرهابية[10].

3- الجرائم الالكترونية:

في عالم اليوم، أصبحت هذه الجريمة من الجرائم المستحدثة التي واكبت تطور التكنولوجيا، وبالنظر إلى الوسائل الهادئة المستعملة، فقد عجز الفاعلون في هذا الشأن، سواء التقنيون، الفقهاء أو المشرعون في إيجاد تعريف موحد، فمن الناحية التقنية، توجد عدة تسميات (جرائم الحاسوب، جرائم الأنترنيت، جرائم التقنية العالية، جرائم الياقات البيضاء وجرائم الجيل الخامس) أما من الناحية القانونية، فقد ركز المشرعون على تعريف نظام المعلومات لتعدد وظائفه في حين أوكلت مهمة تعريف نظام المعالجة الالية إلى القضاء لتكييف الاختراق وفق الاعمال المجرمة قانونيا.

- **التعريف التقني:** الجريمة المعلوماتية هي العمل الضار الذي يفترض فيه المعرفة الجيدة للتكنولوجيا من طرف الفاعل وتوظيف تقنيات الحاسوب، للوصول إلى البيانات والبرامج بهدف النسخ، الحذف، التزوير، التخريب، الحيازة أو التوزيع بصورة غير شرعية[11].

- **التعريف القانوني:** الجريمة الالكترونية هي ذلك العمل غير الشرعي المقترف بهدف الاستيلاء على ممتلكات الغير أو تخريب الأنظمة، بمعنى أخر، هي تلك الاعمال المعاقب عليها قانونيا والتي ترتبط بالعمل الإجرامي وتكنولوجيا الاتصالات[12].

ولتنفيذ خططها تستعمل هذه الجريمة الهادئة سلاح الفيروسات وذلك بالدخول الغير شرعي ونسخ برامج خبيثة في أجهزة المستخدمين من غير معرفتهم لتحدث بذلك خلل بغية تدمير البيانات أو الحصول عليها أو استبدالها بملفات خاصة به من الجهاز المستهدف، مما يتسبب بعدم قدرته على الإقلاع[13] ، كما تهدف الهجمة الإلكترونية إلى تعطيل الخوادم والأجهزة التابعة للمنشآت، وحذف محتويات الأقراص الصلبة.

ومن بين الفيروسات الأكثر خطورة، يمكن ذكر ما يلي:

- حصان طروادة[14] Cheval de 3، الدودة الإلكترونية، القنابل المنطقية، حسب المختصين في الاعلام الالي والأمن السيبراني، فإن القاسم المشترك بين هذه الفيروسات، يبقى الاضرار بالبرامج والبيانات، للقيام بمهام غي مشروعة" كالاحتيال أو الغش في النظام"، بالإضافة، فإنها تمثل حرب قائمة بذاتها بسبب استغلال الفاحش للإعلام الالي والأنترنت، الذي وفر المجال الحيوي لشن هجمات منظمة عبر العالم .كما

توجد فيروسات سرية (برامج التجسس)، تستخدم لنقل المعلومات الشخصية (برنامج تسجيل نقرات لوحة المفاتيح، برنامج الإعلأنات، الصفحات الأنبثاقية)[15].

في هذا الإطار، يحصي المختصون في الأمن الرقمي أكثر من 300 ألف عينة لفيروسات وبرامج ضارة في اليوم، ما يشكل تهديدا مستمرا للكائن البشري خاصة وأن عمليات الاختراق تهدف إلى الحصول على بيانات شخصية (بطاقة معلومات خاصة) بالإضافة إلى بطاقات الائتمان والصحة للاستهلاك.

ومهما تعددت أسباب الجريمة الإلكترونية، فإن عدم فعالية النصوص القانونية في مواجهتها، دفع بالمحترفين للبحث عن المزيد من الفرص لجعل هذا النشاط وسيلة اكتشاف خبايا المجتمع الرقمي (البنية المعلوماتية الكونية)، لتحويله إلى وسيلة ثراء على حساب الأمن والسلام العالميين. فإن كانت الدوافع المالية هي الغالبة حاليا، حسب ما أكده تقرير قسم الجرائم الحاسوبية وقضايا الملكية الفكرية الأمريكي، 89 % من الهجمات الالكترونية تتضمن دوافع مالية لمجموع الفاعلين في الاقتصاد الفعلي)، إلى جانب الدوافع الشخصية[16] والدوافع السياسية (هجمات التجسس التي تنفذها أجهزة الاستعلامات الرسمية أو الوكالات المأجورة)[17]، فإن المرحلة القادمة سوف تشهد حرب سيبرانية.

- **علاقة الجريمة الالكترونية بالعمليات العسكرية في الفضاء السيبراني:** من خلال دراسة وتحليل للتقارير التقنية الصادرة عن الشركات المتخصصة في مجال الإعلام الآلي وبالعودة إلى الإحصائيات المتضمنة الجرائم الواقعة، تبين أن هذا السلاح أصبح يمثل البديل عن التهديدات اللاتماثلية (الإرهاب، الجريمة المنظمة والسلاح النووي)، لأنه لا يحتاج إلى حدود جغرافية ولا توجد وسائل مراقبة لتحديد هويته في الشبكة العنكبوتية على غرار الحروب التقليدية من جهة، كما وفرت ثغرات عدم حماية البيانات والأنظمة المعلوماتية، الاطار المناسب للاختراق ق والتلاعب بالبيانات والمعلومات المتواجدة عليها.

هذه الوضعية إن استمرت سوف تتغذى بمنطق الأبعاد العنيفة (جمع المعلومات الاستخباراتية، برمجة عمليات تستهدف المعنويات" الحرب النفسية"، التخطيط لعمليات هجومية[18]، نظرا للفوضى التي أصبحت تميز النظام الدولي وعدم السيطرة على توزيع القوة بين الفاعلين من دون الدول[19].

4- الإرهاب الالكتروني:

بقدر ما فسحت العولمة الحديثة مجال للتكنولوجيا للتطور وإضفاء حوكمة في جميع المجالات من أجل تقريب وتسهيل المعاملات بين الدول والشعوب، بقدر ما أعطت فرص للجماعات الإرهابية ليتفاعل وينصهر مع هذا العالم الافتراضي من خلال استخدام شبكات المعلومات والأنترنت والكمبيوتر وتوظيف التقنيات الحديثة في مجالات الاتصال والمعلوماتية من أجل الاطلاع على مختلف المعلومات الأساسية للدولة خاصة الأمنية منها واختراق المواقع الالكترونية للمؤسسات والمسؤولين [20]،بالإضافة إلى فتح العديد من المواقع وتأجير مواقع أخرى لنشر ثقافة التطرف الديني في أوساط الشباب وطمس الهوية وتجنيدهم في صفوف المنظمات الجهادية من أجل التخويف والإرغام والبدا في تحقيق أهداف سياسية من خلال شن هجمات على مختلف القطاعات السياسية، الاقتصادية، العسكرية، مما أحدث شرخا كبيرا في النسيج المجتمعي وخلق نوع من عدم الاستقرار الأمني الدولاتي[21].

ازدياد خطر الإرهاب الالكتروني في ظل التهديدات الأمنية الحالية، عجلت صناع القرار والمنظمات الحكومية والغير حكومية على مستوى المجتمع الدولي على اتخاذ كافة الإجراءات والاستراتيجيات لمواجهة الظاهرة، كما دفعت بالاكاديميين لدخول مسرح التنظير من أجل وضع تعريف لمصطلح ما زال غير محدد في شكله التقليدي، مما صعب من مهمة تحديد الاليات الفعالة، ومن بين التعاريف القابلة للتوافق، نذكر ما يلي:

- باري كولين Barry Collin رجل القانون الامريكي، الذي عرفه" بأنه هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب"، رغم هذه المحاولة، إلا أنه يعترف بصعوبة تعريف شامل للإرهاب التكنولوجي نظرا لتعدد زواياه واختلاط مجالاته.

- جيمس لويس James Lewiss، خبير في مركز الدراسات الاستراتيجية والدولية بالولايات المتحدة الامريكية يعرفه "أنه استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البني التحتية الوطنية المهمة مثل الطاقة والنقل، أو بهدف ترهيب الحكومة والمدنيين."

- دورثي دينينغ Dorothy Denningg ترى "أن الإرهاب الالكتروني هو الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية، وينبغي أن يكون الهجوم مدمراً وتخريبياً لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب"[22].

هذا وقد أكد الأستاذ في جامعة هارفارد ومساعد وزير الدفاع سابقا (الولايات المتحدة الامريكية) جوزيف س .ناي، الابن، في إحدى مقالته عن أهمية مواجهة هذا الخطر بالقول" هناك أربع فئات رئيسية للتهديدات السيبرانية للأمن الوطني، وكل منها تحتل فترة زمنية مختلفة وتتطلب من حيث المبدأ حلولاً مختلفة، فالحرب السيبرانية والتجسس الاقتصادي، ويرتبطان إلى حد كبير بالدول، أما فئة الجريمة السيبرانية والإرهاب السيبراني، فهما يرتبطان في أغلب الحالات بجهات فاعلة غير تابعة لدولة. من أجل التجسس والجرائم، ولهذا فإن الفئتين الأخريين ربما تصبحان أعظم تهديدٍعلى مدى العقد المقبل مقارنة بحالهما اليوم .وعلاوة على ذلك، فإن تطور التحالفات والتكتيكات، سوف يساعد على تداخل الفئات بشكل متزايد[23].

فالمتفحص للمواقع الالكترونية الإرهابية، سوف يلاحظ مدى أهمية هذا المجال وقدرته لتحقيق الأهداف الاجرامية على حساب السلم والأمن العالميين[24]، فتنظيم القاعدة وظف العديد من المواقع سواء لشن الهجمات أو لإعطاء توجيهات أو تبادل رسائل، ومن بينها، موقع النداء : أرضية رسمية تم استخدامها بعد أحداث الحادي عشر من سبتمبر 2001 لإصدار البيانات الإعلامية، ذروة السنام : وهي صحيفة إلكترونية دورية للقسم الإعلامي لتنظيم القاعدة، صوت الجهاد : وهي مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب، وتتضمن مجموعة البيانات والحوارات مع قادة التنظيم ومنظريه، موقع البتار: وهي مجلة عسكرية إليكترونية متخصصة، تصدر عن تنظيم القاعدة، وتختص بالمعلومات

العسكرية والميدانية والتجنيد، أما تنظيم داعش فله أزيد من 53 ألف موقع إلكتروني، 93 ألف صفحة باللغة العربية و13 ألف بلغات أخرى، مفتوحة للمطالعة خاصة على مواقع التواصل الاجتماعي[25]، ويركز العاملين على هذه المواقع في التنظيم إلى توظيف هذه المواقع لاستدراج فئة الشباب وضمهم لصفوفهم من خلال حملات التوعوية الإلكترونية.

الشكل الأول والثاني : "احذر التجنيد الإلكتروني"

المصدر: جريدة حضرموت 29 يونيو 2018 .على الرابط www.7adrmout.net/emaratlyoum

الشكل الثالث "صواب» يحذّر من 8 طرق «داعشية» لتجنيد الشباب"

المصدر: أحمد عابد أبوظبي التاريخ 2015.10.17 جريدة الإمارات اليوم على الرابط www.emaratalyoum.com

5- الحروب السيبرانية:

ارتبطت ثورة المعلومات بالمجال العسكري أثناء الحرب الباردة، نظرا لشدة التنافس بين القطبين لذا بدأ التفكير في تطوير مجالات البحث التقنية ودخلت التكنولوجيا في صناعة الأسلحة التقليدية، لتصبح إحدى أهم العناصر المكونة لمنظومة الأمن الشامل" القوة الصلبة+القوة الناعمة"، وأصبحت السرعة والدقة في تنفيذ العمليات تتجه نحو القطاعات الحساسة باستهداف أجهزة الأنترنت والحواسيب، ومن بين العمليات، نذكر(الحرب الإلكترونية التقليدية، القرصنة الإلكترونية وحرب المعلومات الاقتصادية)[26].

من هذا المنطلق، أصبح السباق نحو التفوق في القدرات العسكرية من اجل السيطرة على العالم بواسطة التكنولوجية المعلوماتية العصب الرئيسي الذي حاول توظيفه أكثر من فاعل في الساحة الدولية خلال القرن الواحد والعشرون، وبذلك أصبحت التقنيات المستعملة خاصة الأنترنت من اهم الوسائل في النشاط العسكري والأمني للضغط والتجسس على الدول[27] .

لكن التوقعات التي عجزت الأنظمة عن تفسيرها لوضع حد للجرائم السيبرانية التي تطال الأشخاص، الممتلكات والمؤسسات، تفاقمت حدتها وأصبح الخوف ينتاب المجتمع الدولي بمختلف تركيباته من وصول الايادي الاجرامية إلى مفاتيح التحكم في القدرات العسكرية لدول خاصة الأسلحة النووية .ويمكن قراءة سيناريو هذه الحروب من خلال تصور الامين العام للاتحاد الدولي للاتصالات في سنة 2011 السيد حمدون توري في بحث علمي تقدم به تحت عنوان "البحث عن السلام السيبراني[28].

