جامعة العربي التبسي – تبسة – الجزائر
كليّة الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر في العلوم االسياسية
تخصص: دراسات إستراتيجية
بعنوان:

مكانة الأمن السيبيراني في منظومة الأمن الوطني الجزائري

إعداد الطالبـة:
– سعيدة رشاش

إشراف الدكتورة:
– د/ إدريس عطية

أعضاء لجنـة المناقشـة:

الاسم واللقب	الصفة	الرتبة العلمية
د/ سمير كيم	رئيسا	أستاذ محاضر – ب –
د/ إدريس عطية	مشرفا ومقررا	أستاذ محاضر – أ –
د/ يوسف أزروال	ممتحنا	أستاذ محاضر – ب –

السنـــة الجامعيـــة: 2017 – 2018

جامعة العربي التبسي – تبسة – الجزائر
كليّة الحقوق والعلوم السياسية
قسم الحقوق

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر في العلوم االسياسية
تخصص: دراسات إستراتيجية
بعنوان:

مكانة الأمن السيبيراني في منظومة الأمن الوطني الجزائري

إعداد الطالبـة:
– سعيدة رشاش

إشراف الدكتورة:
– د/ إدريس عطية

أعضاء لجنـة المناقشـة:

الاسم واللقب	الصفة	الرتبة العلمية
د/ سمير كيم	رئيسا	أستاذ محاضر – ب –
د/ إدريس عطية	مشرفا ومقررا	أستاذ محاضر – أ –
د/ يوسف أزروال	ممتحنا	أستاذ محاضر – ب –

السنـــة الجامعيـــة: 2017 – 2018

University Larbi Tebessi-Tebessa- Algeria
Faculty of Law and political scionces
Departepent of political science

An additional thesis to the reqw rements to the obtention of the
Master Degree in Political scienes
Specialiy : Strategic Studies

The Weirght of Cyberntics in the system of the Algerian National Security

By : the student :
Saida Rechache

Under the Supervision of Prof :
Doctor : Idriss Attia

The member of Panel of deliberation

Nam and Frst name	Scientific Status	Qality in the research
Samir kim	Prof lectured - b -	President
Idriss Attia	Prof lectured - A -	Supervison and rapporteur
Youcef Azaroual	Prof lectured - b -	Discoursed

Academic Year : 2017/2018

بسم الله الرحمان الرحيم

﴿هَلْ أَتَى عَلَى الْإِنْسَانِ حِينٌ مِنَ الدَّهْرِ لَمْ يَكُنْ شَيْئًا مَذْكُورًا (1) إِنَّا خَلَقْنَا الْإِنْسَانَ مِنْ نُطْفَةٍ أَمْشَاجٍ نَبْتَلِيهِ فَجَعَلْنَاهُ سَمِيعًا بَصِيرًا (2) إِنَّا هَدَيْنَاهُ السَّبِيلَ إِمَّا شَاكِرًا وَإِمَّا كَفُورًا (3)﴾ سورة الإنسان الآية [1-3]

صدق الله العظيم

شكر وتقدير

أشكر الذي خلقنا وشق سمعنا بحوله وقوته، الله سبحانه عز وجل، فأحمده حمدا كثيرا طيبا مباركا لتوفيقه لي في إتمام هذا العمل الذي ما هو إلا قطرة من بحر الأبحاث العلمية.

ولقوله تعالى: "ولا تبخسوا الناس أشيائهم"(من سورة الأعراف، الآية: 84)

وقول رسوله الكريم (صلى الله عليه وسلم): "من لا يشكر الناس لا يشكر الله"

(أخرجه الترمذي)

و عليه أتقدم بخالص إمتناني وتقديري إلى مرجعي الأكاديمي أستاذي الكريم الدكتور "إدريس عطية" الذي وضع حجر الأساس بآرائه السديدة ونصائحه الرشيدة، لأبني من خلالها قدراتي العلمية المكتسبة طيلة مشواري العلمي بجامعة العربي التبسي تبسة، لأسلمه في الأخير مفتاح ما إستخلصته من توجيهاته القيمة.

كما لا أنسى شكري وتقديري لكل الأساتذة بكلية الحقوق والعلوم السياسية بصفة عامة وقسم العلوم السياسية بصفة خاصة.

و لا يفوتني أن أتشكر أساتذة جامعة "قاصدي مرباح–ورقلة– على المعلومات القيمة التي قدموها لي بكل إخلاص، وعلى رأسهم، الدكتور: كاهي مبروك، والدكتورة الفاضلة: فريدة طاجين، والدكتور: بارة سمير، والدكتور: حجاج قاسم.

ملخص:

يتمحور هدف الدراسة حول الانفتاح التكنولوجي الذي شهدته الجزائر، لتكتب بداية جديدة للعصر الحالي، بلغه الكترونية أحدثت طفرة غير مسبوقة في تاريخ الجزائر، وأوجدت فوارق كبيرة، وأضافت مجالات جديدة، وأعادت بناء تشابك العلاقات الحياتية الأقل وضوحا والأكثر تعقيدا بأكثر كفاءة وأقل تكلفة، كما أسهمت في تنامي التهديدات السيبرانية (كالتجسس والاختراق والتجنيد الإرهابي والقرصنة وغيرها)، مما دفع بإسراع الجزائر إلى إنشاء هيئات أمنية مختصة ووضع خطط استراتيجية لمكافحة تلك التهديدات وتحقيق أمن سيبراني وطني.

الكلمات المفتاحية:

الأمن السيبراني . الأمن الوطني . التهديدات السيبرانية . الاستراتيجية الأمنية.

Summary :

The purpose of the study deals with technological opening witnessed by Algeria which storted a new beginning of tge current era in electronic language. That language has created an unprecedent leep in the history of Algeria. Led to huge differences and it added new horizon and rebuilt new relationship between the least clear life and the most complicate with the greatest cometence and the smallest cost. However it contributed to the technological evolution in developing new modern threat of cyberntics (such an spying and transperception. Recruitnet of terrorist. Piracy and so in) this fact has compelled Algeria to mak a qwik move to set up security units specialized and to create srategic plans aimed at struggling against those threats and to achieve national cyber security.

Key words :

Cyber security- National Security- cCyber threat- Scurity Strategy.

جدول لأهم المصطلحات:

Terminologies in the English	المصطلحات اللغة العربية
Cyber Age	العصر السيبيري
Cyber Space	الفضاء السيبيري
Cyber Security	الأمن السيبراني
Cyber Politics	السياسة السيبيرية
Grups Default	مجموعات إفتراضية
Infrastructure Cyber	بنية تحتية سيبرية
Cyber Threats	تهديدات سيبرانية
Cyber challenges	التحديات السبرانية
Cyber Attaks	هجمات سيبرانية
Cyber Power	القوة السيبيرية
Cyber Terrorism	الارهاب السيبراني
Cyber Espionage	التجسس السيبراني
Cyber Crime	الجريمة السيبرانية
Cyber Diplomacy	الدبلوماسية السيبرانية
Cyber Intelligence	الاستخبارات السيبرانية
Cyber Allies	الأحلاف السيبيرية
Cyber Deterrence	الردع السيبراني

جدول المختصرات:

اختصارها	الجملة بالانجليزية	الجملة بالعربية
ICU	International Communication Union	الاتحاد الدولي للاتصال
CNO	Computer Network Operation	ادارة العمليات الالكترونية
CCC	Convention on Cybercrim	الاتفاقية المتعلقة بالجريمة السيبرية
NII	Nationalism Infrastructure Information	البنية التحتية القومية للمعلومات

مقدمة

لقد شهدت مدركات مفهوم الأمن تحولات كبيرة، خاصة بعد نهاية الحرب الباردة، حيث تمثلت هذه التحولات في توسع المفهوم من أمن عسكري إلى مجالات أخرى غير العسكرية، حيث بات موضوع الأمن يركز على تفاعلات الظاهرة الأمنية مع غيرها من الفواعل المهددة لها، لاسيما في منتصف القرن العشرين، أين بدأ العالم يشهد إعادة تشكل القوى والفواعل المؤثرة في بنية النظام الدولي، بشكل جعل من إدراك هذه التهديدات والمخاطر يدفع بالتحليل الأمني إلى الإنتقال من المستوى الدولاتي إلى مستويات أخرى غير دولاتية. وأمام هذه الأوضاع الأمنية غير المستقرة التي شهدها العالم، ومع تسارع التطورات التكنولوجية وفي ظل الثورة الرقمية المعاصرة التي شكلت ثورة حقيقية في كل مناحي العالم، أسست البنية التحتية لتقنيات المعلومات والإتصالات، حركة تدفق المعلومات عبر الحدود الجغرافية بين الدول، محولة بذلك العالم إلى قرية كونية صغيرة فرضت واقعا جديدا على السيادة الوطنية، الأمر الذي جعل الدول تعاني من مشكلات أشد وأخطر من تلك التي واجهتها من قبل، فمن مسائل أمن الحدود ومسائل الأمن القومي ومسائل السباق نحو التسلح ومسائل أمن الأفراد، إلى مسألة جديدة تتمثل في مفهوم "**الأمن السيبراني**" (Cyber Sucirity)، هذا المفهوم الذي ظهر نتيجة العلاقات التي تحاك عبر الفضاء الإلكتروني بين أشخاص موجودين على أراض مختلفة، خاضعة لعدد من السيادات، حيث يختلف فيها بلد مصدر العمليات السيبرانية عن بلد تحقيق النتائج، والبلاد التي تمر بها البيانات، إذ تحول "**الأمن السيبراني**" إلى ساحة التفاعلات الدولية من خلال العديد من الأنماط التوظيفية سواء على صعيد الإستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعل "**الفضاء السيبراني**" مجالا للصراعات المخلفة من طرف الفاعلين الدول أو من غير الدول لحيازة أكبر قدر من النفوذ السيبراني.

ففي عصر سمته الأساسية هي تحقيق "**الأمن السيبراني**"، تشكلت فيه المخاطر و"**التهديدات السيبرانية**" وتعددت فيه أشكال الهجمات الإلكترونية وتضاربت فيه المصالح والأهداف المعلوماتية والتسابق نحو التسلح الإلكتروني. أصبح للجزائر وكغيرها من دول العالم تواجه على المستوى المؤسساتي، سواءا الحكومية أو غير الحكومية والمجتمع المدني والأفراد، ولاسيما القطاعات المتعددة منها قطاع الإعلام والإتصال، قطاع المال والأعمال، قطاع التجارة وغيرها، حيث أصبح لزاما على الدولة الجزائرية إنشاء هيئات وطنية متخصصة في مجال محاربة "**المخاطر السيبرانية**"، ليكون بالإمكان من خلالها الإستجابة والمساعدة للمؤسسات والأفراد والقطاعات العامة والخاصة. من مواجهة حوادث الإختراق والتجسس والقرصنة والتقليل من تأثيرها وزيادة

الوعي والفهم للتهديدات التي تفرضها التطورات الهائلة في وسائل التواصل والإتصال عبر "**الفضاء السيبراني**" (Cyber Space)، حيث توجهت منظومة الأمن الجزائري التي لا تخلو من الإهتمامات السيبرانية إلى وضع إستراتيجية أمنية شاملة من أجل ضمان "**الأمن السيبراني**"، لأن أمن المعلومات يعتبر ضمن الأمن الوطني العام والشامل، فالأجهزة الأمنية الجزائرية تدرك أن التغيرات المتسارعة في التكنولوجيا تؤدي إلى خلق تهديدات ليست بالسهلة، لذا لابد من ضرورة العمل على ضمان أمن المعلومات وشبكات الأنترنت خلال خطوات مهمة تعتمد على مجموعة كبيرة من وسائل قانونية وتقنية لمقاومة الإستخدام غير الشرعي للشبكة العنكبوتية من أجل حماية نظم المعلومات ووسائل الإتصالات لحماية الوطن والمواطن والمؤسسات من مخاطر "**التهديدات السيبرانية**".

الإطار المنهجي والمفاهيمي والنظري

أولا : مشكلة الدراسة:

الإشكالية الرئيسية:

يقتضي إستمرار منظومة الأمن الوطني الجزائري والمحافظة على كيانها، ضرورة التكيف مع التغيرات التي تواجهها سواء في البيئة الداخلية أو الخارجية، وتحديد التهديدات السيبرانية التي يواجهها الوطن والمواطن والقطاعات العامة والخاصة، إنطلاقا من أهمية الفعل داخل المنظومة بصورة عقلانية لنشاط يقوم به مجموعة من المختصين الفاعلين بإستراتيجية واعية لتحقيق أهداف مشتركة وواضحة. من هنا يطرح الإشكال الذي يفرض نفسه في هذه الدراسة: **ما مدى تأثير التهديدات السيبرانية على إستقرار الأمن الوطني الجزائري؟ وكيف تتعامل منظومة الأمن الوطني مع تلك التهديدات؟**

الإشكاليات الجزئية:

لتبسيط الإشكالية الرئيسية يتم طرح التساؤلات التالية:

1. ما المقصود بعقيدة الأمن الوطني الجزائري؟ وكيف تم تطويرها؟

2. ماذا نتج عن إستخدامات الأنترنت في الجزائر؟

3 . ما هو دور الأجهزة الأمنية المختصة في إرساء الأمن السيبراني؟ وهل ستنجح في وضع خططتها الإستراتيجية لمكافحة المخاطر السيبرانية؟

ثانيا: مجالات الدراسة:

1. المجال المكاني: يتحدد المجال المكاني لهذه الدراسة من خلال عنوان الموضوع، والذي يتعلق بالدولة الجزائرية وتحديدا منظومة الأمن الوطني الجزائري.

2. المجال الزماني: تقتصر الدراسة على الفترة الزمنية التي تمتد منذ بداية إنشاء هيئات ومؤسسات أمنية مختصة في مجال مكافحة التهديدات السيبرانية منذ سنة (2009 إلى غاية 2018).

3 . المجال الموضوعي: كثرة المتغيرات والمحددات المؤثرة في الأمن الوطني الجزائري وتعددها، التي يستوجب تحديدها وتحليلها ووضع خطط وإستراتيجيات للبحث عن حلول لها.

ثالثا: أهمية الدراسة:

1. الأهمية العلمية: يكتسي موضوع الدراسة أهمية علمية إنطلاقا من المتغيرات المراد تحليلها، حيث باتت إشكالية "**الأمن السيبراني**" تحظى بوتيرة إهتمام متزايد وإجتهادات من طرف الباحثين والأكاديميين، بهدف فهم وتبسيط هذا المفهوم الجديد "**الأمن السيبراني**" وقدرة التفسير لمختلف الحركيات المرتبطة بعاملي التحدي

والتهديد من جهة ومدى ضبطه في إطار علمي يمكن الباحث من إستيعاب هذه التحولات من خلال معرفة أسبابها وعمق تأثيرها على واقع البنى الأساسية (الدول).

2 . الأهمية العملية: أما عمليا فتقع الأهمية على مدى إدراك مختلف تجلياتها، ومدى تعميق هذا الواقع الراهن ومعرفة العلاقة الترابطية بين الأمن الوطني والتهديدات السيبرانية (تأثير وتأثر)، ما بات يحتم على الأجهزة الأمنية العملياتية المختصة ضرورة تبني إستراتيجيات وسياسات قطرية تهدف إلى التمكن من مكافحة هذه التهديدات والتحديات الإلكترونية وضمان "**أمان سيبراني**" شامل.

رابعا : فرضيات الدراسة

1. الفرضية الرئيسية: تنطلق الدراسة من فرضية رئيسية مع محاولة التثبت من صحتها مفادها أن الجزائر تواجه تحديات سيبرانية تشكل تهديدا لعناصرها ومرتكزات أمنها وإستقرارها، وفي إنتظار الإجابة على الإشكالية المطروحة تم الإعتماد على فرضية رئيسية كإجابة مؤقتة: **يعد التشخيص الإستراتيجي لمتغيرات البيئة الداخلية والخارجية، من تمكن للأجهزة الأمنية من تحديد نقاط القوة ومواطن القصور وإقتناص الفرص وتجنب التهديدات السيبرانية.**

2.الفرضيات الجزئية:

1- تساهم تكنولوجيا المعلومات والإتصالات في تحقيق مزايا تعاونية في المجال السيبراني للمؤسسات الأمنية الجزائرية في ظل إعتمادها على أسلوب التسيير.

2- تجد الأجهزة الأمنية نفسها مجبرة على إختيار البديل الإستراتيجي المناسب، في إطار مواجهة التحديات السيبرانية في الجزائر.

3- كلما كانت الخطط الإستراتيجية محكمة، كلما تحققت الأهداف الأمنية السيبرانية.

خامسا: مناهج وإقترابات الدراسة:

أولا: الإقترابات : من خلال طبيعة الإشكالية المطروحة يتوجب ضرورة إيجاد وإتباع مجموعة من المداخل المنهجية لمقاربة هذا الموضوع بطريقة علمية، وذلك بهدف التأسيس العلمي للموضوع من جهة، وبغية التوصل إلى نتائج علمية وعملية تمكننا من الوقوف على إتجاه وأهداف الدراسة بطريقة سليمة من جهة أخرى.

1.الإقتراب النسقي: يقوم هذا الإقتراب على فكرة أسياسية مفادها أن الحياة السياسية عبارة عن نسق موجود في بيئة يتفاعل معها أخذا وعطاءا، حيث وضع "**دافيد ايستون**" (David Eston) عدة مفاهيم يمكن إستخدامها في التحليل (مدخلات، المخرجات، التحويلية التغذية ...)، فهذه المفاهيم لها علاقة مرتبطة

بالموضوع وذلك من منطلق أن السياسة الأمنية الجزائرية هي عبارة عن مخرجات للنظام الأمني القائم في بيئة داخلية وخارجية للدولة والبيئة المجتمعية ككل، وتشكل المعلومات الواردة إلى المنظومة الأمنية الوطنية عبارة عن مدخلات مهما كان نوعها (بيانات حقائق، أحداث، وردود أفعال ...)، فكلها تمد الأجهزة الأمنية بمعلومات تساعدهم على بناء سياسات وإستراتيجيات واضحة؛ حيث يتم تحويل المعلومات الإلكترونية في شكل قرارات إلى الأجهزة الأمنية عبر فتحة المخرجات، ثم تعود العملية من جديد عبر التغذية العكسية، فهذا الإقتراب يساعد الدراسة في معرفة العلاقة بين المعلومة ومصادرها وصناع القرار في منظومة الأمن الوطني الجزائري، فمن خلال هذه المقاربة يمكن النظر للمؤسسات الأمنية كجهاز يضع الخطط والإستراتيجيات على أنها مبنية على عملية تدفق المعلومات.

2.الإقتراب الإتصالي: تعبر هذه المقاربة عن تدفق المعلومات بين طرفين (مرسل ومستقبل)، عبر وسيط محدد قصد التأثير والتغيير، وذلك حسب العالم الأمريكي "**كارل دويتش**"(karl deutsh) فهذا الإقتراب يساعد الدراسة في معرفة العلاقة بين المعلومات الإلكترونية ومصادرها وبين صناع القرار في منظومة الأمن الوطني الجزائري، وكيفة التعامل مع تلك المعلومات، فهناك علاقة جوهرية بين العملية الأمنية والعملية الإتصالية، من حيث أن المؤسسات كجهاز يضع الخطط والإستراتيجيات على أنها عملية تدفق المعلومات.

ثالثا: الإقتراب الوظيفي: تعتبر فكرة الوظيفية عند علماء السياسة الوظيفيون هو كل ما يترتب عن نشاط إجتماعي من نتائج تؤدي إلى تكيف هذا النشاط مع بناء معين أو جزء منه، حيث ينطبق هذا المقترب على نشاط المجتمع الجزائري المعلوماتي وتكيفه مع إستخدامات الأنترنت ووسائل التواصل الإجتماعي، وما خلفته من نتائج سلبية تتمثل في المخاطر التي تهدد أمنهم وأمن الدولة، أما "**غابريال ألموند**" (Gaberiel A.Almond) فيرى أنها مجموعة الأنشطة الضرورية التي يعد إنجازها ضروريا لبقاء النظام واستمراره ككل، وهو ما تسعى إليه الحكومة الجزائرية بقياس مدى فاعلية الإستراتيجيات الأمنية من خلال تفاعل الأجهزة الأمنية مع مسألة التحديات والمخاطر السيبرانية التي تهدد أمن الوطن والمواطن.

ثانيا: **المناهج:** إستدعت الدراسة ضرورة الإستعانة في خطوات البحث بمجموعة من المناهج التي تساعد في إنجاز دراسة بحثية وفق أسس محضة والتعريف بأهم المناهج التي يتم توظيفها في سياقات الدراسة.

1.المنهج التاريخي: يهدف هذا المنهج لتوضيح السيرورة التاريخية للأهم الأحداث من خلال تتبع مراحل تطوير العقيدة الأمنية الجزائرية عبر مسار تاريخي إرتبط بالتغيرات الحاصلة في مجال الظواهر الأمنية التي عرفتها

الجزائر منذ الإستقلال. كذلك الحركات الديناميكية لاستخدامات الانترنت في الجزائر التي تستمد أسسها منذ أواخر التسعينيات إلى يومنا هذا.

2.**النهج الوصفي التحليلي**: تبرز أهمية هذا المنهج في قدرته على فهم عمق الظواهر المتعلقة بموضوع الدراسة وتحليلها وفق أسس علمية سليمة، حيث يمكن إستعمال هذا المنهج في توصيل البيئة الأمنية السيبرانية في الجزائر وتحليل مختلف الفواعل والديناميكيات المرتبطة بالموضوع من تفسير وتحليل التحولات الأمنية في الجزائر وفهم تجلياتها وأبعادها على واقع ومسار منظومة الأمن الوطني الجزائري.

3.المنهج المقارن: يتم الإعتماد على هذا المنهج من خلال طبيعة الموضوع الذي يقتضي ضرورة المقارنة في إستخدمات الانترنت في الجزائر مقارنة مع نظيراتها من باقي الدول الأخرى، كما تم التطرق لأوجه الشبه وأوجه الإختلاف في الخطط الإستراتيجية التي تتخذها الأجهزة المختصة في مجال مواجهة التحديات السيبرانية.

سادسا: تحديد مصطلحات الدراسة:

يفضي المجال المعرفي في الغالب لأي دراسة إلى تحديد طبيعة ونوع المفاهيم التي من المحتمل أن تتعامل معها الدراسة، فإن الغموض قد لا يكون دائما هو الدافع الأساسي لتحديد المصطلحات، وإنما الإستخدام الوظيفي للمصطلح ضمن الدراسة هي التي تفرض تحديد دلالاته، ومن أهم المفاهيم التي تتماشى مع الموضوع ما يلي:

1.الإستراتيجية: (Strategies) لا يمكن أن تنغلق الإستراتيجية على نفسها في الحقل العسكري فقط، بل ميز المفهوم الكلاسيكي للإستراتيجية بين مجالي الحرب والسلام وترك المكان لنظام جديد يتواجد في داخله المفهومان بشكل مندمج، ويكملان مفهوم الاستراتيجية التي لا يمكنها أن تحد نفسها في مجال واحد فقط،[1] فالإستراتيجية هي مجموعة المحددات التي توجه أو ترشد صناع القرار في سعيهم لبلوغ الأهداف المحددة الآجال. أما الإستراتيجية الأمنية فقد عرفت منحنى متوافق مع تغير مفاهيم الأمن التي عرفت تراجع واضح للإستراتيجية العسكرية من خلال التذبذب الواضح الذي ظهر على مستويات التسلح العسكري للدول.[2]

التحديات الأمنية: (Security Challenges) هي تلك المشاكل أو الصعوبات أو الأخطار التي تواجه الدولة، وتحد وتعوق من تقدمها، وتشكل حجر عثرة أمام تحقيق أمنها واستقرارها ومصالحها الحيوية الذاتية

[1] – صلاح نيوف، "**مدخل للفكر الاستراتيجي**"، (الدنمارك، المركز الأكاديمي المفتوح للعلوم السياسية)، ص 89

[2]– نسيمة طويل، "**الاستراتيجية الأمنية الأمريكية في منطقة شمال شرق آسيا: دراسة لمرحلة ما بعد الحرب الباردة**"، أطروحة دكتوراه علوم، (جامعة الحاج لخضر، باتنة كلية العلوم السياسية: تخصص علاقات دولية، 2009–2010)، ص 58

والمشتركة، ويصعب تجنبها أو تجاهلها، وقد تبدأ أو تنتهي بزوال أسباب بلوغ المفروض عليه التحدي مستوى نفسه، دون الوصول إلى مستوى التهديدات، حيث يصبح هناك توازن بين الطرفين، بيد أن الوصول إلى مرحلة التوازن يستغرق وقتا زمنيا أكبر من ذلك الوقت الذي يستغرقه التهديد.[1]

السياسة الأمنية: (Security Politics) يعتقد الكثيرون أن السياسة الأمنية تمثل سياسة دفاعية فقط. كونها لا تسعى لاستغلال الفرص المتاحة من أجل تحسين الوضع الأمني بصورة دائمة، فالمفهوم العسكري للسياسة الأمنية يقوم على وضع برامج ومخططات وسياسات تضمن أمن الدولة من أخطار خارجية تحدق بها، إلا أن التحولات التي مست مفهوم الأمن من الإنتقال إلى هتمامات الأمن بعد الحرب الباردة ومن ثم إلى تهديدات أخرى متعلقة بالبيئة الرقمية. فالسياسة الأمنية في جوهرها هي مجموعة من البرامج والإستراتيجيات المحددة لتحقيق أهداف ومصالح الأفراد والمجتمعات.[2]

التهديدات التكنولوجية:(Technologie Thread) في ظل الثورة الهائلة في تكنولوجيا الإعلام والإتصال التي يشهدها العالم اليوم، أصبحت المعرفة والإختراع والإبتكار أساس الثروة والنفوذ والسلاح الرئيسي للريادة الإقتصادية والإجتماعية والثقافية، وهو الأمر الذي أدى إلى رفض تحديات متزايدة على الدول النامية والمتقدمة في جميع المجالات، حيث بدأت تطرح شكوكا حول إيجابية كل تطور تقني.[3]

سابعا: المدخل النظري للدراسة:

مما لا يمكن تجاهله تلك العلاقة بين عالم النظرية المجردة وعالم الواقع الفعلي، فالنظرية تفسر الظاهرة، من ثم تسهم في تحليلها وفهمها كما أنها توفر القدرة على التنبؤ بما يحمل أن يؤول إليه تطور الظاهرة في المستقبل.

