استعدادات الجزائر لمقتضيات حروب الجيل الرابع بين الواقع والآفاق

Algeria's preparations for the requirements of fourth-generation wars between reality and prospects

الدكتور بكرارشوش محمد*

أستاذ محاضر "أ" بجامعة قاصدي مرباح ورقلة، الجزائر

bekrarchouchmohamed@gmail.com

تاريخ الإرسال: 2021/02/24 * تاريخ القبول: 2021/05/17 * تاريخ النشر: 2021/06/21

ملخص:

باتت الدول الحديثة تعتمد على المعلوماتية، وتسعى لتأمين توزيع الخدمات على مواطنيها لمواكبة العصرنة. لكن تغيب عن الدول المستهلكة للتكنولوجيا، على غرار الجزائر، استراتيجية حماية وتوعية المستهلك بالمخاطر على أمن البيانات الكترونية. وعمليا، فإنّ الأضرار المحتملة لهجوم ما، تتباين وفقا لدرجة استعداد الدولة وقدرتها الأمنية المتأصلة ببنيتها التحتية، ومن زاوية أخرى فإنّ أولوية واضعي السياسات الاستراتيجية يجب أن تركز على التصدي لأي هجوم سيبراني، ثم معرفة نوع الهجوم وهوية الخصم بسرعة، ثم التحضير للرد بالشكل المناسب وهذا يعني الاستعداد للجيل الرّابع من الحروب.

الكلمات المفتاحية:

الانترنت ، الجيل الرابع ، الحرب السيبرانية ، الردع الالكتروني ، الحدود الافتراضية.

Abstract:

Modern countries have become dependent on information technology, and seek to secure the distribution of services to their citizens to keep pace with modernity. However, technology consuming countries, such as Algeria, are absent from a strategy to protect and educate consumers about the risks to the security of electronic data. In practice, the potential damage of an attack varies according to the degree of readiness of the state and its inherent security capacity in its infrastructure, and on the other hand, the priority of strategic policy makers should focus on addressing any cyber-attack, then knowing the type of attack and the identity of the opponent quickly, and then preparing to respond appropriately and this It means preparing for the fourth generation of wars.

***Keywords**: Internet, fourth generation, cyber warfare, electronic deterrence, virtual borders.*

* مؤلف المقال المرسل.

مقدمة:

إن مواكبة الجزائر لتطورات الحرب الالكترونية والاستعداد لأي تحدي من هذا النوع الذي بات عرضة له كل مجتمع أو بلد أو كيان اقتصادي أو شخص، بصرف النظر عن مستوى التطور التكنولوجي والبنية التحتية لديه، حيث أنّ الهجوم الالكتروني استهدف أقوى البلدان وأغناها من حيث جميع الأصعدة، فلقد شاهد العالم السجال الدائر بين الولايات المتحدة الأمريكية وروسيا حول تعرّض هذه الأخيرة إلى هجمات الكترونية في مناسبتين مشهودتين عالميا، الأولى في مناسبة الانتخابات الرئاسية الأمريكية التي أسفرت عن فوز الرئيس دونالد ترامب عن الحزب الجمهوري، حيث اتهمت دوائر مخابراتية وإعلامية دولة روسيا بتدخلها في توجيه الرأي العام الأمريكي والتأثير عليه من خلال التلاعب بالآلاف من الحسابات على شبكة التواصل فيسبوك من أجل خلق رأي عام وانطباعات سياسية تؤدي إلى اختيار اتجاه سياسي معين.

والثانية عند قرب انتهاء ولاية الرئيس الأمريكي نفسه، حيث صرّحت دوائر أمن أمريكية ان الولايات المتحدة الأمريكية تعرضت منشآتها الحيوية إلى سلسلة من الهجمات الالكترونية أدت إلى انتقال بيانات هامة واتلاف أخرى وتخريب أنظمة وتعطيل بعض المنشآت، حيث أشرات الاتهامات دائما إلى دوائر سيبرانية تتبع دولة روسيا الاتحادية، فيما توعدت الولايات المتحدة الأمريكية الفاعلين بأشد العقاب والرد بالمثل.

ولقد تزايدت العمليات السيبرانية من قبل كل من الجهات الفاعلة الحكومية وغير الحكومية والوقت نفسه الذي تتصدى فيه للهجمات وتقوم بالدفاع عن شبكاتها وبنيتها التحتية، وتطور قدراتها على تطبيق مبادئ الردع للأنشطة على الإنترنت، وفي المقابل تزيد أهمية الردع السيبراني باعتباره يوفر المرونة ويزيد الخيارات من غير أدبيات الردع التقليدية التي وضعت في الحرب الباردة النووية أي الانتقام التقليدي.

ويشمل الردع الإلكتروني خيارات مثل اتخاذ الإجراءات الدفاعية وجعل الشبكات غير مرئية ومرنة ومترابطة كما يقدّم طرقا جديدة لعرض وتطبيق مبدأ الهجوم كاستراتيجية متقدمة، وهو ما يطرح قضايا قانونية كتوافق هذه الاستراتيجية مع القانون الدولي، وقانون النزاعات المسلحة، وفي هذا الاتجاه سوف نحدد ونناقش نظرية الردع السيبراني وتحليل القضايا المرتبطة بهذا المجال الحيوي لتوفير أفضل الطرق لدعم الأهداف الوطنية الجزائرية والتي ينبغي لها اتباع نهج ثلاثي في محاور استراتيجية.

تبدأ بالدفاع الإلكتروني القوي وهو الخطوة الأولى للحماية من المعتدين وثني العدو من المهاجمة، وثانيا وهو الإسناد وتعني به القدرة علي عزو الهجوم إلى مصدر محدّد للحفاظ على المصداقية وضمان الشرعية في الداخل والخارج، وثالثا الانتقام بحيث يجب ضمان الاستعداد والقدرة على الانتقام من أي مصدر هجوم تحت أي ظرف من الظروف.

وأمام هذه التحديات، فلقد اتخذت الجزائر سلسلة من الخطوات من أجل الوقاية من الهجمات الإلكترونية التي تستهدف المجتمع الجزائري والمنشآت الحيوية الاقتصادية والأمنية والعسكرية على حد سواء، توزعت هذه الخطوات بين ما هو قانوني ومؤسساتي، فالخطوات القانونية تمثلت في سن سلسلة من القوانين ونصوصها التطبيقية تهدف إلى سد الفراغ أو القصور التشريعيين في الفضاء الالكتروني، أمّا المؤسساتي فلقد قامت بإنشاء العديد من الهيئات التي تعنى بمواجهة التحديات السيبرانية لا سيما الحروب الالكترونية.

وعليه، فإنّ الإشكالية المطروحة في هذا الصدد، تتمثل في: **ما هي استراتيجية الجزائر في التصدي للحروب الالكترونية؟**

وللإجابة على هذه الإشكالية، فإنّه قد اتبعنا المنهج التحليلي، بغرض تحليل بعض المعطيات القانونية والفنية بالإضافة إلى المنهج المقارن لأهميته بالنظر إلى حداثة الموضوع وارتباطه بالتطور التكنولوجي ومسايرة الأنظمة القانونية المقارنة لذلك.