من خلال ما تقدم، يتضح أن اختلاف تشريعات الدول الفاعلة في الحقل الدولي لوضع تعريف محدد لهذه الحرب أجهض جهود المنظمات الدولية والمراكز البحثية لاقتراح الآليات الناجعة لمواجهة هذا التهديد، رغم وجود الادلة الدامغة على الجرم المستنتج من بعض الاحداث التي عرضها الخبراء كعينات، مثل الهجمات السيبرانية التي استهدفت المصالح الحيوية (المنشآت النووية، العسكرية) لبعض الدول على غرار أستونيا، جورجيا، العراق وإيران، فهذه الجرائم وإن لم تحدث خسائر بشرية، فإنها من الناحية القانونية، تعتبر بمثابة إعلأن حرب على دول سيادية، منعت المادة الثانية من الفقرة الرابعة، من ميثاق هيئة الأمم المتحدة المساس بها "الامتناع عن استخدام القوة، حفظا على السلم والاستقرار الدوليين"[29].

من جهة ثانية، يرى الباحثون أن هاجس الاعتداءات ووقعها المحتمل على شاكلة الحرب، يوحي بوقوع حرب عالمية ثالثة، ومصدر قلق في كل هذا، أن المتغيرات الدولية التي تميزها الصراعات الدولية أصبحت تدق صفرات الأنذار في مكاتب صناع القرار ومخابر القيادات العسكرية ومراكز الابحاث الاستراتيجية لاتخاذ الاجراءات اللازمة لتفادي هيروشيما جديد، فمن وصل إلى اختراق المواقع الحساسة الاكثر حماية في الولايات المتحدة الامريكية وغيرها، كيف يعجز على الوصول إلى لوحة أزرار المفاعل النووي.

6- معضلة الأمن السيبراني العالمي:

ثغرات الأمن والدفاع أصبحت من الازمات الدائمة التي لم تجد طريقها إلى الحل في الدول العظمى رغم الإمكانيات المادية، البشرية والتقنية التي تتمتع بها، لأن الفجوة التي تم اكتشافها وتتكرر في كل مرة، أن هناك إخلالا وعدم احترام لقواعد حماية الأنظمة المعلوماتية من طرف المستخدمين، لذا نجد أن أنظمة

الأمن والدفاع كثيرا ما تقف عاجزة أمام الاختراقات[30] ، ويمكن قراءة ذلك في تقرير الوكالة الاممية للاتصالات في طبعته الثانية 2017(المؤشر العالمي للامن السيبراني GCI)، الذي أثبت الوكالة وجود اعطاب كثيرة في أنظمة حماية المعلومات لدى الدول، خاصة المتقدمة منها، مع العلم أن الكثير منهم جعل هذا الملف(الأمن السيبراني) من أولويات السياسة الدفاعية، على اعتبار أن الهجومات السيبرانية أصبحت من الاعمال المتوقعة التي لا يمكن التصدي لها ولا يمكن تحديد مجالها ولا خطورة نتائجها، ومن بين الثغرات، نذكر ما يلي:

1- الاختراقات التي تطال المواقع الرسمية والحساسة للدول، لا يتم الكشف فيها عن نقاط الضعف أنظمة التشغيل لأسباب أمنية، وإنما تتخذ إجراءات بديلة لتطوير البرمجيات لتفادي هجمات جديدة، ومثل هذه الثغرات التي سمحت للقراصنة إعادة الهجوم بوسائل متطورة، ومن أمثلة ذلك الهجوم على وكالة الأمن القومي الأمريكي سنة 2016، ورغم الاجراءات، لا توجد ضمانات للوصول إلى المعلومات المخزنة التي قد تكون لها آثار سلبية على السلم العالمي[31].

2- عدم التوافق والاجماع على إعطاء الجانب القانوني حقه (تعريف دقيق للجريمة) للتصدي لهذه الجرائم وإلزام الدول على التعاون للحد من هجرتها، أدراج المعاملات الإلكترونية في الميادين المالية، الاقتصادية والتجارية في خانة الخطر للحفاظ على المتداولين عليها لغياب الحماية رغم مرونتها، وهذا ما سمح للأيادي الاجرامية منة استغلال هذا الضعف وتحويله إلى وسيلة للضغط وتحصيل الفدية، كما سمحت للجماعات الإرهابية بتمويل عملياتهم الإجرامية.

3- عجز الفكر البشري على إيجاد الحلول لميادين هو مكتشفه (تكنولوجيا الإتصال)، أي عدم القدرة على حماية الاهداف الاستراتيجية (السياسية، الاقتصادية، الدفاعية والأمنية) التي تمثل إحدى أولويات السياسة الدفاعية الدولتية، هذا لا يعني تفوق الالة الاجرامية بقدر ما هو صراع الفواعل التي أصبحت تستعمل هذه الوسيلة للضغط على الدول لتحقيق مصالحها على حساب السلم العالمي، وماذا يفكر قادة العالم غدا إذا تم اكتشاف تخطيط لهجوم إلكتروني على منشآت نفطية، نووية وصحية.

4- إذا كانت نتائج تحقيق أغلبية الهجومات الإلكترونية تفيد أن الدوافع المالية هي الاساس في اقتراف هذا العمل غير مشروع، فإن الأنظمة يجب عليها توسيع دائرة الاجراءات الأمنية لتشمل القطاعات الاخرى لتفادي البحث عن وصفة لمرض جديد لم يتم تشخيصه من قبل، فاليوم يحصي قسم الجرائم الحاسوبية وقضايا الملكية الفكرية الأمريكي في تقريره أن هناك 4000 هجوما من برمجيات الفدية الخبيثة يحدث يوميًا منذ بدء عام 2016، لكن في المستقبل سوف تشمل الاحصائيات عدد الضحايا البشرية الناتجة عن الهجمات السيبرانية.

5- جانب الربح لا يمكن حسابه كمحصلة عمل إجرامي قام به القراصنة، ما دامت هيمنة الشركات المتعددة الجنسيات العاملة في هذا المجال منصبة هي الاخرى على الربح، باختيارها لبرامج ترصد من خلالها أموال طائلة دون التفكير في تطوير برامج أخرى مكملة أو كبدائل لحماية الأنظمة المربحة، وهذا ما سهل من مهمة القراصنة للدخول بسهولة إلى الأنظمة بطريقة ميكانيكية.

7- التحديات التي يمثلها الأمن السيبراني:

من خلال عملية تحليل للأرقام التي سوف أعرضها، سوف يتمكن القارئ لهذا المجال الحافل بالمفاجآت من معرفة الاخطار التي يمثلها الاجرام الالكتروني على الأمن الأنساني والعالمي، خاصة ونحن نعيش في عالم بلا حدود، بنيته فوضوية، لا وجود فيه للأقطاب، دائرة اختصاصه صراعات مصلحية لا متناهية، الحكم فيه يعود لأصحاب القوى، فواعله غير معروفين، الأمن والسلام فيه غير مضمون.

1- حسب التقرير التحليلي الصادر من طرف المخابر المختصة سنة 2016، فإن حالة انعدام فعالية الاجراءات الأمنية، تسببت في تسجيل لأكثر من 100 ألف واقعة و 2260 اختراقًا في 82 دولة، وتبين أن 88 % من الاختراقات هدفها دوافع مالية أو تجسوسية، كما اعاد قراصنة (وسطاء الظل) الكرة سنة 2017 وأحدثوا كارثة في البرامج المستعملة في أكثر من 100 دولة[32].

2- في الهجوم الذي استهدف عشرات آلاف من أجهزة الكمبيوتر في أكثر من 100 دولة بتاريخ 2017، اعتبرته شركة فورسبوينت سيكيوريتي الأمنية من أضخم العمليات التي قام بها قراصنة الويندواز، بحيث وصل معدل انتشار الهجمات مع نهاية اليوم الأول فقط إلى خمسة ملايين رسالة في الساعة، كما أعلنت شركة أفاست للأمن المعلوماتي أنها رصدت أكثر من 75 ألف هجوم في 99 بلدًا، وهو العدد الذي تجاوز مائة دولة فيما بعد[33].

3- الولايات المتحدة الامريكية تعتبر من أكبر ضحايا الجريمة السيبرانية، فهي تحصي كل ساعة أكثر من 500 ألف هجوم في مواقعها الاستراتيجية (وزارة الدفاع الوطني، مجلس الأمن القومي....إلخ)، ومن العمليات التي ما زالت تثير تساؤلات وجدل في الاوساط الأمنية والسياسية بأمريكا "تسلل قراصنة من روسيا سنة 2016 واختراقهم البريد الالكتروني الخاص بالقائمين على الحملة الأنتخابية لمرشحة الديمقراطيين للرئاسيات الامريكية هيلاري كلينتون، وتسريب المعلومات لموقع ويكي ليكس، مما دفع السلطات العليا (الرئيس باراك أوباما) إلى اتخاذ قرار طرد 35 ديبلوماسيا روسيا"[34] ، رغم نفي تهمة التسلل من طرف الرئيس الحالي دونالد ترامب في لقائه الاخير بالرئيس الروسي فلاديمير بوتين بهلسنكي2018.

4- المواقع التي بحوزة التنظيم الإرهابي داعش 53 ألف موقع إلكتروني، 93 ألف صفحة باللغة العربية، 13ألف اً صفحة بلغات أخرى، تكفي لإعلأن حرب نفسية على أية دولة عربية، كما تساهم لا محال في تحقيق جميع أهدافها (التجنيد، الابتزاز، التمويل، شن الهجومات) .

5- التحديات التي أصبحت تفرضها خطورة الجرائم السيبرانية على الأمن والسلم العالميين، أصبحت من بين من المواضيع الأكثر تداول ونقاش في اللقاءات العلمية المنظمة بشكل دوري من طرف الحكومات بالتعاون مع الاكاديميين والمؤسسات الخاصة بالأمن المعلوماتي، لكن قلة الحلول الرادعة لهذا التهديد، لم تعطي دفع جديد للخروج من هذه المعضلة، واقتصرت اللقاءات ككل مرة على إصدار توصيات تطالب في مجملها بالمزيد من اليقظة والحذر واتخاذ التدابير اللازمة لتدارك النقائص، لكن ما يلاحظ، أن إسهامات الدول في ضخ أموال طائلة (96.3 مليار دولار) حجم الأنفاق العالمي سنة 2018 ، منها 2.2 مليار حصة دول الشر الأوسط وشمال إفريقيا، لم تجد نفعا لوضع حد لهذه الازمة الأمنية[35].

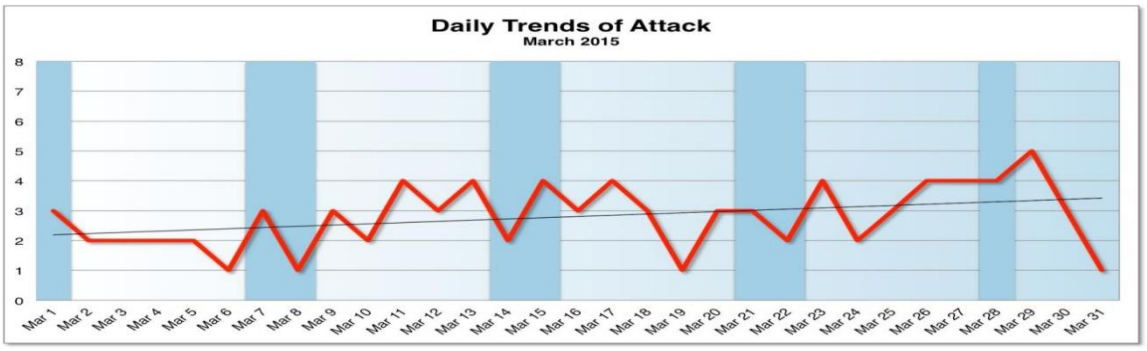
6- برأي أحد المختصين "بردي رئيس هيئة البحث في مجموعة هواوي الامريكية"، أنه بحلول سنة 2020سيدخل أكثر من 50 مليار جهاز كمبيوتر خدمة الأنترنت وهذا ما سيوفر إيرادات تقدر ب 07 تريلين دولار، ورغم هذا التقدم والتفوق الهائل، فإن القلق ما زال ينتاب المختصون حول المخاطر التي سيسببها اختراق هذه الفضاءات.

7- في تقرير لشركة" كاسبرسكي "المختصة في مجال الأمن المعلوماتي، فإن مجموعة من" الهاكرز " تمكنوا سنة 2015 ، من قرصنة العديد من الحسابات في مصارف عالمية، مستغلين في ذلك ثغرة في الأنظمة المعلوماتية لأجهزة الاعلام الالي للمصارف، استخدموا تقنيات معقدة للدخول ونسخ بيانات الحسابات في مدة لا تتجاوز 20 ثانية، واستحوذوا في الاخير على نحو مليار دولار.