تمثل **"الأمننة"** أحد التطورات في الدراسات الأمنية لتحليل النموذج الجديد للأمن الذي ظهر خلال الحرب على الإرهاب (أحداث 11 سبتمبر 2001)، ففي عصر المعلومات إختفت أنواع التهديدات الأمنية عن التهديدات التقليدية للأمن في نواح كثيرة، والأمر الأكثر وضوحا في هذا السياق هو الطريقة التي يتم من

---

[1]– إدريس عطية،"**الإرهاب في إفريقيا: دراسة في الظاهرة وآليات مواجهتها**"، رسالة ماجيستير، (جامعة الجزائر–3–، كلية الحقوق والعلوم السياسية، والعلاقات الدولية، تخصص: دراسات إفريقية، 2011)، ص 29

[2] – خديجة بتقة، "**السياسة الأمنية الأوروبية في مواجهة الهجرة غير الشرعية**"، رسالة ماجيستير، (جامعة محمد خيضر، بسكرة، كلية العلوم السياسية والعلاقات الدولية، تخصص: علاقات دولية استراتيجية، 2013–2014)، ص 15

[3] – أحمد براهيم، "**الدولة العالمية والنظام الدولي الجديد**"، أطروحة دكتوراه، (جامعة السانيا، وهران ، كلية العلوم الاجتماعية،2009–2010)، ص 187

خلالها التصدي لهذه التهديدات الجديدة، حيث لا يمكن التصدي لها بالقوة الساحقة، ولا حتى من خلال بعض أنواع توازن القوى، وإنما من خلال شبكات معقدة، من السياسات المتشابكة، فالحروب الجديدة لا تخاض، وإنما يتم إدارتها. فمفهوم "**الأمننة**" (**لمدرسة كوبنهاغن**) يمثل إطارا يمكنه أن يكون مثمرا من خلال دعواته إلى تحديد آليات أساسية، خلف إعلان الأمن في مجموعة متنوعة من القطاعات، فهذا المفهوم يصف عملية القيام بتحويل قضية معينة إلى نهاية أمنية ثم تقديمها بلغة أمنية وهذه العملية في حد ذاتها تستدعي عدد من المفاهيم الأخرى، مثل: "**الموضوع المرجعي**" (refrent object)، ويعني الشيء الذي يتم تهديده والذي يحتاج إلى الحماية كالدولة والأمة وسيادتها وغيرها، ف "**حركة الأمننة**" (securitizing move)، والتي تعني عملية تقديم قضية معينة باعتبارها "**تهديدا وجوديا**" (existential threat)، للموضوع المرجعي المحدد، وهذه الحركة تتم من طرف الجهات الفاعلة في عملية الأمننة (securiting actor)، تقدم إلى الجمهور (audience). بحيث قدمت أمننة القضايا المرتبطة بتكنولوجيا المعلومات عموما في أواخر التسعينيات، ووضع بعد ذلك "**هانسن**" (Hansen) و"**نيسنباوم**" (Nissenbaum) تصورا "**للأمن السيبراني**" كقطاع منفصل إلى جانب قطاعات الأمن الخمسة التي حددها "**باري بوزان**" (Barry Buzan) وزملائه من قبل في إطار الدراسات الأمنية النقدية، وقطاع الأمن السيبراني يتميز بمجموعة مركبة من المسؤوليات في القطاعين العام والخاص والسلطة الحكومية، كما يتميز عن بقية القطاعات بالطريقة التي ترتبط من خلالها الموضوعات المرجعية المتمثلة في الفرد والشبكة بالأمن القومي أو أمن النظام والدولة. كما تحاول هذه الدراسة توظيف "**مفهوم الأمننة**" **لمدرسة كوبنهاغن** من خلال أمننة قضايا البيئة الرقمية والفضاء السيبراني بتشخيص التهديدات للدولة والمجتمع الجزائري، ومن خلال تحديد فواعل أمنية متمثلة في القطاعين الحكومي والخاص، بالإضافة إلى تحديد سياسات وإستراتيجيات الأجهزة الأمنية المختصة لمواجهة تلك التهديدات.[1]

ثامنا: أدبيات الدراسة:

تبلور موضوع الدراسة إنطلاقا من مجموعة الأدبيات السابقة التي تعتبر منطلقا مهما في خوض هذه التجربة البحثية، وفي هذا الصدد يمكن الإشارة إلى مجموعة منها:

[1] – فريدة طاجين،"**سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية: واقع وتحديات**"، جامعة قاصدي مرباح، ورقلة، كلية الحقوق والعلوم السياسية، ص 341

الدراسة الأولى: كتاب لـ "**منى الأشقر جبور**"بعنوان: "السيبرانية هاجس العصر"، حيث تندرج الدراسة في إطار جهود جامعة الدول العربية، التي أخذت على عاتقها منذ سنوات مهمة نشر الوعي، على مستوى مراكز القرار العربي، بأهمية الأمن السيبراني، والحاجة إلى التعاون لتحقيقه، كما تندرج الدراسة أيضا في إطار الإهتمام الدولي المتصاعد "**بالأمن السيبراني**" بدءا من الممارسات الحكومية، مرورا بالعلاقات بين الدول، وصولا إلى جهود المنظمات الدولية والإقليمية، منها الأمم المتحدة، الإتحاد الأوروبي، دول الكومنولث، جامعة الدول العربية.

الدراسة الثانية: "**أحمد عبيس الفتلاوي**" الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، حيث تهدف هذه الدراسة إلى المرتبة المتقدمة التي يحتلها موضوع "الهجمات السيبرانية" في الجهد القانوني، وبالذات عند المؤسسات المتخصصة لتحليل أحكام القانون الدولي العام والجهود الدولية ذات الصلة بتنظيم إستخدامها بالخطر أو التقييد.

الدراسة الثالثة: الدراسة التي قام بها كل من: " **عنترة مرزوق** " و"**محي الدين حرشاوي**" حول: "الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية"، وتهدف هذه الدراسة إلى الجهود الجزائرية في مجال تحقيق الأمن السيبراني، والتي تعتبر أن الإرهاب الإلكتروني كأحد أخطر التهديدات المحتملة على الأمن الوطني الجزائري في ظل الثورة التكنولوجية الحديثة.

الدراسة الرابعة: كتاب لـ"**إيمان بن سالم**" بعنوان: "جريمة التجنيد الإلكتروني للإرهاب وفقا لقانون العقوبات الجزائري"، حيث يهدف الكتاب إلى محاولة الإحاطة بالشكل المستحدث للإرهاب المتمثل في التجنيد الالكتروني ورفع الستار عن أهم العوامل والاستراتيجيات المتبعة من أجل إنجاح عملية التجنيد، وتوضيح الرؤية وتسيير سبل الحد من الظاهرة.

تاسعا: هيكل الدراسة:

لتحقيق الأهداف المرجوة ونظرا لإتساع الموضوع وتشعب فروعه وقصد إعطاء القدر الكافي من الإهتمام والتركيز، تم الإعتماد على منهجية تقسيم الدراسة إلى ثلاث فصول مقسمة حسب ثلاثة مباحث ويحتوي مضمون كل مبحث على ثلاث مطالب وفق ترتيب الفصول كما يلي:

الفصل الأول: يتمحور حول "**الأمن السيبراني**" حيث يعالج مفهوم الأمن السيبراني وأبعاده وأهم الفواعل في الفضاء السيبراني، ثم التطرق إلى التهديدات السيبرانية وأنواعها، ومدى تأثيرها على الأمن القومي.

الفصل الثاني: يسعى هذا الفصل إلى تحولات في مفهوم الأمن وتأثيرها على أمن الدول، وبما أن الجزائر واحدة من تلك الدول خاصة بعد استقلالها عرفت مجموعة من التهديدات الأمنية، فبتوسع تلك التهديدات جعل الجزائر تفحص عقيدتها الأمنية وتعمل على تطويرها للحد من تلك التهديدات والتحديات.

الفصل الثالث: يحتوي هذا الفصل على دراسة تحليلية لإستخدامات الأنترنت في الجزائر وما خلفته من ظهور مجتمع معلوماتي مما أدى إلى بناء حومة إلكترونية، حيث عرفت الجزائر وكغيرها من الدول مجموعة من التهديدات السيبرانية جعلها تعمل على إنشاء هيئات مختصة لمحاربة تلك التهديدات.

الفصل الأوّل: البناء الإيتومولوجي للأمن السيبيراني.

المبحث الأوّل: مقاربة مفاهيمية للأمن السيبيراني.

المبحث الثاني: التهديدات الأمنية السيبيرانية.

المبحث الثالث: آليات استخدام القوة السيبيرانية.

تمهيد الفصل الأول:

لقد حازت مسألة "**الأمن السيبراني**" على المزيد من الاهتمام على جميع المستويات العالمية والإقليمية والوطنية سواء من جهة ارتفاع عدد الهجمات والتهديدات أو الأضرار الناجمة عنها، حيث شهدت جل دول العالم بما فيهم الجزائر في الآونة الآخيرة اختراقات أمية مقلقة إستهدفت المؤسسات والشركات وحتى الأفراد إلى سرقة البانات والقرصنة والتجسس والتجنيد والإرهاب الإلكتروني وغيرها. فقد أصبحت هذه التهديدات السيبرانية الجديدة أكثر شيوعا في الوقت الراهن كما أنها مسألة المستقبل أيضا. وعلى ضوء تلك التهديدات يطرح التساءل التالي: **ما هو الأمن السيبراني؟ وهل أثر هذا المفهوم على تحولات في إستخدامات القوة وظهور فواعل جديدة؟**

المبحث الأول: مقاربة مفاهيمية للأمن السيبراني

المطلب الأول: مفهوم الأمن السيبراني

السيبرانية لغة: يعود منشأ كلمة "**السيبراني**" إلى اللغة اليونانية، وبالذات كلمة "**كبيرنتيك**" (Kebrentic) وتحمل هذه الكلمة معنى يدمج بين المقصودين: **التوجيه** (steering)، و**الحوكمة** (gouvermance) حيث استخدم "**نوربرت فينر**" (Norbert Wiener)، فمصطلح "**السيبرانية**" لأول مرة عام 1948، من أجل وصف نظام التغذية الراجعة (Feedbak)، الذي يعمل على الإستفادة من مخرجات الأنظمة في ظبط مدخلاتها والتحكم فيها، واستقرار أدائها ورأى "**فينر**" أنه يمكن تطبيق هذا النظام على نطاق واسع.[1]

و حسب قاموس الأمن المعلوماتي، فمصطلح "**السيبرانية**" تعني هجوم عبر الفضاء الإلكتروني، يهدف إلى السيطرة على مواقع إلكترونية أو بنى محمية إلكترونيا أو تدميرها، أما بالرجوع إلى مختصين في اللغة العربية فنجدهم يواجهون تحديا في إختيار مصطلح مقارب لمصطلح (cyber) بالنسبة للغة الإنجليزية، سوى الترجمة العربية لعنوان إتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، والتي كانت ترجمة غير صائبة، إذ تم ترجمة العنوان (convention on cybercrime)، إلى اللغة العربية (**الإتفاقية المتعلقة بالجريمة الإلكترونية، ويعود السبب في عدم وجود مصطلح مناظر في اللغة العربية**).[2]

السيبرانية إصطلاحا: تعني ترابط الحواسب مع أنظمة أوتوماتيكية، والنظم الإلكترونية المركزية بتنسيق كل الآلات والمعتدات التي تستخدم المدينة، الأمة، والعالم بشكل شامل، لتحقيق أعلى رفاهية للبشر جميعا ويمكن للمرء أن يفكر بهذا كنظام إلكتروني عصبي، لا إداري يمتد في كل مناطق التركيبة الإجتماعية.[3]

الأمن السيبراني هو مجموعة الوسائل التقنية والإدارية، والتي يتم استخدامها لمنع الإستخدام غير مصرح به وسوء الإستغلال واستعادة المعلومات الإلكترونية ونظم الإتصالات والمعلومات التي تحتويها بهدف ضمان توافر

---

[1] – سعد علي الحاج علي بكري، "**الأمن السيبراني ومعضلة حمايته.. عولمة التعليم العالي.. الرقمي**"، جريدة العرب الإقتصادية الدولية، العدد 25، (24 أوت 2017)، ص24

[2] – أحمد عبيس نعمة الفتلاوي، "**الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر**"، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، (السنة الثامنة، 2016)، ص 214

[3] – تولاي آسر، "**ما هي السيبرانية؟ وما دورها في صناعة القرار**"؟ 20 جانفي 17:53/2018 http//Zeitgeistarrabia.com

واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطن من مخاطر الفضاء السيبراني.[1]

فيمكن تعريف الأمن السيبراني على أنه أمن الشبكات، والأنظمة المعلوماتية، البيانات، المعلومات، والأجهزة المتصلة بالانترنت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض إتخاذها، أو الإلتزام بها، لمواجهة التهديدات، أو للحد من آثارها في أقسى وأسوأ الأحوال. ويرتبط هذا الأمن إرتباطا وثيقا، بأمن المعلومات، فالوصول إلى هذه الأخيرة أو بثها أو الإطلاع عليها والمتاجرة بها، أو تشويهها واستغلالها، هو ما يقف غالب الأحيان وراء عمليات الإعتداء على الشبكات وعلى الانترنت.

كما أن الأمن السيبراني ذلك النشاط الذي يؤمن حماية الموارد البشرية والمالية، المرتبطة بتقنيات الإتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقيق المخاطر والتهديدات. كما يتيح الفرصة لإعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، ولا تتحول الأضرار إلى خسائر دائمة.[2]

إذا، "**الأمن السيبراني**" (cyber security) هو سلاح إستراتيجي بيد الحكومات والأفراد، لا سيما أن التهديدات السيبرانية أصبحت جزءا لا يتجزأ من التكتيكات الحديثة للمخاطر والهجمات السيبرانية بين الدول.

المطلب الثاني: أبعاد الأمن السيبراني

أولا: الأبعاد العسكرية:

تطورت بدايات الأنترنت في بيئة عسكرية، بشكل أساسي، لتضاف إليه فيما بعد البيئة الأكاديمية، تتمثل في أبحاث تخدم تطوير القدرات العسكرية، والإنجازات العلمية التي تحافظ على تفوق بلد آخر، فتتمثل خطورة الهجمات السيبرانية، والتجسس والسرقة والإختراق التي ترجمت ماديا، سواء بإندلاع صراع مسلح لاحق، كالذي وقع بين روسيا وجورجيا، أو بانقطاع الإتصال بالانترنت في استونيا، بين الدولة والمواطنين والتشويش على الإدارات الحكومية، كما واجه خبراء أمريكيين خطابا مفتوحا إلى الرئيس "**جورج بوش**" (George W. Bush) في أيلول 2007 محذرين إياه، من خطر الهجمات السيبرانية على البنية التحتية

[1] – ليال بيطار، "**ماذا يعني الأمن السيبراني**"؟ 20 جانفي 2018 ، الوقيت 17:58، http//anbaaoline.com

[2] – منى الأشقر جبور، "**السيبرانية هاجس العصر**"، (بيروت، المركز العربي للبحوث القانونية والقضائية،2013)، ص29

الأمريكية، التي تضم إلى الدفاع، إمدادات الطاقة الكهروبائية، والمياه والإتصالات السلكية واللاسلكية، والخدمات الصحية والنقل والانترنت.[1]

ثانيا: الأبعاد الاقتصادية:

ليست الغاية من الأمن المعلوماتي، كسب المال وإنما حماية الموارد الاقتصادية وتفادي خسارتها أو فقدانها، إذ تقرير الربح الحاصل من المعلومات غير متيسر، وإن تقدير تكلفة الأمن التي تتمثل بالميزات المرصودة، وتكلفة نواتج الأمن والتدريب وبناء مراكز السيطرة، وغيرها من الأمور المتعلقة به، إذ أن حساب تكاليف أمن المعلومات والخسائر الناتجة عن الأخطاء والأعمال الخبيثة، أمر صعب جدا لأنّ إحتياجات المؤسسة هي التي تحدد تلك التكاليف، وهي التي تعمل على الموجودات التي يراد حمايتها، والأضرار الناجمة عن عدم كفاية الأمن واحتمال التعرض لهجمات أو إختراقات، حيث لا يمكن تحديد المخاطر التي تتعرض لها المؤسسة أو الدولة، ولا يمكن أيضا تحديد القيمة الإقتصادية للأمن السيبراني، يجب أن تفهم من باب إجتماعي واسع، مع مراعاة تأثير التكنولوجيا الحديثة على الأفراد والمؤسسات والدول.[2]

ثالثا: الأبعاد الإجتماعية:

يشير تقرير مؤسسة (we Are Sosial) إلى نحو 2.5 مليار نسمة، أي ما يعادل 35% من سكان العالم يستخدمونه، ولا شك في أن هناك دورا للانترنت في تعبير المواطن عن تطلعاته في المجالات المختلفة، سواء سياسية أو علمية أو إقتصادية أو ثقافية، ....الخ، وبعض من الموارد المنشورة والمفيدة وتؤثر بالإيجاب على أخلاقايت المجتمع، والبعض الآخر يمثل تهديدا له، كالإرهاب ونشر الفكر المتطرف، ومحاولة تجنيد الشباب، والترويج للإتجار بالممنوعات ... الخ. بالإضافة إلى جعل المواطنين أكثر إنكشاف على الثقافات الأخرى، ومن ثم تعرض القوميات والهويات لعمليات إختراق خارجي قد تؤثر على الأفكار والتوجهات والعادات، خاصة أنها قد تخرج عن النسق العام للدولة، وتسبب في تهديد السلم الإجتماعي،

[1] – منى الأشقر جبور، "**الأمن السيبراني: التحديات ومستلزمات المواجهة**"، المركز العربي للبحوث القانونية والقضائية، (مايو 2012)، ص16

[2] – أوس مجيد غالب العوادي،"**الأمن المعلوماتي السيبراني**"، (بيروت، مركز البيان للدراسات والتخطيط، 2016)، ص06

وعليه فلا بد من العمل على توعية المواطنين بتلك النوعية من المخاطر لتحقيق الأمن السيبيري في بعده المجتمعي.[1]

رابعا: الأبعاد السياسية:

وتتمثل في مسؤولية الدولة وسيادة الدول

- **مسؤولية الدولة:** تقع على عاتق الدولة مسؤولية كبيرة لتحقيق الأمن السيبراني، حيث لا ينبغي لعمل الدولة أن تقتصر على مجرد تعزيز وتشجيع البحث والتطوير في مجال الأمن، وإنما يجب أن يتعدى ذلك إلى تعزيز ثقافة أمنية، ومن الضروري على المستوى الاستراتيجي تأمين إدارة الوقاية، والإبلاغ وتقاسم المعلومات والانذار وزيادة الوعي بأفضل الممارسات في مجال الأمن وإدارة المخاطر.
- **سيادة الدول:** تتعارض الرغبة في اتباع البساطة والفعالية في الأمن، مع تعقد الاحتياجات والبيئات، الأمر الذي يجعل أمن النظم والمعلومات إلى موردين مختصين أمرا أكثر جاذبية، ويختلف هذا الاتجاه درجة عالية من التبعية وهذه المخاطر الرئيسة للأمن، وعلى الدول أن تحاذر من أن تصبح معتمدة في إدارتها الاستراتيجية والتكتيكية والتشغيلية لأمنها، على كيانات خارجية تقع خارج سيطرتها، وللحكومات دور في تقليل خطورة نقاط التعرض في التكنولوجيا والحلول الأمنية.[2]

خامسا: الأبعاد القانونية:

أعلن المستشار القانوني للجنة الدولية للصليب الأحمر " **لوران جيسل**" (Laura Gisil) أن المادة 36 من البروتوكول لعام 1977، يلزم الدول الأطراف بأن تكون الأسلحة الجديدة متوافقة مع أحكام القانون الدولي، إلا أن عدم تنظيم استخدام الفضاء السيبراني لا يعني تركه لمشيئة المتعاديين، فهناك أحكام عامة تفرضها قواعد الأخلاق، ومبادئ الإنسانية، وهناك أيضا نصوص مدونة بشأن الهجمات الجوية والبحرية، تلائم طبيعة التهديدات السيبرانية، ويمكن أن تطبق عليها، حيث كشفت تسريبات أن الحكومة الأمريكية تنفق

[1] – محمد مختار، "**هل يمكن أن تتجنب الدول مخاطر الهجمات الالكترونية**"؟، اتجاهات الأحداث، العدد 06، (يناير 2015)، ص 06

[2] – حمدون توريه، "**الأمن السيبراني في لبلدان النامية**"، الاتحاد الدولي للاتصالات، (2006)، ص 15

4.3 مليار دولار سنويا، على العمليات السيبرانية سنة 2011، وتم إعلان أكثر من 130 دولة حول العالم عن تخصيص أقسام قانونية خاصة بالتهديدات السيبرانية.[1]

المطلب الثالث: الفواعل الأساسية في الفضاء السيبراني

يمكن تقسيم الفواعل في الفضاء السيبراني ومن لديهم القدرة على الفاع السيبراني أو شن الهجمات الالكترونية إلى ما يلي :

أولا: الدولة:

تمثل الخطر الأكثر والفاعل قوة في مجال الفضاء السيبراني، فهي نهاية عام 2008، إستطاعت حوالي 180 دولة أن تمتلك ترسانة من الأسلحة الالكترونية، مما قد يدفع الفواعل من الدول ومن غير الدول للتنافس في السنوات القادمة من أجل تحقيق التفوق الإلكتروني. ونتيجة لما يقدمه الفضاء السيبراني فرض الفواعل لتحقيق مصالحهم، تسعى عديد من الدول إلى تطوير قدرتها في هذا المجال، وتنقسم القدرات السيبرانية للدول بشكل عام إلى قدرات دفاعية وأخرى هجومية، ولكن أضاف كل من "**ريتشارد كلارك**" (Ritchard Clarke) و"**روبرت كناك**" (Robert Knake)، في كتابيهما عن الحرب الإلكترونية باعتبارها الخطر القادم الذي يهدد الأمن القومي للدول. ويعتبر بعدا آخر يرتبط بمدى إعتماد الدول في الفضاء السيبراني لإدارة شؤون الدولة، فقدرة الدولة تزيد كلما زادت قدراتها الهجومية والدفاعي، وقل اعتمادها نسبيا على الفضاء السيبراني مقارنة بغيرها من الفواعل.[2]

ثانيا: الفواعل من غير الدول:

إن تصاعد خطر الفاعلين من غير الدول على الأمن السيبراني في العلاقات الدولية قد أثر بدوره على سيادة الدول، وبخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود الدولية وبروز أخطار القرصنة والجريمة الإلكترونية والجماعات الإرهابية، ومن جهة أخرى فقد فرض ذلك تحدي الحفاظ على الأمن دون إشراك هؤلاء الفاعلين الجدد في تحمل المسؤولية والعبء في تأمين البنية التحتية المعلوماتية وبدأ يظهر اتجاه التعددية في

[1] – طارق المجذوب، "**ساحة "خفية" لحرب "ناعمة" قادمة"!**، منشورات الدفاع الوطني اللبناني، العدد 89، (تموز 2014)، ص58

[2] – نوران شفيق،"**أثر التهديدات الالكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني**"، (القاهرة، المكتب العربي للمعارف، 2014)، ص 40

الحفاظ على الأمن بين كافة أصحاب المصلحة من الحكومات والمجتمع المدني والقطاع الأكاديمي والتقني والقطاع الخاص ووسائل الإعلام.[1]

إن ظهور الأطراف الجدد من غير الدول في تزايد مستمر، فعبور نشاطات هذه الأطراف للحدود جعل التفاعلات الدولية أكثر تعقيدا، حيث أفرزت هذه الأطراف أنماطا جديدة من المشكلات والمنازعات، فقد ساهمت هذه التنظيمات في (خصخصة الحرب وأصبحت تساهم في التدريب والتجنيد والحوار...الخ). وبرزت مشكلات الحروب الفضائية التي تمثل الفيروسات بخسائر وصلت إلى حوالي 15 مليار دولار، كما أن جماعات الجريمة المنظمة كلفت من خلال انتهاكات للملكية الفكرية وسرقة البيانات حوالي تريليون دولار في عام 2008، كما أن شبكات التجسس الإلكتروني إقتحمت 1295 حاسوبا في 103 دولة منها 30% أهداف حكومية مهمة.

ثالثا: الفرد:

أضحى الفرد فاعلا مهما في الفضاء السيبراني، حتى أن له القدرة على إحداث ثورة الرقمية، لتصبح تلك الثورة مجال إستخدام للدولة نفسها، ومثال ذلك ما قام به "**مارك زوكربارغ**" (Mark Zoukberg) عام 2004، حين أسس الـ (facebook)، لتستقطب أكثر من مليار مستخدم عبر العال. وغيرها من وسائل التواصل الاجتماعي بمختلف أنواعها، حيث تبقى هذه الوسائل بحرا لحرية الأفراد الذين يمارسون نوعا من المعارضة الإفتراضية، إلا أن هذا الجانب من الحرية أعطى الوقت للأفراد على اختلاف توجهاتهم وانتماءاتهم سواءا كانو رسميون أو غير ذلك، فسحة واسعة لنشر الأفكار والمعلومات سواء كانت سليمة أو ضارة بالآخرين، يبقى هنا يجب أن يتحلى الأفراد من وعي كاف كي يميز بين هذه الصفحات الإلكترونية ويبني مقاربة ثقافية توعوية. [2]

[1] – عادل عبد الصادق، "**خطر الحروب " السيبرانية" عبر الفضاء الإلكتروني**"، مجلة الأهرام لكمبيوتر الانترنت والاتصالات، (مارس2017)، ص27

[2] – اسماعيل قادير، "**إدارة الحروب النفسية في الفضاء الالكتروني: الاستراتيجية الأمريكية الجديدة في الشرق الأوسط**"، الندوة الدولية: عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية، جامعة الجزائر –3 –، 2016 ص05

رابعا: المجموعات الإفتراضية (Virtual Community):

تتخذ هذه المجموعات سمات متميزة تجعلها فضاءا مثاليا للتواصل، خاصة بالنسبة إلى الأجيال الشابة التي أضحت الثقافة الرقمية المرتكزة على الصورة تشغل حيزا مهما من حياتها بكل ما تحملهمن رموز ودلالات، وقواعد التواصل والتبادل، وعلاقات إجتماعية وغيرها، فالمجموعات الإفتراضية حسب "**هاورد رينغولد**" (Hawrd Rengold) وهي مجموعات تنشأ من الشبكة حين يستمر أناس بعدد كاف من الزمن لتشكيل علاقات شخصية في الفضاء السيبيري. أما البحث الإجتماعي "**نديم منصوري**"، فيرى أنها مجموعة من الأفراد يتشاركون عبر الانترنت لفترة زمنية، لتحقيق غاية أو هدف أو هواية، من خلال علاقة إجتماعية إفتراضية تحددها منظومة "**تكنو– إجتماعية**". فتتحقق المجموعات الإفتراضية من خلال بروزه كفاعل أو متفاعل أثناء عمليات التواصل عبر الشبكة، وتختلف هذه المجموعات حسب هوياتها حسب الباحثة الفرنسية "**فاني جورج**" (Vanny Gzorges) وهي الآتي: [1]

1. **الهوية التصريحية:** (Identité déclarative) تبرز من خلال المعلومات التي يجرى إدخالها من قبل صاحب الحساب.
2. **هوية ثنائية القطب:** (Diasporiens Bipolaires) تضم أقلية تعبر عن إرتباطها العميق في الوقت ذاته بالوطن الأم والبلد والمستقبل.
3. **هوية عالمية:** (Les Cosmopolites) تعرض إنفتاحا على مختلف الثقافات العالمية، وتشير الباحثة إلى أن هذه المجموعات لا تخفي حقيقة التغيرات والممارسات الهوياتية بفعل سهولة التواصل والتفاعل عبر الفضاء السيبراني.