وهذا ما سنتناوله من خلال مبحثين اثنين، نتناول في الأول مسألة امتلاك الردع الالكتروني في مواجهة الحرب السيبرانية، أمّا الثاني، فخصصناه لدراسة تنفيذ الردع بين الإمكانية والاحتمالية.

المبحث الأول: امتلاك الردع الإلكتروني في مواجهة الحرب السيبرانية

يتحقق الأمن الوطني لأي دولة من خلال تبادل المعلومات عبر مختلف الهيئات الحكومية ذات الصلة؛ لحماية شبكات الكمبيوتر الوطنية، وتأمين البنية التحتية الحيوية للبلاد، وذلك من خلال إعطاء هيئة حكومية مستقلة بالتعاون مع وزارة الدفاع الوطني غالبا مزيدا من الصلاحيات لرقابة جهود الأمن السيبراني المدنية، ومكافحة الجرائم السيبرانية ضمن التعاون مع الدول الأخرى لتعقب منفذيها وهذا هو المفهوم الكلي لقوة الدولة التي ظهر فيها حرب الفضاء الإلكتروني، وبات لزاما على الدول المختلفة إعادة تقييم قوتها استنادا لهذا المتغير وتبني نظرية الردع، وفق تطور المشهد السيبراني العالمي، وما تتوافر عليه من بنى تحتية رقمية حساسة، وهذا ما سنتناوله في المطالب الآتية:

المطلب الأول: تطور مفهوم الردع الإلكتروني

مرّ مفهوم نظرية الردع بعدة مراحل أو موجات، منها الردع لتجنب الحروب عندما كانت الدول الغربية تمتلك الأسلحة النووية، وبرزت موجة ثانية مع صعود الاتحاد السوفياتي كقوة نووية وما نتج عنه من وجود عالم ثنائي القطبية، ثم مع ظهور مفهوم الدول المارقة، ظهرت موجة ثالثة من نظرية الردع، والتي ارتبطت أيضا بظهور فاعلين من غير الدول والحكومات مما تتطلب وجود تدابير وقائية.

ونظرا للعواقب الخطيرة التي قد تسببها المقاومة السيبرانية، وجد بعض الخبراء أن ثمة إمكانية لتطبيق نظرية الردع على الفضاء السيبراني، فيما أطلق عليه بـالردع السيبراني، والذي يعتمد على عنصرين هما: ردع الهجمات السيبرانية أو الردع بالمنع، والردع بالتهديد أو الردع بالانتقام.

أما الردع بالمنع، فينطوي تحته الردع بالمقاومة، والردع بالصمود، ويعني القدرة على استعادة الشيء بشكله الأصلي قبل الهجوم الذي تم، وهذا من شأنه أن يحد من المكاسب المحتملة، ويمكن أن يقنع الخصم بعدم الهجوم خاصة إذا كانت التكلفة مفرطة. ويظل الهدف من المقاومة والصمود هو تقليل خيارات الطرف الذي ينوي الهجوم، سواء من خلال بناء هياكل دفاعية يصعب التغلب عليها أو من خلال ضمان الاستعادة السريعة لأصل الشيء بعد الهجوم وقد ظهرت عدة اتجاهات لنظرية الردع الإلكتروني وهي:

الفرع الأول: اتجاه أول يرى عدم جدوى نظرية الردع على صعيد الفضاء السيبراني، مشككا في جدواها وفعاليتها، فطبيعة العمليات السيبرانية تقوّض من الدور المحتمل للردع، وقد تجعله عديم الفائدة كليا. ويركز هذا الاتجاه على الإشكاليات التي تواجه الردع السيبراني، ومنها: صعوبة تحديد هوية مرتكبي الهجمات أصلا، ناهيك عن غياب القوانين اللازمة والرادعة، على نحو يوفر لمرتكبيها الملاذ الآمن، ممّا يحول دون ملاحقتهم (https://futureuae.com).

الفرع الثاني: اتجاه ثاني يرى أن نظرية الردع لا تنطبق وكفى في المجال السيبراني، بل إنّها ضرورة ملحّة؛ فبدون الردع السيبراني، ستظل البيانات المفتوحة عرضة لأشكال بدائية وخطيرة من الاستغلال والاعتداء،

ومنها سرقة البيانات، وانتهاك حقوق الملكية الفكرية، وتعطيل الأعمال التجارية، وإيقاف تشغيل النظم الحيوية، ذلك أن الردع السيبراني لابد أن يكون جزءا لا يتجزأ من استراتيجيات الأمن الوطني.

الفرع الثالث: اتجاه ثالث يرى أن نظرية الردع يمكن أن تتلاءم مع الفضاء السيبراني، ولكن بشروط وضوابط محدّدة، منها تبني مفهوم واسع للرّدع، والمزج بين خيارات عدّة في سبيل الوصول إلى استراتيجية متكاملة له، مع مراعاة أنّ الرّدع في عصر المعلومات يختلف كثيرا عنه في عصر الحرب الباردة في النوع والنطاق، ممّا يتطلّب نهجا شاملا يدمج كل المقومات العسكرية والاقتصادية والاستخباراتية والقانونية، تعزيزا لأمن المعلومات من ناحية، وخلقا للردع من ناحية أخرى (https://democraticac.de).

المطلب الثاني: الهجمات والحروب السيبرانية

تزداد الهجمات الإلكترونية بفعل الفيروسات وتتضاعف كل يوم ومن بلد إلى بلد آخر، ومن الراجح هو عدم تمكّن أغلب تلك الفيروسات من الاختراق، إلاّ أنّ نسبة ضئيلة منها قد تتمكن من الاختراق، ومن شأن ذلك أن يحدث آثارا خطيرة، وقد أصبحت تلك الفيروسات، على اختلاف أنواعها، أسلحة حديثة تستخدم في شن هجمات إلكترونية على البنى التحتية الإلكترونية التابعة للدول والمؤسسات المختلفة، وفي أغلب الحالات لا يدرك الضحايا وجود فيروسات أو ديدان إلكترونية (*Electronic Worms*) داخل أنظمة الحوسبة التي يستخدمونها، بل إنهم لن يدركوا ذلك إلا بعد أن يكون قد فات الأوان. وبعض تلك الهجمات يمكن التعافي منه مثل حجب الخدمة، لكن أغلبها تستعصي على العلاج في حالات التجسس، أو حملة التضليل المعلوماتي أو تشويه السمعة وغيرها مما يطلق عليه الحرب السيبرانية التي تتنوع حيث درجة الشدة، وإمكانية التنبؤ بالأزمات الناجمة عنها وأهم هذه الأنواع (studies.aljazeera.net):