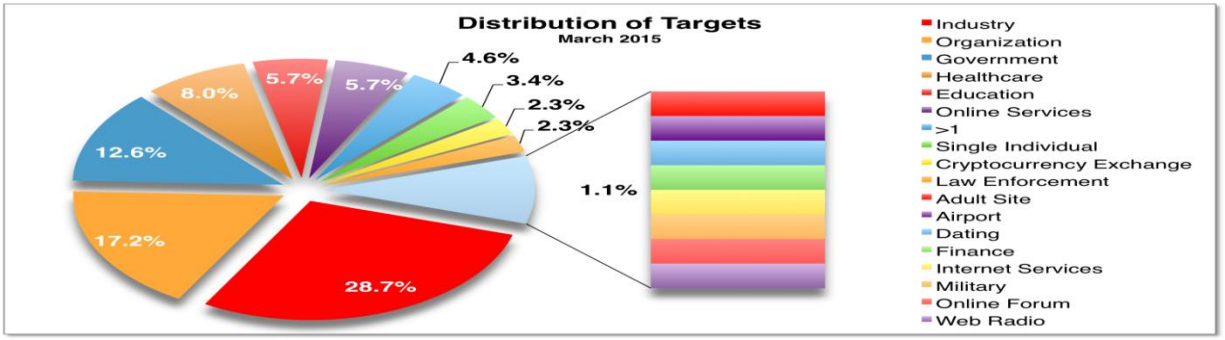
8- في تقريرها السنوي للتهديدات الأمنية لسنة 2016 أكدت شركة ديل الامريكية، أن البرمجيات الخبيثة تضاعف عددها إلى 8.19 مليارات، وباتت أنظمة أندرويد هي الأكثر استهدافًا إلى جانب مواقع إنترنت كبرى مثل:تويتر، وأمازون، وريديت، الذين حجبت لخدمات DDOS من جراء الهجمات التي تُغرق الخوادم بتقنيات عالية تؤدي لتوقفها.

9- أمام التداعيات المستقبلية لهذا الخطر وتأثيراته السلبية على الأمن القومي الامريكي، توجهت السلطات إلى أنشاء مؤسسة خاصة بالأمن السيبراني (مركز حماية البنية الأساسية للأمن القومي) وتم توفير وتجنيد كل الامكانيات المالية والبشرية لضمان حماية أنظمتها المعلوماتية الاستراتيجية المستهدفة، كما تم ربطها بجميع شبكات الأمن الالكتروني، وأوكلت مهمة التحقيق لكبريات أجهزة الأمن(المخابرات، مجلس الأمن القومي ومكتب التحقيقات الفيدرالية [36].

الشكل الأول: توجهات الراي حول الاحداث المرتكبة خلال شهر مارس 2015



الشكل الثاني: توزيع الاهداف خلال شهر مارس 2015



المصدر: علي زغيب: مؤتمر الأمن السيبراني والدفاع السيبراني، تحديات وافاق، من تنظيم الجامعة اللبنانية والوكالة الجامعية للفرنكوفونية، 2017.10.23، الرابط www.ul.edu.hb.

8- التداعيات المستقبلية للأمن السيبراني:

من خلال التحليل الموضوعي لمجمل الدراسات العلمية والتقارير التقنية والاحصائيات العملياتية التي تم تناولها في هذا المحور، يتضح أن التداعيات المستقبلية تدور بين مخاوف تفاقم معضلة الدفاع أمام ثغرات الأمن وعدم فعالية الاستراتيجيات المسطرة لغاية الأن، لأن التهديدات والهجمات السيبرانية التي تستهدف المرافق المستخدمة للأنترنت في تعاملاتها (كالمصارف المالية، المؤسسات العمومية، الشركات المتعددة الجنسية ورجال الاعمال)، بطريقة وإن كانت متسارعة وخطية، فهذا لا ينفي احتمال توجهها في المراحل المستقبلية لمجالات جد حساسة، مما يجعل منها جزءا أساسيا في الصراعات العسكرية بين الدول. هذه الاشكاليات تعتبر بالنسبة للمختصين نتاج لمجموعة من الاسباب أو الحقائق، من بينها:

- افتقار الشركات العاملة في الميدان إلى رؤية صحيحة حول الكيفيات المستعملة في شبكاتها مما سمح للقراصنة بالدخول والخروج بطريقة سهلة.

- الاستخدام المفرط للوسائط الرقمية، لتوظيف المعلومات، أو إتمام المعاملات، أو غيرها، جعل من هذا المجال الواسع، فجوة لاستهداف المعلومة، خاصة وأن القراصنة يتمتعون بدرجات عالية في المهارات الرقمية.

- مواطن الضعف والعطب في الأمن السيبراني يجسدها الخطأ البشري المتعمد أو غير المتعمد، فالمخترعون (البشر) هم من أحدثوا ثورة في التكنولوجيا وأدوات استخدامها وسمحوا للوحدات السياسية (الدول) برعايتها، لكن تبين في الاخير أن الطرفين دخلوا في مواجهة مع الاجرام لن تنتهي بأي حال على المدى القريب.

- عدم وجود معلومات رسمية كافية ودقيقة حول واقع الأمن السيبراني والتهديدات المتوقعة، لم يسمح لأصحاب الاختصاص والمهنيين من تقديم اقتراحات وحلول عملية.

- عدم جدية التعاون الاقليمي والدولي فيما يخص تبادل المعلومات والخبرات.

- عدم إدراك ووعي المستخدمين للإعلام وتكنولوجيا الاتصال بمدى تأثير الجرائم الالكترونية على نمط الحياة الشخصية والمهنية.

- اتخاذ العديد من الدول إجراءات جديدة لحماية فضاؤها الالكتروني الخاص بالقوات المسلحة على غرار الصين التي استبقت الاحداث وأنشأت (الجيش الأزرق)، يمكن إلى حد ما اعتبارها مؤشرات دالة على أن العالم في ثوبه الجديد (عالم بالا أقطاب) يستعد لمواجهة إفرازات حرب إلكترونية متوقعة بين الحين والاخر.

مما سبق ذكره، ولتفادي الوقوع في سيناريوهات (استهداف النظم العسكرية، محطات توليد الطاقة والمياه، البنية التحتية الاقتصادية، ونظم الاتصالات)، يناشد المختصون في مجال الاعلام بمفهومه الواسع (التقني والأمني) زعماء العالم للتنسيق مع منظمة الامم المتحدة بغية إنشاء منظمة دولية يقودها جيش من

المستشارين في مجال القانون والعلاقات الدولية، وتقنيين في مجال تكنولوجيا الاتصال وخبراء ميدانيين قادرين على صد هذه الهجمات الشرسة.

المحور الثاني

الاستراتيجية الجزائرية

ما جاء في المحور الاول من معطيات عن هذا العالم الافتراضي الذي عجزت الدول المتقدمة على مواجهته، سوف أسقطه على الجزائر، على اعتبار أن هذا التحدي يقتضي من صانع القرار الرد عليه بجدية في الجبهة الداخلية من خلال تنسيق الجهود بين الفاعلين في الميدان، وفي الجبهة الخارجية بالتعاون مع الدول والمنظمات المتخصصة، بهدف بناء نظام دفاعي لحماية أنظمتنا المعلوماتية ضد الهجمات السيبرانية، لأن المعلومات والبيانات الحساسة أصبحت تقارب في أهميتها النفط (الممول الرئيسي لاقتصاد العديد من الدول).

تعتمد الدول في مكافحتها لأفة الجريمة السيبرانية الماسة بالأمن، الاستقرار، القيم الاجتماعية والثقافية إلى تفعيل الاليات القانونية وتكليف كل السلطات (المؤسسة العسكرية، القضائية، الأمنية) بالتنفيذ الصارم للإجراءات للحد من خطورة الجريمة، كما تلتزم الدول في هذا الاطار إلى مراعاة الشرعية الدولية للاستفادة في إطار التعاون من الخبرات في مجال، لأن مثل هذه الجرائم لا تعترف بالحدود ولا الهوية ولا يستطيع مواجهتها إلا من له القدرة في التحكم في تكنولوجيا المعلومات.

من هذا المنطلق، وفي إطار رسم السياسة الأمنية العامة طرح صناع القرار في الجزائر مخططا وطنيا لتفادي الوقوع في مأزق امني جديد (اختراق انظمة المعلومات الحساسة لرئاسة الجمهورية، وزارة الدفاع الوطني، أجهزة الأمن)، أخذين بعين الاعتبار من جهة، الازمة الأمنية التي تحاصر البلاد في شقها المتوسطي، المغاربي والساحل الافريقي، ومن جهة ثانية، الحفاظ على الحقوق الشخصية والحريات الفردية وفق ما تضمنته المواثيق الدولية والقوانين الوطنية، وسوف نطرح تصور أو مقاربة الجزائر للموضوع من خلال النقاط التالية:

أولاً- على المستوى الوطني:

أدرجت الجزائر الأمن السيبراني كإحدى الاولويات في برنامج المواجهة ضد الجريمة الالكترونية والارهاب الالكتروني، بل أصبح يشكل جزءً لا يتجزأ من استراتيجيات الدفاع، لأن الدروس المستخلصة من الدول التي لها تجربة في هذا المجال، أثبتت أن النجاعة في التطبيق وفعالية المعايير والوسائل المستعملة لا يمكن لها أن تتجسد ما لم يكن هناك تخطيط محكم وتنسيق بين الفاعلين في الميدان، وعليه توجهت الجزائر إلى رسم استراتيجيتها مركزة على النقاط التالية:

- تحديد المخاطر،
- اتخاذ التدابير اللازمة،
- تحديد الهيئات المكلفة بإدارة الأمن،
- تحديد الهيئات المكلفة بالتنسيق،

- تحديد الهيئة المكلفة بالجانب التقني للبحث عن الثغرات وتوجيه التحقيق، ليبقى الهدف في الأخير، زيادة قدرات الأمن السيبراني لحماية الأنظمة المعلوماتية وتعزيز سبل المواجهة الوقائية (التوعية)والمواجهة الردعية (ملاحقة المجرمين)، وسوف نستعرض لهذه النقاط بالتفصيل.

1- من الناحية القانونية:

اعتمد المشرع الجزائري في سن الاحكام القانونية لمحاصرة الجريمة الالكترونية على ثلاثة معايير متفق عليها إلى حد ما لدى الفقهاء والتشريعات المقارنة[37]، أولا: وسيلة الجريمة المتمثلة في استخدام تكنولوجيات الاتصال، ثانيا: موضوع الجريمة المتمثل في المساس بالأنظمة المعلوماتية، ثالثا: الجانب الشرعي والمتمثل في العقوبات المحددة في القانون، ويهدف المشرع من هذه الخطوة إلى تحديد النطاق الذي تنشط فيه الجريمة الالكترونية حتى يتسنى للفاعلين التحكم في الموضوع، ومن خلال القراءة التحليلية لمواد القوانين المستحدثة أو المعدلة، يتضح أن المشرع الجزائري قد طرح تصورا يتوفر على العلاج الوقائي والردعي لمحاصرة الجرائم السيبرانية من الجوانب التالية:

أولاً- تم تعريف الجريمة الالكترونية وإدراجها ضمن الأعمال المعاقب عليها قانونا (المادة 02) من القانون رقم 09-04 المؤرخ في 2009.05.09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كما تبني القانون النقاط الاساسية المذكورة في المعيار الاول والثاني، أما المعيار الثالث، فقد تناوله المشرع من خلال إدراج المادة 323 من القانون05-10 الصادر في 2005.06.20المتضمن الدليل الالكتروني، (أنظر القانون المدني طبعة 2014)، كما تم تعديل المواد (720.238.212.156.143.79.65) من قانون الاجراءات الجزائية ،والمواد (396.394.333.303) من قانون العقوبات المتضمنة تجريم وتسليط العقاب على كل من يثبت في حقه اختراق انظمة معلومات المؤسسات أو الافراد بطريقة غير شرعية ، كما جاءت المادة 87 من نفس القانون صريحة في تجريم وتسليط العقاب على كل من يثبت تورطه في اعمال الاشادة والتجنيد لصالح الجماعات الارهابية (الارهاب الإلكتروني)[38].

بالإضافة إلى ذلك تدعمت الاجراءات القانونية بألية تقنية جديدة تتمثل في صدور القانون 16.03 المؤرخ في 2016.06.19 المتضمن البصمات الجنائية في الاجراءات الجزائية لتحديد هوية الاشخاص، كما تم تعزيز الجهات القضائية على المستوى الوطني بأربعة محاكم خاصة pôles de magistrats spécialisés (الجزائر، قسنطينة، وهران، ورقلة)، لتسهيل عمليات البحث والتحري لذوي الاختصاص من الاجهزة الأمنية والبت في القضايا المعروضة دون الرجوع إلى الوصاية، كما شمل التشريع بعض المجالات التي يحتمل أن تشملها الجريمة والتي لها صلة بمجال الحريات الخاصة على غرار قانون الملكية الفكرية، الثقافية، حقوق المؤلف (قانون 05.03 و03-06 الصادرين بتاريخ 2003.07.19)، وقانون مكافحة تبييض الاموال (01-05 الصادر بتاريخ 2005.02.05)، وقانون الوقاية ومكافحة المخدرات (04-18 الصادر بتاريخ 2004.12.25).