[1] – كلثوم بيبيمون، السياقات "**الثقافية الموجهة للهوية الرقمية في ضوء تحديات المجتمع الشبكي من التداول الافتراضي إلى الممارسات الواقعية**"، مجلة "إضافات" العدد 23، (ربيع2016) ص 26

المبحث الثاني: التهديدات الأمنية السيبرانية.

المطلب الأول: مفهوم التهديد السيبراني.

التهديدات السيبرانية:

هي تلك التهديدات التي تواجه النظم المعلوماتية وإمكانية ممارسة أعمال القرصنة المعلوماتية بأبعادها المختلفة، فإن إمكانية إختراق تلك النظم من شأنه أن يخلق تهديدات أمنية خطيرة كالتأثير على حركة الطيران والمعاملات من خلال ميكانيزمات التجارة الالكترونية والأعمال البنكية والمؤسسات وغيرها، التي تستخدم الأسالب الآلية الحديثة في المعاملات. هذا إضافة إلى إمكانية إختراق منظمات الإتصال والتحكم في إدارة العمليات.[1]

فالتهديدات السيبرانية هي إستغلال الحاسبات وتكنولوجيا المعلومات في تخريب وتدمير البنية المعلوماتية للخصوم، بل وتعطيل شبكات الدفاع الجوي واختراق أنظمة المعلومات للبريد الإلكتروني لمكاتب رؤساء الدول والتجسس عليهم وفق خطة ممنهجة،[2] وهو ما فعلته الولايات المتحدة الأمريكية ومخابراتها لزعزعة الدول وتفتيتها وتدميرها من الداخل باستخدام بعض مواطنين هذه الدول وجماعاتها الداخلية لانتهاك إدارة بلادهم ونشر الفوضى فيها دون التدخل العسكري الذي يكبدها المال والأرواح.

إذا، التهديدات السيبرانية أو الهجمات السيبرانية هي التي تهدد أمن المجتمع وأمن الإقتصاد الوطني والجانب الأمني والعسكري للدول،كما أن للتهديدات السيبرانية أهداف مسطرة، حيث تمس كلا من الجانب المعنوي والجانب المادي وعلى جميع الأصعدة،[3] لكن ما يتوجب على الدول المعرضة لتلك التهديدات وضع خطط إستراتيجية من أجل مكافحتها والتخلص منها ويمكن التوضيح أكثر من خلال الجدول الآتي:

[1]– محمد سعد أبو عامود،"**المفهوم العام للأمن المعلوماتي**"، (مصر ، جامعة حلوان، 2013)، ص07

[2] CERT-UK. Common Cyber Attaks Reducing The Impact.the Informatio Cecurity Arm of GCHQ. 2015. P 05

[3]– أحمد السيد النجار، محمد عبد الهادي علام، "**حروب المعلومات ..من يواجهها**"؟، مجلة الأهرام، العدد 139، (13يوليو2015)، ص26

	الدفاع المجتمعي السيبراني	الدفاع الاقتصادي السيبراني	الدفاع العسكري السيبراني
القيم المهددة	الدين – الشباب – التراث – الأخلاق	الجودة – السرعة – التنافسية – الاختراعات التنموية – المعاملات المالية – التطوير الاقتصادي	العقيدة العسكرية – ميزان الرعب – ثقة الشعب بالجيش والأمن
أهداف التهديدات السيبرانية	نشر الإنحراف لتشكيل خلاليا إلكترونية مشوشة للدولة – الحصول على معلومات من الأفراد – التحريض على العنف – تشكيك الشعب بقدراته	تدمير التنمية الاقتصادية الإلكترونية – سرقة الأموال – تدبير التجارة الالكترونية – ايقاف التصدير والاستيراد –الحاق الخسائر المادية الاقتصادية	الحصول على معلومات تخص التسليح – التجسس على الاستخبارات– امكانية إعادة توجيه القتال والصواريخ الذكية – التجسس على البيانات الرقمية
استراتيجيات الدفاع الوطني	توصية الهيئات الشخصية والأجهزة الأمنية المختصة الوطنية وتوجه وتركز الدفاع الشعبي الالكتروني وتخطيط له	ضرورة توعية الخبراء والمختصين بمخاطر التهديدات والسيبرانية – الحرص على استمرار عدم انقطع الاتصال بشبكة الانترنت	الهجوم الالكتروني المضاد – محاكاة عملية الاختراق الأمني العملياتي – ولاء المسؤولين الأجهزة الأمنية – تطوير ترسانة السلاح الرقمي
أدوات الدفاع السيبراني	الشبكات الاجتماعية الالكترونية – البريد الالكتروني – مواقع وسائل الاعلام – تقنيات الحماية الالكترونية	مواقع الحماية من الفيروسات – إدخال نشاط أمن المعلومات إلى الشركات–تحفيز مواقع الانترنت الاحتياطي وتجهيز بريد الكتروني	توفير برامج الحماية– تجهيز منشآت هجوم الكتروني– توظيف النظمية الإكترونية في الهجوم على مواقع العدو
المسؤول عن الدفاع	كل من لديهم القدرة على عمل السلاح الرقمي	مديرية المعلوماتية في المؤسسات	وحدات خاصة بتقييم إحداثيات داخل الجيش والمخابرات، تكون مهمتها الدفاع والهجوم .

جدول يوضح: طرق استخدام التهديدات السبرانية وكيفية التعامل معها[1]

[1] – أحمد السيد النجار، محمد عبد الهادي علام، **حروب المعلومات ..من يواجهها ؟**، مجلة الأهرام، العدد 139، (13يوليو2015)، ص26

المطلب الثاني: أنماط التهديدات السيبرانية

تتعدد أشكال التهديدات السيبرانية وتختلف من حيث الطبعية والمصادر والأهداف كالتجسس وسرقة المعلومات وشن الحروب وبالتالي بات العديد من الفواعل الدوليين يلجئون الى آليات الكترونية لتحقيقها. وعلى الرغم من تعدد صور وأشكال الهجمات الإلكترونية، غير أنه من الممكن تقسيمها الى المجموعات رئيسية التالية:

أولا: خطر الكوارث الطبيعية أو (العرضية للكابلات البحرية):

تعد الكبلات (Submarine Cable) جزءا هاما لتوفير خدمة الاتصالات بين دول العالم في مجال الانترنت، وشبكات الكمبيوتر وغيرها. فمنذ عام 2005، أصبحت الكابلات البحرية مأهولة على مجال الإتساع والإنتشار، أما على نطاق التقدم والتطور تحولت إلى تقنيات أخف وزنا وأصغر حجما، كما تعرضت تلك الكابلات إلى عدد من المشكلات التي تؤثر سبا على أعما البنى التحتية بالضرر، حيث لا تقع في مياه المحيط العميق، هذا وقد تعرضت دول الشرق الأوسط لإنقطاع مفاجئ للانترنت بنسبة 80%، وحدث إنقطاع لـ50% كابلا في المحيط الأطلنطي في يونيو 2005، كذلك حدث خلل في شبكة الانترنت جراء زلازل في جنوب شرق آسيا في 27% ديسمبر 2006، أدى إلى تعطيل الاتصال.[1]

ثانيا: التجسس الإلكتروني: (Cyber Espionage):

يعد أحد أنواع التجسس التقليدي، باستخدام وسائل التكنولوجيا الفائقة، ومعظم الهجمات السيبرانية المتطورة التي تقع ضمن هذه الفئة، حيث يتم الحصول على معلومات سرية بطرق غير مشروعة بهدف الحصول على أفضلية إقتصادية، أو إستراتيجية أو عسكرية.[2] فالتجسس السيبراني هو ذلك التجسس الذي يعتمد علة إستخدام التقنيات الإلكترونية في الحصول على معلومات، ويختلف التجسس السيبراني من حيث النوع، فهناك التجسس عن طريق الأفراد، ومن خلال الشبكات السلكية أو التجسس من خلال الأقمار الصناعية.[3]

---

[1] عادل عبد الصادق،"**الفضاء الالكتروني وتهديدات جديدة للأمن القومي**"، المركز العربي للأبحاث الالكترونية، (2012)، ص13

[2]– نانسي البنا، "**الأمن السيبراني.. بيئة تكنولوجية أكثر أمنا**"، 20 جانفي 21:14/2018 http//boutiqueceena.eg

[3]– حسن بن أحمد الشهري،"**الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس**"، مركز النور للأبحاث الإلكترونية، (2010) ص11

ثالثا: الجريمة السيبرانية: (Cyber Crime):

الجريمة السيبرانية هي كل فعل أو إمتناع يتم إعداده أو التخطيط له، ويتم بموجبه استخدام أي نوع من الحواسيب الآلية سواء حاسب شخصي أو شبكات الحاسب الآلي أو الانترنت أو وسائل التواصل الاجتماعي لتسهيل إرتكاب جريمة أو عمل مخالف للقانون، أو تلك التي تقع على الشبكات نفسها عن طريق إختراقها بقصد تخزينها أو تعطيلها أو تحريف ومحو البيانات أو البرامج التي تم تحويلها، وتتكون الجريمة السيبرانية أو الإفتراضية من مقطعين هما: الجريمة (crime) والسيبرانية (cyber) ويستخدم مصطلح السيبرانية لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما الجريمة فهي السلوكيات والأفعال الخارجية على القانون. والجرائم السيبرانية هي المخالفات التي ترتكب ضد الأفراد أو مجموعات من الأفراد بدافع الجريمة قصد إيذاء سمعة الضحية بأذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الإتصال مثل الانترنت (كغرف الدردشة، البريد الالكتروني والموبايل) فالأعمال ذات الصلة بالحاسوب لأغراض شخصية أو مكاسب مالية أو ضرر، بما في ذلك أشكال الجرائم المتصلة بالهوية، والأفعال المتعلقة بمحتويات الكمبيوتر جميعها تقع ضمن معنى أوسع لمصطلح "**الجريمة السيبرانية**".[1]

فالجريمة السيبرانية أو المعلوماتية هي الإمتناع العمودي أو فعل ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب، ويهدف إلى الإعتداء على الأموال والممتلكات والخصوصيات المادية والمعنوية.[2] فالجريمة السيبرانية لها مسميات كثيرة هي: الجريمة المعلوماتية، جرائم الفضاء الافتراضي، جرائم الكمبيوتر والانترنت، جرائم مجتمع المعلومات وجرائم مجتمع المعرفة وجرائم مجتمع ما بعد المعلومات، وعلى اختلاف التسميات وتعدد مداخل الدراسات والتعاريف تتفق كلها على عنصر وحيد رئيسي لمفهوم الجريمة السيبرانية وهو الحاسب الآلي كأداة لكنه أيضا قد يكون معتدى عليه أو بيئة الجريمة.[3]

---

[1]– ذياب موسى البداينة،"**الجرائم الالكترونية: المفهوم والأسباب، ملتقى علمي حول: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية**"، كلية العلوم الاستراتيجية، عمان، المملكة الأردنية الهاشمية، (2014)، ص05.

[2]– سليم مزيود،"**الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها**"، جامعة المدية، الجزائر، (2015)، ص 96.

[3]– خديجة قصعة، جمال بن مرزوق،" **تفعيل آليات الحماية القانونية للحد من إنتشار الجريمة الإلكترونية في العالم والجزائر**"، مجلة تاريخ العلوم، العدد السادس، (جانفي 2010)، ص 247

فالجريمة السيبرانية أو الجريمة الإلكترونية هي الإستخدام السيئ لجهاز الحاسب الآلي وما يماثله بوسائل غير مشروعة للوصول إلى أهداف متعددة ومتنوعة ، وجميع جرائم الحاسب المعروفة والمسجلة تتضمن أدوارا أخرى والتي يكون للحاسب أثرا فيها وتتمثل في "**الهدف والبيئة والأداة والرمز**"، ومنه فجرائم الحاسب الآلي هي نشاط إلكتروني يؤدي إلى إلحاق الضرر بالغير ماديا أو معنويا عن طريق إستخدام الحاسب من الجاني ضد حاسب المجني عليه، فلقد يمكن أن يكون الحاسب الآلي بيئة للجريمة كتدمير البيانات أو التخريب لأجزاء الحاسب الآلي أو برامجه.[1] فالجريمة المعلوماتية هي كل إستعمال إحتيالي أو غير قانوني للشبكات المعلوماتية والإعتداءات على أنظمة المعلومات أو المعطيات المعالجة، وكذا الإعتداءات على الحياة الخاصة والمعلومات الشخصية، ونشر الفيروسات المعلوماتية وتبييض الأموال، والإحتيال والنصب على الأشخاص وتنظيم الشبكات الإرهابية وغيرها. والجريمة المعلوماتية تنطوي على صنفين من الجرائم المرتبطة مباشرة بتكنولوجيا المعلومات كأداة لارتكاب هذا النوع من الجرائم وهي تتضمن الجرائم التي تواجه في العالم المادي وأما اليوم فهي تواجه في العالم الإفتراضي للأنترنت.[2]

فالجريمة المرتكبة عبر الانترنت هي نشاط إجرامي يستخدم فيه التقنية الإلكترونية بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف، وهي نوع من الجرائم التي تتطلب الموضوع إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقق فيها ومقاضاة فاعليها.كما أن أي تصرف غير مشروع من أجل العمليات الإلكترونية تمس بأمن الأنظمة المعلوماتية والمواضع التي تعالجها فالجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها ويمثل إغراء بذلك، أو جريمة يكون الحاسب نفسه ضحيتها.[3]

رابعا: الارهاب السيبراني : (Cyber Terrorism):

المقصود بالإرهاب المعلومات أو الإرهاب السيبراني هو ذلك الإستخدام للموارد المعلوماتية، المتمثلة في الإعلام وأجهزة الحاسوب وشبكة الانترنت والفضائيات من أجل أغراض التخويف أو الإرغام لأغراض

---

[1]– عباس حفصي، "**جرائم التزوير الالكتروني، دراسة مقارنة**"، أطروحة دكتوراه، (جامعة وهران –1–، أحمد بن بلة، كلية العلوم الإسلامية، تخصص شريعة وقانون، 2015)، ص14

[2]– حنان براهمي، "**جريمة تزوير الوثيقة الرسمية الإدارية، ذات الطبيعة المعلوماتية**"، أطروحة دكتوراه علوم، (جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، تخصص قانون جنائي ، 2015)، ص 38

[3]– يوسف صغير، "**الجريمة المرتكبة عبر الانترنت**"، رسالة ماجيستير، (جامعة مولود معمري، تيزي وزو، كلية الحقوق، تخصص: قانون دولي للأعمال، 2014)، ص 52

سياسية، أو الاقناع الفكري والتثقيف السلبي والعدواني، ويرتبط الإرهاب المعلوماتي إلى حد كبير بالمستوى المتقدم للغاية والذي باتت تكنولوجيا المعلومات والإعلام تؤديه في جميع مجالات الحياة في العالم، ويمكن أن يتسبب الإرهاب المعلوماتي في إلحاق الشلل بأنظمة القيادة والسيطرة والإتصالات أو قطع شبكات الإتصاليين والوحدات والقيادة المركزية وتعطيل أنظمة الدفاع الجوي وغيرها. فقد ركز الرئيس الأمريكي السابق "**بيل كلينتون**" (Bee Klenton) على التصدي لإحتمالات الإرهاب المعلوماتي، حيث أن إنتشار الجماعات الجهادية على شبكة الانترنت مشكلة بذلك تهديدا إلكترونيا ويعد هذا التهديد هو الأكبر والأقرب لكل دول العالم، لأنه يمس بصفة مباشرة فكر الإنسان وعقله، حيث أرجع كثير من الباحثين المتخصصين في ظاهرة الإرهاب بعود بصفة عامة إلى وجود إنحراف فكري لدى من يقوم بهذه الأعمال.[1]

فالإرهاب السيبراني هو عبارة عن هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيا، توجه من أجل الإنتقام أو الإبتزاز أو الإجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي لتحقيق أهداف سياسية أو دينية أو إجتماعية معينة.[2] كما أن الإرهاب السيبراني هو التخويف أو التهديد ماديا أو معنويا بإستخدام الوسائل الإلكترونية الصادرة من الدول أو الجماعات أو على الإنسان سواءا في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق بشتى أشكاله وصور الفساد في الأرض.[3] كما أن الإرهاب السيبراني أيضا هو نشاط أو هجوم متعمد يملك دوافع سياسية ويسعى للتأثير في القرارات الحكومية والرأي العام العالمي، ويستخدم الفضاء الالكتروني بوصفه عاملا مساعدا ووسيطا في عملية التنفيذ للعمل الارهابي، ويأتي هذا العمل في صورة رقمية عبر إستخدام آليات الأسلحة الإلكترونية الجديدة لتصل إلى الإضرار بأهداف مادية تتعلق بالبنية التحتية الحيوية.[4]

---

[1] – إدريس الطيب عطية،"**الظاهرة الإرهابية في زمن ما بعد الحداثة، دراسة تحليلية في الأشكال والأساليب والإجراءات المضادة**"، المجلة العربية للدراسات الأمنية والتدريب، المجلد 31، العدد 63، الرياض، (2015)، ص ص 24 25

[2]– سارة بوحادة،"**أثر الإرهاب الالكتروني على أمن واستقرار الدول**"، أطروحة دكتوراه، (جامعة الجزائر–3–، المدرسة الوطنية العليا للعلوم السياسية، تخصص: دراسات دولية، 2014، ص63

[3] – أيسر محمد عطية،"**دور الآليات الحديثة للحد من الجرائم المستحدثة، الإرهاب الالكتروني وطرق مواجهته**"، الملتقى العلمي، الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، المملكة الأردنية الهاشمية، عمان، الأردن، 2014، ص 06

[4] – أمجد المنيف،"**الإرهاب الالكتروني– معركة حديثة**"، المجلة العربية العربية، العدد07، (يوليو2015)، ص 02

خامسا: الحروب السيبرانية: (Cyber Warfare):

تشمل الحروب السيبرانية الناجحة على أكثر من "مشغلي" حروب إلكترونية، وتعتمد على فريق من المختصين في المعارك الإلكتروني، حيث كل منهم يتميز بمسؤولياته ومهاراته الخاصة لترسيخ القدرة على القتال والتحكم بها وإبرازه ضمن الفضاء السيبراني، ويقوم مشغلو" الحروب السيبرانية" بالتخطيط للنشاطات الهجومية والدفاعية وإدارتها وتنفيذها عبر الفضاء السيبراني.[1]

المطلب الثالث: تأثير التهديد السيبراني على الأمن القومي

تبلورت المصالح القومية للدول في الفضاء السيبراني، إثر تزايد الإعتماد على ربط البنى التحتية لها، بذلك الفضاء في بيئة عمل تشابكية واحدة، تعرف بالبنية التحتية القومية للمعلومات (NTI)، فأي هجوم أو تهديد محتمل على تلك المصالح قد يشكل حدوث عدم توازن إستراتيجي، وهو ما يكشف عن نمط جديد من التهديدات للأمن القومي للدول، وأبرزها:[2]

- تزايد إرتباط العالم الفضائي السيبراني، الأمر الذي إتسع معه خطر البنية التحتية الكونية للهجمات السيبرانية.
- تراجع دور الدولة في ظل العولمة وانسحابها من بعض القطاعات الإستراتيجية لمصلحة القطاع الخاص.
- نشوء نمط جديد من الضرر على خلفية الهجمات السيبرانية، يمكن تسببه الدولة (أ) للدولة (ب) دون الحاجة للدخول المادي إلى أراضيها.
- تحول الحروب السيبرانية إلى إحدى أدوات التأثير في المعلومات في مستويات مراحل الصراع المختلفة
- توظيف الفضاء الإلكتروني في تعظيم قوة الدول، من خلال إيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة، وبالتالي ظهر ما يسمى بـ"**الإستراتيجية السيبرانية**" للدول.
- إتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون، سواء الدول أو من غير الدول.

فتفرض طبيعة المجال الذي يتعرض له الأمن القومي للمخاطر السيبرانية، إجراءات وأساليب مناسبة يمكنها الحفاظ عليه، فالأسلحة التقليدية منها المتطورة، وحتى النووية، عاجزة عن حماية "**الفضاء السيبيري**"

---

[4]– Timothy Franz.TheCyber Warfare professionnel Realization for Devloping the Next Generation. Summer 2011.p 04.

[2]– عادل عبد الصادق، "**أنماط "الحرب السيبرانية" وتداعياتها على الأمن العالمي**"، مجلة الاتجاهات النظرية، البنك العربي الافريقي، (14 ماي 2017)، ص32

(Cyber Space)، بل أن القواعد العسكرية، وأجهزة الإتصال وغيره، يمكن أن تكون هي نفسها هدفا لمقتحمي الأنظمة المعلوماتية والمواقع، لكن ذلك لا يمنع أوجه التشابه بين سياسات الأمن، كما لا يمنع إعتماد بعض المبادئ في سياسة وإستراتيجية الدفاع والحماية. وعلى خط مواز يشمل الأمن القومي، أمن المعلومات ليس فقط بالمعنى المادي، أي ضمان عدم تخريبها، أو تشويهها، والقضاء عليها أو سرقتها، بل أيضا ضمان سريتها، وعدم إطلاع الآخرين عليها ومصداقيتها وصحبتها.[1] ومن أهم سمات المخاطر السيبرانية التي لها تأثير على الأمن القومي ما يلي:

1- **السرعة الفائقة**: هناك فجوة في السرعة بين الدول المتقدمة والنامية، ومن أمثلة هذا التسارع تنامي معدل المعاملات الإلكترونية العالمية عبر شبكات الانترنت.

2- **اللامحدودية**: (**إنهيار الفواصل الجغرافية**): يحقق النظام الدولي للمعلومات الفرصة للجميع من أجل الخروج إلى العالمية، فوق كل الحدود، وفوق كل الفواصل، ويخلق ما يسمى "**الفضاء اللامتناهي**" يتسابق فيه الجميع نحو تلك العالمية.

3- **اللازمنية**: (**التنافس في الوقت**): يتسم النظام الدولي المعلوماتي بالعمل في الزمن الحقيقي، حيث تعمل كل المواقع والخدمات بلا توقف في جميع أنحاء العالم 24سا/7 بالرغم من الفواصل الزمنية

4- **اللامادية**: (**تضاؤل قيمة المكونات المادية**): تضاءلت قيمة المكونات المادية إلى 30% من قيمة المنتج، فإنها قد وصلت إلى حوالي 10% سنة 2011 [2]

فبما أن المخاطر السيبرانية ترقى إلى مستوى الأمن القومي ككل، فإن وسائل المواجهة والحماية لا بد وأن تظللها منظومة الأمن القومي، لأنه من الخطأ أن تكون الأخطار والتهديدات شاملة وربما منسقة ومخططة أحيانا: ثم تأتي سبل وسائل مواجهتها جزئية وعفوية وخالية من التخطيط وتفتقر للتنسيق والرشد، وقد قدمت اليبان نموذجا لهذا المستوى من التعامل مع الأمن السيبراني، حينما أعلنت منذ أوائل أكتوبر 2005 في تنفيذ برنامج شامل، على مستوى مؤسسات وهيئات الدولة والشركات الخاصة يستهدف التدريب ضد

[1] عزيز ملحم بربر،"**أمن الشبكات والانترنت**"، (القاهرة، جامعة نايف العربية للعلوم الأمنية، 2008)، ص 04

[2]- محمد علي قطب،"**الجرائم المعلومات وطرق مواجهتها**"، مركز الاعلام الأمني، الأكاديمية الملكية للشرطة،(2009)،ص 11

الهجمات السيبرانية الشاملة بتنويعاتها المختلفة. فإدارة التهديدات السيبرانية داخل البنية المعلوماتية القومية يتطلب بيئتين للأمن القومي (بيئة داخلية وبيئة خارجية): [1]

- **البيئة الداخلية للأمن القومي**: إدارة التهديدات المتداولة داخل البيئة المعلوماتية الداخلية يتطلب فهما ورؤية جديدة لأساليب ومناهج وأدوات تداول المعلومات بين الدولة الواحدة أو بينها وبين أفرادها، ومجتمعاتها ومؤسساتها الحكومية وغير الحكومية.
- **البيئة الخارجية للأمن القومي**: إدارة التهديدات يتطلب مناهج وأدوات وأساليب بين الدولة وباقي الدول الأخرى والفواعل الرسمية وغير الرسمية.س

[1] – جمال محمد غيطاس،"**الأمن المعلوماتي والجرائم الالكترونية.. أدوات جديدة للصراع**"، (القاهرة، مركز الجزيرة للدراسات، 2012)، ص 06

المبحث الثالث: آليات إستخدام القوة السيبرية.