الفرع الأول: الحرب السيبرانية الباردة منخفضة الشدة

ويعبر هذا النوع عن صراع مستمر بين الفاعلين المتنازعين، وقد تكون ذات طبيعة ممتدة ذات بعد تاريخي وديني وإيديولوجي ممتد، كأن تكون امتدادا أو جزءا من الصراعات التقليدية الممتدة (الصراع العربي الإسرائيلي، الصراع الإيراني الأمريكي، الصراع بين الكوريتين). وخلالها عادة ما يتم اللجوء إلى القوة الناعمة التي تجمع بين الجيلين الرابع والخامس للحرب، حيث تشمل وسائل عدة، مثل الحروب النفسية وحرب الأفكار. ويستخدم هذا النوع من الحرب السيبرانية أساليب خلق الأزمات السياسية لإثارة الاضطرابات وإثارة الرأي العام ضد الدولة، وبث الإشاعات للإضرار بالاقتصاد القومي، وخلق مناخ غير آمن للاستثمار، وغيرها. وقد شهدنا نماذج منها مع بدء تنفيذ استراتيجية الفوضى الخلاقة عام 2011 (بوغرارة، الأمن السيبراني، مجلة الدراسات الإفريقية وحوض النيل، المجلد الأول العدد الثالث، سبتمبر 2018، ص ص 100-119).

الفرع الثاني: الحرب السيبرانية متوسطة الشدة

ويبرز هذا النوع عند تحول الصراع عبر الفضاء إلى ساحة موازية لحرب تقليدية دائرة على الأرض. وينجم عن العمليات مجموعة متداخلة من الأزمات التقليدية، وهي ليست في حاجة إلى سيناريوهات أو بدائل كما في الأزمات السياسية، الأمر يتوقف على القدرات السيبرانية، وامتلاك برامج قادرة على الردع الإيجابي أو الهجوم المحدود أو الشامل، وينجم عنها بعض الأزمات نتيجة عدم القدرة والسيطرة على إدارة الشبكات، ومنها اختراق المواقع الإلكترونية، وسرقة المعلومات وتخريبها، وعرقلة شبكات الطاقة الكهربائية أو شبكات الطرق والمواصلات البرية والسكك الحديدية والطيران، وشبكات البنوك، وإدارة المفاعلات النووية. وشهد العالم بعض نماذج هذا النوع خلال الحرب بين روسيا وجورجيا 2008، وأمريكا وإيران 2010.

الفرع الثالث: الحرب السيبرانية مرتفعة الشدة وأزماتها الكارثية

ويعبر ذلك النوع عن نشوء حروب في الفضاء الإلكتروني منفردة، وهي غير متوازية مع الأعمال العسكرية التقليدية. ولم يشهد العالم هذا النوع من الحروب، وإن كانت احتمالات حدوثها واردة في المستقبل مع تطور القدرات التكنولوجية وزيادة الاعتماد عليها، وينطوي هذا النوع من الحروب على سيطرة البعد التكنولوجي على إدارة العمليات العسكرية، حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، والاستحواذ على القوة الإلكترونية. والهدف من وراء ذلك تحقيق الهيمنة الإلكترونية الواسعة بشكل أسرع ويرى بعض الخبراء شن إسرائيل هجمات فيروس ستاكسنت ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة في عام 2010 نموذجا تقريبيا لهذا النوع من العمليات (https://www.roayahnews.com).

المطلب الثالث: المشهد الجزائري في الفضاء السيبراني

عند النظر للعقيدة الأمنية الجزائرية نجدها تستمد توجهها العام من المبادئ العامة المستمدة من عدم التدخل في شؤون الآخرين، وهو ما لاحظناه في التحرك الجزائري حيال الكثير من الأزمات، خاصة ثورات الربيع العربي التي أنتجت تغييرات في طبيعة الأنظمة العربية، وهي الرؤية التي تجد لها ركائز قانونية ودستورية تحدد المهام الأساسية لأجهزة الأمن الجزائرية التي تنحصر مهامها في حماية وصون سيادة الدولة وحدودها (برابح حمزة، مجلة الباحث للدراسات القانونية والسياسية، العدد السادس، جوان 2017، ص ص 262-263).

غير أن الخطر الأساسي الذي يشكله الفضاء الإلكتروني اليوم لا يعالج من عقيدة عدم التدخل في شؤون الآخرين، لأن الدولة ذاتها مستهدفة من قبل الجماعات الحكومية وغير الحكومية التابعة للدولة من الهجمات السيبرانية ويكمن الخطر في تبني هذه العقيدة وعدم وجود استراتيجية التصدي لهذا التهديد، وفي هذا السياق، لا تشكل الهجمات المباشرة تحديا متزايدا فحسب، بل تشكل أيضا تحديا خطيرا من خلال استغلال الشبكات الاتصالية للتجسس على برامج التسليح والقدرات القتالية ونقاط الضعف (Eric Talbot Jensen, Emory International Law Review, usa, volumes, 26/2, 2012, pp.773-824).

وهذا ما يضع الدولة في تحد في توفير دعامة قوية لبناء استراتيجية فعالة من خلال: المشورة الجيدة تقليديا من أجل فهم أنواع التهديدات، تقييم من مسار استراتيجية الردع بالمنع المتخذ، أن تستخدم للكشف عن الهجمات السيبرانية في المستقبل للتخفيف من حدة أضرارها، وهذا بالتعاون المحلي والدولي (برابح حمزة، 265).

الفرع الأول: على المستوى المحلي

يتحقق التعاون المحلي من خلال شبكة دفاعية قوية قائمة على التعاون بين القطاع العمومي والخاص، ويتطلب هذا التعاون قدرا كبيرا من الثقة المتبادلة، لأن المساعدة التقنية لا يمكن أن تقدم إلا إذا ضمنت تعاملا فعالا، كما يجب الاعتماد على أسلوب المنافسة لاستمالة القطاع الخاص، واعتماد الجدية في نشر وتفعيل الأنظمة الدفاعية والهجومية معا للشبكات الرئيسية، ومن ثم تحسين أساسيات أمن الشبكات، وحماية البنى التحتية الحيوية، وتحسين أمن الشبكات العسكرية والأسلحة، وكذا التركيز على توعية الشعوب والعامة بمخاطر تلك الحروب، مما يحد منها.

كما يتطلب ذلك وجود خبرات علمية لدى البرلمانات حتى يتم تبادل تلك المعلومات والخبرات بين البرلمان والقطاع العمومي والقطاع الخاص، وأيضا تطوير نظم للردع الضيق ضد فاعلين محددين، لحماية أنظمة بعينها،

وتحدد الخطوات الانتقامية في حالة الهجمات السيبرانية ضد مجموعة ضيقة من الأهداف أو باستخدام مجموعة ضيقة من آليات الهجوم التي يمكن أن تجعل الردع فعالا (برابح حمزة، 266).