ثانياً- تم مطابقة التشريع الداخلي مع ما جاء في التشريعات الدولية وخاصة الاتفاقية الدولية المبرمة في عاصمة المجر بودابيست بتاريخ 2001.11.23) المتضمنة الجرائم السيبرانية وتعتبر هذه الاتفاقية بمثابة المرجعية القانونية لكل التشريعات الدولية الصادرة في هذا المجال، ومن بين النقاط التي شملتها المطابقة:

- استعمال المصطلحات المعمول بها في مجال الاعلام الالي وتكنولوجيات الاتصال :معطيات الاعلام، معطيات متعلقة بالاختراق، ممول الخدمات، (أنظر المادة الاولى من الاتفاقية ومقدمة القانون 04.09 الجزائري)، ليبقى الهدف، تسهيل عمل المختصين في الاعلام الالي من قراءة صحيحة للعمل المطلوب أو الملف المطروح.

- الدخول الغير شرعي للأنظمة المعلوماتية، (أنظر المادة الثانية من الاتفاقية والمادة 394 مكرر قانون العقوبات الجزائري)، أهمية تجريم هذا العمل هو تحديد نقاط الضعف للنظام المستهدف مع إمكانية تحديد هوية الجاني.

- الاعتراض الغير شرعي للمكالمات والمعطيات المتبادلة سواء في إطار خاص أو مهني (أنظر المادة الثالثة من الاتفاقية والمادة 303 من قانون العقوبات الجزائري).

- المساس بنزاهة أو استماتة المعطيات (انظر المادة الرابعة من الاتفاقية والمادة 394 مكرر قانون العقوبات الجزائري)، لأن الحصول على المعطيات بطريقة غي شرعية من شأنه أن يحول من مسار المعلومة في جانبها المهني أو الشخصي، وهذه الخطوة من أخطر التهديدات الإلكترونية.

- المسؤولية المعنوية للجهات المكلفة بتسيير مجالات تكنولوجيا الإعلام تبقى قائمة، لأنهم في نظر القانون الضامن الوحيد على حسن وسلامة الأنظمة المعلوماتية (أنظر المادة 12 من الاتفاقية والمادة 394 مكرر قانون العقوبات الجزائري).

- التعاون الدولي من اجل سلامة الاجراءات القانونية (الأنابة القضائية، تسليم المجرمين) وهي من أهم العناصر التي ركزت عليها الاتفاقية في الباب الثالث والمواد 614-713 من قانون الاجراءات الجزائية والمادة 15 من القانون 09-04، لأن هذه الخطوة تبقى السبيل الأمثل بالنسبة للخبراء للحد من الجريمة الالكترونية كما تشكل عائق لحسن سير المتابعة القضائية إذا كانت طلبات الأنابة أو التسليم تمس بسيادة الدولة.

بالرغم من المجهودات المبذولة من طرف الدولة، إلا أن المختصين يرون أن البنية التنظيمية والتشريعية ما زالت في طور التشكيل حتى تكتمل المعادلة، على اعتبار أن القوانين التي تحوي قواعد ملزمة، ورادعة، أخذت حصة الاسد في التشريع في حين هناك العديد من الجوانب لم يتم تطويرها بما يتوافق مع البيئة الوطنية، كالمقاييس الدولية للحماية، المواصفات التقنية للمعلومات، البيانات، الأنظمة، البرامج والأجهزة.

لاستدراك هذه النقائص، تجتهد الجزائر من خلال الهيئات المختصة على التحسين المستمر لأليات المواجهة وتعزيز الاطار القانوني، لمواكبة المتغيرات والتحولات الطارئة في هذا المجال، ومن بين أهم النقاط التي تعتزم السلطة التشريعية القيام بها، إصدار قانون لحماية المعطيات الخاصة بالمواطن من الجرائم الالكترونية تماشيا مع ما جاء في دستور 2016 الذي أوصى باحترام وحماية الحقوق الخاصة (المواد 51-50-46).

كما تعكف لجنة من الخبراء على تحضير الأرضية لقانون ينظم مهام سلك البريد والاتصالات الالكترونية وجعلها من أولويات سلطة الضبط، لأن أغلبية الاخطاء المهنية المؤدية إلى هذا النوع من الجرائم سببها الاستعمال المفرط والغير عقلأني لأجهزة الاتصالات، نفس الطرح تعمل وزارة العدل على تجسيده من خلال مشروع القانون الجديد المتضمن تنظيم كل ما يتعلق بخصوصية المعلومات وسريتها، للمحافظة عليها في ظل التعاملات الإلكترونية عبر شبكات الاتصالات.

2- من الناحية العملية:

لضمان التنفيذ الفعلي والجدي لمختلف التدابير الهادفة لتحقيق الأمن السيبراني، أوكلت السلطات العليا للدولة هذه المهمة إلى هيئات متخصصة ضمن أسلاك الأمن، وأوصت باحترام الحريات في إطار الشرعية الدستورية والمواثيق الدولية، من بين الهيئات، نذكر ما يلي:

1- المصلحة المركزية لمكافحة الجريمة المعلوماتية (SCLC) :

التابعة لمديرية الأمن الوطني، وتعتمد هذه المصلحة على موارد بشرية لها من الكفاءة المهنية ما يؤهلها لتنفيذ مهامها على المستوى الدولي من خلال التعامل مع المصالح المختصة (أنتبول، أفريكوم) أو مصالح الشرطة لكبرى الدول، وعلى المستوى الوطني تتواصل هذه الهيئة مع الشرطة العلمية والمكاتب اللامركزية المختصة في الاجرام(الشرطة القضائية.)

2- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية (CPLCIC):

التابعة للقيادة العامة للدرك الوطني، لا تختلف كثيرا في مهام التحقيق والتحريات في هذا المجال عن نظيرتها التابعة للأمن الوطني سواء محليا أو وطنيا، بل بالعكس يتم التنسيق بينهما تحت المسؤولية المباشرة للنائب العام على مستوى دائرة الاختصاص.

3- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني (INCC):

التابع للقيادة العامة للدرك الوطني، يعتمد المعهد في أداء مهامه على الخبرة العلمية والتجارب المخبرية الدقيقة لكل الأدلة المتحصل عليها من مكان ارتكاب الجريمة عامة، من أجل تنوير العدالة وتوجيه الجهات الأمنية كلما تعلق الامر باستكمال التحقيق.

ومن بين النتائج المتوصل إليها من طرف هذه المصالح، اتضح أن الجرائم الالكترونية بالجزائر تتضاعف بطريقة سريعة جدا، وهذا ما كشفت عنه الأرقام المسجلة التي تم البت فيها، حيث سجلت سنة 2017 أكثر من 2500جريمة ويتعلق أبرزها 70% انتهاك الحريات الشخصية، والتهديد عبر الأنترنت، ونشر صور فاضحة، الابتزاز، والقرصنة الإلكترونية وغيرها.

وحسب تقدير نفس الاجهزة، فإن هذه الارقام لا يمكن تسجيلها لولا الممارسات الغير عقلأنية التي جسدها الاستعمال المفرط وغير المنتظم لوسائل الاتصال وتكنولوجيات الاعلام، فقد تم إحصاء أكثر من حيث 28 مليون مستعمل للأنترنت، 18 مليون لهم حسابات ومواقع فايس-بوك و13 مليون متفحص يومي لشبكة التواصل الاجتماعي)[39].

عمليات الإختراق طالت كذلك وزارة الدفاع الوطني، وحسب المسؤولين، فإن المؤسسة تجهض يوميا ما يقارب 3500 محاولة اختراق لمواقع قيادات قواتها ومديرياتها المركزية، بمعدل 130 ألف محاولة اختراق في السنة، من قبل عصابات" الهاكرز "من مختلف دول العالم، في إطار ما يعرف ب"الحرب الإلكترونية.

3- من الناحية الادارية:

لتفادي الوقوع في تداخل الصلاحيات بين مختلف الاجهزة الفاعلة في مسائل الأمن والدفاع الوطني، حرص المشرع الجزائري على وضع ضوابط لاحترام الاطار الاداري المنظم لصلاحيات الهيئات المدنية، العسكرية والتقنية في إدارة الاستراتيجية الجزائرية للأمن السيبراني، ويمكن قراءة ذلك من النقاط الاتية:

أ- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

التي أنشئت سنة 2009، ووضعت تحت السلطة المباشرة لوزير العدل حافظ الاختام، ولم تدخل حيز التنفيذ إلا بعد صدور المرسوم الرئاسي رقم 15-261المؤرّخ في 2015.10.08 ، من أبرز المهام المنوطة بها:

- استغلال المعطيات المتوفرة بطريقة تسمح بمتابعة كل ما يجري في الفضاء السيبراني من نشاطات غير شرعية وبالتالي توجيه القدرات البشرية والمالية للحد من الثغرات، مع العلم ان هذا المجال أصبح مفتوحا على كل الاحتمالات في ظل التطور السريع لتكنولوجيا الاعلام والاتصال.

- تعزيز التنسيق بين مختلف الفاعلين في الميدان والتشديد على ضرورة التعاون بين القطاعين العام والخاص والمجتمع المدني، من أجل نشر ثقافة المواجهة لكل الممارسات التي تخالف القانون في الفضاء السيبراني وحماية الحقوق والحريات الأساسية[40].

- العمل من أجل خلق إطار مركزي للمعلوماتية على شاكلة وحدة بحث، يتم من خلالها جمع المعطيات والاحصائيات في هذا المجال من أجل التحليل المستمر للتهديدات واقتراح الحلول المناسبة.

- التنسيق والتعاون بين مختلف الأجهزة الأمنية، المالية والإدارية التي لها علاقة مباشرة بأنشطة تكنولوجيا الاعلام، من اجل تحديد المسؤوليات لفرض مراقبة صارمة بعد حصر المجالات المستهدفة من طرف محترفي الجريمة الالكترونية، مع العلم أن الدولة متوجهة إلى تحقيق الحوكمة الالكترونية التي تعتمد في أعمالها على المعاملات الالكترونية في جميع مجالات الحياة، ويمكن اعتماد المعايير التي ذكرها البنك الدولي" للحوكمة الالكترونية، التي تستطيع من خلالها المؤسسات الحكومية في استخدامها لتكنولوجيا المعلومات التي لديها القدرة على تغيير وتحويل العلاقات مع المواطنين ورجال الاعمال والمؤسسات الحكومية.....وزيادة قناعة المواطن بدور المؤسسة الحكومية في حياته"[41].

- اقتراح الأرضية اللازمة لتجسيد الاستراتيجية الوطنية للوقاية ومحاربة الجرائم الالكترونية (حسب ما جاء في المادة الرابعة من المرسوم أعلاه)، وتعتبر هذه الخطوة من الصلاحيات الدالة على أهمية إدارة الأمن السيبراني بالنسبة للدولة.

- بالعودة إلى الدراسات العلمية والميدانية التي تجمع أن الجانب التوعوي يلعب دورا مهما للحد من الجرائم المعلوماتية، فإن الجهات المختصة (الهيئة الوطنية) إذا أرادت النجاح في تحقيق وتطوير الأمن السيبراني، عليها بالعناية الكافية بتوعية كل من له صلة مباشرة أو غير مباشرة بمجال المعلومات، ومتى تحقق ذلك، فإن التوعية تستحق أن تكون من العناصر المكملة للجوانب الاخرى على غرار، تفعيل القوانين، التنسيق والتعاون وتوفر الأدوات التقنية اللازمة لتحقيق الأمن والتعاون الدولي[42]، لتجسيد هذه الفكرة، سطرت الدولة كذلك برنامج اعتمدت في تطبيقه على اجهزة السمعي-البصري، اللقاءات العلمية، الدورات التكوينية داخل المؤسسات، توزيع مطويات وألواح إشهارية، وأشركت في ذلك جميع الوسائط (مؤسسات الدولة والمجتمع المدني).

ب- بالنظر لحساسية قطاع الدفاع الوطني:

أستحدث بتاريخ 2015.06.11 ، على مستوى دائرة الاستعمال والتحضير لأركان الجيش الوطني الشعبي" مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة"، وأوكلت لها مهمة، حماية المنظومات والمنشآت الحيوية للبلاد ضد كل أنواع الجريمة السيبرانية، ومن بين المحاور التي تناولتها الارضية العملياتية لهذه المصلحة، نذكر ما يلي:

- توجيه، تنفيذ وتأطير الاعمال في هذا المجال لا يجب أن يتعدى الاطار الوظيفي أو التنظيمي.