المطلب الأول: مفهوم القوة السيبرانية

يعد "**جوزيف ناي**" (Joseph Nye) من أبرز المهتمين بالقوة السيبرية، وله السبق في الحديث عنها، حيث يعرفها بأنها: القدرة للحصول على نتائج مرجوة من خلال إستخدام مصادر المعلومات المترابطة بالفضاء الإلكتروني، أي أنها القدرة على إستخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى (Operation Environments)، وذلك عبر أدوات الإلكترونية، ويوضح "**جوزيف ناي**" أن مفهوم القوة السيبرانية يشير إلى مجموعة المواد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية للتعامل مع هذه الوسائل.[1]

فالقدرات السيبرانية تتصل بتهديدات مشتركة، وتعتمد كلتاهما على الطيف الكهرومغناطيسي (Electromagnetic Sepectrum) والبنية التحتية التكنولوجيا المعلومات التي تمنح قدرات عظيمة ولكنها تخلق أيضا نقاط ضعف وتحديات مشتركة، وقد يبدأ الهجوم على القدرات الفضائية من الفضاء الإلكتروني، وقد توجه محاولات الإختراق للقوة الإلكترونية. [2] وقد يسمح ضعف الحواجز التي تعيق دخول الهيئات الحكومية وغير الحكومية من المنافسة في إستخدامات كل من الفضاء والفضاء الالكتروني التي تعيق تطبيقه على القوة السيبرانية، فقد سمح ضعف الحواجز لمجموعة من الأعداء أن يكون لديهم قدرات فعالة ضد شبكات وأنظمة الكمبيوتر، وهي قدرات مختلفة عن القدرات الموجودة في أي مكان آخر.[3]

[1] – إيهاب خليفة،" **نمط جديد لممارسة التأثيرات غير التقليدية في العلاقات الدولية**"، اتجاهات الأحداث، العدد 06، (يناير 2015)، ص 06

[2] Josepf S.Nye. the Future of Power. Newyork. 2011. P 132

[3] – مادلين آر كريدين،"**الفضاء والفضاء الالكتروني: التحديات المشتركة، مجلة الفضاء والفضاء الالكتروني التابعة للقيادة الاستراتيجية الامريكية**"، (يناير 2012)، ص 35

والجدول التالي يوضح أهم القوى السيبرانية على مستوى العالم التي تستخدم القدرات السيبرانية في شؤونها الدولية:

الدولة	الهجوم الالكتروني	الاعتماد على الفضاء السيبراني	الدفاع السيبراني	المجموع
الولايات المتحدة	8	2	1	11
روسيا	7	5	4	16
الصين	5	4	6	15
ايران	5	5	2	12
كوريا الشمالية	2	9	7	18
المجموع الكلي	27	25	20	72

جدول يوضح القدرات السيبرانية للدول الخمسة الأولى في العالم[1]

المطلب الثاني: التحول في إستخدام القوة السيبرانية

أولا: القوة السيبرانية والقوة الصلبة:

تتنوع مظاهر الإستخدامات الصلبة للقوة السيبرانية في التفاعلات الدولية بحيث يتم إستخدام القوة السيبرانية في التأثير على سلوكيات الفاعل الدولي، ودفعه للقيام بأعمال لم يكن ليقوم بها، ويتم ذلك من خلال نشر فيروسات تدمر أجهزة الدولة. وتستهدف نظم الكمبيوتر الخاصة الخدمات الحكومية، أو من خلال الحرمان من خدمة الأنترنت أو قطع خدمات الأنترنت عن الدولة كاملة، فعلى سبيل المثل تم شن هجمات على البرنامج النووي الإيراني للعمل على تعطيله، حيث أعلنت الإستخبارات الإيرانية أن فيروس "**ستاكسنت**" (Stuxnet)* أصاب حوالي 16 ألف جهاز كمبيوتر. فقدرة الفاعل الدولي على التحكم في أجندة الآخرين من خلال منعه من تنفيذ بعض من الخطة الإستراتيجية، مثال: منع بعض الناشطين السياسين

[1]– نوران شفيق،"**أثر التهديدات الالكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الإلكتروني**"، مرجع سابق، ص 41.

من عرض فيديوهات خاصة بعيد الثورة الإيرانية عام 2010 على موقع اليوتيوب مضادة للنظام الحاكم، حيث عمدت الحكومة على إبطاء سرعة الانترنت وإعادة بث هذه الفيدوهات.[1]

ثانيا: القوة السيبرانية والقوة الناعمة:

يتعلق الإستخدام الناعم للقوة السيبرانية من خلال التأثير في سلوك الفاعل. مثل إستخدام موقع "**اليوتيوب**" في تخطي أسوار التعتيم التي تفرضها الأنظمة المستبدة وفضح الإنتهاكات التي ترتكبها أمام العالم، كما حدث في عام 2008، عندما استخدمت كاميرات المحمولة لتصوير قمع النظام العسكري للحاكم في "**ميامي**" (**بورما سابقا**) للمظاهرات المطالبة بالديمقراطية، وثم بثها على الانترنت. كمثال: قدرة الفاعل (أ) على التأثير في سلوكيات الفاعل (**ب**) ودفعه للقيام بأعمال لم يكن ليقوم بها وتكون في هذه الحالة مصدر للقوة الناعمة، كما في حالة إتجاه الدولة لوضع معايير ملزمة البرمجيات أو إستخدام الجماعات الإرهابية الفضاء الإلكتروني في تجنيد بعض الشباب.[2]

ثالثا: القوة السيبرانية والصراع الدولي:

ظلت الصراعات التقليدية والقوة العسكرية تحددان لفترة طويلة طبيعة الخطابات السياسة، وحدود وهيكل النظام العالمي، وموقع القوى الكبرى منه، إلا أن إتساع تأثيرات العامل التكنولوجي في السياسات الدولية، بعد إنتهاء الحرب الباردة، أضاف أبعاد أخرى للقوة العسكرية، حيث تلاشت الفواصل والحدود بين ما هو مدني وعسكري، ومن ثم أخذت الصراعات غير التقليدية، سواء من حيث الفاعلون أو القضايا، أو ديناميكيات التفاعل في العالم اليوم، فاختصر الفضاء السيبراني حاجز الزمان والمكان، وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الإفتراض، ومن ثم برزت فضاءات جديدة للصراع بأدوات مختلفة، وأنماط جديدة تختلف عن الصراعات التقليدية، وتعود أسباب إهتمام الفاعلين، سواء كانو من الدول أو

---

[1]– إيهاب خليفة، "**القوة الالكترونية والصراع الدولي**"، المركز العربي لأبحاث الفضاء الالكتروني، 20 جانفي 2018/:20:32 http//alaeabycyberspace.com

[2] – عادل عبد الصادق،"**أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني**"، وحدة الدراسات المستقبلية، سلسلة أوراق، مكتبة الإسكندرية، العدد 23، (يناير 2015)، ص 20

*– تعاونت الاستخبارات الأمريكية والاسرائيلية لتطوير الفيروس المعلوماتي "ستاكسنت" الذي استهدف البرنامج النووي اليراني حسبما زعمت صحيفة نيويورك تايمز الأمريكية.

غيرها، وبهذا الفضاء، كمجال لتحقيق الهيمنة، وتنفيذ الأهداف، وإدارة الصراعات، إلى إمتلاكه عدة سمات أساسية.[1]

رابعا: القوة السيبرانية والردع السيبراني:

وتعني قدرة الدولة على تطوير قدرات عسكرية موثوقة ومتبادلة ومتماثلة على الفضاء السيبراني، تكون قادرة على التأثير على قرارات الخصم وتمنعه من شن هجمات عسكرية عبر الفضاء السيبراني، فيتشابه الردع بصفة عامة مع الردع السيبراني في عدة نقاط، منها صعوبة تطبيق القانون في العلاقات العابرة للحدود، حيث يتميز الفضاء السيبراني بعدم وجود حدود جغرافية له توضيح سيادة الدول عليها، ولما كانت الأسلحة المستخدمة في الفضاء السيبراني غير محددة سلفا وتخضع التطور التكنولوجي، وغالبا ما تظهر الهجمات نتيجة ثغرات تم إكتشافها، ومن ثم فإنه يصعب حصر هذه الأسلحة لمنع أو تقنين إستخدامها.[2]

المطلب الثالث: القوة السيبرانية في الشؤون الدولية

إن القدرة على تحقيق القوة السيبرانية في الشؤون الدولية من خلال الإستقطاب، أكثر مما يمكن تحقيقه عبر الإكراه، حيث يقول "**جوزيف ناي**" في هذا السياق، لقد أضحى من الصعب في العالم المعاصر، إستخدام العصا... إذ القوة العسكرية على الرغم من ضروريتها كسياسة ردع وإكراه، فهي أصبحت صعبة جدا...، لذا يجب على الدول أن تنتهج وسائل أخرى ذكية في شؤونها الدولية بدلا من تلك القوة الصراعية.

أولا: الدبلوماسية السيبرانية (Cyber Deplomatcy):

إستطاعت تكنولوجيا الإتصالات والمعلومات تحدث تغيرات جذرية على العديد من المجالات وأبرزها المجال السياسي، حيث أتيحت الفرصة للأفراد والمؤسسات والحكومات القدرة على ممارسة الأنشطة السياسية عبر الانترنت بأدواته المختلفة، وهذا ما يطلق عليه: "**السياسة السيبرانية**" (Cyber Politics) ولعل مجال الدبلوماسية العامة، أحد أبرز المجالات التي تأثرت بذلك، حيث بدأ إستخدام مواقع التواصل الإجتماعي وتكنولوجيا الإتصالات والمعلومات للقيام بالأنشطة المتعلقة بالدبلوماسية العامة، والتي أطلق عليها إسم "**الدبلوماسية السيبرانية**" ، لأنها أداة جديدة مهمة لتحقيق أهداف السياسة الخارجية بوجه عام، وتعزيز

---

[1]– سماح عبد الصبور، "**اصراع السيبراني.. طبيعة المفهوم وملامح الفاعلين**"، مجلة السياسة الدولية، البنك العربي الافريقي الدولي،(9 أفريل2017)، ص 21

[2]– إيهاب خليفة،"**إمكانيات تحقيق الردع في الصراعات الفضاء الالكتروني**"، مجلة تحليلات المستقبل، العدد 13، (أوت 2015)، ص 49

المصالح الأمنية الوطنية من خلال توسيع وتقوية العلاقات الرسمية وغير الرسمية، بين حكومات وشعوب الدول وبعض البعض. فالدبلوماسية السيبرية هي وسيلة لتحقيق أهداف الدبلوماسية العامة عن طريق إستخدام أنظمة الإتصال الحديثة، أو ما يعرف بالمجتمعات الإفتراضية.[1]

ثانيا: الإستخبارات السيبرية (Cyber Intelligence):

وهي إمتلاك وتحليل المعلومات لتحديد وتتبع والتنبؤ بقدرات الخصوم في الفضاء السيبراني، وكذلك الإلمام بنواياهم وأنشطتهم، وهو الأمر الذي يساعد على إيجاد خيارات مختلفة لعملية صنع القرار، فمع قيام "**إدوارد إيستون**" (Edward Eston) الموظف السابق في وكالة الأمن القومي الأمريكي بكشف العديد من الوثائق التي تدين الولايات المتحدة وبعض الدول للقيام بعمليات تجسس وإستخبارات سيبرية واسعة النطاق، بدأت تتضح الرؤية حول سعي الدول لتوظيف الأنشطة الإستخبراتية في الفضاء السيبراني لتشمل ليس الدول فقط، بل والحركات والجماعات والشخصيات المهمة وحتى الأفراد العاديين، وقد بات الصراع الرئيسي بين الدول ليس من أجل إمتلاك الموارد المادية، وإنما الحصول على المعلومة التي باتت سلاحا جديدا في مواجهة الدول، وخاصة في ظل الكم الهائل من المعلومات.[2]

ثالثا: التحالف السيبري (Cyber Allies):

وهو النمط الرسمي النابع عن الإتفاق الصريح بين الجهات تجاه بعضها البعض، وفق شروط ينظمها الإطار القانوني الحاكم لمسار هذا التحالف، ويعد "**تحالف الناتو السيبري**" أحد أهم الأمثلة، والذي يتجه نحو معالجة مجموعة واسعة من التهديدات عبر تعزيز السياسة السيبرية التي جاءت بموجب إتفاقية إستونيا 2007، "**فالتحالف السيبري**" يدور حول الإتجاه الذي تتبناه الأطراف لتدعيم مراكز قوتها في مجال الأمن السيبيري من خلال الإتفاقات والشراكات الضمنية والعمليات المشتركة، وكما في العلاقات (الروسية- الصينية) التي تتسم بالتقارب على المستوى التكنولوجي، أو قد تكون شراكات صريحة، كما في حالة (الشراكة بين كوريا الشمالية وايران بموجب إتفاقية 2012)، وتسعى هذه الأطراف عبر وسيلة الأحلاف الإلكترونية إلى تحقيق مصالحها واكتساب حليف دفاعي قوي يعزز قدراتها الأمنية السرية، ولعل أبرز التحالف بين الدول

---

[1]- سارة يحي،"**بعد غير تقليدي في العلاقات غير الرسمية بين الدول**"، اتجاهات الأحداث، العدد 06، (يناير 2015)، ص 08

[2] - ريهام مقبل،"**كيف يمكن أن تمارس الدول نفوذها في العلاقات الدولية**"؟، إتجاهات الأحداث، العدد 06، (يناير 2015)، ص 05

وشركات التكنولوجيا، التحالف في مجال الأمن السيبيري عام 2010، وهو التحالف الذي نشأ في الولايات المتحدة بين دائرتي الدفاع والأمن الداخلي، وبين كبريات الشركات الصناعية الخاصة، ويقوم هذا النوع من التحالف السيبيري على إشراك أصحاب المصالح كحليف قوي لتحقيق الأمن السيبيري.[1]

رابعا: الإعلام السيبراني (Cyber Informating):

فالإعلام السيبراني هو ذلك التزاوج ما بين تكنولوجيا الإتصال والبث الجديدة والتقليدية مع الكمبيوتر وشبكاته، ويأخذ هذا الإسم باعتباره أنه لا يشبه وسائط الإتصال التقليدية، فهو الإعلام الرقمي (Digital Media) الذي تعتمد عليه مختلف الدول في وصف وبث الأخبار التي تتعلق بسياساتها وبعض تطبيقاتها التي تقوم على التكنولوجيا الرقمية مثل: التليفيزيون الرقمي والراديو الرقمي وغيرها، أو للإشارة إلى نظام أو وسيلة إعلامية تندمج مع الكمبيوتر ويطلق عليه الإعلام التفاعلي أيضا (Interactive media) طالما توفرت حالة العطاء والإستجابة بين المستخدمين لشبكة الانترنت والتليفيزيون والراديو وغيرهم من النظم الإعلامية التفاعلية الجديدة.[2]

[1] – دعاء الجهيني،"**طريق مختمل لمواجهة تهديدات الفضاء الالكتروني**"؟ اتجاهات الأحداث، العدد 06، (يناير 2015)، ص 11

[2] – مصطفى صادق عباس،"**الإعلام الجديد، دراسة في مداخلة النظرية وخصائصه العامة**"، (القاهرة، دار العلم، 2012)، ص 19

خلاصة الفصل الأول:

ويستنتج من خلال ما سبق أن العالم اليوم يشهد مجموعة من التغيرات في الدراسات الأمنية أثرت على مختلف المفاهيم وتطويرها إلى مفاهيم جديدة مواكبة للعصر. ومن أهم هذه المفاهيم نجد الفضاء السيبراني هذا المجال الكبير الذي أنتج مفهوم "**الأمن السيبراني**" في ظل "**تهديدات جديدة سيبرانية**" خلفت تحولا كبيرا في استخدامات القوة من قوة صلبة وناعمة إلى قوة "**ذكية سيبرانية**" مما جعل ظهور "**فواعل سيبرانية**" أخرى جديدة لها تأثير على العلاقات الدولية وعلى الأمن والوطني ككل وأمن الأفراد أيضا.

و عليه فالأمن السيبراني في الدراسات الأمنية والعلاقات الدولية، هو مسألة الحاضر كما أنه موضوع المستقبل أيضا.

الفصل الثاني: الإدراكات الجزائرية الأمنية.

المبحث الأوّل: التصور الجزائري للأمن.

المبحث الثاني: العقيدة الأمنية الجزائرية.

المبحث الثالث: التحديات الأمنية السيبرانية.

تمهيد الفصل الأول:

لقد أفرزت التحولات الأمنية خاصة بعد الحرب الباردة إلى يومنا هذا أثرا كبيرا على الأمني الوطني لجميع الدول، وكانت الدولة الجزائرية واحدة من تلك الدول، حيث عرفت الجزائر ومنذ استقلالها مجموعة من التهديدات الأمنية أثرت على أمنها واستقرارها، مما جعلها تعمل على تطوير عقيدتها الأمنية لمكافحة تلك التهديدات من خلال وضع مجموعة من السياسات الاستراتيجيات من أجل التفاعل مع تلك التهديدات، لكن الجزائر وكغيرها من الدول تواجه تحديات نتيجة لتأثير تلك التهديدات الأمنية على جميع الأصعدة لأمنية والسياسية، والتساؤل حول هذا الفصل: **ما هو تأثير التحولات الأمية على الأمن الوطني الجزائري؟**

المبحث الأول: التصور الجزائري للأمن

المطلب الأول: تحولات في مفهوم الأمن

أولا: مفهوم الأمن

المفهوم الضيق للأمن: كثيرا ما يستخدم للتعبير عن الإجراءات الخاصة بتأمين المواطنين وممتلكاتهم داخل الدولة من الأخطار المحتملة ولمواجهة غيرها من الدول بداء بالإجراءات الوقائية في الداخل وتشكيل القوات المسلحة وعقد الأحداث العسكرية إلى حد قيام الدولة بتحقيق أمنها.[1]

المفهوم الموسع للأمن: لقد توسع نطاق مفهوم الأمن من المعنى التقليدي العسكري والذي يركز على إحتياجات البقاء الوطني وحماية الدولة والحدود والشعب والنظم والقيم وضد العدوان الخارجي إلى المعنى العالمي الذي يشمل قطاعات أخرى غير العسكرية تتمثل في الأمن المجتمعي وأمن البشر الأمن البيئي والأمن الصحي وغيرها وأمن الكوكب ككل.[2] فقد تم الإقرار بالحاجة إلى تطبيق سياسات غير عسكرية والذي أصطلح عليه بالأمن الناعم الذي تندرج في إطاره كل التحديات غير العسكرية التي تواجه الدولة كالعنف الإجرامي، والجوع، الأوبئة، الإرهاب وغيرها.[3]

فالأمن وإن كان نسبيا في الحصول عليه وفقا لطبيعة النظام السياسي السائد ومدى التهديدات المنبثقة عنه وضده، فإنه يتم عن طريق ظرف خاص تبعا لما خلفه من تطور أو تراجع أخذا بعين الإعتبار على دول الجوار أو تأثيراتها على الدولة المعنية.[4] فأصبح "**مفهوم الأمن**" مختلفا في سياق متطلبات المجتمع ككل، وهو

---

[1]– وهيبة تباني،"**الأمن المتوسطي في استراتيجية الحلف الأطلسي، دراسة حالة: ظاهرة الإرهاب**"، رسالة ماجستير، (جامعة مولود معمري، تيزي وزو، الجزائر، كلية الحقوق والعلوم السياسية، تخصص: دراسات متوسطية ومغاربية، 2014)، ص 49

[2]– ذياب موسى البداينة،"**الأمن الوطني في عصر العولمة**"، (الرياض، جامعة نايف العربية للعلوم الأمنية،2011)، ص 22

[3]– حنان بن عبد الرزاق،"**تأثير المأزق الأمني الاثني على الاستقرار الداخلي لدولة. دراسة للنموذج الاسباني**" أطروحة دكتوراه، (جامعة محمد خيضر، بسكرة، كلية العلوم السياسية، تخصص: علاقات دولية ودراسات استراتيجية، 2016-2017)، ص19

[4]– ميلود عامر الحاج،"**الأمن القومي العربي وتحدياته المستقبلية**"، (المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف للنشر، 2017)، ص21

أمن يتسع ليشمل نواح كثيرة يحتاجها المجتمع ككل، ففي الزمن الأخير لم تقتصر الدفاعات للمصالح والأوطان على الأعمال العسكرية فقط، بل تعداها إلى مفاهيم ووقائع أخرى.[1]

ثانيا: أسباب تحول مفهوم الأمن

شكلت نهاية الثمانينيات وبداية التسعينيات من القرن الماضي، بداية التحول في ميدان الدارسات الأمنية، إذ بدأ الحديث عن إعادة النظر في مسألة توسيع "**مفهوم الأمن**" وعدم حصره في الإطار العسكري فقط، وذلك بتوسيع قائمة التهديدات إلى مجالات أخرى غير عسكرية، ولم يكن ممكنا حدوث تغيير في المناهج الأمنية لو لم تتغير التهديدات المحددة لمفهوم الأمن، والجزائر وكغيرها من باقي الدول كانت تعاني من أنماط تلك التهديدات التي أثرت على العالم ككل.[2]

1.أثر نهاية الحرب الباردة على تحول مفهوم الأمن:

أ. زوال الثنائية القطبية: بسقوط وتفكك منظومة الدول الإشتراكية ثم الإتحاد السوفياتي نفسه، إختفى الصراع بين الغرب والشرق نتيجة تراكم التداعيات المترتبة على التقدم العلمي والتكنولوجي منذ الثورة الصناعية وحتى الأن لما أدى إلى بروز تحولات على مفهوم الأمن.[3] فيرى الباحثون والمحللون السياسيون أن إستراتيجية الهيمنة وعالمية الطموحات أصبحت واقعية بالنسبة للولايات المتحدة الأمريكية، كونها تهدف إلى توسيع سيطرتها من الناحية الجيوبولتيكية والإستراتيجية وهو أمر لابد منه، ولن يتم هذا من خلال سياسة توازن القوى، بل من خلال الأخذ بسياسة الهيمنة الأمريكية، وهذا ما ساعد على تحول في "**مفهوم الأمن**".[4]

ب. ظهور فواعل من غير الدول: إستمدت الدولة القومية بأنها الفاعل الأساسي والوحيد في العلاقات الدولية ولكن مع ظهور العولمة والإعتماد المتبادل ثم نهاية الحرب الباردة ظهرت فواعل جديدة وأصبحت تتنافس الدول في قضايا كانت تعتبر من صميم وظائف الدولة السياسية كالمنظمات غير الحكومية، والشركات

---

[1]– سالم المعوش،"**مجتمع المعرفة وتعزيز الأمن القومي، المشهد العالمي الجديد**"، (لبنان، مركز الأبحاث العلمية، 2011)، ص18

[2]– علي مدوني،"**قصور متطلبات بناء الدولة في إفريقيا وانعكاساتها على الأمن والاستقرار فيها**"، أطروحة دكتوراه، (جامعة محمد خيضر، بسكرة، كلية العلوم السياسية والعلاقات الدولية، 2013 –2014)، ص 69

[3]– إنعام عبد الكريم أبو تمور،"**مفهوم الأمن الإنساني في حقل نظريات العلاقات الدولية، مقاربة معرفية**"، رسالة ماجستير في العلوم السياسية، (جامعة الأزهر، غزة، فلسطين، كلية الإقتصاد والعلوم الإدارية، 2013)، ص28

[4]– براهيم أحمد،"**الدولة العالمية والنظام الدولي الجديد**"، أطروحة دكتوراه، (جامعة السانيا – وهران، 2009–2010)، ص193

المتعددة الجنسيات وغيرها. وأصبح الأمن الذي كان مرتبطا بالدول أصبح الشغل الشاغل لهذه الفواعل غير الدولاتية.[1]

ج.تغيير طبيعة النزاعات: أصبحت الصراعات تدور بين الأفراد داخل الدولة القومية الواحدة، وليس بين الدول، في خلال التسعينيات من القرن العشرين لقي 50 مليون شخص حتفهم جراء الصراعات الداخلية، فقد شكل التغيير في طبيعة النزاعات في فترة ما بعد الحرب الباردة عاملا رئيسيا في فشل المنظور التقليدي للأمن، ويناقض فرضية أن أمن الدولة يعني بالضرورة أمن أفرادها.[2]

ثانيا: تأثير العولمة في المفهوم:

والذي يتحدد من خلال التفاعل بين المدلولات ونتائج العولمة التي كشفت عن الضعف والتدهور الذي تمر به دول العالم، التي قد تصل إلى حد السقوط، مما يستدعي تدخل خارجي يسعى إلى دعم إعادة بناء على أساس مكافحة الفساد والإصلاح، وحققت طفرة هائلة في حجم التبادلات التي تنتقل عبر الحدود الوطنية بسرعة.

ثالثا: التحول في الوسائل والأدوات.

جاءت نتيجة الثورة التكنولوجية التي أحدثت قفزة نوعية للتطور في مختلف المجالات، وأدخلت الوسائل الحديثة في العلاقات الدولية والسياسات العالمية تحولا كبيرا في "**مفهوم الأمن**".[3]

رابعا: التحول في مصادر التهديد:

لم تعد مصادر التهديد ذات صبغة عسكرية فقط بل تعدت ذلك إلى مصادر تهديدات أخرى مشاكل بيئية، قضايا اللاجئين، الفقر، الأوبئة، تجارة المخدرات، الجريمة المنظمة والإرهاب الدولي، كذلك تهديد

---

[1]– فايزة غنام،"**(التعاون)؟ الأمني الأورو–مغاربي: دراسة حالة حوار 5+5 (2001–2011)**"، رسالة ماجستير، (جامعة مولود معمري، تيزي وزو، الجزائر، كلية العلوم السياسية، 2011–2012)، ص62

[2]– وسيلة قنوفي،"**حق الانسان في الأمن: بين مقاربة الأمن الإنساني ومبادئ القانون الدولي**"، أطروحة دكتوراه، (جامعة محمد لمين دباغين، سطيف–2–، كلية الحقوق والعلوم السياسية، 2016–2017)، ص48

[3]– سفيان طبوش،"**الشراكة الأورو متوسطية في ظل التحديات الأمنية الراهنة**"، أطروحة دكتوراه، (جامعة حسيبة بن بوعلي، الشلف، كلية العلوم السياسية، تخصص: دراسات أورو متوسطية،2016–2017)، ص27

أمن الفرد وغيرها من المخاطر والتحديات فتعدد التهديدات وتنوع المصادر وتشابك نتائجها وتوسع رقعة تأثير أدى إلى مخاطر لا يمكن توقعها أو التنبؤ بها.[1]

المطلب الثاني: الأمن الوطني الجزائري

أولا: مفهوم الأمن القومي: (Nationalist Security).