كما يجب عدم التركيز فقط على الجيش لمواجهة تلك الحروب، فالجيش له مجاله في الدفاع عن شبكاته الخاصة، لكنه لا يملك بعض الخبرات الخاصة في التعاون مع الجمهور، وخبرة أقل في التعاون مع القطاع الخاص. ومع ذلك، فهو جزء أساسي من الأمن السيبراني.

الفرع الثاني: على المستوى الدولي

تعاني دول شمال إفريقيا من تصاعد الحروب السيبرانية عليها لعوامل، أهمها: سهولة الاختراقات الإلكترونية، ضعف الإنفاق على نظم الحماية، والطبيعة غير المتماثلة للمواجهات العسكرية، وصعوبات اكتشاف الفاعلين، وانتفاء أدلة الإدانة المباشرة، وغياب الأطر القانونية لتحديد العقوبات لتوظيف الفضاء الافتراضي في الاعتداء على الدول، وكذا نقص التعاون الدولي من خلال خلق بيئة قانونية وتشريعية مناسبة لمواجهة الحروب السيبرانية، مما يزيد من فرص توقف شن مزيد من الهجمات السيبرانية، كما يجب تحديد قواعد عالمية واضحة للممارسة المقبولة وشرعية الأهداف في الفضاء السيبراني، فوجود خلاف حول وضع معايير دولية لتقييد الحرب الإلكترونية (الجريدة الرسمية للجمهورية الجزائرية، العدد 2019/42)، لا تخدم سوى الفاعلين الإجراميين.

ضرورة دخول الدول في حوار استراتيجي مع شركائها لضمان استعدادهم للحروب السيبرانية، وهذا يمكن أن يكون أساسا للردع الممتد، كما يجب على الحلفاء أن يوضحوا للجناة المحتملين بأنّ الانتهاكات ضد حليف واحد سوف يؤدي إلى رد فعل مشترك (عبد الغفار الديواني https://futureuae.com). فعلى سبيل المثال تم استهداف الصفحات الإيرانية للمنطقة المغاربية، عن طريق وسائل التواصل الاجتماعي في حالة التموقع في شمال أفريقيا كمدخل لأفريقيا ووسيلة ربط مع أوروبا (عبد الغفار الديواني https://futureuae.com).

الفرع الثالث: التأمين من الاختراق السيبراني وقدرة الكشف على مصدر الخطر

تعتبر نظم تكنولوجيا المعلومات والاتصالات جزءا لا يتجزأ من الحياة اليومية، فهي تتيح للحكومة والشركات والمؤسسات والأفراد الوصول إلى المعرفة والمعلومات ذات الأهمية وتحويل أي دولة إلى مصاف الدول المتقدمة، وما زالت القطاعات الحيوية عرضة إلى أنواع الاختراقات.

ويستخدم مصطلح *الاختراق* بشكل حصري لوصف مسائل أمن المعلومات. لأنه من الصعب تصور كيف يمكن للإشارات الرقمية السفر عبر سلك أو ناقل لتمثل هجوما، وفقا لمفهوم الظاهرة الرقمية أنها ظاهرة مادية. فالهجوم السيبراني هو هجوم يتم شنه ضد الأجهزة الرقمية عن طريق الفضاء الإلكتروني، وهو الفضاء الافتراضي الذي لا وجود له، والذي يتطلب أدوات للأمن السيبراني لحماية الدولة في بياناتها الشخصية والاقتصادية، في ظل المعارك الصامتة وعنصر المفاجأة التي يمتاز بها هذا المجال.

أ- متطلبات تأمين البنى التحتية الرقمية من الاختراق

إنّ الأمن السيبراني أصبح يتطلب استراتيجية محددة لصون المصالح الوطنية الحساسة في الفضاء السيبراني هذه الاستراتيجية تنفذ من قبل الحكومات والأفراد على حد سواء، وهي جزء من التكتيكات الحديثة للحروب والهجمات والحلقة الأهم والأكثر تعقيدا من بين حلقات الأمن الوطني، أما القدرة على تحقيقها فهي تحد صعب محفوف بالعديد من المخاطر والتهديدات، خاصة وأن التطورات التكنولوجية والمعلوماتية تتسارع باطراد وهو ما يتطلب من الدول مواكبة هذه التطورات من أجل توفير الحماية اللازمة سواء الاستباقية أو العلاجية في وقت أصبح

فيه التفوق في الفضاء السيبراني يشكل عنصرا حيويا في تنفيذ الهجمات ذات الفاعلية في الأرض والبحر والجو والفضاء، فضلا عن تجنب وقوع هجمات سيبرانية العابرة للحدود الجغرافية.

إن أمن الفضاء السيبراني يتطلب وجود إجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السليم لتكنولوجيا الاتصال والمعلومات والاهتمام بعملية وضع المعايير والإجراءات المتخذة لتفادي وصول المعلومات إلى أيدي أشخاص غير مخولين قانونا بها عبر الاتصالات ولضمان سلامة تلك الاتصالات.

زادت أهمية حماية البنى التحتية بشكل كبير في السنوات الأخيرة، وتشمل البنى التحتية الحيوية تلك الموارد المادية، والخدمات، ومرافق تكنولوجيا المعلومات، وشبكات وأصول المرافق العامة التي إذا تعطلت أو دمرت، سيكون لها تأثير شديد على الصحة أو السلامة أو الأمن أو الرفاهية الاقتصادية للمواطنين أو كفاءة أداء الحكومات والاقتصادات، وتشمل هذه الفئات البنية التحتية للمرافق العامة في الدول العصرية مثل: الاتصالات والخدمات المصرفية والمالية ومع ظهور العصر الرقمي والإنترنت، تصبح هذه المؤسسات مترابطة ومتشابكة وأكثر سهولة، سواء للمستخدمين الشرعيين أو المخترقين والخصوم. عليه فإنّ مهمة حماية الوصول الرقمي إلى هذه المرافق أولوية وتركيز خاص.

ونعني بالتأمين القدرة على التكيف السيبراني فضلا عن التنسيق الوطني والتعاون الدولي في مجالات الأمن السيبراني والدفاع السيبراني، عبر إنشاء فضاء نقاش وتبادل بين مختلف الفاعلين في الفضاء السيبراني بغرض تفهم رهانات الأمن السيبراني والدفاع السيبراني وتحديد أثر التهديدات السيبرانية على أمن الأشخاص، الممتلكات والأمن الوطني (https://www.elitihadonline.com).