- تطوير وتعزيز المنظومة القانونية لتفادي التجاوزات أثناء استخدام التكنولوجيا وضمان حماية منظومات الاعلام.

- اعتماد التكوين التقني والعلمي لأنتاج الكفاءات والمهارات القادرة على خلق نظام الدفاع السيبراني في كافة أنشطة المؤسسة العسكرية وبالتالي تفادي الاخطار الاجرامية.

- غرس ثقافة الاستعمال الكيفي لهذا العنصر الحيوي" تكنولوجيات الاعلام والاتصال "من خلال حملات تحسيسية لكافة مستخدمي المؤسسة بغض النظر عن الرتبة أو الوظيفة[43].

- الاعتماد وبطريقة مستمرة على البحث العلمي لتطوير وسائل الدفاع استجابة للتطورات الحاصلة في مجال التكنولوجيا.

- فتح مجال التعاون الدولي مع المؤسسات العسكرية الاجنبية، خاصة تلك التي لها رصيد في المجال لتبادل الخبرات والاستفادة من تجاربهم في هذا المجال[44].

ج- أصدرت العديد من الوزارات على غرار وزارة البريد والاتصال، المالية، التعليم العالي، الداخلية، تعليمات وتوجيهات إلى مصالحها التنفيذية تتضمن الاليات والكيفيات الواجب تطبيقها من الناحية العملية لتفادي الوقوع في الاخطاء، نلخصها فيما يلي:

- عدم السماح لأي كان من الحصول على معلومات من الأنظمة المعلوماتية الموصولة بشبكة الأنترنت، ما لم يكن هناك إذن أو موافقة من المصلحة المؤهلة قانونا، كما لا يمكن استخدام الحسابات الخاصة للأفراد أو تداول أرقامهم السرية.

- احترام المقاييس المعمول بها في تداول المعلومات المشفرة "إرسالا واستقبالا"، سواء تعلق الامر بالأنظمة المعلوماتية الداخلية للشبكات الوطنية أو الدولية.

- احترام القواعد العلمية والمهنية المعمول بها عالميا في توظيف تكنولوجيا الاعلام سواء لأغراض شخصية أو مهنية حتى لا تعرض الأنظمة للقرصنة، لأن الاستخدام المفرط بقدر ما يخلق ثغرات، فإنه يساهم كذلك في حرمان الاخرين من الاستفادة من خدمات التكنولوجيا.

ما يلاحظ في هذا الباب، أن المجهودات التي تبذلها الجزائر للإلمام بأهم العناصر الكفيلة بتحقيق الأمن السيبراني، ما زالت بعيدة، لأن الاجراءات الادارية المتخذة لحد الأن من طرف الهيئات المذكورة أعلاه للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تبقى غير كافية وتتطلب المزيد والاستمرارية في الموقف والنهج.

4- من الناحية التقنية:

الحصول على أفضل الوسائل التكنولوجية، الاعتماد على الكفاءات والإطلاع على أفضل طرق الحماية تعتبر حلقة وصل صلبة لتفادي الثغرات ومقاومة الاختراقات، ولتحقيق هذه المهمة، أصبح من الضروري على السلطات الاستثمار في الجانب التقني وتشجيع المبادرات الهادفة لتطوير سياسات أمن وحماية البنية المعلوماتية، خاصة إذا علمنا، أننا على عتبة تجسيد مشروع الحكومة الالكترونية التي أصبحت مطلب للمواطن لتحسين الخدمات.

لكن ما يعاب من هذه الناحية، أن النقائص التي تم حصرها من طرف الخبراء[45] ، أضعفت مجالات الأمن المعلوماتي وجعلت منه فضاء مفتوح للتهديد والاختراق، ومن النقائص المذكورة، أن الكيفيات المستعملة في التوظيف غير مطابقة أو غير ملائمة للمواصفات الدولية لأمن الأنظمة المعلوماتية[46] التي أقرتها علامات المطابقة العالمية إزو 17799/2005 و27002 وغيرها من المخابر المتخصصة في التكنولوجيات الحديثة.

كما يشير الخبراء إلى عدم تفعيل وتطوير مختلف تقنيات الأمن السيبراني التي أكد عليها الاتحاد الدولي للاتصالات (ITU)[47] ويمكن تفحص جميع المعطيات من خلال الاطلاع على تقرير الاتحاد الدولي السنوي (نوفمبر2017) الذي خلص في النهاية إلى تصنيف دول العالم في مجال الأمن السيبراني معتمدا في ذلك على مقياس "مدى التزام الدول في جميع أنحاء العالم بتفعيل وتطوير مختلف تقنيات الأمن السيبراني"، وقسمها الى ثلاث فئات، دول متخلفة، الناضجة والمتقدمة، وبين التصنيف والتقسيم احتلت الجزائر المرتبة الثامنة والستون (68) عالميا من مجموع 164 دولة شملها التقرير والمرتبة التاسعة (09) من مجموع 22 دولة عربية[48].

كما يمكن قراءة نفس الاستنتاجات السلبية من خلال تحليل المقاييس العالمية لمستويات التأهب في مجال الأمن السيبراني المستعملة من طرف المؤسسات المتخصصة في هذا المجال (القوانين، الاجراءات التقنية اللوائح تنظيمية، بناء القدرات والتعاون)، أين وجدت الجزائر نفسها في مؤخرة القائمة، حيث احتلت (المرتبة الثالثة والعشرين (23) عالميا من أصل 29 دولة بمؤشر 0.176 مقارنة بالولايات المتحدة الامريكية

صاحبة المرتبة الاولى، بمؤشر 0.824 ، والمرتبة العاشرة (10) عربيا بمجموع 0.1765 مقارنة بالمملكة الاردنية الهاشمية صاحبة المرتبة الاولى بمجموع 0.7647[49].

5- من الناحية العلمية:

حتى تتمكن الهيئات من السيطرة على مختلف الجوانب المتعلقة بعملية تحقيق الأمن السيبراني وفق ما تم ترسيمه في الاستراتيجية الوطنية، توجهت المؤسسات السيادية (رئاسة الجمهورية، وزارة الدفاع، المؤسسات الأمنية، الوزارات)[50] إلى تنظيم دورات تكوينية وسخرت لها كافة الوسائل المادية والبشرية، كما استنجدت الجزائر بخبراء دوليين لتمكين الإطارات الناشطة في المجال من جميع الاسلاك لمعرفة أفضل الممارسات في تكنولوجيا الأمن والسياسات العامة للأعمال الالكترونية المعمول بها في الخارج، كما تم إرسال بعثات للحضور والمشاركة في المؤتمرات الدولية للاستفادة من الخبرات التي تهدف إلى إصدار التوصيات المناسبة لأمن وسلامة المعلومات في الفضاء السيبراني.

كما ساهمت الجامعات ومؤسسات البحث العلمي من خلال تنظيم أيام دراسية وملتقيات الأكاديمية، نذكر على سبيل المثال، الملتقى الدولي الذي نظمته كلية الحقوق، جامعة برج بوعريريج بتاريخ 2017.04.12 تحت عنوان "الاجرام السيبراني، المفاهيم والتحديات"، وكذا الملتقى الدولي الذي نظمه كل من الجيش الوطني الشعبي وقيادة الدرك الوطني في الفترة الممتدة بين شهر مارس وماي 2017. كل التوصيات التي انتهت إليها اللقاءات العلمية تجتمع حول نقاط مشتركة يمكن استخلاصها في العناصر التالية:

- تنسيق الجهود، الاعتماد على الكفاءات، إنشاء هيئة مديرة، تعزيز الجانب المادي والبشري، إطلاق مشاريع بحثية، تشجيع المهارات، تعزيز التعاون الدولي.

هذه المطالب وإن لم تكن جديدة الطرح، إلا أن المختصين يعتبرونها بمثابة جسر للتواصل بين الباحثين والاكاديميين والمهنيين لتعزيز الهياكل الوطنية وتقييم الأنجازات التي تم تجسيدها من طرف الهيئات المدنية أو العسكرية المعنية بمكافحة الجريمة السيبرانية وذلك في إطار التحول التكنولوجي والرقمي الكبير الذي تشهده الجزائر.

ثانياً- على المستوى الإقليمي:

- المستوى العربي:

من خلال الدراسات الاكاديمية وتحليل المعطيات المستقاة من المؤسسات المتخصصة في الأمن السيبراني المتضمنة النقائص والثغرات في حماية الأنظمة المعلوماتية للدول العربية، المعلن عليها خلال اللقاءات، يتضح أن المقاومات البشرية والمادية المتوفرة والقادرة على تفادي المخاطر لم تجدي نفعا، والدليل أن السلبيات التي أصبحت تشكل نسبة كبيرة من المخاطر لا تزال تطرح نفسها بشدة، ومن بينها نذكر ما يلي:

- المنظومة التشريعية والتنظيمية العربية تشهد حركة بطيئة، مما يجعلها غير جامعة للعديد من الجوانب الحساسة في الفضاء السيبراني، بحيث يلاحظ أن معالجة العديد من حالات التهديد تتم من خلال

تفعيل الجانب العقابي سواء بإدراج مواد جديدة أو تعديل القوانين السابقة وهذا ما يتعارض والتوجهات العالمية (المرونة والتطور)[51].

- عدم توازن المعادلة في الموارد البشرية بين ما هو موجود (افتقار وعجز الكفاءات المؤهلة لتغطية النقائص) وما يجب أن يكون (مواكبة التحديات المترتبة عن التطور السريع للتكنولوجيا).

- الآليات الموظفة لتنفيذ الإجراءات الأمنية في عالم التكنولوجيا ميدانيا غير ملائمة وغير مطابقة للمواصفات العالمية، والاحصائيات المتوفرة لدى الاتحاد الدولي للاتصالات تبقى شاهدا بدون منازع على ما تقدم من طرح، والسبب في ذلك (كثرة الصعوبات والعراقيل البيروقراطية)، نفس الوضع، يمكن ملاحظته من خلال الفوارق الموجودة في القياسات العالمية بين الدول المتقدمة ودول العالم الثالث، وهذا بدورة يعطي صورة واضحة عن غياب التعاون الخارجي.

- عدم جدية التعاون داخليا وما الأرقام المصرح بها من طرف أجهزة الأمن عن نسبة الاختراقات المتزايدة لدليل على عدم قدرة هيئات التنسيق على إدارة ملف الأمن السيبراني.

أمام هذه التحديات، لجأت الجزائر في بداية الامر إلى التعامل مع هذه الجريمة من خلال تفعيل المبادئ العامة المتعارف عليها عالميا في مجال مكافحة الجريمة (تبادل المعلومات، تبادل الخبرات والمساعدة الفنية).

أولاً- تبادل المعلومات:

مع انتشار وتصاعد النشاط الاجرامي الالكتروني ونظرا لتعقيدات التحكم في هذا المجال، سارعت الجزائر إلى تفعيل الاحكام المتعلقة بتبادل المعلومات والمساعدة التقنية التي تعتبر من المبادئ العامة التي اعتمدتها العديد من الصكوك الدولية، وأوصى بها مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، وتعتبر هذه الوسيلة (المعلومة) من الجانب الوقائي عنصراً جوهرياً وقاعدة أساسية لمتابعة الجريمة الالكترونية، أما من الجانب العقابي فإن المصالح الخاصة بمكافحة الجريمة والأجهزة القضائية يستندون عليها كإحدى الدعائم الموثوقة لتنفيذ القوانين في كافة المجالات [52].

ثانياً-تبادل الخبرات والمساعدة التقنية:

في نفس الإطار، وبغية تحقيق التكامل بين المؤسسات الأمنية والقضائية العربية، وسعت الدولة من دائرة التقارب لتشمل تبادل الزيارات الميدانية، الدورات التكوينية واللقاءات التشاورية في المجالات التي شملتها السياسة الجنائية لمكافحة الاجرام عامة والاستفادة من خبرات بعض الدول العربية والتعرف على البيئة التشريعية التي ينشطون فيها وكذا الاليات التقنية المستعملة في مواجهة الفضاء السيبراني و القدرات البشرية المسخرة لهذه المهمة.

كما تشمل هذه الخطوة، العمل الميداني المتضمن المساعدة التقنية الثنائية والمتعددة الأطراف التي تخص الأنابة القضائية وتسليم المجرمين (حالات تستدعي تشريعا خاصاً للإحاطة بكافة الضمانات القانونية من الجوانب الموضوعية والإجرائية)، ورغم الصعوبات التي تواجهها العديد من الدول في تحقيق التسليم نظرا لارتباط إجراءاته بالسيادة الوطنية من جهة، وعدم التزام بعض الدول المطالبة بالتسليم بالتنفيذ

حجة حقوق الأنسان من جهة ثانية، إلا أن الدول استطاعت أن تتخطي هذه العقبات، وأبرمت اتفاقيات تعاون قضائية خاصة في إطار ثنائي ومتعدد الأطراف[53].