يمكن إرجاع مفهوم الأمن القومي إلى فكرة سيادة الدولة، التي أسست معالمها "**معاهدة واستفاليا 1648**"، في أوروبا، والتي أعلنت نظاما دوليا جديدا يقوم على أساس الدولة القومية،[2] فارتبط مفهوم الأمن القومي بالوجود المجتمعي السياسي بعناصره وجوانبه كلها، فلم تعد مفاهيم الأمن وتطبيقاته مجرد أنشطة فردية أو مجتمعية، بل إكتسبت إلى جانب ذلك بعدا مركبا مجتمعيا وسياسيا في آن واحد لتحقيق أهداف سياسية عبر مسؤولية وظائف المؤسسات السياسية.[3] ويتم ضمان "**الأمن القومي** " عبر إتباع إستراتيجية شاملة أو فرعية تضمن بقاء الدولة ووجودها، كالإستراتيجية السياسية والإقتصادية والإجتماعية والعلمية والعسكرية التي تصب بمحلها في خدمة الإستراتيجية العليا للدولة.[4]

ثانيا: مفهوم الأمن الوطني: (Patiriot Security)

يعود إستخدام مفهوم "**الأمن الوطني**" إلى نهاية الحرب العالمية الثانية، وذلك من أجل إيجاد حالة التوازن بين تحقيق الأمن، فيعني الأمن الوطني حالة الإستقرار النسبي التي يفترض أن يرافقها مستويات مقبولة من التطور والتنمية في ظل حماية الدولة.[5]

---

[1]– ياسين سعيدي،"**التحدبات الأمنية الجديدة في المغرب العربي**"، رسالة ماجستير، (جامعة وهران –2– ، كلية العلوم السياسية والعلاقات الدولية،2016،2015)، ص36

[2]– فوزي حسن الزبيدي،"**منهجية تقييم مخاطر الأمن القومي، دراسة تحليلية لمنهجية تقييم مخاطر الأمن القومي**"، (دبي، رؤى استراتيجية، 2015)، ص 13

[3]– مراد علي عباس، "**الأمن والأمن القومي، مقاربات نظرية**"، (بيروت، دار الروافد الثقافية – ناشرون، 2017)، ص24

[4]– دنيا محمد جبر، ابتسام حاتم علوان،"**الاستراتيجية الشاملة للأمن القومي العراقي بعد عام2003، (رؤية لمبادئ العمل اللازمة وأليات التفعيل)**"، مجلة الأهرام، (مارس 2007)، ص03

[5]– إبراهيم عبد القادر محمد،"**التحديات الداخلية والخارجية المؤثرة على الأمن الوطني الأردني في الفترة (2013–1999) دراسة حالة**"، رسالة ماجستير، (جامعة الشرق الأوسط، الأردن، كلية العلوم السياسية والاقتصاد، قسم العلوم السياسية، 2012–2013)، ص 29

فالأمن الوطني من المفاهيم التي تتخذ معنيين، **مفهوم ضيق:** يشير مباشرة إلى تحرر الدولة من القلق والخوف والتوتر لاتخاذ الإجراءات للقضاء على التهديدات التي يمكن أن تؤثر في مصالح الدولة، **أما الثاني موسع:** فيتضمن شعور الدولة بالإطمئنان لإستفاء مواطنيها ومتطلباتهم المشروعة التي تتضمن تحقيق العدالة الإجتماعية والإقتصادية.[1]

فالمقصود بالأمن الوطني هو تلك الجهود التي تبذلها أجهزة الأمن للمحافظة على أمن وتماسك المجتمع الإنساني، وعاداته وتقاليده وإنجازاته المختلفة من خلال إتخاذ كافة الإجراءات اللازمة التي تكفل أمن وإستقرار المجتمع ودوام التقدم والإزدهار.[2]

ثالثا: الأمن الوطني الجزائري.

يقوم الأمن الوطني الجزائري على مجموعة من المحددات الهيكلية والنسقية والتكيفية، فمحددات البيئة الأمنية الجزائرية ترتبط بطبيعة تكوين الدولة الجزائرية الحديثة، وبطبيعة المخاطر والتهديدات التي تهدد الأمن الوطني الجزائري، وهي محددات نتيجة لعوامل تاريخية وجغرافية وإستراتيجية تتمثل هاته المحددات في:

1.على المستوى الهيكلي: مرتبطة بطبيعة الدولة ما بعد الإستعمار بحدود شاسعة أكثر من 7000 كلم وغير متوافقة مع دول الجوار، ورقعة جغرافية واسعة وتوزيع ديموغرافي مضطرب وغير متوازن، مما يصعب بناء خارطة أمنية ثابتة المعالم.

2.على المستوى النسقي: فطبيعة الإقتصاد الوطني تبعي وريعي للمورد النفطي يشكل أحد عناصر الإنكشاف للأمن الكلي، لارتباطه بالتنمية والإستقرار السياسي والإقتصادي.

3.على المستوى التكيفي: هناك تهديدات ظرفية تحدد أولويات الدولة على المستوى الوطني مثل مكافحة الإرهاب والجريمة المنظمة والوقاية من الأخطار الكبرى لإرتباطها باستقرار الدولة والمجتمع، وإمكانية بناء تصور

---

[1]– فهد بن محمد الشقحاء،"**الأمن الوطني: تصور شامل**"، (الرياض، جامعة نايف العربية للعلوم الأمنية، 2004)، ص 14

[2]– عبد الجواد بشار ناجح عايد،"**المسؤولية المجتمعية التي يتبناها جهاز الامن الوطني الفلسطيني وأثرها على الصورة النمطية للسلطة الفلسطينية**"، رسالة ماجستير، (جامعة النجاح الوطنية، نابلس، فلسطين، كلية الدراسات العليا لتلخطيط والتنمية السياسية، 2017)، ص 48

لأمن وطني واسع ومتعدد الأبعاد وموحد، فالإرهاب بقي في التصور الرسمي للتهديد الأساسي للأمن الوطني الجزائري.[1]

المطلب الثالث: علاقة التنمية بالأمن الوطني الجزائري.

إن الجزائر مدركة للبنية العلائقية التي تربط الأمن بالتنمية، ففشل ومحدودية التنمية يدفع إلى إضعاف وتقهقر الوضع الإنساني من فقر، مجاعة وأمراض إضافة إلى التشتت وضعف الإنتماء والصراع الطائفي والجهوي، وهذا الضعف والتراجع في حيازة القوة والفرص الإقتصادية كله عوامل قد تدفع إلى العنف والضعف، لهذا تعزيز العلاقة بين الأمن والتنمية، يشير إلى أنه لا يمكن نمو مستمر بدون سلام وأمن، واستئصال الفقر وتحقيق التنمية، فلن يكون هناك سلام مستمر، أين يتم الإعتراف بأطراف المجتمع المدني الذين تسهم نشاطاتهم في تسريع عمليات بناء السلام والتنمية، مع العمل على تنمية القدرات من أجل تحسين الروابط بين الأنشطة الإنسانية ومنع النزاعات، بتوفير منهاج لإدماج نهج تحليل النزاعات وبناء السلام في برامج التنمية العادية. فعلى رغم من التهديدات المنتشرة كالإرهاب والجريمة المنظمة قد تبدو أكثر إلحاحا. فإن الفقر والإفتقار إلى الحكم الراشد هي في واقع الأمر الأسباب الجذرية لإنعدام الأمن، وبالتالي الأمن الإنساني يقدم ببساطة نقاط تدخل واضحة لربط وتنسيق إستراتيجيات الأمن والتنمية فالتقاطع بين التنمية والأمن يشير إلى أن الأمن الوطني لا يكمن فقط في القوة العسكرية، بل بصورة مماثلة في تنمية نماذج مستقرة من النمو الإقتصادي والسياسي في الداخل، فالأمن يتطلب حدا أدنى من النظام والاستقرار، وإذا لم توجد تنمية أو يتوفر الحد الأدنى منها، فإنه من المستحيل تحقيق السلم والإستقرار، وهو ما يوضحه ما يلي:

1. **أمن التنمية:** يقصد به توفير مناخ ومحيط مستقر يؤدي إلى خلق بيئة دافعة وضامنة لأي استراتيجية تنموية، مع توفير ضمانات تكفل إستمرارها وإستخدامها.

2. **تنمية الأمن:** يقصد بها عملية التطوير المستمرة للأجهزة الأمنية مؤسسيا، إستراتيجيا وعملياتيها لتفاعل مع هذه الأجهزة بكفاءة وفعالية مع القضايا الأمنية المرتبطة بعملية التنمية.[2]

---

[1] – محمد الأمين بن عائشة، "**مفهوم الأمن الوطني الجزائري**"، في: 03 فيفري 21:33/2018
www.maqualaty.com

[2]– بوعلام نصر،"**دور الجزائر الإقليمي في ظل تنامي التهديدات في منطقة الساحل (2006–2014)**"، مذكرة رسالة ماجستير، (جامعة ملود معمري تيزي وزو، الجزائر، كلية العلوم السياسية،تخصص في: دراسات متوسطية ومغاربية، 2015–2016)، ص ص 87–88

وتتمثل إستراتيجية التنمية في الجزائر في إستخدامات موارد الدولة وإمكانياتها لتحقيق الأهداف العامة المسطرة لها، والرؤية الشاملة لتحقيق العدالة الإجتماعية والرفاهية الشاملة القادرة على الإرتقاء بعملية نشر القيم الحضارية. ويعتبر الفقر والبطالة من أهم معوقات التنمية، فضلا عن إرتقاء نسبة الأمية، بالإضافة إلى الفساد الذي عم مختلف مناطق الدولة، خاصة وأن هذا الأخير يعد من أهم عناصر الإعاقة التي تحول دون تحقيق التنمية في مختلف الميادين. فعملية التنمية لا تقتصر على الإمداد ببعض الإسهامات على المستوى الإقتصادي والتقني، إنما الحضور الفعال والقوي للدولة من خلال وضع القواعد التي توضح كيفية إستعمال هذه الإسهامات، ذلك أنه بدون إرادة قوية لا يمكن الوصول إلى تنمية شاملة، ما فرض على الدولة التدخل في كافة المجالات ووضع إستراتيجيات من شأنها النهوض بالتنمية.[1] وأهمها تعزيز الحكم الراشد الذي يعتبر أهم شرط لتحقيق التنمية المستدامة والشاملة، إذ يدور مفهومه حول حسن إدارة الحوكمة من خلال الربط بين الحكومة والقطاع الخاص والمجتمع المدني لتحقيق الأهداف المرجوة عن طريق إستخدام آليات مختلفة تتمثل في: المشاركة، الشفافية، المحاسبة، المساءلة، العدالة، الإستقرار السياسي، كفاءة وفعالية الحوكمة ومحاربة الفساد وغيرها من مؤشرات قياس الحكم الراشد، كما يتسع تطبيق آليات ومبادئ الحكم الراشد في عدة مستويات، تربط المجتمع بالدولة في ميادين التنمية الإقتصادية والإجتماعية والثقافية وغيرها من الحقوق السياسية والخدمات العامة.[2]

[1] – نعيمة آكلي،"**إستراتيجيات التنمية في الجزائر**"، أطروحة دكتوراه، (جامعة مولود معمري، تيزي وزو، الجزائر، كلية العلوم السياسية، 2010)، ص 05

[2] بوزيد سايح، "**دور الحكم الراشد في تحقيق التنمية المستدامة بالدول العربية حالة الجزائر**"، أطروحة دكتوراه، (جامعة آبي بكر بلقايد، تلمسان، كلية العلوم السياسية والعلوم الاقتصادية، 2011)، ص 365

المبحث الثاني: العقيدة الأمنية الجزائرية

المطلب الأول: عقيدة الأمن الوطني الجزائري

أولا: مفهوم العقيدة الأمنية:

تعتبر "العقيدة الأمنية" دليلا يوجه ويقرر به القادة أو صناع القرار "**السياسة الأمنية**" للدولة ببعديها الداخلي والخارجي، ومن هنا نشأت العلاقة بين العقيدة الأمنية والسياسة الخارجية، إذ يلاحظ تنامي تأثير العقيدة الأمنية باعتبارها تمثل المبادئ المنظمة التي تساعد "**صناع القرار**" كما تساعد الدولة على التفاعل مع التهديدات والتحديات البارزة والكامنة التي تواجه أمنها على المستويات الزمنية (قريبة المدى- متوسطة وبعيدة المدى).[1]

و يقصد بالعقيدة الأمنية أنها مجموع الآراء والإعتقادات التي تشكل نظاما فكريا لمسألة أمن الدولة، وتسطر الدولة عقيدة أمنها لمحاولة التعاطي والتفاعل مع التحديات والقضايا التي تواجهها من خلالها ما تقوم به الدول للتعريف بالتهديدات والمخاطر التي تواجهها تلك الدول، فهي تمثل تصور أمني يحدد المنهجية التي تقارب بها الدولة تلك التهديدات، كما يحدد أفضل السبل لتحقيقه، وعادة ما تكون توجهات صناع القرار.[2]

فالعقيدة الأمنية هي مجموع القواعد والمبادئ والنظم العقائدية المنظمة والمترابطة التي توجه سلوك الدولة سواءا (تعاوني/غير تعاوني) وقراراتها على المستوى المحلي والدولي، وهي تحدد نظرة وقراءة قادتها لبيئتهم الأمنية وكيفية إستخدام القوة القومية، وكيفية توظيف هذه القوة لتحقيق الأهداف الإستراتيجية للدولة.[3]

وكثيرا ما تضع العقائد الأمنية من طرف قائد سياسي، خصوصا رئيس الدولة أو كبير دبلوماسي وتتجنب العلاقة بين القادة السياسيين والعقائد الأمنية على أن هذه الأخيرة "**إدراكات قادة الدولة لمصالحها**" وأن دوافع الدولة ليست منفصلة عن دوافع صناع القرار في الإطار العقلاني.[4]

---

[1] – عمر سعداوي،"**عقيدة الأمن القومي الجزائري من منظور جيواستراتيجي : قراءة في عملية تيقنتورين**"، مجلة الرائد المغاربي للدراسات السياسية والبحوث ، العدد الرابع ، (سبتمبر2014)، ص 13

[2] – سليم بوسكين،" **تحولات البيئة الإقليمية وانعكاساتها على الامن الوطني الجزائري 2010-2011**"، رسالة ماجستير، (جامعة محمد خيضر- بسكرة الجزائر كلية العلوم السياسية والعلاقات الدولية، تخصص: علاقات دولية واستراتيجية، 2014-2015)، ص 89

[3] – بوحنيه قوي،" **استراتيجية الجزائر تجاه التطورات الأمنية في الساحل الافريقي**"، مركز الجزيرة للدراسات في: 27 فيفري2018 22:17/Studies.aljageera.net

[4] –حسام حمزة، " **الدوائر الجيوسياسية للأمن القومي الجزائر**"، رسالة ماجستير، (جامعة الحاج لخضر- باتنة كلية الحقوق والعلوم السياسية، تخصص: علاقات دولية، 2010-2011)، ص 63

ثانيا: عقيدة الأمن الجزائري:

وهي المنطلق الموجه للسلوكيات والفعل الأمني والسياسي للدولة، كما أنها المحدد لمختلف الإستراتيجيات والسياسات التي تنتهجها الدولة الجزائرية في مواجهة التهديدات والمخاطر التي تحدق بها وتهدد أمنها واستقرارها، وتعمل على خلق الفرص للتفاعل مع هاته التهديدات، وهي المنطلق في تحديد السياسات العامة الوطنية، كما تعمل الجزائر على تطوير إستراتيجياتها وآليات المواجهة لمختلف التهديدات الأمنية غير التقليدية، حيث تبذل جهدا كبير سياسيا وأمنيا ودبلوماسيا وعسكريا وإقتصاديا من أجل الحد من خطورتها، فتوسع هذه التهديدات الأمنية جعل الجزائر تقوم بفحص عقيدتها الأمنية التي يستمد منها الأمن القومي الجزائري عناصر فلسفته وإجراءاته العملية عند التعاطي والتفاعل مع تلك المخاطر والتهديدات والتحديات الأمنية.[1]

المطلب الثاني: مرتكزات عقيدة الأمن الوطني الجزائرية

هناك عوامل كان لها تأثير واضح على العقيدة الأمنية منذ الأيام الأولى للإستقلال الجزائري منها:

أولا: العامل التاريخي:

تعد الثورة التحريرية أحد أهم روافد العقيدة الأمنية الجزائرية في فترة الإستقلال، حيث ساهمت هذه الثورة بشكل عام في رسم المشهد السياسي والإجتماعي الذي ميز الجزائر عقب دحر المحتل الفرنسي. فعملية بناء الدولة وبناء عقيدتها الأمنية ورسم إلتزاماتها داخليا وخارجيا، خضع كثيرا لهذا العامل التاريخي، فرغم التحولات التي عرفتها الجزائر في ظل تنامي العولمة، لكن هاجس التاريخ يظل حاضرا ولا يزال يطبع عقيدته الأمنية، ولا أدل على ذلك رفض الجزائر في إقامة علاقة مع إسرائيل.

ثانيا: العامل الجغرافي:

موقع الدولة الجيوبوليتكي يساهم في عملية صياغة العقيدة الأمنية للدولة، فتأثير عامل الجغرافيا على طبيعة العقيدة الأمنية للجزائر متنوعة، فإلى غاية نهاية الحرب الباردة مثلت قضايا دعم حركات التحرر في العالم والدفاع على مكانة الجزائر كقوة إقليمية أحد أهم عناصر هذه العقيدة، أما التحولات التي أعقبت نهاية الحرب الباردة وعلى رأسها الإنكشافات الأمنية، وازدياد عملية الإعتماد المتبادل والترابط والتشابك على العديد من الأصعدة، اتجهت هذه العقيدة للإرتكاز على عناصر جديدة، وعلى رأسها قضايا تتعلق بمحاربة الإرهاب

[1]– عمر سعداوي، مرجع سابق، ص 15

وتجارة المخدرات وأمن الدولة أي الإنتقال من البعد الخارجي إلى البعد الداخلي الذي أثر بشكل واضح في صياغة العقيدة الأمنية الجزائرية.[1]

ثالثا: العامل الأيديولوجي:

تشير كل الدلائل في الجزائر إلى وجود مجتمعين إثنين تتسم كل واحدة منهما إلى إنسجام ثقافي، الأولى تعيش وتفكر بحسب أنماط ومعايير الثقافة الغربية والثانية تنتمي إلى الثقافة العربية الإسلامية، ولا ترضى بمنافس لها، ولقد طغت هذه الإزدواجية على كل الإزدواجيات الأخرى وغطتها، وأخذت في العقدين الأخيرين تتزايد حدة وشدة لا سابق لهما، ووصلت درجة من العمق والتأثير، بحيث صار عندها الإنسجام والتماسك الإجتماعيين في خطر، فكل فئة من الفئتين المتنازعتين تفكر وتعمل ليس فقط من أجل الهيمنة على المجتمع بكامله، ولكن أيضا من أجل إقصاء الأخرى ومحوها من الخريطة.[2]

كما رسمت الأيدولوجية الإشتراكية مبادئ وأهداف العقيدة الأمنية الجزائرية لفترة تقارب ثلاثة عقود منذ الإستقلال، ولعل من أبرز تلك الأهداف مناصرة حركات التحرر في العالم ونصرة القضية الفلسطينية ودعم النزاع العربي الإسرائيلي، والعمل على المحافظة على مكانة الجزائر كقوة إقليمية وكذلك الإستعانة بالمؤسسة العسكرية أو الجيش الوطني الشعبي في مجهودات التنمية الوطنية.

المطلب الثالث: مراحل تطوير العقيدة الأمنية الجزائرية.

مرت عقيدة الأمن الوطني بثلاثة مراحل مفصلية من التحول، وذلك حسب طبيعة التهديدات التي مرت في كل مرحلة مما أدى إلى إدراك صناع القرار لتحديدهم لتلك المخاطر وقراءتهم له:

المرحلة الأولى: (1963–1990) مرحلة (التحدي المغربي)

حيث أقدمت المملكة المغربية على خطوة مفاجئة وغير منتظرة، مستغلة ضعف الجيش الوطني الشعبي الجزائري منهك بعد خوضه حرب تحريرية كبرى، فقامت بغزو "**تندوف**" وبعض المناطق المجاورة لها، فاندلعت حربا بينهما عرفت "**بحرب الرمال**" أو حرب الحدود، ومن هنا أصبح المغرب تهديدا مباشرا للأمن القومي الجزائري ويضاف الى كل هذا إنفجار قضية الصحراء الغربية سنة 1975، أثارت كذلك في العقيدة العسكرية

[1]– صالح زياني، "**تحولات العقيدة الأمنية الجزائرية في ظل تنامي تهديدات العولمة**"، جامعة محمد خيضر، بسكرة كلية الحقوق والعلوم السياسية، ص290

[2]– مراد بن سعيد، صالح زياني،" **النخب والسلطة والأيدولوجيا في الجزائر: بيمن بناء الدولة والتغيير السياسي**"، جامعة باتنة الجزائر، قسم العلوم السياسية، ص84.

والدفاعية وسياسة التسلح الجزائرية، حيث تغير نمط تشكيل القوات المسلحة الجزائرية، وعليه زادت النفقات العسكرية من 285 مليون دولار أمريكي عام 1975 إلى 856.8 مليون دولار عام 1982، أي بزيادة 400% مقارنة بزيادة 40% بين عامي 1965 إلى 1973.[1]

كما عرفت هذه المرحلة تطورا كبيرا في إعداد الجيش الوطني الشعبي، حيث فتحت المدارس العسكرية بمختلف أنواعها كمدارس الدرك الوطني بسيدي بلعباس، وتم سن قانون الخدمة الوطنية سنة 1968، الذي أعطى دفعا كبيرا في تعزيز قوات الجيش الوطني الشعبي.[2] فلم تكد تمر ثلاثة سنوات على الاستقلال حتى برز الجيش والمؤسسة العسكرية الأكثر قوة في البلاد، ومع مرور الوقت تحولت إلى المؤسسة الراعية والمؤتمنة على سيادة البلاد، بحيث أصبح لها كامل الصلاحية في استبعاد أي منافس على مقاليد السلطة أو تحييده.[3]

وحتى عام 1989، ظل الجيش جزاء من العملية السياسية، بحيث تخصص له جزء لتمثليه في اللجنة المركزية لجبهة التحرير الوطني، لكن بعد ظهور "**دستور 23 فيفري**"، أصبحت مهمة الجيش بموجب الدستور تقتصر على ما هو مذكور النص في التالي: "تتمثل المهمة الدائمة للجيش الوطني الشعبي في المحافظة على الاستقلال الوطني والدفاع عن السيادة الوطنية كما يضطلع بالدفاع عن وحدة البلاد وسلامتها الترابية، وحماية مجالها البري والجوي ومختلف مناطق أملاكها البحرية".[4]

المرحلة الثانية: فترة التسعينيات مرحلة (التطرف والإرهاب):

على إثر انتفاضة أكتوبر 1988، وإقرار دستور جديد للبلاد 1989، وقانون الإنتخابات الجديدة خضعت التجربة الديمقراطية في الجزائر ولأول مرة منذ الإستفتاء الشعبي على الإستقلال عام 1962 جسدته إنتخابات بلدية محلية، تمت في جويلية 1990، وقد عكس نجاح "**الجبهة الإسلامية الأنقاض**" في هذه الإنتخابات بنسبة 60% تغلغل الظاهرة الأصولية في الجزائر وهو لم يكن بحسبان "**الشاذلي بن جديد**"

---

[1]– سمير قط،" **البعد الافريقي في سياسة الأمن والدفاع الوطني الجزائري**"، أطروحة دكتوراه في العلوم السياسية، (جامعة محمد خيضر، بسكرة، تخصص: علاقات دولية واستراتيجية، 2016–2017)، ص15.

[2]– أحمد سويقات،" **دور الجيش الوطني الشعبي من خلال التجربة الدستورية في الجزائر**"، جامعة قاصدي مرباح، ورقلة، ص 422

[3]– الطاهر سعود،" **أدوار الجيش في المراحل الانتقال في الجزائر، سياسات عربية**"، مركز دبي للأبحاث العلمية (يناير 2017)، ص30

[4]– بوجمعة غشير،" **تطور خطاب حقوق الانسان في الجزائر والوضع الراهن**"، معهد السياسات بالجامعة والمواطنة، تقرير بحثي، (2010)، ص11

بحيث لم يعط وزنا كبيرا للإسلاميين منذ البداية، واعتقد أن للقوى الديمقراطية ثقلا أكبر منها، وهو ما أثبتت عدم صحة نتائج الإنتخابات الأولى.[1]

إن إحاطة ظاهرة الإرهاب في الجزائر بالظروف الزمنية والموضعية (**الداخلية والخارجية**) المصاحبة لظهورها تحيل إلى إستخلاص أن هناك العديد من المسببات المتشابكة التي غذت ظهور الإرهاب، وزادت من إستفحاله. ويبقى التضييق السياسي والتفكير الأحادي المقصي لكل رأي مخالف والرافض لكل معارضة من بين المسببات غير المباشرة للنزوع إلى العنف الذي يعد المحطة الأولى لنشوء الإرهاب.[2]

سخرت الجزائر حصة معتبرة من ميزانيتها للقطاع العسكري، بغية تدعيم القوات النظامية سواء من جيش أو قوات الأمن أو درك الوطني ...الخ، ودفعها للميدان بقوة فمنذ سنة 1993 تشكلت قوات خاصة لمكافحة الإرهاب بقوة تقدر بـ 15 ألف عضو ليتضاعف العدد ويصل إلى 60 ألف عضو سنة 1998 يضاف إلى ذلك الحرس البلدي بقوة 100 ألف فرد سنة 1997، وقوات الدفاع الذاتي بأكثر من 100 ألف عضو؛ أي أن الكل مسؤول عن حفظ الأمن الوطني.[3]

فقد أثبتت السلطات الجزائرية من خلال تنسيق عملية مكافحة الإرهاب عبر ما يسمى قوات الأمن المشترك المكون من "**الجيش– الشرطة–الدرك**"، وضم أيضا الميلشيات المدنية المكونة من جماعات الدفاع الذاتي والوطنيين، والتي تجاوز تعدادها 200 ألف عنصر؛ أي أنه برز تطور كبير منذ سنة 1995 في كافة المجالات ولم يعد الجيش يسقط بسهولة في كمائن الجماعات الإسلامية المسلحة. [4]

المرحلة الثالثة: مرحلة ما بعد أحداث الـ 11 سبتمبر 2001

إن أهم التغيرات التي طرأت إليها العقيدة الأمنية الجزائرية بعد أحداث الحادي عشر سبتمبر 2011 وحتى هذا الوقت تكمن في الشراكات الإستراتيجية والمبادرات الأمنية التالية:

---

[1]– سميرة باسط،" **الاستراتيجية الجزائرية لمكافحة الإرهاب 1999–2014**" رسالة ماجستير، (جامعة الجزائر–3–، كلية العلوم السياسية والعلاقات الدولية، تخصص: دارسات استراتيجية وأمنية، 2013–2014)، ص75

[2]– منصور لخضاري، " **تطور"ظاهرة الإرهاب "في الجزائر من الصعيد الوطني إلى الصعيد غير الوطني ن مركز الامارات لدراسات والبحوث الاستراتيجية**"، أبو ظبي، العدد 194، (مايو 2014)، ص31

[3]– احميدي بوجليطة،" **سياسات مكافحة لإرهاب في الوطن العربي، دراسة مقارنة بين الجزائر ومصر**"، رسالة ماجستير، (جامعة دالي براهيم –2–، كلية العلوم السياسية، تخصص: دبلوماسية وتعاون دولي، 2009–2010)، ص 122

[4] – اليمين زرواطي،" **التجربة الجزائرية في مكافحة الإرهاب– 1978–2008**"، (لندن، مطبوعات إيي، 2014)، ص113

1. الهيكلة العسكرية والإجراءات الأمنية: عملت الجزائر على تعزيز جهودها لمراقبة حدودها البرية والبحرية والجوية بأن أوكلت لعدة مهام أمنية وتنظيمية لعبور الأفراد وضبط الحدود من مخاطر العمليات الإرهابية والجريمة المنظمة والهجرة الغير الشرعية وغيرها من المخاطر والتهديدات الحدودية ومن بين هذه الوحدات:

2. قيادة وحدات حراس الحدودGGF: ويتشكل هيكلها التنظيمي بتعدد الوحدات المركزية على المستوى المركزي، وتتكفل هذه المجموعة بالعمل على مراقبة الحدود وحمايتها.