فقد لوحظ أنه مع نهاية الحرب الباردة أصبح الأمن المعادلة الصعبة في الاستراتجيات الحكومية، نظرا للتغيرات والتحولات الكبيرة التي شهدها العالم أثرت على أمن واستقرار الدول، بسبب بروز تهديدات جديدة لم تكن لها وحود مؤثر من قبل في ظل هيمنة التهديدات التماثلية التي مصدرها القوة العسكرية للدول، وتعددت بتعدد مصادرها، وهو ما جعل الأمن بمفهومه التقليدي الضيق عاجزا عن محاربة التهديدات اللاتماثلية (جون بيليس وستيف سميث، 2005، ص 211)، وبذلك تم التوسع في مفهوم الأمن ليشمل مجالات جديدة هي في حد ذاتها مصادر للتهديد، ومع التحولات التي جاء بها الربيع العربي زادت حدة وخطورة التهديدات الإقليمية، ولأول مرة منذ حرب الرمال 1963 أصبح الأمن القومي الجزائري مهددا من الخارج، وبطرق مباشرة وغير مباشرة، وعلى مستوى كل الحدود تقريبا، وبنسب متفاوتة، خاصة في ظل تأزم وتفاقم الأوضاع الأمنية في دول الجوار، والذي يرجع لعاملين الأول الفشل الدولاتي في دول الساحل الإفريقي، والثاني سقوط الأنظمة السياسية في كل من تونس وليبيا ومصر، وما ترتب عن ذلك من آثار جد سلبية على الأمن الوطني في الجزائر (جون بيليس وستيف سميث، ص 214).

ولتعزيز الأمن الرقمي ضمن ست ضرورات عامة ملحة، يجب التركيز على: البنية التحتية، والاستثمار، وتوعية المستهلكين، ومتطلبات الحاجة إلى اقتصاد رقمي عالمي عادل ومفتوح إضافة لعامل رئيس هو إنشاء بيئة رقمية موثوقة ومستدامة، بحيث يثق جميع المشاركون بسلامة الاستثمار فيها، وتحقيق الازدهار من خلالها، وتتسق هذه الضرورة مع دورة حياة الأمن الإلكتروني، التي تتضمن التخطيط والكشف والحماية واسترداد الأصول الرقمية، من أجل التخفيف من حدة خطر وقوع الحوادث الإلكترونية. وقد يكون الحل الأكثر فعالية لمواجهة اتساع طبيعة التهديدات الإلكترونية هو تطبيق نهج شامل دائم للأمن الإلكتروني من خلال:

1) حماية ودفاع وتأمين بنية المعلومات التحتية والشبكات الرقمية.

2) ابتكار ودفع عجلة الاستثمار في تأمين وتنمية الشبكات الرقمية والاقتصاد الرقمي.

3) إعداد المستهلكين لتحقيق الازدهار في ظل العصر الرقمي.

4) بناء قدرات القوى العاملة في الأمن الإلكتروني.

5) تجهيز الإدارات الحكومية بشكل أفضل للعمل بفعالية وبصورة آمنة في العصر الرقمي.

6) ضمان تحقيق قيم الانفتاح والنزاهة والتنافسية والأمن في الاقتصاد الرقمي العالمي (حسين باسم عبد الأمير، جامعة كربلاء، 2018. http://kerbalacss.uokerbala.edu.iq).

ب- امكانية الكشف على مصدر الخطر الإلكتروني

عند النظر إلى الحوادث السيبرانية في السنوات الأخيرة يبدو أن الهجمات تستخدم كهدف رئيس لإخفاء الهجوم الفعلي ومن أجل تحويل تكنولوجيا المعلومات وتتميز بغياب أو شبه غياب للضوضاء الإعلامية، وتتزامن مع انقطاع ملحوظ للخدمة مع نوع مختلف من الحوادث الأمنية، مثل هجوم البرامج الضارة، واقتحام الشبكة أو أي نوع آخر من الهجمات، والشركات وللتحقيق في مسألة ما إذا كانت بعض الأنشطة السيبرانية قد تبقى مخفية حتى على الرغم من أن لديهم تأثير كبير على حياتنا اليومية أو كيف غير معروف حتى الآن، ونعني بعنصر المفاجأة القدرة على شن هجوم دون سابق إنذار وهذا ما يظهر في مفاجأة العدو، وهي الشرط المسبق للتفوق، ويتطلب القيام بـ:

- القيام بعمليات التجسس على الخصوم.
- شن الهجمات الالكترونية التي تسبب الضرر للبنى التحتية والاقتصاد والمواقع الحكومية في الدول الاجنبية المعادية.
- شن حروب معلوماتية في وسائل الإعلام والشبكات الاجتماعية، عن طريق القيام بعمليات اختراق الحسابات الاجتماعية والبريد الالكتروني، وانشاء حسابات وهمية على شبكة المعلومات الدولية، وفتح الآلاف من الحسابات المزيفة على مواقع التواصل الاجتماعي: (فيسبوك، تويتر، انستجرام... وغيرها)، للرد على الآلاف من التعليقات والمقالات، ونشر الشائعات وتظليل الحقائق في محاولة لدعم الموقف الوطني وتوجيه الرأي العام ضد الخصوم.

وتلعب السيبرانية الهجومية دورا أكبر في العمليات العسكرية في إطار استراتيجية الردع، بالرغم من أن الجيش الجزائري لا يفصح عن اعتناق العقيدة السيبرانية لأسباب هيكلية وعقدية على حدٍ سواء، لكن يفهم كل هذا في اطار الحرب الصامتة ومن فحوى التصريحات المتضمنة تعزيز القدرات الأمنية الدفاعية السيبرانية (إيهاب خليفة، دار العربي للنشر والتوزيع، ص 147).

ولغرض الحفاظ على الأمن السيبراني الوطني من الهجمات الخطيرة؛ على الحكومة تبني رؤية واضحة وتكوين جيش دفاع وطني الكتروني بعدة حديثة وبعدد مناسب تكون النواة الحقيقية للحكومة الالكترونية، ويشمل هذا الحفاظ تعزيز رأس المال البشري الذي يتطلب الموظفين الموهوبين والمعرفة لإدارة العمليات وتطورا مستمرا من خلال إعادة التقييم والتعزيز لهذه القدرات.

ج- عنصر الإسناد الصحيح

إنّ واحدة من المشاكل الأكثر إثارة للقلق المرتبطة بالعمليات السيبرانية هي مسألة الإسناد، وتدور حول قدرة الدولة أو غيرها –الضحية- على تحديد مصدر الهجوم والمهاجم وتحديد الجهاز الذي تم إنشاؤه التشغيل السيبراني، الواقع أن منشأ الهجمات السيبرانية الغامض غالبا ما يزيد من صعوبة تطبيق نظرية منطقية للردع في العالم السيبراني ذلك أن تحديد الطرف المسؤول عن الهجوم، أمر نسبي، فإنّ عدم القدرة على عزو العمليات السيبرانية على وجه السرعة يطرح عقبات قانونية أمام الردع الفعال. حتى يعرف الضحية من يعتدي على أنظمة الكمبيوتر الخاصة به، فإنه من الصعب معرفة كيفية ردعها. بحيث يجب أن يكون هناك عاملان هامان آخران في الردع.