ثالثاً- مبادرة مركز البحوث والدرا سات القانونية والقضائية:

مع التطور المذهل لثورة المعلومات وتزايد نسبة الجرائم السيبرانية، سارعت الجزائر كذلك إلى توقيع العديد من الاتفاقيات الثنائية والمتعددة الاطراف مع الدول العربية في إطار الاتفاقية العربية لمكافحة الارهاب لسنة 1998والاتفاقية العالمية لمكافحة الجريمة المنظمة العابرة للحدود لسنة 2000، وتعزيز التعاون بين الدوائر المختصة لوضع مقاييس ومعايير مطابقة لبرامج الأمن والسلامة المعلوماتية العالمي لضمان الأمن السيبراني الوطني من جهة وتحضير الأرضية لسن تشريع خاص بالجرائم السيبرانية، كما دعمت كل المبادرات المطروحة لمواجهة الظواهر الاجرامية عامة والجريمة الالكترونية خاصة، ومن بين الإسهامات المحسوبة للجزائر "المشاركة بفريق من خبراء القانون في العديد من الدورات لأشغال مركز البحوث التابع للجامعة العربية لمناقشة مشاريع القوانين والاتفاقيات المطروحة للتكيف مع التطورات المتسارعة، لا سيما في المجال التكنولوجي، ومن بين المشاريع المنجزة (الاتفاقية عربية لضمان أمن وسلامة الفضاء السيبراني)[54].

- المحاور الكبرى التي تناولتها الاتفاقية:

- بناء الثقة في الفضاء السيبراني، يعتبر الهدف الأساسي للاتفاقية.

- تسخير طاقات تقنيات المعلومات والاتصالات لخدمة النمو والتطوير الأنساني.

- حماية أمن المجتمعات العربية في العصر الرقمي، من خلال التعاون بين الحكومات العربية، و إقرارها للأطر التشريعية والتنظيمية الملائمة والمنسجمة، التي تتضمن تبادل المعلومات بين الأجهزة المعنية، وتظافر جهود السلطات القضائية لمكافحة الجريمة السيبرانية[55].

- على المستوى الاوروبي:

لتجسيد مبدأ الشراكة الاورو متوسطية الذي وقعت عليه الجزائر مع الدول الاعضاء في الوحدة الاوروبية بتاريخ 2002.04.22 المتضمن التعاون في المجال الأمني والقضائي لمحاربة مختلف الجرائم، وكذا الاتفاق المبرم مع فرنسا بتاريخ 2003.10.25 المتضمن التعاون في مجال الأمن ومكافحة الاجرام المنظم، انطلقت الجزائر في خطوة جديدة بعنوان"التعاون لمواجهة الجرائم السيبرانية في الضفة الجنوبية"، للاستفادة من التجربة الاوروبية، وعقدت في هذا الشأن، عدة لقاءات في الجزائر جمعت فريق من الخبراء من مختلف المؤسسات الفاعلة في هذا المجال وخبراء اجانب، وانتهت المشاورات بمجموعة من التوصيات، من بينها:

- تعزيز المنظومة القانونية ومطابقتها للتشريعات الدولية (اتفاقية بودابست)[56] للرد على تحديات الاجرام السيبراني سواء على المستوى الوطني، الجهوي أو الدولي مع احترام مبدأ السيادة الوطنية وحقوق الأنسان.

- تعزيز الامكانيات المادية والبشرية للمؤسسات الأمنية المكلفة بمواجهة الاجرام السيبراني، وكذا التنسيق بين ذات المصالح والهيئات المشرفة.

- استعمال الدليل الالكتروني كمعيار للقيام بالإجراءات القضائية الصحيحة.

- الديمومة في تكوين الإطارات الأمنية والقضائية وفق المناهج العلمية المعتمدة دوليا لتسهيل عملية التأقلم مع التطورات الحاصلة في الميدان.

- الإسراع في رسم استراتيجية فعالة تتضمن كل الجوانب التنظيمية، العملية والتقنية لتدارك الأخطار الناجمة عن هذه الجرائم.

- على المستوى الدولي:

مع الأنفتاح الذي عرفه العالم بعد الحرب الباردة، أضحت كل المعاملات تخضع إلى مبدأ الحرية في التنقل لأي نقطة في العالم (اقتصاد الأنترنت) بأقل تكلفة وذلك من خلال ما توفره التكنولوجيا من وسائل اتصال، ومع مرور الزمن أصبحت هذه الوسيلة في متناول الجميع، بالمقابل تزايد النشاط الاجرامي الالكتروني، مما استدعى من المجتمع الدولي التحرك للحد من هذه التهديدات التي باتت تشكل خطرا على الحريات الفردية والسلامة الجماعية (السلم والأمن الدوليين).

من هذا المنطلق وأمام تصاعد الاهتمام العالمي بهذا العالم الافتراضي، توجهت الهيئات المتخصصة سواء على المستوى الدولاتي (الشركات المتعددة الجنسيات) أو على المستوى الامي (الاتحاد الدولي للاتصالات) بوضع مقاييس وضوابط لحماية البيانات، سلامة التحويلات الالكترونية في جميع المجالات، (حوكمة الأنترنت)، كما تم وضع مناهج وأليات للحماية من الجريمة السيبرانية وتداعياتها المستقبلية[57]، ومن بين الخطوات المسجلة نذكر ما يلي:

1- أوكلت مهمة متابعة قضايا التنمية من أجل تحسين الخدمة في ضل المرونة التي توفرها تكنولوجيا الاتصالات عامة والأنترنت خاصة إلى المجلس الاقتصادي الاجتماعي التابع لهيئة الامم المتحدة.

2- نفس المهمة أوكلت إلى اللجنة الخاصة المكلفة بالعدالة الجنائية ومنع الجريمة لمتابعة الجهود الدولية في مكافحة ومنع الجرائم الوطنية والعابرة للحدود (الجرائم الالكترونية).

3- تم التوقيع على مذكرة تفاهم بين المكتب الامي المكلف بالمخدرات والجريمة والاتحاد الدولي للاتصالات للاستفادة من خبرة هذا الاخير لمساعدة الدول لاتباع الاجراءات الملائمة للحد من المخاطر التي تشكلها الجريمة السيبرانية.

4- توجت المجهودات الدولية بصدور سنة 2000 من جامعة ستاتدفورد (الولايات المتحدة الامريكية) على مسودة اتفاق عالمي حول مكافحة الإرهاب الالكتروني والتي بفضلها تم فتح مجال جديد لتجسيد التعاون دولي لمواجهة الجرائم السيبرانية.

5- أصدرت الأمم المتحدة 2002 العديد من القرارات المتضمنة إرساء ثقافة الأمن في الفضاء السيبراني من خلال التحسيس الدول على تكثيف التعاون لحماية البنية التحتية للمعلومات وتفعيل سياسات موجهة الارهاب الإلكتروني[58].

6- تم إنشاء سنة 2004 مجموعة الخبراء الحكومية GCE وفريق دولي بهدف مناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات الدولي والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية[59].

7- حثت الهيئة الأممية المختصين بالأجرام المرتبط بالأنظمة المعلوماتية في المؤسسات العمومية والخاصة للبحث من أجل تحديد الإطار العقابي لهذه الجرائم، وجاءت هذه التوصيات خلال المؤتمر الحادي عشر حول الوقاية من الجريمة والعدالة الجنائية المنعقد في العاصمة التايلاندية في الفترة الممتدة بين18-2005.02.25 .

8- سياسة التحسيس التي اعتمدها المجتمع الدولي للوقاية من أخطار هذه الجريمة، انتهت إلى إصدار قوانين أو عقد اتفاقيات لمكافحة الإجرام، تبادل المعلومات والمساعدة الفنية بين العديد من الدول.

هذه الخطوات وغيرها كان لها أثر إيجابي ومباشر على الاستراتيجية الجزائرية التي تفاعلت مع كل صور التعاون الدولي بمختلف مظاهره خاصة وأن معدل الاختراقات على الشبكة العالمية للمعلومات، وعلى الأنظمة المعلوماتية الوطنية بلغ درجات من الخطورة المهددة للأمن الوطني، القومي والعالمي[60].

الخاتمة:

من خلال المعطيات والارقام التي تم تداولها في هذه الورقة البحثية وبعد التحليل الموضوعي لمختلف الجوانب، توصلنا إلى النتائج التالية:

1- الجريمة السيبرانية جعلت من كل الأنظمة المعلوماتية للمؤسسات السيادية، الشركات الكبرى، المراكز المالية والحسابات الخاصة للأفراد عرضة للاختراق والتهديد من أجل الابتزاز، المساومة والتجسس، رغم ما توفره الدولة من وسائل مادية، التقنية والبشرية للحماية.

2- الصراعات الدولية أصبحت حافز رئيسي لطغيان الجريمة السيبرانية على جميع مجالات الحياة، لدرجة أن المخاطر الأنية والمستقبلية قد بلغت مستويات من شأنها المساس بالأمن الوطني، القومي والعالمي، مما يستدعي إطلاق صفرات الأنذار لإعادة النظر في المنظومة الأمنية.

3- ردود الافعال المطالبة بإرساء أليات فعالة للتعاون، تأكد أهمية الضغوط المجتمعية لحمل الحكومات على تجاوز حواجز الصراع للحد من المخاطر، وما تبذله الدول من مجهودات إنما هو استجابة لهذه المطالب للحد من مخاطر الهجمات السيبرانية، إلا أن العقبات المصلحية والصراعات بين الفاعلين في المجال وقفت عائقًا، مما جعل من القابلية العطب ترافق كل المبادرات منذ اطلاقها.

4- كافة المؤشرات تنبئ أن الجريمة السيبرانية في طريقها إلى الازدياد وإذا أضفنا لها الأوضاع الأمنية المتردية من جراء التهديدات اللأتماثلية، فإن الوضع بالنسبة للجزائر أصبح صعب من الناحية الأمنية خاصة في محيطها المغاربي، المتوسطي والأفريقي.

5- القصور في البنية التشريعية والتنظيمية وعدم إلمام قوانينها بمختلف الاجزاء المكونة للثورة المعلوماتية (التعاملات البنكية، الشبكة العنكبوتية) والتوجه نحو الاجراءات الردعية والتدابير الوقائية للحد من القرصنة، أثبت عدم التحكم في تكنولوجيات الاعلام والاتصال.

الاقتراحات:

1- الاسراع في رسم استراتيجية شاملة، تعمم فيها ثقافة مواجهة الأخطار في أوساط مستخدمي تكنولوجيا الاعلام سواء في القطاع العام أو الخاص للتفاعل مع الاجراءات العملية والأمنية لمكافحة القرصنة، مع تنظيم دورات تكوينية في التطبيقات الصحيحة لاستغلال ثورة المعلومات وفق المواصفات الدولية التي أوصت بها علامة أيزو والاتحاد الدولي للاتصالات، مع إشراك كل الفاعلين في المجال الأمني والمعلوماتي.

2- تطوير التشريعات السيبرانية تماشيا مع التطورات الحاصلة في عالم التكنولوجيا، من أجل بناء مجتمع معرفي، مع غلق كل منافذ الخطر والتهديد، تسهيل التعاملات في جميع المجالات، تحفيز التكامل داخليا وخارجيا، تدعيم التعاون الفعلي لمواجهة المخاطر وبالتالي تأهيل المناخ لحد من الجريمة وحماية الأنظمة المعلوماتية.

3- الانضمام الى الاتفاقيات الدولية في مجال حماية الأنظمة المعلوماتية على غرار اتفاقية بودابست، مما يحفز على التنسيق والتعاون مع الناشطين من خبراء ومؤسسات في ميدان الأمن السيبراني إقليميا ودوليا، المواظبة على المشاركة في اللقاءات العلمية والدورات التكوينية للاستفادة من الخبرات في مجال التوظيف والاستغلال العقلأني لعالم التكنولوجيا.

الهوامش:

(1) يعتبر جون بيربارلو، الشاعر الأمريكي الذي وافته المنية شهر فيفري 2018، من أهم الرواد في هذا المجال، فبعد تأسيسه لمؤسسة الحدود الالكتروني سنة 1990 وبعد صدور قانون ينظم الاتصالات في الولايات المتحدة الامريكية سنة 1995، تحدى السلطات واعلن من دايفوس عن استقلال الفضاء السيبراني سنة 1996 وتوجه إلى السلطات بالقول" ياقادة العالم لن تمنعنا قواتكم ولا قوانينكم من ممارسة حقنا في هذا الفضاء"، للمزيد أنظر موقع عنب بلادي أولاين مقال منشور بتاريخ 2018.02.11 .