3. **حراس الشواطئ:** وهي مصلحة تابعة لوزارة الدفاع الوطني تتكفل بحراسة الموانئ والشواطئ وحمايتها من كل محاولات التهريب في المجال البحري الطبيعي.

4. **مصالح شرطة الحدود:** من مهامها مكافحة الهجرة غير الشرعية والمخذرات والتهريب وضمان حراسة المطارات والسكك الحديدية ومراكز المراقبة، كما تتكفل بالأجانب.

5. الفرقة الجمهورية للتحري حول الهجرة غير الشرعية BRIK: والتي من مهامها متابعة شبكات الهجرة غير المشروعة والتحري عن أسبابها.

6. الديوان المركزي لمكافحة الهجرة غير الشرعية OCLCI: والذي أنشأته المديرية العامة للأمن الوطني وهو جهاز للقيادة والتنسيق بين مختلف الفرق الجهوية.[1]

و عليه، تمثل المؤسسات العسكرية جوهر النظام السياسي الجزائري، وذلك لما تحظى به من شرعية ثورية وموقع متميز في المنظومة الدستورية وقوة في التنظيم والإخراط في الحياة الإجتماعية والسياسية بل أنه مؤسسها. فبالرغم من تلازم المسعى الذي يشير إلى أن صلاحيات القيادة التي أعلنت الثورة تشمل الميداني والسياسي والعسكري، وأن هيئات الثورة وقيادتها المركزية والتنفذية شكلت على هذا الأساس، فإن الفروق ظلت قائمة بين السياسيين والعسكريين. إستمرار الجبش العسكري في مرحلة ما بعد الثورة يطور ويعتقد أن طريقته الأنجح والأصوب في معالجة المشاكل في مكافحة المسائل والقضايا التي في غاية الأهمية والخطورة وذلك أن يقوم الجيش العسكري بمهامه الأساسية عند اللزوم حيث يمارسها متى قدر أن المصالح العليا والمصالح العامة مهددة وفي خطر.[2]

---

[1] – نور الدين دخان، عيدون الحامدي،"**مسار تأمين الحدود الجزائرية: بين الإدارة الأحادية والصيغ التعاونية الإقليمية**"، دفاتر السياسة والقانون، العدد الرابع عشر، (جانفي 2016)، ص174

[2]– محمد بوضياف، "**مستقبل النظام السياسي الجزائري**"، أطروحة دكتوراه، (جامعة الجزائر، العلوم السياسية والعلاقات الدولية، 2007–2008)، ص51

المبحث الثالث: التحديات الأمنية الجزائرية.

المطلب الأول: التحديات السياسية والأمنية.

أولا: التحديات الداخلية.

تشير معطيات البيئة السياسية إلى وجود إختلال واضح في هيكل السلطة وممارستها منذ الإستقلال، وقد نجم عن هذا الإحتلال إنغلاق النظام السياسي فانقطعت من خلاله الدولة عن المجتمع، وبالتالي تراكمت مسببات الأزمة التنموية الشاملة منها:

1.أزمة الشرعية: ذلك أن الجزائر غداة الإستقلال إعتمدت الشرعية الثورية ركيزة نظام الحكم، وكان الجيش الضامن الرئيسي لها والممارس الفعلي للسلطة، وتشكل النظام بتحالف الجيش والحزب الواحد (**جيش جبهة التحرير الوطني**) والجهاز البيروقراطي الحكومي نظاما ظل مغلقا وبعيدا عن المشاركة الشعبية، وأبقى إرث النظام الأحادي على النزعة التسلطية بثبوت ديمقراطي بعد الإصلاحات السياسية عام 1989، بالرغم من أن مختلف الدساتير الجزائرية أكدت مبدأ السيادة الشعبية وإعتبارها مصدرا لكل مشروعية.

و من أسباب ظهور أزمة الشرعية كذلك ما يرتبط بإخفاق الدولة في مجالات تحقيق الإندماج السياسي والإجتماعي والتنمية الإقتصادية والعدالة في توزيع الثروة والسلطة.

2.أزمة المشاركة السياسية: تمثلت هذه الأزمة عن عجز المؤسسات والهياكل السياسية من إستيعاب كل القوى الموجودة في المجتمع، ورفض النخب الحاكمة إشراك هذه القوى في صناعة واتخاذ القرار الوطني إذ بقيت المشاركة عديمة الفعالية حتى مع تعدد الأحزاب والتنظيمات السياسية، حيث لم تتجاوز نسبة المشاركة في الإنتخابات التشريعية في 30 ماي 2002 مثلا (46.09%)، وفي سنة 2007 بنسبة (35,65%) فمن مجموع 18 مليون و760 ألف ناخب لم يصوت سوى 06 مليون و687 ألف، وبلغ عدد الأصوات المعبر عنها 05 مليون و726 ألف أي حوالي 12 مليون قاطعو الإنتخاب، وهذا يوضح أن فئة عريضة من المواطنين لم تقتنع لا بالإنتخابات ولا بالمترشحين، وبالتالي فقدت عملية الإنتخابات دورها في التعبير والمحاسبة.[1]

[1]– جهيدة ركاش ، قسايسية إلياس،"**التحديات الثقافية والاجتماعية لتنمية السياسية في الجزائر وآليات تفعيلها**"، جامعة حسيبة بن بوعلي، شلف، ص 05

3.غياب الإستقرار السياسي: إن المتتبع للمشهد السياسي الجزائري منذ الإستقلال وحتى الوقت الراهن، يلاحظ أن النظام الجزائري تميز في العديد من المرات بعدم الإستقرار، سواء في الأبنية الحكومية أو العلاقات السياسية والإجتماعية، هذا ما يؤثر سلبا على مسار التنمية السياسية وتجسيد حكم راشد فيها.

4.غياب مؤسسات المجتمع المدني: يتبين ضعف دور المجتمع المدني (بنيويا ووظيفيا) في التنمية السياسية بالجزائر، بسبب نزوع السلطة نحو الهيمنة على تنظيمات المجتمع المدني وتدخلها المستمر في شؤونها من خلال فرض الكثير من القيود السياسية والإدارية والمالية عليها، مما يحد من فاعليتها واستقلاليتها. [1]

ثانيا: التحديات الخارجية:

1.**أزمة مالي وانعكاساتها على الأمن الوطني الجزائري:** فيما يخص رفض النظام الجزائري التدخل العسكري في مالي إلى عدد من العوامل بدءا من قاعدة "**عدم التدخل**" إلى القلق إزاء التدخل الجزائري وامتداد التهديد إلى أراضيها، فهذا التدخل في مالي سيورط الجزائر في مأزق ودوامة أمنية، فحرب مالي هي حرب خارج حدود الجزائر، ومن غير الممكن أن يتورط الجيش الجزائري في حرب خارج الحدود، فانتهجت الجزائر ثلاثة مسارات لمحاولة وقف تداعيات أزمة شمال مالي فيما يلي:

أ. الأول سياسي: من خلال عقد لقاءات لدراسة وسائل التكفل بمطالب سكان المناطق الحدودية بجنوب الجزائر والتي يغلب عليها عنصر الطوارق وهو العنصر العرقي نفسه للمتمردين شمال مالي.

ب. الثاني أمني: يهدف إلى منع تسلل الجماعات الجهادية نحو ترابها بفعل العملية العسكرية شمال مالي

ج. الثالث دعوي: لتفادي تبعات الفكر المتطرف الذي إنتشر في الساحل الافريقي.[2]

2.**أثر التهديدات الأمنية في منطقة الساحل الإفريقي على الجزائر:** الحدود والخللافات الترابية ومطالب الإنفصال. مظاهر لم تغب عن المشهد السياسي في منطقة الساحل الإفريقي منذ السنوات الأولى لاستقلال الجزائر، فدول الجوار كانت أول بداية للمشاكل القادمة من هذا العمق الإفريقي، ثم الإنفجار الدوري لنزاع التوارق في مالي والنيجر وكذلك مشكلة قضية الصحراء الغربية.كلها معطيات دفعة الجزائر لإعطاء الجزائر أهمية

[1] – جهيدة ركاش ، قسايسية إلياس، نفس المرجع، 06

[2] – زكرياء بودن،" **أثر التهديدات الإرهابية في شمال مالي على الأمن الوطني الجزائري واستراتيجيات مواجهتها 2010-2014**"، رسالة ماجستير، كلية العلوم السياسة والعلاقات الدولية، تخصص: علاقات دولية ودراسات استراتيجية، 2014-2015)، ص 104

قصوى لمنطقة الساحل والصحرى الكبرى باعتبارها متخمة لحدودها الواسعة.[1] في إطار التعاون في مكافحة الإرهاب والجريمة المنظنة وتجريم الفدية، تبني الجزائر تصورها في تحقيق الأمن على مقاربة أمنية إقليمية في منطقة الساحل، تدعو من خلالها دول المنطقة إلى ضرورة التعاون فيما بينها لمواجهة التهديدات الأمنية، وإن كان التدخل الأجنبي في أصله بمثابة ضربة قاضية لفلسفة الأمن على المستويين الوطني والإفريقي.[2]

3.**إنعكاس أحداث الربيع العربي سلبا على الامن الوطني الجزائر:** بسقوط النظامين التونسي والليبي من الشرق والجنوب الشرقي وفوضى انتشار السلاح في المنطقة، إنعكس ذلك بشكل مباشر على الأزمة في شمال مالي. هذه الأخيرة كان، لها تأثير كبير على الأمن الوطني الجزائري، فالفراغ الأمني والمؤسساتي في الدول التي مسها الربيع العربي أدى إلى ظهور العديد من الحركات الإرهابية في المنطقة، كما أدى إلى تمدد جماعات إرهابية أخرى وفروعه إلى منطقة الساحل والصحراء، وتمركزها في شمال مالي، خصوصا بعد إعلانها العداء ضد الجزائر وقواتها الأمنية ومصالحها الأمنية، وهي التي تمتلك حدود جغرافية مع سبع دول إفريقية على مسافة تقدر بـ6427 كلم (المغرب 1643كلم، مالي 1376كلم، ليبيا 982كلم، تونس 966 كلم، النيجر956 كلم، موريتانيا 463 كلم، الصحراء الغربية 42 كلم) وهي حدود واسعة يصعب مراقبتها في ظل إنعدام المنظومات الأمنية والمؤسساتية للدول التي سقطت أنظمتها جراء العصيان المدني.[3]

المطلب الثالث: التحديات الإقتصادية والإجتماعية

أولا التحديات الإقتصادية:

1. التوازن الإقتصادي: الجزائر على غرار كل الدول في سعيها لتحقيق التوازن الإقتصادي مرت منذ إستقلالها بعدة محطات، كان أولها الإقتصاد الموجه والمخططات التنموية خلال فترة ستينيات وسبعينيات القرن الماضي، نفذت خلالها عدة برامج طموحة ترتكز على تأميم المحروقات والتصنيع، ثم مرحلة اللامركزية التي تميزت بأزمة البترول وما خلفته من نتائج كارثية على الوضع الإقتصادي والإجتماعي، ثم مرحلة تبني الإنفتاح، لتأتي بعدها الإصلاحات الخاصة بعد خروجه من الأزمة الأمنية.

---

[1]– شاكر ظريف،" **البعد الأمني الجزائري في منطقة الساحل والصحراء الإرفيقية، التحديات والرهانات**"، رسالة ماجستير، (جامعة الحاج لخضر– باتنة، كلية العلوم السياسية، 2009–2010)، ص47

[2]– عربي بومدين، فوزية قاسي،" **المقاربة الأمنية الجزائرية في منطقة الساحل الإفريقي: نحو تفعيل مبدئ الإنسانية، المستقبل العربي**"، كلية العلوم السياسية والعلاقات الدولية، قسم الدراسات الدولية، جامعة–3–، ص137

[3]– محمد الأمين بن عائشة،" **الدبلوماسية الجزائرية والمعضلة الأمنية في مالي: بين الاستمرار والتغير**"، ملخص أطروحة دكتوراه في العلوم السياسية والعلاقات دولية، جامعة الجزائر–3–، المجلة العربية للعلوم السياسية، ص 109.

فالجزائر تعتمد بشكل أساسي على صادرات المحروقات في تمويل إحتياطاتها من العملة الصعبة، ولم تكن الإجراءات وتدابير الدعم وتشجيع الصادرات خارج المحروقات التي شرع فيها سنة 1996، لترفع من مستوي نجاعة المؤسسات الجزائرية في قطاع التصدير إذ ظلت لا تتعدي 33% في أحسن الظروف، ولم تتطلق بالشكل المخطط لها، فالأرقام تدل على وجود إنحراف ما بين الأهداف المخططة وبين الأرقام المنجزة. حيث إكتشف وجود محيط غير سليم تتخلله المشاكل والعراقيل التي تعترض إنطلاقة الصادرات بشكل جيد.[1]

2. **التضخم**: كذلك التضخم من خلال تأثيره على الإدخار إذ يؤدي إلى التقليل من الميل الى الادخار بل والتقليل المدخرات الموجودة فعلا، وإذا إستمر الوضع هكذا فمن الممكن أن يؤدي إلى هبوط معدل الإدخار الوطني الجزائري إلى مستويات غير مرغوب فيها، وقد شوهد في بداية التسعينيات إرتفاعا كبيرا في معدلات التضخم بالجزائر، ترجمت بارتفاع مستوى أسعار السلع وزيادة تداول الكتلة النقدية.[2]

3. **التبعية الإقتصادية للمحروقات**: فبتأكيد العديد من الخبراء، أن الجزائر تواجه تحديات هامة ما لم تسارع في إعادة هيكلة النسيج الإقتصادي من خلال وضع خطط إستراتيجية مستقلة ترفع من فاعليته، فبالرغم من أن القطاع الإنتاجي الخاص يمثل حوالي 80% من الناتج المحلي الإجمالي خارج قطاع المحروقات إلا أن المحيط البيروقراطي والمؤسسات غير المسيرة جيدا يمثلان لب التحدي الذي يواجه النمو والتنمية الجزائرية.[3]

---

[1]– طارق قندور، السعيد قاسمي،"**تحديات ورهانات استراتيجية ترقية الصادرات الجزائرية خارج المحروقات (مقاربات وصفية تحليلية)**"، جامعة محمد بوضياف، المسيلة، الجزائر، ص 07.

[2]– بومدين نورين، زيدان محمد،"**دور السوق المالي في تمويل التنمية الاقتصادية بالجزائر، معوقات وآفاق**"، الملتقى الدولي حول سياسات التمويل وآثارها على الاقتصاديات والمؤسسات، دراسة حالة الجزائر والدول النامية، يومي 22/21 نوفمبر ،(2006)، بسكرة، ص 12

[3] – تسعديت بوسبعين،"**آثار التغيرات المناخية على التنمية المستدامة في الجزائ– دراسة إستشرافية–**"، أطروحة الدكتوراه، (جامعة امحمد بوقرة، بومرداس، كلية العلوم السياسية، تخصص: تسيير منظمات، 2014–2015)، ص 148

البلد	التبعية
المغرب	تبعية متوسطة (الخدمات الزراعية والسياحية)
الجزائر	النفط والغاز (72%من إيرادات الميزانية)
تونس	تبعية ضعيفة (الخدمات. الزارعة. السياحة. تكنولوجيا المعلومات والاتصال)
ليبيا	تبعية قوية اتجاه الغاز والنفط (70%من الناتج المحلي)
مصر	تبعية متوسطة (الغاز. الزراعة. السياحة)
السودان	تبعية متوسطة (التجارة. تربية المواشي)
موريطانيا	تبعية قوية اتجاه المعادن (الحديد. النحاس. والذهب) 27% من الناتج المحلي و52% من إيرادات الميزانية

جدول يوضح: تبعية بعض الدول العربية اتجاه الموارد الطبيعية.[1]

ثانيا: التحديات الإجتماعية.

1 . العامل الديمغرافي: بالرغم من النقص المسجل في النمو الديمغرافي في السنوات الأخيرة إلا أن تأثيره بقي كبيرا، حيث عدد طالبي الشغل في تزايد مستمر خلال الثلاثين سنة الماضية، كما إنتقلت النسبة المئوية من 45% سنة 1977 إلى 52% سنة 1987 لتصل إلى 59 سنة 1998، وسيبقى هذا حسب المنظمة العالمية إلى غاية 2030، وستصل الشريحة العمرية بين 16 و59 سنة 2000 إلى 56,76% لتسجل 61,36% سنة 2030، بمعنى أن مسألة التشغيل سيكون من الأمور المهمة جدا لسنوات عديدة قادمة.[2]

2 . تفشي البطالة: إن إنخفاض معدل البطالة من 17,7 % في سنة 2004 على 13,79 % سنة 2007 ، كان راجع إلى حجم مناصب الشغل التي تم إنشاؤها، وذلك نتيجة النمو الاقتصادي المسجل سنة 2007، والمقدر بـ 56 % مما أدى إلى إنخفاض البطالين من 1,671,534 شخص سنة 2004 1,374,663 شخص سنة 2007، فرغم معدل البطالة في الجزائر منخفض إلا أن مستواه يبقى مقلقا حسب الملاحظات التالية :

[1] – أحمد مصنوعة ، "**بركتو نصيرة، الأمن الاقتصادي العربي الواقع والتحديات، مجلة الزيادة لاقتصاديات الأعمال**"، المجلد 02، العدد03، (2016)، ص 75

[2] – مليكة فريمش ،" **دور الدولة في التنمية: دراسة حالة الجزائر، بحيث مقدم لنيل شهادة دكتوراه علوم السياسية والعلاقات الدولية، تخصص تنظيمات سياسية وإدارية**"، 2012، ص 407

- طبيعة مناصب الشغل التي تم إنشاءها سنة 2004 معظمها مؤقتة، ففي سنة 2005 نجد 58 % من الأجراء المؤقتين.
- ضعف مستوى تأهيل اليد العاملة بحيث نجد 64,86 % من طالبي العمل هم غير مؤهلين و 26,60 % منهم من لهم مستوى جامعي.

بالنسبة لتوزيع الشغل حسب القطاعات الإقتصادية، نجد هيمنة قطاع التجارة والخدمات الإدارية بحيث نجد 56,70 % من السكان المشغلين، وهذا على حساب قطاع الصناعة وكذا الفلاحة الذي يشغل 12% و13,60 % على التوالي.

3 . أزمة الهوية: فقد كانت من أهم أسباب عدم اللإستقرار في الجزائر، حيث أن أسبابها تاريخية ميزها التنوع الثقافي، فإلى جانب الثقافة الفرنسية وأصبحت تستخدم في العديد من أوجه الحياة، هذا التنوع أصبح يشكل أزمة للهوية عندما إستخدمته التيارات المتصارعة على الحكم لإقصاء بعضها البعض، كل ذلك أدى لزيادة التهميش الإجتماعي وعجز النظام السياسي وقنواته عن إستقبال وامتصاص التطورات الإجتماعية والتعبير عنها.[1]

المطلب الثالث: التحديات البيئية والتكنولوجية

أولا: التحديات البيئية

تميزت الدول النامية بانتقادها لمفهوم الأمن البيئي الذي يتمثل في توفير أساليب الحياة النظيفة الخالية من الأضرار والتلوث، وهذا فضلا عن المخلفات السلبية للشركات المتعددة الجنسيات من توطين التكنولوجيا الملوثة للبيئة التي لم تجد لها وطنا أفضل من البلدان النامية.[2]

فتدهور البيئة في الجزائر جاء نتيجة السياسة الإستعمارية في الجزائر خلفت أوضاعا متدهورة في جميع مجالات الحياة، حيث لم يحضى الجانب البيئي في الجزائر باهتمام كاف في التنمية الجزائرية مما أسفر عنه إفرازات خطيرة هددت توازن البيئة الطبيعية، ونوعية الحياة البشرية والحيوانية، حيث تعرض المجال الجزائري إلى تحديات مختلفة. كانت عنصر هدم وتخريب للخصائص البيئية في غياب أي إهتمام يذكر بدور الحماية والمحافظة. الشيء الذي أدي إلى مزيد من الضغوطات على الوسط الطبيعي، والإخلال بالتوازن والإستقرار الايكولوجي

[1] – مراد ناصر، "**التنمية المستدامة وتحدياتها في الجزائر**"، مجلة التواصل، العدد 26، (جوان 2010)، ص 150

[2] – سوسن مريبعي،" **التنمية البشرية في الجزائر – واقع وآفاق**"، رسالة ماجستير، (جامعة منتوري –02– ، كلية علوم سياسية وعلوم التسيير، 2012–2013)، ص 37

ومسار الغلاف الحيوي، وقد إقتصرت إجراءات حماية البيئة المستدامة لتقليل من المخاطر المتصاعدة، دون ملائمة المتطلبات الإقتصادية مع الإشتراطات البيئية لترشيد إستغلال النظم البئية والمحافظة عليها، لضمان إستمراريتها لفائدة الأجيال القادمة، وهذا لا يعني أن الدولة أهملت البيئة تماما في سياستها، وإنما لم تكن بالحجم الكافي الذي يصون البيئة بشكل مستديم، وذلك نتيجة لعدة ظروف تاريخية كان لها الأثر البالغ في السياسات المنتهجة تجاه البيئة.[1]

ثانيا: التحديات التكنولوجية.

عرف العالم تطورا كبير في إستخدام الانترنت وتكنولوجيا الإعلام والإتصال إلا أن هناك تباين واضح في إستخداماتها بين الدول المتقدمة والدول النامية، بما في هذه الأخيرة الجزائر وفيما يلي مقارنة بين فرنسا وأمريكا:

1.الدول المتقدمة: أصبح إستخدام تكنولوجيا الإعلام والإتصال النشاط الرئيسي في الدول الصناعية المتقدمة، حيث يعمل ما يزيد عن نصف السكان بصورة مباشرة أو غير مباشرة في إنتاج المعلومات ومعالجتها وتوزيعها، فبخصوص البيوت المجهزة بالكمبيوترات نرى أن فرنسا تتأخر بنسبة 18,5% مقارنة بالدول الغربية الأخرى كبريطانيا 23%. ألمانيا 25% في كندا إلى اسبانيا 11% وأخيرا اليونان 06% سنة 1997. أما بخصوص التجارة الإلكترونية فقد بلغ رقم المعاملات 53 مليار دولار سنة 2000 و96 مليار دولار سنة 2001 منه 74 مليار دولار للولايات المتحدة الأمريكية، أي نسبة 77% و169 مليار دولار سنة 2002 و284 مليار دولار سنة 2003 أي بنسبة 59 % و452 مليار دولار سنة 2004 أي بنسبة 59%.

2 . الدول النامية : أما الدول النامية بما فيها الجزائر تعاني من ندرة وسائل التكنولوجيا الإعلام والإتصال والتي سببها مشكلة توزيع هذه الوسائل ووصولها بشكل صحيح، فبخصوص إقتناء الحواسيب المصغرة لا تتجاوز 25% في أمريكا اللاتينية و0,01% في أمريكا الوسطى سنة 1997، بينما الدول العربية بين 5,62% في الكويت و3,5% في البحرين و0,3% في الجزائر و0,17% في المغرب ثم 0,01% في تونس 0,01% في سوريا، حيث بلغ عدد الحواسيب الموزعة للأنترنت حسب إحصائيات 1998 إلى 100 نسمة. فالإمارات العربية المتحدة 13,519%، الكويت 5,579%، مصر 2,013%، لبنان 1,400%، عمان 666. (مجموع الدول العربية 10 أي 24,024%). فإجمالي مستخدمي الانترنت في الدول النامية

[1]– محمود الأبرش،"**السياسة البيئية في الجزائر في ظل الاتجاهات البيئية العالمية**"، أطروحة دكتوراه، (جامعة محمد خيضر، بسكرة، كلية العلوم الإنسانية والاجتماعية، تخصص: علم اجتماع البيئة، 2016–2017)، ص 108

لإحصائيات 2001 تتراوح إلى 10,2% وأقل من 03% بما يعادل 2,3% مقارنة بالدول المتقدمة. ومن المؤشرات ذات العلاقة بقياس إنتشار الانترنت في التجارة الإلكترونية بمعدل أقل من 05% وفي 24 دولة إسلامية وأقل من 01% في 28 دولة (2001-2002) مما يشير إلى تدني مستوى البنى التحتية الإلكترونية وانخفاض معدل الدخول في الانترنت.[1]

3. **الجزائر:** يرجع تاريخ التطور التكنولوجي في الجزائر إلى سبعينيات القرن الماضي، في ورقة قدمتها الحكومة الجزائرية في التنمية متعلقة بسياسة البحث العلمي والتطور التكنولوجي، ورغم ما تقدمه الجزائر من محاولات في التطور التكنولوجي إلا أنها ما تزال بعيدة عن المستوى المطلوب في هذا المجال، ولقد أشارت دراسات حول معوقات التطور التكنولوجي في الجزائر ترجع عموما إلى عدة أسباب وأهمها: [2]

- قلة التخصصات في المشاريع التكنولوجية
- قلة الموارد المالية التي تواجع عملية الإبداع التكنولوجي
- عدم التنسيق بين الجهات الدولية المختصة
- نقص المعلومات المتاحة عن التطور التكنولوجي في القطاع الذي تعمل فيه المنشآت

[1]- عبد الوهاب بن بريكة، بن التركي زينب ،" **أثر تكنولوجيا الإعلام والاتصال في دفع عجلة التنمية**"، مجلة الباحث، العدد07، بسكرة، (جوان 2010)، ص ص 248-249.