وفي هذا الإطار فقد تم تدشين المركز الرئيسي لصيانة أجهزة الحرب الإلكترونية الذي يتبع لوزارة الدفاع، وهو المرفق الذي سيتولى مهمة الصيانة الشاملة والمراقبة الدورية لوسائل الاتصالات بمختلف أنواعها، وهو المركز الذي يتوفر على قدرة كبيرة لتصليح وصيانة الأجهزة من الجيل الحديث في مجال إلكترونيك الدفاع، وهنا نفرّق بين الحرب الإلكترونية والجرائم الإلكترونية، فالأخيرة هي الأهم وتشمل الكثير من القطاعات من بينها الدفاع الوطني، أما الحرب الإلكترونية فهي من اختصاص الجيش حصرا في إطار الحفاظ على الأمن الوطني ضد هجمات إلكترونية تستهدف الأنظمة المعلوماتية للجيش نفسه أو التي تخص مؤسسات سيادية في الدولة .(https://www.ennaharonline.com)

ومع انخراط مختلف الدول في التجسس الاقتصادي، وأنشطة سيبرانية خبيثة، والنظر إلى الفضاء السيبراني على أنه ساحة يمكن فيها تحييد القوة الاقتصادية، والعسكرية، والسياسية، وتقويض تماسك الدول واستقرارها، تجيز الاستراتيجية العمليات السيبرانية الهجوم السري، تماشيا مع سياسة جديدة تخفف من قواعد استخدام الأسلحة السيبرانية لحماية البلاد من هجمات سيبرانية لا تهدد فقط الدولة في بياناتها الحساسة، ولكن المؤسسات الاقتصادية والأمنية، وتعمل الاستراتيجية السيبرانية أيضا على الحد من القيود الأخلاقية المقيدة للقيام بهجمات سيبرانية على الخصوم والمنافسين وتهدف في المقام الأول إلى لحماية أنظمة والشبكات التي يؤثر استهدافها على الدولة ومؤسساتها.

المبحث الثاني: تنفيذ الردع بين الإمكانية والاحتمالية

تعد التكنولوجيا الرقمية وأمن المعلومات أحد أهم العوامل التي ساهمت في تطوير القدرات والإمكانيات الداخلية والخارجية للدول، والتأثير على فكرها السياسي والاستراتيجي الذي انعكس بصورة واضحة في جملة التفاعلات الإقليمية والدولية.

كما أن التقدم في الميدان التكنولوجي وصناعة المعلومة أصبح أكثر عامل داعم للقدرة العسكرية للدولة، حيث يمكنها من تعبئة الطاقات البشرية والموارد لصراعات طويلة، لذا شكّل هذا التقدّم القاعدة الأساسية لاقتصاديات الدول، ومعلوم أنّه ينشط في العالم اليوم شبكة معقدة من التفاعلات تتخطى الحدود القطرية، بسبب أفراد ومجموعات، ومنظمات سياسية ثورية، ربما الأكثر فاعلية في هذه الشبكة من تفاعل الدول فيما بينها ويثار سؤال حول حقيقة تحقق الرّدع الإلكتروني وحماية السيادة الوطنية في ظل ثورة رقمية وعمليات الكترونية متجدّدة وهو ما سنتناوله في المطالب أدناه.

المطلب الأول: إمكانية تنفيذ الردع الالكتروني

الهدف من الردع هو منع العمل العدواني من خلال قدرة الدولة على تطوير قدرات عسكرية موثوقة ومتبادلة ومتماثلة على الفضاء الإلكتروني تكون قادرة على التأثير على قرارات الخصم، وتمنعه من شن هجمات عسكرية عبر الفضاء الإلكتروني (إيهاب خليفة، مجلة اتجاهات الأحداث العدد 13 أغسطس 2015، ص 49)، وقد لعبت نظرية الردع دورا هاما في نظرية الأمن الوطني مع التطور الحديث للعمليات السيبرانية، فضلا عن الأكاديميين والممارسين، وقد تحول انتباههم إلى الإنترنت وقد تسببت طبيعة العمليات السيبرانية في بعض التقليل من دور محتمل للرّدع، ويطرح افتراض هو أن تحقق الرّدع السيبراني ممكن مثل تحقق الرّدع النووي بعد الحرب العالمية الثانية، فالعمليات السيبرانية تبدو بطبيعتها مختلفة عن العديد من الأسلحة الأخرى التي تسخّر العنف على مستوى الدولة، من حيث أنّها في متناول مجموعة واسعة من الجهات الفاعلة.

وتفيد التقارير بأنّ أكثر من دولة لديها أسلحة إلكترونية أو تقوم بتطويرها، وأكثر من ثلاثين بلدا يقوم بإنشاء وحدات السيبرانية في جيوشها (إيهاب خليفة، 2015، ص 148). ورغم الاختلاف الذي يطرحه تغير الفواعل وطبيعة جغرافيا الفضاء الإلكتروني، ونوعية السّلاح إلاّ أنّ هناك تشابه على مستوى القوانين الضابطة لانتشار هذه الأسلحة المستعملة بغرض التهديد، فكما هو موجود على مستوى استراتيجية الرّدع التقليدية والنووية فيما يخص التقنين ينطبق على الرّدع الالكتروني أيضا، لأنّه من الصعب تطبيق القوانين على العلاقات العابرة للحدود هذا من جهة، كما أنّ ملامح الرّقعة الجغرافية غير محدّدة، وبالتالي من الصعب تحديد سيادة الدول ومن غير الممكن تحديد نوعية الأسلحة التي هي في تطوّر مستمر والحد منها صعب (إيهاب خليفة، ص 49).

إن نظرية الردع السيبراني يجب أن تشمل كل الخصوم المحتملين لكونها قادرة على ردع الكثير، ويجب أن ينطبق الرّدع على مجموعة كاملة من الجهات الفاعلة، من الأفراد إلى الدول والأمم، والنظر في مجموعة كاملة من الإجراءات، من العمليات الصغيرة في أنظمة الكمبيوتر إلى الهجمات على نطاق واسع التي تنتج حركية كبيرة الآثار على المهاجمين.

هذا النوع من الهجمات المحتملة والمهاجمين يتطلب الردع العام لتطبيق على نطاق واسع وقبل أي هجوم محتمل، فعلى سبيل المثال، وجود ترسانة نووية التي يمكن استخدامها ردا على مختلفى الهجمات من مختلف الأنواع هو رادع عام يقابله في عالم الإنترنت بعض الإجراءات، مثل تثبيت جدار الحماية، التي تنطبق كرادع عام لجميع الجهات الفاعلة، ومنع جميع حركة المرور السيبرانية التي تأتي من خادم معين، أو التي تحمل معين نوع الملف. لأن الدولة المستهدفة يجب أن تدافع عن منظومتها وشبكاتها بكل قدراتها ضد كل الإمكانات الخصوم أو المهاجمين، والعوامل المذكورة تؤدي إلى استنتاج أن الردع يجب أن تغطي كمجموعة متنوعة من الجهات الفاعلة، وأنواع الهجمات، ومستويات العمل، وبعبارة أخرى، فالعمليات السيبرانية تتطلب هيمنة النوع الكامل إذا ما أريد لها تكون أكثر فعالية.