(2) في تقرير وكالة تطبيق القانون الأوروبية، بخصوص هجوم قراصنة الويندواز في أكثر من 100 دولة بتاريخ 12 مايو 2017، تبين أن كبريات الدول كانت من بين المستهدفين على غرار روسيا، والهند، والصين، وبريطانيا، وفرنسا، وإيطاليا، وألمانيا، والبرتغال، وفيتنام، وتايوان، بحيث استطاعت جماعة وسطاء الظل من إطلاق برمجية الفدية الخبيثة التي يطلق عليهاWanna Cry، والتي تسببت في تعطيل تعاملات وخدمات مؤسسات متعددة وإعطاب شبكاتها وأجهزتها الإلكترونية، و تكبيد الدول خسائر مالية ضخمة.

(3) الشبكة المعلوماتية ARPA The Advanced Research Project Administration التي أنشأتها وزارة الدفاع الامريكية، كانت تهدف من خلالها إلى تسهيل التواصل بين الادارة مع متعهدي القوات المسلحة، وعدد كبير من الجامعات، لكن الاستخدام الكثيف للشبكة، من قبل الجامعات ومراكز الابحاث، أدى إلى ازدحام حركة العمل عليها، فأنشئت شبكة جديدة في العام1983 ، سميتMILNET ، أي الشبكة العسكرية، وخصصت لخدمة المواقع العسكرية، وتم ربطها بواسطة بروتوكول الأنترنت مع الشبكة الام (ARPA).

(4) Le terme cybernétique (en anglais cybernetics), formé à partir du mot grec κῠβερνήτης (kubernêtês) « pilote, gouverneur », Voir à ce sujet. Le site internet Wikipedia

(5) عادل عبد الصاد، "الفضاء الإلكتروني والرأي العام : تغير المجتمع والأدوات والتأثير"، المركز العربي لأبحاث الفضاء الإلكترونى :قضايا استراتيجية، 2013، العدد 2459.

(6) Dans son livre « Cybernetics or control and communication in the Animal and the machine » .publié en 1947, il a proposé ce concept pour promouvoir une vision unifiée des domaines naissants de l'automatique, de l'électronique et de la théorie mathématique de l'information.

(7) National Cyber Security Strategy 2016 -20121 UK, page 16.

(8) 8Martti Lehto,Pekka Neittaanmäki, "Cyber Security: Analytics, Technology and Automation, edition springer (USA), 30.05.2015.

(9) يحصي المختصون في الأمن الرقمي أكثر من 300 ألف عينة لفيروسات وبرامج ضارة في اليوم، ما يشكل تهديدا مستمرا للكائن البشري خاصة وأن عمليات الاختراق تهدف إلى الحصول على بيانات شخصية للاستهلاك على غرار الاسم والعنوان الالكتروني والمنزلي وتاريخ الميلاد ومعلومات الهوية لبطاقات الائتمان والصحة.

(10) في عام 2010 ظهر ما يعُرف باسم "إعصار ويكي ليكس" الذي استغل شبكة الأنترنت العالمية لتسريب وثائق سرية للغاية مُتداولة بين الإدارة الأمريكية وممثليتاها بالخارج.

-في مارس 2014 هاجمت مجموعة "سايبر بيكوت الأوكرانية" المواقع الإلكترونية للحلف الاطلسي، مما أدى إلى تعطيل مواقع الحلف لعدة ساعات.

-أكدت صحيفة نيويورك تايمز في تقرير لها في 26 إبريل 2015 أن قراصنة روسيين اطلعوا على رسائل إلكترونية للرئيس الأمريكي باراك أوباما العام الماضي، بعدما تمكنوا من اختراق الشبكة الإلكترونية غير السرية للبيت الأبيض، واطلعوا على أرشيف الرسائل الإلكترونية لموظفين في البيت الأبيض الذين يتواصلون يومياً مع أوباما، للمزيد أنظر شيرهان نشأت المنيري،"مخاطر جرائم الأنترنت على استقرار النظام الدولي"،مجلة السياسة الدولية.

(11) يونس عرب، "جرائم الكمبيوتر والأنترنت، المعنى والخصائص والصور واستراتيجية المواجهة القانونية"، المركز الوطني للتوثيق، أكتوبر 2006

(12) د.عبد الفتاح بيومي حجازي،" الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت"، دار الكتاب القانونية، مصر، دون تاريخ النشر، ص9 .

(13) هدى حامد قشقوش،" جرائم الحاسوب الالكتروني في التشريع المقارن"، القاهرة، دار النهضة العربية للنشر والتوزيع، 1992، ط.1 ص11 .

(14) Cheval de Troie: programme qui exécute des instructions sans l'autorisation de l'utilisateur, instructions qui lui sont généralement nuisibles en communiquant par exemple à l'extérieur. Il prend l'apparence d'un programme valide mais il contient en réalité une fonction illicite cachée, grâce à laquelle il contourne les sécurités informatiques. Il pénètre ainsi par effraction dans les fichiers de l'utilisateur pour les modifier, les consulter ou même les détruire.

(15) موقع ويكي ليكس لم يعلن بوضوح عن حجم التسريبات كلها ولكن أفاد أن جهاز الاستخبارات الأمريكية" سي أي أيه"، يتجسس على العالم، أما عن طريقة الاختراق التي يقوم بها محترفو الاجهزة فتكون عن طريق هجمات اليوم صفرZero Day Attack ، وهي برمجة خبيثة تستعمل عند اكتشاف الثغرات في الفترة ما بين قيام الشركة بإصلاحها،كما يفيد الموقع ان هناك شبكة تجسس في وادى السيليكون في ولاية كاليفورنيا، وهى تضم غالبية شركات الكمبيوتر والمعلوماتية والأنترنت الأمريكية، كما توجد شبكة ضخمة للتجسس الإلكتروني بين الولايات المتحدة الأمريكية والعديد من الدول لرصد المكالمات الهاتفية والرسائل والمعلومات العسكرية.

(16) د. ع الفاروق،" المشكلات الهامة في الجرائم المتصلة بالحاسوب الالي وأبعادها الدولية، دراسة مقارنة" ، مصر، الطبعة الثانية، ص 15

(17) سامي علي عياد حامد،" الجريمة المعلوماتية وإجرام الأنترنت"، دار الفكر الجامعي، الاسكندرية (مصر) 2007، ص .77

(18) ميديا بنجامين" حرب الطائرات بدون طيار، القتل بالتحكم عن بعد"، ترجمة أيهم الصباغ، الدوحة (قطر) ، منتدى العلاقات العربية والدولية، 2014 ص .14.

(19) جون باسيت،"الحروب المستقبلية في القرن الحادي والعشرون"، مركز الامارات للدراسات والبحوث الاستراتيجية، 2014، الطبعة الأولى، ص .53.

(20) رفد عيادة الهاشمي،" الارهاب الالكتروني"، عدم وجود البلد وسنة الإصدار، ص.00 .

(21) أيسر محمد عطية، " دور الآليات الحديثة للحد من الجرائم المستحدثة : الإرهاب الالكتروني وطرق مواجهته"، الملتقى العلمي . عمان (الاردن)، 02-04 ديسمبر 2014، ص.9 .

(22) Daniel Ventre, « La cyber paix, un thème stratégique marginal », Cairo.Info, 2012, p.83

(23) د-عادل عبد الصادق،" أنماط الحرب السبرانية وتداعيتها على الأمن العالمي"، مركز الاهرام للدراسات السياسية والاستراتيجية، القاهرة، .2017.05.14

(24) مشبب ناصر محمد أل زيران،" المواقع الالكترونية ودورها في نشر الغلو الديني وطرق مواجهتها من وجهة نظر المختصين"، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض (المملكة العربية السعودية)، 2011، ص .19

(25) حسب المتتبعين لشأن التونسي فإنه تم إحصاء منذ أحداث الربيع العربي ودخول البلد دوامة الارهاب، انضمام حوالي 3400 شاب بالتنظيم، الارهابي داعش وتمثل هذه الفئة حوالي40 ٪ من مجموع الشباب المستقطب من بين الطلبة الذين يدرسون الاختصاصات العلمية

كالطب،الفيزياء والكيمياء، كما تم استدراج التلاميذ المتفوقين الذين تتراوح أعمارهم بين 17 و 28 سنة ء حيث يقوم التنظيم باستغلال مهاراتهم العلمية لأغراض تخريبية داخليا أو خارجيا (العراق، سوريا وبعض الدول الاوروبية).

(26) د.ذيب بن عايض القحطاني،" أمن المعلومات"، مدينة الملك عبد العزيز للتعليم والتقنية، الرياض (المملكة العربية السعودية)، 2015، ص58.

-أنظر كذلك كتاب لإريك ليوبولد، سيرج لوست" أمن المعلومات"، ترجمة فتحي علي زمال، مدينة الملك عبد العزيز للتعليم والتقنية، الرياض، (المملكة العربية السعودية)، 2014 .

(27) حسب المحللين الأمنيين، فإن حملات الهاكرز اليوغسلافيين على مواقع الناتو ابان ضربات هذا الاخير خلال حرب الكوسوفو 1998، تعتبر من قبيل حرب معلومات، كما وصفت هجمات المخترقين الأمريكان الناشطين في جمعيات الدفاع عن حقوق الأنسان على مواقع صينية بحرب معلومات مع العلم أن هذه العملية تمت بدعم من الحكومة الأمريكية.

(28) أصبحت تكنولوجيا المعلومات والاتصالات جزءا لا يتجزأ من الحياة اليومية لكثير من الأشخاص في أنحاء العالم والاتصالات الرقمية والشبكات والأنظمة تقدم موارد حيوية وتمثل بنية تحتية لا غنى عنها في كل جوانب المجتمع العالمي، وهي ضرورات لا يمكن لكثير من سكان العالم الازدهار أو حتى البقاء بدونها . وهذه الهياكل والأنظمة تمثل ميدانا جديد اً تقترن به تحديات جديدة للحفاظ على السلام والاستقرار . وبدون آليات كافلة للسلام فإن مدن العالم ومجتمعاته ستكون عرضة لهجمات تتسم بتنوع غير مسبوق وغير محدود .وهذه الهجمات يمكن أن تأتي دون مقدمات .فالحواسيب والهواتف الخلوية تتوقف عن العمل فجأة كما أن شاشات آلات صرف النقد والآلات المصرفية تنطفئ في وجه العملاء وتتعطل أنظمة مراقبة الحركة الجوية والسكك الحديدية وحركة السيارات وتعم فوضى الطرق السريعة والجسور والممرات المائية وتتوقف السلع غير المعمرة بعيد اً عن السكان الجائعين . ومع اختفاء الكهرباء تهوي المستشفيات والمساكن والمراكز التجارية بل ومجتمعات بأكملها في غياهب الظلام . ولن تستطيع السلطات الحكومية معرفة مدى الضرر أو الاتصالات ببقية العالم لإبلاغه بالكارثة أو حماية مواطنيها الضعفاء من الهجمات التالية .وهذه هي المحنة القاسية التي يواجهها مجتمع تعرض للشلل بسبب ضياع شبكاته الرقمية في لحظة واحدة .وهذا هو التدمير الذي يُمكن أن ينجم عن نوع جديد من الحروب هي الحرب السيبرانية.

(29) د.منى الأشقر جبور، السيبرانية هاجس العصر"، الجامعة العربية، دون تاريخ النشر.

(30) عبد الله بن عبد العزيز بن فهد العجلأن،" الارهاب الالكتروني في عصر المعلومات"، المؤتمر الدولي الاول حول حماية المعلومات والخصوصية في قانون الأنترنت، القاهرة (مصر)، 02-04 جوان 2008 . في هذا الاطار، يحصي الخبراء، أنه أكثر من 70 ٪ من الاجهزة لا تستعمل أي احتياطات أمنية خلال تحميل للبرمجيات أو تخزين للبيانات لتفادي اختراقات قراصنة المعلوماتية.

(31) مثل هذه الفجوات أثارت جدل في الاوساط التقنية وقد أشار إدوارد سنودن، العامل السابق مع وكالة الاستخبارات الأمريكية، في إحدى مداخلته أن المسؤولية ملقاة على عاتق وكالة الأمن القومي الأمريكي التي لم تكشف عن الثغرات المتسببة فيها لحظة اكتشافها.

(32) Daniel Ventre, « la Stratégie américaine en matière de sécurité Février 2015 », étude réalisée pour le compte du CNRS, publiée par la Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris, en Avril 2015.

(33) حسب تصريحات وكالة تطبيق القانون الأوروبية فإن هذا الهجوم اكتسى طابعًا استثنائيًا، لسببين الاول" لم يسبق وإن سجلت مثيل لهذا الهجوم، الثاني: بينت الوقائع بالدليل عن وجود ثغرات في الأمن الرقمي العالمي، خاصة وأن هذه الجماعة سبق أن أعلنت في أغسطس 2016 أنها اخترقت وكالة الأمن القومي الأمريكي، واستحوذت على" أسلحة إلكترونية" قدّرتها بقيمة 500 مليون د ولار، كما عرضت تلك البرمجيات الخبيثة للبيع في مزاد تحت اسم "مزاد الأسلحة السيبرانية لمجموعة التسوية"، كما بعثت رسالة في شهر أفريل تحتج فيها على الرئيس الامريكي دونالد ترامب مشهرة في ذلك برنامج للتجسس على التحويلات المالية التي تحصلت عليها من خلال اختراقها لأجهزة وكالة الأمن القومي الامريكي.