[2]- حنان بن عاتق، توفيق حجماوي، "**واقع التطور التكنولوجي وتأثيره على آداء المنظمة في الجزائر**"، ملتقى دولي حول: الإبداع والتغيير التنظيمي في المنظمات الحديثة، جامعة سعد دحلب، البليدة، كلية العلوم الاقتصادية، وعلوم التسيير، 2013، ص 17

خلاصة الفصل الثاني:

نستنتج مما سبق أن الجزائر تفاعلت مع التهديدات الأمنية التي كانت محدقة بها، حيث بذلت جهدا كبيرا سياسيا وأمنيا دبلوماسيا وعسكريا واقتصاديا من أجل الحد من تلك المخاطر، إذ يلاحظ تنامي تأثير عقيدة الأمن الوطني باعتبارها تمثل المبادئ المنظمة التي تساعد الجزائر على التفاعل والتعامل مع تلك التهديدات والتحديات البارزة والكامنة التي تواجه أمنها واستقرارها.

الفصل الثالث: اليقظة الإستراتيجية الجزائرية لإرساء الأمن السيبيراني

المبحث الأوّل: استخدامات الأنترنت في الجزائر.

المبحث الثاني: دور المؤسسات الأمنية في تحقيق الأمن السيبيراني.

المبحث الثالث: رؤية إستشرافية للأمن السيبيراني.

تمهيد الفصل الثالث:

يعتبر العصر الحالي "عصر سيبراني" بامتياز، فقد أصبح العمود الفقري لمعظم التفاعلات اليومية، وأصبحت الانترنت سلاحا ذا حدين، فكما هي وسيلة لتحقيق التقدم البشري، هناك جانب آخر يتمثل في تزايد التهديدات والمخاطر السيبرانية الناجمة على الاعتماد المتزايد عليه، في ظل عالم مفتوح تحكمه تفاعلات غير مرئية وغياب سلطة قانونية عليا تسيطر عليه، حيث اتجهت معظم الدول والحكومات لتبني استراتيجيات وسياسات لتعظيم أمنها من التهديدات والتحديات بهدف تحقيق الأمن السيبراني، والجزائر وكغيرها من الدول اهتمت بهذه الأخيرة وتحاول أن تتبنى نموذج حكومة ذكية في ظل مجتمع جزائري معلوماتي، كما أنها تعمل على إنشاء هيئات أمنية مختصة لمكافحة تلك المخاطر السيبرانية. وعليه، **ما هي المخاطر السيبرانية التي عرفتها الجزائر؟ وما هي الإستراتيجيات الأمنية المتخذة؟**

المبحث الأول: إستخدامات الأنترنت في الجزائر.

المطلب الأول: تطوير الأنترنت في الجزائر.

سعت الجزائر إلى الإستفادة من خدمات شبكة الأنترنت والتقنيات المرتبطة بها من خلال إرتباطها بشبكة الأنترنت في شهر مارس من عام 1994، عن طريق مركز البحث في الإعلام العلمي والتقني (Cerist) الذي أنشئ في شهر أفريل سنة 1986 من قبل وزارة التعليم العالي والبحث العلمي،[1] وقد قدر عدد الهيئات المشتركة في الأنترنت سنة 1996؛ أي بعد سنتين من دخول الأنترنت إلى الجزائر بحوالي 130هيئة. كما قدر في سنة 1999 عدد الهيئات المشتركة في الشبكة بـ 800 هيئة، منها 100 في القطاع الجامعي و50 في القطاع الصحي و500 في القطاع الإقتصادي و150 في قطاعات أخرى. وفي نفس السنة أي 1999 كان لمركز البحث في الإعلام العلمي والتقني حوالي 3500 مشترك. [2]

وعام 2001 قامت وزارة البريد والموصلات بعد إنشاء مؤسسة "**الجزائر تيليكوم**" -Algérie Telecom) بتعاقد مع شركتين عالميتين هما: "**لوستن تكنولوجي**" (Losent-Technologie) و"**أريسكون**" (Ericson) السويدية لإنشاء قواعد خاصة، ستمكن من الحصول على بث يتجاوز 30 ميغابت/ثا. وقد تعرضت الأنترنت في الجزائر إلى مجموعة من العوائق تتلخص في إرتفاع أسعار الهاتف الثابت وكذا بطء في الشبكة سنة 2003.[3] كما كشفت إحدى الإحصائيات أن مجموع مستخدمي الأنترنت بلغ نحو ثلاث ملايين بحلول 2006، إذ بلغ مع نهاية 2006 المرتبطين بالأنترنت عن طريق(ADSL) إلى 300000. إلى أن إتجه الوضع نحو تبني سياسة توفير جهاز كمبيوتر لكل عائلة جزائرية بحلول 2010[4]

---

[1]– زهوة خلوط،"**التسويق الإبتكاري وأثره على بناء ولاء الزبائن، دراسة حالة: مؤسسة اتصالات الجزائر**"، رسالة ماجيستير، (جامعة امحمد بوقرة، بومرداس، كلية العلوم الإقتصادية تجارة وعلوم التسيير، 2013– 2014)

[2] – نعيمة برنيس، "**الوظيفة الإعلامية لشبكة الأنترنت في عصر ثورة المعلومات**"، رسالة ماجستير، (جامعة منثوري قسنطينة، كلية العلوم الإنسانية والإجتماعية، فرع: صحافة مكتوبة وسمعية بصري، 2009–2010)، ص101

[3] – باديس لونيس،"**جمهور الطلبة الجزائريين والأنترنت، دراسة في إستخدامات إشباعات طلبة جامعة منتوري قسنطينة**"، رسالة ماجستير، (جامعة منتوري– قسنطينة، كلية العلوم الإنسانية والعلوم الإجتماعية، قسم علوم الإعلام والاتصال 2007–2008)، ص62.

[4] – خيرة روابحي،" **ثقافة الأنترنت: دراسة ميدانية لاستعلامات الشبكة بمدينة تيهيرت**"، رسالة ماجستير، (جامعة وهران، كلية العلوم الإنسانية والحضارة الإسلامية، قسم علم المكتبات والعلوم الوثائقية، 2009–2010)، ص78

أما حسب الإحصائيات الأخيرة فقد بلغ عدد مستخدمي الأنترنت لسنة 2012، حوالي 5 مليون و230000 مستخدم بنسبة تبلغ 14%.[1]

المطلب الثاني: ظهور مجتمع المعلومات في الجزائر:

يعتبر مجتمع المعلومات دائرة متحدة تهتم بالأوضاع العامة من حشود وروابط ومصادر متنوعة تتشكل ما بين المؤسسات والأفراد لرعاية إهتمامات المجتمع حول توفير وتبادل المعلومات، والمعرفة الهادفة إلى سرعة الحصول على المعلومات وزيادة المعرفة، كما أن مجتمع المعلومات أيضا هو جميع الأنشطة والممارسات المرتبطة بالمعلومات إنتاجا ونشرا وتنظيما وإستثمارا، ويشمل انتاج المعلومات أنشطة البحث والجهود الإبداعية بالتأليف الموجه لخدمة الأهداف التعليمية والتثقيفية.[2]

ولقد عرف المجتمع الحديث تسميات عديدة مثل المجتمع ما بعد الصناعي والمجتمع الإستهلاكي ومجتمع المعرفة نظرا للتزايد الكبير في حجم المعلومات والتراكم المعرفي الذي ميز هذا العصر وما صاحبه من تطور في تكنولوجيا المعلومات والإتصال وظهور شبكة الأنترنت، وهي عوامل زادت من أهمية المعلومات في حياة الفرد والمجتمع.[3]

وما يميز مجتمع المعلومات في الجزائر عن غيره هو تناوله لجل العناصر المكونة لمجتمع المعلومات، فهناك من تناول الأنترنت من الناحية القانونية كدراسة ظاهرة الإجرام الإلكتروني، أو طرح مشكلة الملكية الفكرية للأعمال الإبداعية على الشبكة، وأن هناك من إنفرد ببحث موضوع الفضائيات، وفي كل هذا يمكن القول أنه واحد من مكونات مجتمع المعلومات، حيث عملت الجزائر على ما يلي:

أولا: إنشاء لجنة خاصة بمجتمع المعلومات: حيث تم إنشاء لجنة خاصة بمجتمع المعلومات في الجزائر في 9 ماي 2001 تتكون من 20 شخصا وهم ممثلون من وزارات وهيئات عمومية وخاصة وأعضاء من

---

[1]– كريمة صراع،" **واقع وآفاق التجارة الإلكترونية في الجزائر**"، رسالة ماجستير، (جامعة وهران، كلية العلوم الإقتصادية وعلوم التسيير، تخصص: إستراتيجية، 2013–2014)، ص139

[2]– هند علوي،" **المرصد الوطني لمجتمع المعلومات بالجزائ، قياس النفاذ إلى تكنولوجيا المعلومات والاتصالات بقطاع التعليم بالشرق الجزائري**"، أطروحة دكتوراه، (جامعة منتوري– قسنطينة، كلية العلوم الانسانية، تخصص: علم المكتبات 2007–2008)، ص 41

[3]– مراد كريم،"**مجتمع المعلومات أثره في المكتبات الجامعية، مدينة قسنطينة–أنموذجا**–"، أطروحة دكتوراه، (جامعة منتوري – قسنطينة، كلية العلوم الإنسانية والاجتماعية، قسم علم المكتبات، 2007–2008)، ص 36.

الدواوين الوزارية وأساتذة ومانحي خدمات الأنترنت لتقديم تقرير حول الرهانات التي يطرحها مجتمع المعلومات والشروط اللازمة توفرها لتحقيقه.[1]

ثانيا: إصلاح قطاع الاتصالات:

لتعويض التأخير وسد الثغرات ورفع تحديات القرن العشرين وضمان ولوج الجزائر إلى مجتمع المعلومات، قررت الحكومة الجزائرية إجراء إصلاحات تهدف إلى تكييف قطاع الإتصالات مع التوجيهات والتحولات العالمية الناتجة عن تطور النمو التكنولوجي، ومن بين أهداف برنامج إعادة تأهيل الهياكل الإتصالية، الرفع من العرض على الخدمات بإنجاز هياكل جديدة لتحسين الإرتباطية.

ثالثا: إتصالات الجزائر:

أنشئت إتصالات الجزائر بتاريخ 5 أوت 2000 المتعلق بإعادة هيكلة قطاع البريد والإتصالات والذي يفصل النشاط البريدي عن الإتصالي، وهي شركة ذات أسهم وبرأسمال عمومي يتم تنشيطه في سوق الشبكات والخدمات الإتصالية الإلكترونية. والجدول التالي يوضح أنه لا تستطيع البنى التحتية والأدوات والخدمات الخاصة بتكنولوجيا المعلومات والإتصالات أن تكون الوسيلة الفعالة للوصول إلى المعلومات، ولتشجيع توليد المعرفة وتشاركها من دون توفر المعلومات للعامة وإمكانية النفاذ إلى المحتوى الرقمي دون قيود وبأسعار مقبولة للجميع.[2]

	2009-2008		2011-2010		2012		2013		2014	
	القيمة	الترتيب	القيمة	الترتيب	القيمة	الترتيب	القيمة	الترتيب	القيمة	الترتيب
الأردن	5.1	46	5.2	45	5.3	50	5.4	48	3.5	54
الامرات المتحدة	3.5	34	5.9	26	5.9	30	6.1	23	6.1	20
البحرين	5.5	29	5.9	28	6.1	19	5.9	31	5.3	38
تونس	5.1	48	4.9	61	4.8	79	-	-	4.5	110
الجزائر	3.2	125	3.6	122	3.6	126	3.3	137	3	144

جدول يوضح: إمكانية النفاذ إلى المحتوى الرقمي في بعض البلدان العربية

[1] – آمنة بن عبد ربه،" **النظام الإقتصادي الجديد المبني على المعرفة وتطور مجتمع المعلومات والتكنولوجيا الحديثة للإتصال، الحلول المقترحة لإرساء مجتمع معلومات ناجح ومتكامل في الجزائر**"، رسالة ماجستير، (جامعة الجزائر كلية العلوم السياسية والإعلام، قسم علوم الإعلام والإتصال، 2005-2006)، ص33-35

[2] – آمنة بن عبد ربه، نفس الراجع، ص 39

المطلب الثالث: مشروع الجزائر الإلكتروني 2013.

إستراتيجية الجزائر الإلكترونية أو ما يعرف "**بمشروع الجزائر الالكتروني 2013**" حيث يندرج هذا المشروع ضمن المبادرات والمشاريع التنموية التي تتبناها الحكومة الجزائرية لتحقيق التنمية المستدامة في مختلف جوانب الحياة، ليندرج في إطار بروز مجتمع العلم والمغرفة للجزائريين والذي يرمي إلى إحلال نظام إلكتروني متطور شامل، وتعميم إستعمال التكنولوجيات الحديثة من خلال ترقية نظام المعلوماتية في قطاعات الإتصالات. فمشروع الجزائر الإلكتروني تم إطلاقه من طرف وزارة البريد والتكنولوجيات والاتصال، وتم التشاور فيها مع المؤسسات والإدارات العمومية والمتعاملين الإقتصاديين العموميين والخواص والجامعات ومراكز البحث والجمعيات المهنية التي تنشط في مجال العلوم والتكنولوجيات الإعلام والاتصال.[1]

وقد تم إعتماد هذه الخطة من خلال تقييم وضعية قطاع التكنولوجيا الإعلام والإتصال من خلال عدة مؤشرات وهي: مؤشر الجدوى والنفاذ الرقمي والتحضير الإلكتروني، ومؤشر نشر تكنولوجيا الإعلام والإتصال.[2] فتبني الجزائر "**مشروع الجزائر الالكتروني**" يعكس مدى إهتمام الحكومة الجزائرية بضرورة عصرنة القطاع الحكومي وما تمليه عليه الحاجة الإجتماعية والإقتصادية والسياسية والتكنولوجيا التي مست أغلب الدول المتقدمة، وتشكل المعركة الرقمية وتدعيم الرأسمالي البشري الأساسي للرهانات التي تطرحها التنمية الإقتصادية والاجتماعية والعامل رئيسي لتحضير البلاد لمواجهة تحديات العولمة ومخاطر التهديدات المعلوماتية بمختلف أشكالها. فتهدف هذه الإستراتيجيات "**مشروع الجزائر الإلكترونية** " إلى بروز مجتمع العلم والمعرفة مع الأخذ بعين الإعتبار التحولات العميقة والسريعة التي يعيشها العالم.[3]

---

[1] – عادل غزال،"**مشاريع الحكومة الإلكترونية من الاستراتيجية إلى التطليق، مشروع الجزائر: الحكومة الإلكترونية 2013 – أنموذجا**–"، مجلة المكتبات والمعلومات، العدد34، (مارس 2014)، ص64

[2] – إلياس شاهد، الحاج عرابة، عبد النعيم دفرو، **تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر**، المجلة الجزائرية للدراسات المحاسبية والمالية، العدد الثالث، (2016)، ص130

[3] – عبد القادر عبان،" **تحديات الإدارة الإلكترونية في الجزائر، دراسة سوسيولوجية ببلدية الكاليتوس العاصمة**"، أطروحة دكتوراه (ل م د)، (جامعة محمد خيضر – بسكرة، كلية العلوم الإنسانية والاجتماعية، 2015 تخصص: إدارة وعمل 2016)، ص91

إن الحكومة الإلكترونية هي نتيجة طبيعية لثورة المعلومات وظهور مجتمع المعرفة، لهذا فإن تفعيل الحكومة الإلكترونية في مواقف الدولة كلها هو جزء من السعي إلى الولوج في عالم المعلومات والإتصالات الحديثة من أوسع الأبواب، وجزء لا يتجزأ من العمل على بناء المعرفة والتفاعل مع العولمة. [1]

كما عرف البنك الدولي الحكومة الالكترونية بأنها : عملية إستخدام المؤسسات الحكومية لتكنولوجيا المعلومات مثل: (شبكات المعلومات العريضة وشبكة الانترنت وأساليب الإتصال عبر الهاتف المحمول) والتي لديها القدرة على التغيير وتحويل العلاقات مع المواطنين ورجال الأعمال ومختلف المؤسسات الحكومية، وهذه التكنولوجيا يمكنها أن تخدم عددا كبيرا من الأهداف مثل: تقديم خدمات أفضل للموطنين، تحسين التعامل والتفاعل مع رجال الأعمال ومجتمع الصناعة، وتمكين المواطنين من الوصول للمعلومات مما يوفر مزيدا من الشفافية، أو إدارة أكثر كفاءة للمؤسسات الحكومية، كما أن نتائج هذه التطبيقات يمكن أن تؤدي إلى تحجيم الفساد، وزيادة الحكومية، كما أن نتائج هذه التطبيقات يمكن أن تؤدي إلى تحجيم الفساد، وزيادة الشفافية، وتعظيم العائد ككل أو تخفيض النفقات وزيادة قناعة المواطن بدور المؤسسة الحكومية في حياته.[2]

[1] – أسامة بن صادق طيب، محمد نور بن ياسين فطاني، عصام بن يحي الفيلالي،" **الحكومة الالكترونية، نحو مجتمع المعرفة**"، معهد البحوث والاستشارات، العدد التاسع، جامعة الملك عبد العزيز، جدة، السعودية، (2013)، ص 04.

[2] – زين عبد الهادي،" **الحكومة الالكترونية في العالم العربي بين النماذج الناجحة ونماذج تطلع للنجاح**"، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، ص 03.

المبحث الثاني: دور المؤسسات الأمنية في تحقيق الأمن السيبراني

المطلب الأول: الأجهزة العملياتية المختصة في الأمن السيبراني

أولا: على المستوى الوطني

1.مركز الوقاية من جرائم الإعلام الالي لدرك الوطني:

يعتبر هذ المركز الذي أنشئ سنة 2008 "**ببئر مراد رايس**" جهازا يهدف إلى تأثير تأمين منظومة المعلومات لخدمة الأمن العمومي، ويعكف على تحليل معطيات وبيانات الجرائم المعلوماتية، المرتكبة وكذا تحديد هويه أصحابها سواء كانو أشخاص فرادى أو عصابات أو غيرها. [1]

ويهدف هذ المركز إلى مساعدة الأجهزة الأمنية الأخرى بالتعاون من أجل مكافحة الجرائم المعلوماتية، حيث يعنى المركز بتطوير أساليب التعامل مع هذه الجرائم ووضع قوانين لتنظيم مجال إستغلال المعلومة من خلال تنسيق مع وزارة العدل وكذا من خلال معهد خاص بعلم الإجرام لتطوير مستوى التعامل مع الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، فالجزائر تعمل جاهدا على الإستفادة من خبرات البلدان الأخرى في تأمين المنظومة المعلوماتية وحمايتها من الجرائم ضمن مجموعة من العناصر أهمها :

– **الوقاية:** وتشمل حملة تحسيسية وتوعية بالتنسيق مع وزارة التضامن الوطني والأسرة، والعمل على ملتقيات ومحاضرات وأياما دراسية ومنتديات دولية، ومشاركة في منتديات صحفية وحصص تلفزيونية وإذاعية وغيرها من وسائل النشر والإشهار.

– **المكافحة:** توعية الجزائريين من خلال إستعمالهم لشبكات التواصل وإستخدام الأنترنت وذلك من خلال تعليقاتهم المدافعة عن الجزائر ومعرفة الأخطار بسلوكات مشبوهة أو إعتداءات عبر نشر فيديوهات توصل إلى الجناة، مما يسهل التحقيق لدى مصالح الدرك وإلقاء القبض على المشبوهين ومرتكبي الجرائم في الوقت المناسب. [2]

---

[1] – سمير بارة،"**الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Cyber Security) في الجزائر: الدور والتحديات**"، جامعة قاصدي مرباح، ورقلة، ص 445

[2] – سهام بو عموشة، " **الفضاء السبراني يتميز بانفتاح شبكة المعلوماتية وانعدام الحواجز الجغرافية**"، جريدة الشعب، العدد 17345، 24 ماي (2017)، ص 06

2.المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني "**ببوشاوي**"، حيث تم إنشاءه بموجب مرسوم رئاسي 04/133 المؤرخ في 26 جوان 2004، ودخل حيز الخدمة إبتداءا من الفاتح جانفي 2009، أما الفترة الممتدة بين 2004 و2009 كرست لتكوين المورد البشري وإقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد بالعديد من المهام التي من شأنها تلبية الطلبات الواردة من السلطة القضائية، ضباط الشرطة القضائية والسلطات المؤهلة ، قانونيا خاصة أثناء معالجة القضايا المعقدة.[1]

- **مصلحة الاعلام الآلي :**

مصلحة تابعة للمعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني، فعلى مستوى هاته المصلحة يتم رصد ومراقبة وتتبع عمليات إختراق وقرصنة المعلوماتية، وكذ اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتي ومن مهام المصحة ما يلي:[2]

. العمل لاستكمال إقامة منظومة إتصال آلية على شكل شبكة تربط مختلف وحدات وهياكل الدرك الوطني تسمح بالإتصال الآلي للمعلومات أفقيا وعموديا مما يسهل على المحققين التحري عن الجرائم وتعقب المجرمين بفعالية.

. العمل على تنظيم هياكل ووحدات مكلفة بممارسة الشرطة القضائية على نحو يعزز تخصص الوحدات أو على الأقل إنشاء فرق متخصصة في المخدرات والتزوير وجرائم الإعلام الآلي، وغيرها من الجرائم المعقدة التي تنفذها شبكات منظمة والتي تصنف على أنها إجرام منظم.[3]

3: المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

تم إنشاء المصلحة المركزية للجريمة الإلكترونية سنة 2011 بعد إستجابة مصلحة الأمن الجزائري لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم الإلكترونية، حيث عملت هاته المصلحة

---

[1] – نسيمة سحواذ،" **الطموح لتوسيع دائرة الاعتماد المتبادل بإدراج طرق تحليلية لفائدة مخابر أخرى**"، في: 02 مارس http // Dikanews.com13:63/2018

[2] – بارة سمير، مرجع سابق، ص436

[3] – أحمد غاي،" **تكييف الشرطة القضائية مع متطلبات إصلاح العدالة، تقييم وآفاق**"، في: 03 مارس w.w.w.mjustice .dg 14:13/2018

على تكييف التشكيل الأمني لمدير الشرطة القضائية، فالمصلحة كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني.[1]

و أكدت مديرية الأمن حول موضوع "**الجريمة المستحدثة**" على أهمية استعداد وجاهزية كافة وحدات جهاز الشرطة بمختلف تخصصاتها، لمواجهة الجرائم المستحدثة ذات الصلة الوطيدة بالمعلوماتية والشبكة المعلوماتية والشبكة العنكبوتية، من خلال الاجتهاد في أساليب إستفحال هذه الظاهرة العابرة للأوطان، التي باتت تعرف "**بالجريمة السيبرانية** "، للتمكن في الأخير لوضع جبهة أمنية فعالة للتصدي لهذه الآفة، التي ما فتئت تأخذ أبعادا خطيرة عاما بعد عام.

فالمدرية العامة للأمن الوطني طالما سعت لوضع مخطط عمل ميداني للرفع من يقظة جهاز الشرطة والمصالح المختصة في متابعة الجريمة المعلوماتية، وهذا بفضل وسائل وآليات التحكم في تكنولوجيا الإعلام الإتصال لقطع دابر هذا الشكل من الجرائم.[2]

4: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها.

نصت على إنشاء هذه الهيئة المادة 13 من القانون 04/09 المؤرخ في أوت المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها من خلال: "**تنشأ هيئة وطنية وتنظيمها وكيفيات سيرها عن طريق التنظيم**" أما مهامها فقد أوردت المادة 14 من نفس القانون وتتمثل في:

أ . الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والإتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الإتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء، إختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية ...الخ

ب . مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال: بحسب نص المادة 14 من القانون 04/09 هناك نوعان من المكافحة تقوم بهما هذه الهيئة :

---

[1]– عبد القادر سعيدي،" **المصلحة المركزية الالكترونية في مواجهة مجرمي العالم الافتراضي**"، في: 03 مارس2018 17:42/www.essalamonline.com

[2]– راضية مناد، " **تطوير قدرات الشرطة في مواجهة الجريمة الالكترونية ، أمن واستراتيجية**"، 03 مارس 2018/www.dgayerinfo.com.21:19

أ . مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الاعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة (ب) من القانون 04/09.

ب . تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها،[1] يقترح المشروع في هذا الفصل إنشاء هيئة وطنية مختصة تتولى مهام أهمها: تنشيط وتنسيق عملية الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية ومصالح الشرطة القضائية من التحريات التي تجريها بشأن هذه الجرائم، وما تقوم به أيضا من تجميع المعلومات من نظيرتها في الخارج قصد محاربة هذا النوع الخطير من الإجرام.[2]

ثانيا: على المستوى الدولي:

المنظمة الدولية للشرطة الجنائية (الأنتربول):

أما على المستوى الدولي فقد نصت المادة (16ق/ و) على أنه في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني من أجل تبادل المعلومات بين الدول في الخارج بشأن الجريمة والتعرف على الفاعلين وتحديد مكان تواجدهم، تقوم الهيئة الجزائرية بمشاركة الأعمال التحضيرية الضرورية مع الهيئات الدولية المماثلة لها بهدف البحث والتعرف على الجرائم المعلوماتية ومرتكبيها وتحديد مكان تواجدهم.