المطلب الثاني: احتمالية عدم تحقق الردع

بغض النظر عن مقدار الجهد الذي يتم بذله في الردع، فإنه لا يمكن أبدا أن يكون فعالا بصورة كاملة. وهذا صحيح ليس فقط من منظور تقني، ولكن أيضا من منظور سوسيولوجي. فبعض الخيارات التي من شأنها ردع بعض الخصوم المحتملين سوف تعطي حافزا للآخرين، وهناك بعض الجهات الفاعلة الذين ببساطة لا يمكن ردعهم، وكما يقال إن الردع السيبراني لا يمكن أبدا أن يكون فعالا لأن الإجراءات التي تهدف إلى ردع نوع واحد من الفاعلين سوف لن تثني الجهات الفاعلة الأخرى على الهجوم (أمين بولنوار، جامعة الجزائر، 2010/2009، ص 138).

كما أن العنصر الأساسي لتحقق الردع يركز على القدرة التدميرية للسلاح المستخدم والذي يحول دون استخدامه نظرا لتبعات ذلك، بمعنى أنه كلما زادت القدرة التدميرية للسلاح كلما قل الميل إلى استخدامه، لذا فإن الصعوبات التي تحول دون تحقيق الردع الالكتروني تتمثل في:

– صعوبة معرفة الطرف المعتدي: لكي يتحقق الردع لا بد من وجود خصم لمواجهته وتحديد طبيعة الخصم دولة او منظمة أو فرد صعب في البيئة الالكترونية.

– القدرة على التتبع والتواصل والمصداقية: لكي يتحقق الردع لابد من توفر هذه الشروط الأساسية، ويقصد بالتتبع معرفة مصدر الهجمة الالكترونية، فعلى الرغم من التطور الواضح في ملاحقة المهاجمين، إلا أن هناك تطور مقابل على مستوى التمويه والإخفاء لدرجة يجعل من معرفته شبه مستحيل وهذا يناقض أساس الردع وهو تحديد جغرافية الخصم.

– صعوبة وضع الخصم في تهديد حقيقي: لا تستطيع الدول التي مستها الهجمات الالكترونية بالرد الانتقامي من الخصم، فتوجه هجمات لدول أخرى بغية التأكيد على قدراتها وإمكانيات الرد وهنا الردع لا يتحقق مادام الخصم غير محدد بدقة، وبالتالي مصداقية العلاقات الردعية مع الطبيعة غير المتكافئة في الفضاء الالكتروني.

– صعوبة منع الهجمات الصفرية: التطورات التي تعرفها الأسلحة الالكترونية تسمح اختراق أنظمة الدفاع الالكترونية، ولا يمكن لشركات الأمن الالكتروني أن ترصدها لتطورها فتكون هجماتها منصبة على المكون المادي للشبكة المعلوماتية أو البرامج الالكترونية أو على مستوى المكون المادي للجهاز الالكتروني (عبلة مزوزي، جامعة باتنة 2018/2017، ص 109).

– عدم توفر المنظومة القانونية: تشكل البيئة التشريعية والقانونية الحالية مصدرا آخر لعدم تحقق نظرية الردع الإلكتروني لأسباب عديدة ليس أقلها النقص في القواعد المختصة أو غيابها وعدم انسجام بعض القواعد مع حاجات وطبيعة النشاط والفضاء السيبراني ويندرج في هذا الإطار أيضا الاختلاف الثقافي بين المجالين القانوني والتقني كما أنّ اختلاف التفسيرات التي يمكن إعطاؤها لهذا العمل أو ذلك انطلاقا من هذه الخلفية في كل الأحوال تتوزع الممارسات الجرمية التي تطال الفضاء السيبراني بحسب الاتفاقية الأوروبية لمكافحة جرائم المعلوماتية على ما هو جرائم كلاسيكية تطورت أساليب ومجالات ارتكابها: كالاحتيال والتزوير وما هو جرائم جديدة لاسيما لجهة الوصف الذي يمكن إعطاؤه لها والذي تدخل فيه تكنولوجيا المعلومات والاتصال بوضوح ونعني بذلك الاختراقات الأمنية للأنظمة المعلوماتية وما يرتبط بها من تعديات على البيانات وانتقالها (عبلة مزوزي، جامعة باتنة 2018/2017، ص 141).

كما أن العمل تحت مبدأ الضرورة الذي ينظم بدء الأعمال العدائية، أو الحرب بالمفهوم الحديث، شرط لأي رد على الدفاع عن النفس ضد أي هجوم مسلح، في حين أن التطبيق العملي لهذه المبادئ على العمليات السيبرانية يطرح مناقشة كبيرة في ظل النظريات التي تحدد كيفية ما إذا كان الهجوم السيبراني عمل مسلح ينسحب على الأعمال المسلحة التقليدية أم لا،غير أن المتفق عليه هو الدفاع عن النفس من قبل الضحية الدولة أو أحد مؤسساتها باستعمال القوة اللازمة لمواجهة التهديد. والإمكانية القانونية لتبرير الرد وفق منظومة قانونية مسبقة.

الخاتمة:

في ختام هذا البحث وقبل التطرق إلى أهم النتائج والاقتراحات والتوصيات نحاول الإجابة على إشكالية البحث المشار اليها في المقدمة وهي ما إن كانت الجزائر قد انتهجت استراتيجية معينة في مواجهة حروب الجيل الرّابع أو الحروب الالكترونية؟

في واقع الحال ان الجزائر ووعيا منعا بضرورة التصدي للهجمات الالكترونية رسمت سياسة عامة تتعامل بواسطتها مع هذا النوع الجديد من التحدي، حيث انقسمت هذه السياسة والتي قد لا ترقى إلى استراتيجية فعالة لمجابهة الحروب الالكترونية، انقسمت إلى قسمين:

القسم الأول: اهتم بما يسمى بالجرائم الالكترونية، حيث اهتمت بوضع الأطر القانونية والهياكل الأساسية اللازمة لمواجهة مثل هذا النوع من الجرائم سواء تعلّق منه بالمساس بالحياة الخاصة واستغلال البيانات الشخصية للأفراد، أو الشق المتعلق بالهجمات الالكترونية التي تمس البنية التحتية وقاعدة البيانات التي تخص المؤسسات المالية والمصارف والبريد الأمر.

القسم الثاني: اهتم بما أصبح يعرف بحروب الجيل الرّابع إشارة إلى تجاوز الحروب التقليدية التي كانت الأسلحة البرية والجوية والبحرية تلعب فيها دورا حاسما، حيث أصبحت الحرب تدار بوسائط الكترونية تعتمد على التكنولوجيا الحديثة والبرمجيات والكمبيوتر وشبكات الاتصال السلكية واللاسلكية والرادارات والطائرات من دون طيار *Drones* إلى غير ذلك من الوسائل والبنية التحتية المتطورة والتي تغني جنود هذه المعركة عبور الحدود والمواجهة الجسمانية، غير أنّ نتائجها قد تكون أكثر فتكا وأقل خسائر.