(34) أغلب الصحف العالمية، خاصة منها الامريكية، اتهمت الرئيس الامريكي دونالد ترامب أنه قام بعمل لاأخلاقي عندما رفض الدفاع عن أمريكا أثناء لقاءه مع الرئيس الروسي بوتين في هلسنكي 2018.07.16، بل أخطر من ذلك وضع نفسه تحت أقدام خصمه بعد ما برأه من حادثة التجسس عن الأنتخابات، للمزيد أقرأ ما جاء في الصحافة العالمية على الرابطWWW.M.ARABI21.COM ، تاريخ المراجعة 2018.07.20 .

(35) أنظر فعاليات المؤتمر الدولي السنوي حول تحديات الأمن السيبراني الذي نظمته مؤسسة فيرتشووبوت في الرياض (المملكة العربية السعودية) بتاريخ 2017.11.23، الخاص بمنطقة الشرق الأوسط وشمال افريقيا والذي ضم حوالي 400 مختص في المجال، للمزيد أنظر جريدة أيلاف الصادرة بلندن، تاريخ التفحص 2018.03.15 .

(36) مصطفى محمد موسى،" الإرهاب الالكتروني دراسة قانونية-أمنية–نفسية– اجتماعية"، الأردن :دار الكتب والوثائق القومية،الطبعة الاولى، 2009، ص.298.

(37) Le législateur algérien a pris en considération certaines dispositions de la législation française de 1988, voir à ce sujet, André Lucas, Jean Devrèze, Jean Frayssinet, Droit de l'informatique et de l'Internet, édition Dalloz, collection Thémis (Droit Privé), Novembre 2001, (France), page 679.

(38) بعد أحداث الحادي عشر سبتمبر 2001، أثبتت المعلومات المتحصل عليها من عديد المصادر، أن التنظيمات الارهابية وعلى رأسها القاعدة كانت تستعمل قواعدها الخلفية في أفغانستان للتدريب البدني والفكري مستغلة في ذلك التكنولوجيا الحديثة، للتواصل،لجمع المعلومات ونقل الرسائل و التوجيهات بطريقة سرية إلى جميع أنحاء العالم .بعد فرض حصار عالمي على التنظيم، استغل نظام الطالبان هذا الفراغ للاستفادة من تجربة ممن سبقوه في توظيف الجيل الخامس وثورة المعلومات، ليس لتمرير رسائل، لكن للقيام بالدعاية لأعماله الإرهابية ضد قوات التحالف في أفغانستان، فقام بتأجير موقع إلكتروني تابع لشركة أمريكية في تكساس، بمبلغ 70 مليون دولارًا في الشهر، ويتم الدفع بواسطة بطاقة الائتمان ليتم التواصل مع أكثر من 16 مليون حساب مستخدم، ودامت العملية لأكثر من سنة .

(39) هذه الأرقام تم الحصول عليها من الوزارة الوصية حصيلة سنة 2017، وتمثل حسب الخبراء زيادة 64٪ بالنسبة لسنة 2016، هذا إذا أخذنا بعين الاعتبار عدد السكان الذي يقارب 41 مليون نسمة، مع الإشارة أن معدلات استغلال تكنولوجية الاتصال بالجزائر في زيادة مستمرة والدليل أن نسبة استعمال الهاتف عموما (الثابت، الخلوي) قد وصلت إلى نسبة 115٪ لتخصم منها نسبة 39 ٪ موجها للاستغلال في شبكات التواصل الاجتماعي.

(40) خلال الندوة الافريقية حول حوكمة الأنترنت (CAGI)، المنعقدة بالجزائر بتاريخ 2017.02.21، بحضور 27 دولة إفريقية والعديد من المنظمات الجهوية BAD, UIT, UA ، ذكرت ممثلة الحكومة الجزائرية وزيرة البريد وتكنولوجيات الاتصال، أن البلاد متمسكة بالمبادئ العامة التي نصت عليها هيئة الأمم المتحدة، للمزيد من المعلومات، انظر الرابطwww.lemaghrebdz.com ،تاريخ 2017.02.22.

(41) أستاذ شريف بسام،" واقع الحوكمة الالكترونية في الدول العربية "مجلة العلوم الاجتماعية والأنسانية، جامعة الجزائر 3، العدد السادس، جوان 2016، ص .157.

-أنظر فعاليات المؤتمر الدولي" الأمن السيبراني والدفاع السيبراني، تحديات وافاق"، المنظم من طرف الجامعة اللبنانية والوكالة الجامعية للفرنكوفونية 23.10.2017 موجود على الرابط. www.ul.edu.lb .

(42) الاتحاد الدولي للاتصالات، "تأمين شبكات المعلومات والاتصالات، أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني"، لجنة الد راسات، التقرير النهائي (الفترة 2014-2017)، جنيف (سويسرا)، افريل 2017 .

(43) ب . بوعلام، " الجيش الوطني الشعبي ورهانات تداول المعلومة عبر شبكات التواصل الاجتماعي"، مجلة الجيش، العدد603 ، جانفي 2016 .

-الهام غازي، "الوقاية ومكافحة الجريمة المعلوماتية في التشريع الجزائري"، مجلة الجيش، العدد603 ، جانفي 2016 .

(44) أنظر الحوار الذي أجرته مجلة الجيش مع المسؤول المباشر على مصلحة الأمن السيبراني في المؤسسة العسكرية،" فضاء العمليات"، العدد 651، أكتوبر 2017، ص.34-35 .

(45) الاتحاد الدولي للاتصالات، "تقرير حول الأمن السيبراني للدول النامية"، مكتب تنمية الاتصالات، جنيف (سويسرا) أفريل 2016 .

(46) في إطار الشراكة لمحاربة الجريمة الالكترونية، نظم بالجزائر العديد من اللقاءات مع خبراء ومختصون أجانب، خاصة من دول الاتحاد الأوروبي، وحسب النتائج المتوصل إليها، تبين أن المصالح المركزية لوزارة البريد والتكنولوجيات الاتصال، تفتقر إلى مصلحة التحليل البيانات ذات المقاييس العالمية التي بفضلها يمكن لأجهزة الأمن تحديد الوجهة لمعرفة مرتكبي الجرم، وإذا كان مركز البحث حول المعلومات العلمية والتقنية التابع لوزارة التعليم العالي والبحث العلمي CERIST هو القائم بمهمة التحليل، فهذا لا يعني حسب الخبراء الاستغناء عن فكرة خلق مصلحة التحاليل في اقرب وقت، لأن التهديد الذي تواجهه الجزائر مطابق لما تعيشه الدول المتقدمة.

(47) أُنشئ الاتحاد الدولي للاتصالات في 1865 في باريس تحت اسم الاتحاد الدولي للبرق ثم أخذ اسمه الحالي سنة 1939، ليصبح وكالة متخصصة تابعة للأمم المتحدة ابتداء من سنة 1947، يقوم الاتحاد الدولي للاتصالات منذ نشأته على الشراكة بين القطاعين العام والخاص، ويبلغ عدد الأعضاء فيه حاليا 193 بلدا وما يزيد على 800 هيئة من القطاع الخاص والمؤسسات الأكاديمية .ويقع مقر الاتحاد في جنيف، سويسرا، ويضم 12 مكتباً من المكاتب الإقليمية ومكاتب المناطق في جميع أنحاء العالم، ويمثل أعضاء الاتحاد مجموعة واسعة من قطاع تكنولوجيا الاتصالات في العالم من شركات التصنيع وشركات التشغيل، بالإضافة إلى مؤسسات البحوث والتطوير الرائدة والدوائر الاكاديمية.

(48) الدول الرائدة في مجال الحماية الالكترونية هي: سنغافورة، الولايات المتحدة الامريكية، ماليزيا، سلطنة عمان، أستونيا، أستراليا، جورجيا، فرنسا وكندا، أما عربيا، فالدول التي احتلت المراتب الثمانية الاولى هم: سلطنة عمان (04 عالميا)، جمهورية مصر (14 عالميا)، قطر (25 عالميا)، تونس (40 عالميا)، المملكة العربية السعودية (46 عالميا)، الامارات العربية المتحدة (47 عالميا)، المملكة المغربية (49 عالميا) واخيرا البحرين (65 عالميا).

(49) د.بن مرزوق عنترة، أ.حرشاوي محي الدين، "الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية"، تاريخ الفحص 2018.04.04 .

-أنظر كذلك المؤشر العالمي للأمن السيبراني GCI النسخة الثانية الصادرة عن وكالة الامم المتحدة للاتصالات 2017.07.05.

(50) الملتقى الدولي الموسوم بعنوان "الدفاع السيبراني مكون اساسي للأمن والدفاع الوطني"، المنظم من طرف قيادة الاركان للجيش الوطني الشعبي، بتاريخ 15-2017.05.16 وكذلك الندوة الدولية المنظمة من طرف قيادة الدرك الوطني بتاريخ 27-2017.03.28، في طبعتها الثانية تحت عنوان "الخدمات الالكترونية والأمن العمومي".

(51) في قراءة للاتفاقية العربية لمكافحة جرائم تقنية المعلومات المبرمة في 2010.120.21، يتضح ان التهديدات الخطيرة التي تسببها الجرائم الالكترونية للمساس بالأمن والاستقرار، اصبحت تشكل إحدى أهم الاهتمامات لدى صناع القرار للدول العربية

(52) من بين الاتفاقيات المتعددة الاطراف (اتفاقية الرياض العربية للتعاون القضائي) التي وافق عليها مجلس وزراء العدل العرب في المؤتمر العربي الاول بتاريخ أفريل 1983، التي قضت في المادة الاولى على ضرورة تبادل المعلومات بين الدول الاطراف فيما يتعلق بالنصوص التشريعية والتنسيق بين الأنظمة القضائية كما قضت المادة الخامسة منها بأن ترسل وزارة العدل في الدول الاطراف أخر بيانات الاحكام القضائية النهائية الصادرة ضد المواطنين أو الاشخاص المولودين أو المقيمين في إقليميا.

(53) د.أبو المعالي محمد عيسى، "الحاجة إلى تحديث أليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية"، مداخلة في المؤتمر المغاربي الاول حول (المعلوماتية والقانون)، طرابلس (الجماهيرية الليبية)، 2009.10.28.

(54) أنظر محتوى الاتفاقية العربية لبناء الثقة في الفضاء السيبراني، وكذلك التوصيات الصادرة عن المؤتمر الرابع للمتخصصين في الأمن وسلامة الفضاء السيبراني (الأنترنت)، المنعقد في مقر المركز العربي للبحوث القانونية (الجامعة العربية)، بيروت (لبنان) 2015.08.19 .

(55) د. منى الأشقر جبور، "الأمن السيبراني، التحديات ومستلزمات المواجهة"، اللقاء السنوي الاول للمختصين في امن وسلامة الفضاء السيبراني، بيروت (لبنان)، 27-2012.08.28، ص.24 .

(56) إتفاقية بيدابيست الاوروبية حول الاجرام المعلوماتي المصادق عليها من طرف المجلس الاوروبي بتاريخ 2001.11.23، دخلت حيز التنفيذ سنة 2004، تعتبر بمثابة الارضية القانونية التي اعطت دفعا للدول الاوروبية خاصة ودول العالم عامة، للإسراع في سن قوانين وفرض إجراءات قانونية وإدارية لمحاصرة الاجرام السيبراني، خاصة وان اهم معضلة تواجه التعاون الدولي "تسليم المجرمين والأنابة القضائية)، قد تم الفصل فيها.

(57) في دليل الأمن السيبراني للبلدان النامية الصادر عن الاتحاد الدولي للاتصالات سنة 2017، أوصى الخبراء بإقامة حلول كافية على الصعيد الأمن والثقة، بإعتبارهم من اكبر التحديات التي يتعين على الاتحاد في أطار الجهود المبذولة لمساعدة البلدان على استعمال الاتصالات وتكنولوجيا المعلومات بطرق سلمية.

(58) نوران شفيق، "اثر التهديدات الإلكترونية على العلاقات الدولية"، القاهرة (مصر)، المكتب العربي للمعارف، 2015، ص.108.

(59) رائد العدوان، "المعالجة الدولية لقضايا الارهاب الالكتروني، توظيف شبكات التواصل الاجتماعي في مكافحة الارهاب"، محاضرة القيت في دورة تدريبية بالرياض (المملكة العربية السعودية)، 2016، ص.09-10.

(60) les Etats-Unis-d 'Amérique, dispose d'un commandement militaire pour la cyberspace, selon le porte-parole du pentagone « les risques liés au cyber sécurité figurent parmi les défis économiques et de sécurité nationale les plus sérieux du XXIe siècle » . Voir le site www.elwatan.com/article: les USA-se-dotent-d 'un commandement…