بدأت الجزائر بالاهتمام بهذا النوع من الحروب وأسست دوائر ومصالح تتبع وزارة الدفاع تعنى بهذا الجيل الجديد من الحروب وتسعى إلى الرقي بهذه الوسائل إلى مصاف الأسلحة الحربية على غرار سلاح البر وسلاح والجو وسلاح البحر وسلاح الإشارة...الخ.

أهم النتائج وهي:

– إن الأمن السيبراني مسؤولية مشتركة بين جميع المؤسسات في الدولة وكذا الأفراد.

– لم يتم تصميم الإنترنت ووضع هدف الردع الإلكتروني في الاعتبار غير أن هذا الأخير ينبغي أن يكون جزءً نشطا من استراتيجية الأمن الوطني.

– إن نظرية الردع الإلكتروني ارتبطت بالعديد من الحقب التاريخية كفترة الحرب الباردة، وتسعى الدول عند توفر القدرات السيبرانية والأدوات الفريدة والمبتكرة لتحقيق الأهداف الوطنية.

– من خلال فهم نظرية الردع، يمكن للدول توسيع دور الردع الإلكتروني والعمل على تحقيق الأهداف الوطنية بشكل أكثر فعالية في عصر الإنترنت.

– يجب أن تكون الجزائر على استعداد لاتخاذ تدابير ردعية قوية ضد المهاجمين باعتماد استراتيجية وطنية لتحسين الكشف عن الهجمات السيبرانية المتطورة والتحرّك نحو تحديد هوية المهاجم، وردّ الهجوم وليس الاكتفاء بالدفاع.

– ضرورة سن التشريعات والقوانين بشكل يضمن بناء مستقبل آمن في عالم الانترنت وتنظيم العمل في الفضاء الالكتروني والحد من الجريمة الالكترونية، وتشمل هذه القضايا القانونية جوانب من القانون الدولي.

كما خلص المقال على أن الاستراتيجية الحديثة تعتبر أن الرّدع في الفضاء السيبراني عملية يصعب تنفيذها، إذن يجب تركيز الجهود على الدّفاع بفعالية، بتوفير كل الوسائل الحيوية.

قائمة المراجع:

أولا: باللغة العربية:

1) أمين بولنوار، الولايات المتحدة الأمريكية ومنطق الهيمنة، ماجستير في العلوم السياسية والعلاقات الدولية، كلية العلوم السياسية الإعلام قسم العلوم السياسية والعلاقات الدولية جامعة الجزائر، 2010/2009.

2) إيهاب خليفة، إمكانيات تحقيق الردع في صراعات الفضاء الإلكتروني، مجلة اتجاهات الأحداث، العدد 13، أغسطس 2015، ص 49.

3) إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، مركز المستقبل للأبحاث، دار العربي للنشر والتوزيع.

4) إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، المرجع السابق.

5) برابح حمزة، الاستراتيجية الأمنية الجزائرية لمواجهة التهديدات الأمنية اللاتماثلية في منطقة الساحل الإفريقي، مجلة الباحث للدراسات القانونية والسياسية، العدد السادس، جوان 2017، ص ص 262-263.

6) برابح حمزة، الاستراتيجية الأمنية الجزائرية لمواجهة التهديدات الأمنية اللاتماثلية في منطقة الساحل الإفريقي.

7) تضمن المرسوم الرئاسي المؤرخ في 22 شوال عام 1440هـ الموافق 25 يونيو سنة 2019 تعيين وتغيير تسمية إحدى الدوائر المركزية بوزارة الدفاع الوطني ويتعلق الأمر بدائرة الإشارة وأنظمة المعلومات، التي أصبحت تحمل اسم دائرة الإشارة وأنظمة المعلومات والحرب الإلكترونية أنظر: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 42، المؤرخة في 30 يونيو سنة 2019.

8) جون بيليس، ستيف سميث، عولمة السياسة العالمية. ترجمة ونشر: مركز الخليج للأبحاث، الإمارات العربية المتحدة، 2005، ص 211.

9) حسام السبكي، الحروب السيبرانية: المفهوم والأنماط والتداعيات على الأمن الدولي أنظر: الدراسة على الرابط: https://www.roayahnews.com تاريخ الاطلاع: 2019/08/16.

10) حسين باسم عبد الأمير، تحديات الأمن السيبراني مركز الدراسات الإستراتيجية، جامعة كربلاء، 2018. تاريخ الاطلاع: 2019/08/10 الموقع:http://kerbalacss.uokerbala.edu.iq

11) رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، تاريخ نشر المقال: 2017/07/17 على الموقع: https://democraticac.de/ تاريخ الاطلاع: 2019/08/20.

12) عبد الغفار الديواني، الردع الإلكتروني بين المنع والانتقام، المعهد الألماني للشؤون الدولية والأمنية مايو 2015 على الموقع: https://futureuae.com تاريخ الاطلاع: 2019/07/17.

13) عبد الغفار الديواني، الردع الإلكتروني بين المنع والانتقام، المعهد الألماني للشؤون الدولية والأمنية مايو 2015 على الموقع: https://futureuae.com، تاريخ الاطلاع: 2019/08/16.

14) عبلة مزوزي، استراتيجية الردع وانعكاساتها على الواقع الإقليمي والدولي بعد نهاية الحرب الباردة-دراسة حالة إيران-، أطروحة دكتوراه علوم، كلية الحقوق والعلوم السياسية، جامعة باتنة 2018/2017.

15) محمد الدوراني، قتال غير مرئي: الحرب السيبرانية في الأزمة الخليجية نشر في 2018/05/13 على الرابط: studies.aljazeera.net تاريخ الاطلاع: 2019/07/12.

16) ملتقى حول تطوّر التهديدات السيبرانية وطرق الأمن السيبراني والدفاع السيبراني، وزارة الدفاع الوطني يوم 25 و 26 مارس 2019، جريدة الاتحاد على الرابط: https://www.elitihadonline.com تاريخ الاطلاع: 2019/07/20.

17) الموقع: https://www.ennaharonline.com تاريخ الاطلاع: 2019/08/25.

18) يوسف بوغرارة، الأمن السيبراني: الاستراتيجية الجزائرية للأمن السيبراني للأمن والدفاع في الفضاء السيبراني، مجلة الدراسات الإفريقية وحوض النيل، المجلد الأول العدد الثالث، سبتمبر 2018، ص ص 100-119.

ثانيا: باللغة الفرنسية:

1) Eric Talbot Jensen, CYBER DETERRENCE, Emory International Law Review, USA, volumes, 26/2, 2012, pp.773-824.