فتسعى الجزائر لتبادل المعلومات بين الدول وتركز على المنظمة الدولية للشرطة الجنائية لأنها أهم جهاز دولي في مجال مكافحة الإجرام بما فيها الجرائم المعلومانية، كما تعمل على تشجيع التعاون الدولي بين أجهزة الشرطة من خلال وضع قائمة تضم ضباط مختصين في المجال البحث والتحري بشان الإجرام المعلوماتي والذين

---

[1]– أحمد مسعود مريم،" **آليات مكافحة جرائم تكنولوجيا الاعلام والاتصال في ضوء القانون رقم 04/09**"، رسالة ماجستير، (جامعة قاصدي مرباح– ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012–2013)، ص 44–45

[2]– الجريدة الرسمية،"**القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وطرق مكافحتها**"، الفترة التشريعية السادسة، السنة الثالثة، الدورة الرابعة، رقم 122،(27 يونيو 2009)، ص04

يمكن الإستعانة بهم من طرف الدول كما تسهل الإجراءات القضائية المتعلقة بتسليم المجرمين وتنفيذ الإنابات القضائية الدولية وكذا نشر أوامر القبض الدولية للمبحوث عنهم والمطالبة بتسليمهم.[1]

ومكن التعاون الجيد لدوائر الشرطة فيما بينها ومع المنظمة الدولية للشرطة الجنائية (**الأنتربول**) من تنظيم دورات تدريبيه متعددة لفائدة موظفي الشرطة في بلدان عديدة ومن تبادل المعلومات وإنشاء قاعدة بيانات للصور وبرامج لتحديد هوية الضحايا ، ونظام لرصد "**إستغلال الأطفال**" وما إلى ذلك. وفي إطار هذا التعاون تم رد الاستبيان الذي وجهته المنظمة من طرف البلدان التالية: (روسيا . الوم أ . اليابان . اليونان . اسبانيا . أستراليا . ألمانيا . الامارات العربية المتحدة . أندونيسيا . تونس . الجزائر . العراق . عمان . مصر . المغرب . قطر . سويسرا . البرتغال . إيطاليا وغيرها من الدول الأخرى في العالم)، ذلك قصد وضع قوانين ومعاقبة مجرمي إستغلال الأطفال في المواد الإباحية على شبكة الانترنت.[2]

المطلب الثاني : الإستراتيجيات الأمنية لمكافحة التهديدات السيبرانية

أولا: اليقضة الإسراتيجية التابعة لمركز الوقاية

تتمثل مهمة المسؤولين عن إستراتيجيات مطاردة وتتبع ورصد كل أشكال وصور المخالفات والجرائم التي تركب بواسطة الشبكة العالمية للمعلومات، الذم والتحقير، التهديد والإبتزاز، القرصنة المعلوماتية على جميع المستويات، التحرش بمختلف أشكاله، سرقة الهوية وإنتحال الشخصية، عرض الأغراض الممنوعة للبيع عبر المواقع التجارية، الدعاية المغرضة والإرهاب وغيرهم من الجرائم، كل هذه الجرائم المعلوماتية وغيرها وضع لها مكتب اليقضة التابع بالمركز مجموعة من الإستراتيجيات لمراقبة الانترنت ومرافقة الجناة المعلوماتيون وأيضا معاقبتهم.[3]

1 . اليقضة الأمنية : يمكن بفضلها متابعة مدى تطور الإجرام وأساليبه بصفة عامة والخطط العملية التي ينتهجها المجرمون بغرض تحضير وتجنيد أفضل للأفراد والوسائل للتصدي لهذا النوع من الجرائم

2. اليقضة التكنولوجية والعلمية :تتمثل في جمع المعلومات والمعطيات التي تسمح بمتابعة الإبتكارات

---

[1] – إيمان بن سالم،"**جريمة التجنيد الالكتروني للإرهاب وفقا لقانون العقوبات الجزائري**"، (برلين، المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية ،2008)، ص80

[2]– نجاة معلا مجيد،" **تعزيز وحماية جميع حقوق الانسان، بما في ذلك الحق في التنمية**"، الجمعية العامة، الأمم المتحدة، الدورة الثانية عشر، البند 03 من جدول الأعمال، ص24

[3] – إسماعيل جنة، "**حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون**"، مجلة الجيش،العدد 599، (جوان 2013)، ص14

والتطورات في المجال التكنولوجي والعلمي في مختلف المجالات التي تهم الدرك الوطني بصفة خاصة والجيش الوطني بصفة عامة.

3. اليقضة الإجتماعية: وتعمى بمتابعة التحليل ومختلف الدراسات التي بالمجتمع وتطوراته والمعايير التي تتحكم فيه وعلاقاتها بالأمن العام.

4. اليقضة القانونية :تهتم بمتابعة التطورات الحاصة في المجال القانوني والنصوص التشريعية متعلقة بمختلق المهام والنشاطات التي تمت بصلة مهام الدرك الوطني لا سيما الحفاظ على الأمن العام .

5. اليقضة الاقتصادية: تهتم بالجوانب الاقتصادية وتطورات السوق الوطنية والأجنبية، وتهدف إلى حماية المصطلح في إطار توقيع العقود أو معاهدات الشراكة الاقتصادية ويعقب هذه الاستراتيجيات تقرير تقني يرسل إلى قيادة الدرك الوطني تقوم بدورها بنشره وتوزيعه على المستوى المركزي الإقليمي (الهيئات التابعة لقيادة الدرك الوطني، قيادة مجموعات حرس الحدود ...)، أو الجهوي الإقليمي (المجموعات الإقليمية، القيادة الجهوية لحرس الحدود ....)، أو المحلي الكتائب وفصائل البحث والتحريات ...).[1]

ثانيا: الندوة الدولية حول الأمن السيبراني في الجزائر

إعتمدت الجزائر مقاربة شاملة تجمع الأمن العمودي والأمن السيبراني من أجل مكافحة ظاهرة الجرائم السيبرانية العابرة للحدود، باعتماد آليات عملية التعاون بغية فهم أفضل للتحديات الكبرى على المستوى العالمي، لاسيما في ظل تنامي التهديدات الأمنية الإلكترونية والأضرار الوخيمة الناتجة عنها بسبب الإختراقات الأمنية المقلقة التي إستهدفت العديد من الدول في الآونة الأخيرة التي مست بأمنها واستقرارها وبنيتها التحتية.

نظمت الجزائر ندوة دولية حول "**الأمن السيبراني**" في شهر ماي 2016. شاركت فيه أكثر من 15 دولة وأكثر من 50 خبيرا دوليا في الأمن السيبراني، تطرقه من خلالها إلى حالة التطور التكنولوجي والتشريعات الخاصة بالفضاء السيبراني، والسياسات المتعلقة بالأمن السيبراني وأمن المنشآت الحساسة والوقاية من جرائم الانترنت ومكافحتها. وقد أجمع الخبراء المشاركون في هذه الندوة على ضرورة إرساء تعاون حقيقي بين الدول يسمح بمحاربة الجريمة الرقمية التي تمس الأشخاص والمؤسسات على حد سواء.[2]

---

[1]– إسماعيل جنة،" **حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون**"، المرجع السابق، ص15.

[2]– مصطفى عباني،"**التدابير الأخرى في مجال نزع السلاح والأمن الدولي**"، اللجنة الأولى للدورة الـ 71 الجمعية العامة للأمم المتحدة، بعثة الجزائر الدائمة لدى الأمم المتحدة، نيويورك، 24 أكتوبر 2016، ص 02

و شهد هذا الملتقى مشاركة مختصين عسكريين ومدنيين في مجال الأمن والدفاع السيبراني وبشكل فرصة للمشاركين من أجل تبادل الخبرات والمعارف ومناقشة المستجدات والتطورات في هذا المجال من خلال محاضرات وورشات عمل تطبيقية تعطي نظرة ملموسة عن "**التهديدات السيبرانية**" بالإضافة إلى التشريعات الخاصة بالفضاء السيبراني، مما سيفضي على الخروج بتوصيات في المجال تسيير الأزمات السيبرانية وتعزيز إستراتيجية الدفاع الوطني لمكافحة التهديدات السيبرانية.[1]

ثالثا: إستراتيجية حفظ النظام والأمن العموميين

شدد قائد سلاح الدرك الوطني اللواء "**مناد نوبة**" في كلمة ألقها في خلال إشرافه على افتتاح الندوة الدولية حول الأمن السيبراني تحت عنوان "**الفضاء السيبراني**" رهانات وتحديات على وضع ضرورة خطط إستراتيجية لمكافحة الجريمة المعلوماتية والمنظمة بكل الطرق، موضحا أن مؤسسة الدرك تضطلع بمهام الأمن العمومي، وتضع لهذا العرض وسائل التحديات الخاصة بالشرطة العلمية والتقنية والخيرة الجنائية. مؤكد أن جهازه يسهر على حفظ النظام والأمن العموميين من خلال اتخاذ إجراءات وقائية بواسطة الرصد العام والمستمر، كما يسهر ضمان الأمن العمومي من خلال حماية الممتلكات وحرية التنقل على وسائط الإتصال، كما يحرص على التطبيق المستمر للقوانين والأنظمة المسيرة داخل التراب الوطني.

رابعا: إستراتيجية إنشاء تشريعات جديدة متعلقة بالتهديدات السيبرانية:

وأمام إنتشار الجرائم الالكترونية، دعا السيد "**مناد نوبة**" إلى سن تشريعات جديدة لكشف الجناة وملاحقتهم وتشديد الرقابة على أجهزة الدولة والشركات والبنوك، إضافة إلى حماية الأفراد من أن يقعوا فريسة للجناة. وقال أن تجريد الفعل الإجرامي من شكله المادي يفرض على الدرك إنشاء شكل تنظمي جديد ووسائل ملائمة وإجراءات عملياتية فعالة وذلك في إطار مقاربة شاملة، للحد من تنامي الجرائم الإلكترونية وتهديداتها التي أصبحت تشكل خطر حقيقي على أمن الدول من خلال محاولة الإختراق الأمني للمؤسسات العامة والحيوية وسرقة البيانات والتجسس والمساس بالنظام العام.

[1]– سليمة مقراني،" **الجيش الوطني الشعبي : ملتقى حول الدفاع السيبراني، مكون أساسي للأمن والدفاع الوطني**" في: 07 مارس 2018/17:51،hltps :www.eljoumhouria.dg

خامسا: إستراتيجية التعاون الدولي للوقاية من الجرائم السيبرانية:

ممثلو قيادات الجيوش الأمريكية والفرنسية والكندية : "**الفضاء السيبراني**" خطر على مؤسسات الدولة وموقها الحساس ، وهو الوسيلة المفضلة للجماعات الإرهابية لتسجيل أكبر عدد من الشباب والنساء وصفوفها . وأكدوا على ضرورة تحصين مؤسسات الدول من "**الإرهاب الالكتروني**"

1.كندا: حيث قال ممثلها على هامش الندوة التي نظمتها قيادة الدرك الوطني حول الجريمة المعلوماتية، أن الأنترنت والخدمات الإلكترونية والمعلوماتية وفرت هامش مهم لجماعات التطرف والعنف بما قدمت لهم من فرص النشر والإتصال بصور لم تكن متاحة سابقا لتنظيمات الخارجة عن القانون، كما أصبحت مواقع التواصل الإجتماعي "**الفاسبوك**" وسيلة لتجنيد الإرهابي والتنظيمات الإرهابية.

2.فرنسا: من جهتها أكد اللواء "**مارك وتين أوغوراد**" ممثل الجيش الفرنسي: أن الجريمة الالكترونية أضحت في الوقت الراهن عابرة للحدود وعلى هذا الأساس فإن جميع الدول مدعوة إلى العمل بطريقة دقيقة وذكية لمواجهتها من خلال استقطاب المخترقي المؤسسات والبنوك "**الهاركر**" واستغلالهم في مجال التأمين المؤسسات كونهم يعتبرون من فئة الأذكياء

3.الولايات المتحدة الأمريكية: قال اللواء "**جون بول باليميروا**" ممثلا للولايات المتحدة في الندوة: أن الجرائم الإلكترونية تعد من أخطر الجرائم التي تواجهها دول العالم، حيث تهدد أمنها وإستقرارها وهي إحدى وسائل الإرهاب التي تستخدم عن طريق الإختراق الأمني للمؤسسات العامة والحيوية.[1]

سادسا: إستراتيجيات الدفاع السيبراني ومراقبة الأنظمة:

قررت القيادة العليا للجيش إستحداث "**مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة** " على مستوى دائرة الإستعمال والتحضير لأركان الجيش بهدف تأمين وحماية المنظومات والمنشآت الحيوية للبلاد ضد التهديدات والإرهاب الإلكتروني والجوسسة على أسرار الدولة الجزائرية. فإنشاء مصلحة الدفاع السيبراني ومراقبة الأنظمة، سيحمي الدولة من كافة التهديدات التي يشكلها الدفاع السيبراني على الأمن، وحتى على سيادة الجزائر، حيث سيتم تغطية كل الجوانب التي لها صلة بتحقيق نظام دفاعي متكامل وفعال لتأمين وحماية

[1]– عبد الرحمان بن حمادي،"**الفضاء الأزرق أصبح مكانا مثاليا للقيام بأعمال غير مشروعة**"، معرض الصحافة، تجزئة سعيد بن حداد، الشراقة ، الجزائر (25 ماي 2016)، ص4-5

المنظومات والمنشآت الحيوية والحساسة للجزائر ضد التهديدات والإرهاب الإلكتروني وإحباط كل محاولة للتجسس على أسرار الجزائر، ومن مهام مصلحة الدفاع السيبراني ومراقبة الأنظمة ما يلي:

مهام المصلحة فمهام مصلحة الدفاع السيبراني ومراقبة الأنظمة تتمثل في تخطيط وإدراج ومتابعة حالة تقوم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات ومنظومات الإتصال وكذا منظومة الأسلحة للجيش. فأهم محاور إستراتيجية الدفاع السيبراني للجيش:

1 . الجانب الوظيفي والتنظيمي: حتى تكون أعمال الدفاع السيبراني ضمن موجهة ومنفذة في إطار سلسلة وظيفية أو تنظيمية مكرسة لضمان تجانس وفعالية هذه الأعمال.

2 . الجانب القانوني: مكلف بتحسين وتعزيز باستمرار الإطار القانوني المتعلق باستعمال تكنولوجيا الإعلام والإتصال عموما وتأمين منظومات الإعلام خصوص.

3. جانب الموارد البشرية: الذي يتطلب جاهزية مورد بشري تقني معتبر وذي كفاءة عالية في مجال الدفاع السيبراني هدفا أساسيا لكي تضمن نجاح إدخال هذا المجال في النشاطات العملياتية والتسيير للجيش.

4 . الجانب التقني: مكلف بتقوية وتكييف القدرات التقنية للحماية والكشف والردع على الهجمات السيبرانية باستمرار، مع يقظة دائمة فيما يخص الطرق والوسائل المستعملة من طرف المهاجمين.

5 . الجانب الوقاية: يتعلق بوقاية وتحسيس مستخدمي الجيش الوطني الشعبي من المخاطر والتهديدات التي تنجر عن إستعمال تكنولوجيا الإعلام والإتصال في الإطار المهني أو الشخصي بطريقة مستمرة.

6 . جانب البحث والتطوير: باستعمال وسائل تقنية خاصة وشخصية من طرف هياكل البحث والتطوير للجيش الوطني الشعبي، لاسيما تلك المستعملة للحماية ضد التهديدات السيبرانية عنصرا حاسما في إستراتيجية الدفاع السيبراني.

7 **. جانب تعزيز التعاون**: التعاون مع الدول الشريكة من أجل السماح لقوات الجيش الجزائري من الاستفادة من الخبرات والوسائل التكنولوجية المتقدمة جدا.[1]

[1]– نوارة باشوش، "**الجيش يدخل الحرب الفضاء الالكتروني**" في: 07 مارس 20:17/2018، www.ehoroukonline.com

سابعا: إستراتيجيات المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني

1. سعت المديرية العامة للأمن الوطني لوضع خطط عمل ميداني للرفع من يقظة جهاز والمصالح المختصة في متابعة الجريمة المعلوماتية، وهذا بفضل وسائل وآليات التحكم في تكنولوجيا الإعلام والإتصال لمكافحة هذا الشكل من الجرائم.

2. إنشاء ندوات أمنية من شانها تسليط الضوء أكثر على ما يتعلق بالجرائم المستحدثة خاصة بالجزائر، حيث تعد فرصة لتبادل الخبرات والأفكار مع المختصين لتشريح هذه الظاهرة بشكل موسع.[1]

3 . برمجت المديرية العامة للأمن الوطني عدة دورات تكنولوجية حول موضوع "**الوقاية السيبرانية**" من خلال توفير دورات تكنولوجية تقنية عالية المستوى في المجال مكافحة الجريمة الالكترونية ومسايرة فرق المحققين من الشرطة لإحداث التكنولوجيا والتحكم فيها والاطلاع عليها على الأساليب المعتمدة دوليا في الوقاية والمكافحة لهاته الجرائم الإلكترونية الهدامة .

4. وضع خطط إستراتيجية في المجال الوقاية والتحسس من هذه الجرائم الناجمة عن سوء إستعمال الشبكات العنكبوتية خاصة من طرف الشباب والأطفال باللجوء إلى العمل الإستباقي لإزالة الأخطار المحتملة وحماية الأفراد والمجتمع من هذا النوع من الجرائم .[2]

المطلب الثالث: نماذج تطبيقة عن أهم المخاطر السيبرانية في الجزائر

تشهد الساحة الأمنية الجزائرية كغيرها من الدول العديدة من المخاطر والتهديدات التي فرضتها الثورة التكنولوجية الحديثة، خاصة بعد إنتشار ووسائل التواصل الإجتماعي والعديد من المواقع الإلكترونية التي تحمل أفكارا تهدم وتهدد إستقرار الوطن ووحدته ، وتدعو إلى نشر الفوضى والعنف والتطرف والكراهية والإنقسام، هذا ما جعل الدولة الجزائرية تبحث عن سبيل مكافحة مثل هذه الجرائم من أجل تحقيق الأمن السيبراني من خلال الأجهزة الأمنية المختصة في مكافحة الجرائم الإلكترونية ومن أهم النماذج التالية أكثر دليلا على تجربة الجزائر في محاربة هذه الجرائم التالية:

[1] – مناد راضية، مرجع سابق

[2] . صالح ميهوبي، "**جرائم الانترنت تنخر المجتمع الجزائري**"، جريدة البلاد ، العدد 18،5369 (جويلية2017)، ص 07

أولا: خطر الإرهاب السيبراني على الأمن الوطني الجزائري :

ويعتبر الإرهاب السيبراني أحد اهم التهديدات التي تستهدف أمن جميع الدول في ذلك الدولة الجزائرية، وهذا ما أكده اللواء "**مناد نوبة**" القائد العام للدرك الوطني الجزائري في كلمة القها بمناسبة إفتتاح الندوة الدولية حول "**الأمن السيبراني**" في ماي 2017، حيث قال : "إن الإرهاب الالكتروني بات من أخطر الجرائم التي تستهدف الجرائم، من خلال تنامي مظاهر الترويج لكل أشكال العنف والإرهاب والتطرف". لذلك دعا إلى إطلاق خلايا أمنية مختصة هدفها للعمل على تعزيز إجراءات الرقابة لحماية المواطن الجزائري، وخاصة عنصر الشباب من مثل هذه الجرائم الإلكترونية الخطيرة جدا على إستقرار البلاد. فيجب على الدولة الجزائرية ضرورة "**التسلح الالكتروني**" بكل الوسائل التكنولوجية والفعالية لمحاربة أيديولوجيات العنف والتطرف وكل أشكال الجريمة المنظمة والعابرة للأوطان، من خلال إعتماد آليات عملية التعاون بين الشركات الفاعلين في هذا المجال.[1]

كما تمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني والأمن الوطني وبالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال من معالجة أكثر من 1000 جريمة إلكترونية منها 30% على مواقع التواصل الإجتماعي، هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول عام 2016 وجود 11 قضية متعلقة بالإرهاب الإلكتروني أغلبها خاصة بتهديدات إرهابية باسم "**تنظيم داعش الإرهابي**" لتسفر جهود البحث والتحري والتنسيق بين مختلف القطاعات المختصة توقيف 58 شخص متورط في قضايا إرهاب إلكتروني تمت إحالتهم على القضاء. هذا وقد إستطاع الجيش الإلكتروني الجزائري من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع "**تنظيم داعش**" في العراق وسوريا وليبيا، كما تمكن فك شفرات الرسائل المتبادلة ومايزيد عن 30 خلية تسعى لإستقطاب الشباب لتجنيد عبر مواقع الأنترنت ومنصات التواصل الإجتماعي، خاصة "**الفيسبوك**" و"**التوتير**"

[1]– عنترة بن مرزوق، محي الدين حرشاوي،"**الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية**"، كلية الحقوق والعلوم السياسية، المركز الجامعي آفلوا، ص 68.

لصالح التنظيمات الإرهابية نتيجة إستعمالها الأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشورات إرهابية تدعو للمشاركة في منتديات إرهابية إلى جانب إتصالات محلية ودولية.[1]

ثانيا: مخاطر الألعاب الإلكترونية على أطفال الجزائر

قام مرصد حقوق الطفل بالتعاون مع الهيئات أمنية مختصة بدراسة حول "**جرائم الأنترنت والأطفال في الجزائر**" وشملت عينة الدراسة 975 طفلا منهم 548 ذكرا و427 أنثى ينتمون إلى 10 بلديات مختلفة على المستوى الجزائر العاصمة، حيث طرح عليهم 16 سؤالا لمعرفة مدى علاقتهم بالتقنيات الجديدة لوسائل الإعلام والإتصال. فقد بينت إجابات المستجوبين أن 23.89% من الآباء مقابل 13.79% من الأمهات الأطفال يعانون من الأمية، في حين أن ,43.69% من الآباء مقابل 49.02% من الأمهات يملكون مستوى تعليميا يتأرجح بين الإبتدائي والثانوي، في حين 32.82% من الآباء مقابل 18,76 % من الأمهات لديهم مستوى جامعي. كما كشفت الإستجوابات أن 56,26% من عائلات الأطفال البحوثين يملكون جهاز كمبيوتر واحد، فيما يملك 8 % منهم أكثر من جهاز كمبيوتر، إضافة إلى ثلث الأسر مربوطة بشكل الأنترنت.

و وجد معدوا الدراسة أن 72,25 % من الأطفال الذين يستخدمون شبكات الأنترنت بحرية في المنزل وعلاوة على ذلك أجاب 68,75% منهم بأن أولياءهم يسمحون بإستخدام تقنية الأنترنت، وإتضح أيضا أن 66،25% من الأطفال يسمح لهم بإستخدام تقنية الأنترنت في منزل الأصدقاء، وأن 43،5 %يلجؤون إلى غرف الدردشة، وهي نسبة معتبرة، وأبرزت الأرقام أن 30.5% من الأطفال المبحوثين تلقوا عروضا للحصول على هدايا والإستفادة من طرف مجهول، وإتضح أن نسبة 48% من الأطفال المبحوثين سمعوا عن جرائم الأنترنت، وهي نتيجة مهمة، كذلك 80،25% من الأطفال يرون أن حماية الطفل من مخاطر الأنترنت ضرورة.

و بموجب هذه المعطيات إستنتج فريق البحث أن الجزائريين متفتحون على التقنيات الجديدة الإعلام والإتصال، كما أن عدة أسر تتعامل معها بثقة كبيرة يعكسها السماح للأطفال بإستخدام الأنترنت دون مراقبة. فتبين هذه الدراسة إرتفاع نسبة تعامل الأطفال مع الأنترنت وإرتفاع نسبة تعرضهم لمخاطرها، كما تبين

[1]– آمال صويلح،"**الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام خطوة هامة نحو مكافحة الارهاب الالكتروني بالجزائر**"، الملتقى الدولي حول "الاجرام السيبراني"، المفاهيم والتحديدات يومي: 11-12 أفريل 2017، جامعة 8 ماي 1945، قالمة . الجزائر، ص09

ضعف المتابعة الأسرية ونقص الوعي الأسري بمخاطر الأنترنت على الأطفال، مما يؤكد على ضرورة تفعيل دور الأسرة والمجتمع ككل لاتخاذ التدابير الوقائية اللازمة، وبالرغم من تناول الدراسة مؤشرات للمستوى التعليمي والوضع الإقتصادي للأولياء، إلا أنه تبين مدى إرتباط ذلك بالوعي بمخاطر الأنترنت أو وجود الرقابة الأسرية على الأطفال.[1]

ثالثا: مخاطر مواقع التواصل الاجتماعي الهدامة:

1.مخاطر التواصل الاجتماعي على الأمن الوطني الجزائري: إن مواقع التواصل الاجتماعي وخاصة "**الفيسبوك**" من أكثر مواقع التواصل خطورة على الأمن الوطني الجزائري، حيث إحتل المرتبة الأولى بنسبة 50.45%، يليه المرتبة الثانية موقع المشاهدة "**اليوتيوب**" بنسبة 30.63 %، في حين جاء "**الويتر**" في المرتبة الثالثة بنسبة 18.92%، وغيرها من المواقع، مما يدل على أن "**الفيسبوك**" يمثل مصدرا خطيرا على الأمن الوطني، نظرا لتداوله أخبارا ومعلومات تختلق الشائعات والأخبار الكاذبة، وهو ما ينعكس على المؤسسات الرسمية للدولة ويفقدها مصداقيتها، والتي من شأنها تكدير الأمن العام للبلاد وتعريضها لهجمات إرهابية، حيث أصبح هذا الفضاء مستغل من طرف الجماعات الإرهابية الجزائرية خاصة بعد إنضمامها إلى تنظيم القاعدة ببلاد المغرب العربي، الشيء الذي سهل في إتصالاتها والتحضير والتخطيط لعملياتها وكذا توقع توجيه تهديدات مستقبلية على مؤسسات الدولة المرتبطة بالأنترنت مثل شبكة الأمن الوطني والجيش وشركة التأمين. ففي الواقع لا يوجد فرق مختصة ومكونة من مصالح الاستعلامات العامة لمتابعة النشاط الهدام للإرهاب المعلوماتي، لذا فإن المرحلة المقبلة يجب أن تتماشى الإستعلامات العامة لمتابعة ومراقبة المعلومات المتعلقة بنشاطات الجماعات الإرهابية مع التطور التكنولوجي.[2]

2.الاشاعات وآثارها على الاستقرار الأمني والسياسي للدولة الجزائرية:

ما يؤشر أن الدولة الجزائرية ليست بمنأى من ظاهرة الإشاعات التي تفتك بالمجتمع وتمس إستقراره واستدامة الأمن والاستقرار السياسي والاجتماعي، حيث عمل موقع التواصل الجتماعي "الفيسبوك" على إيجاد آذان صاغية للأفكار الكاذبة والمعلومات المغلوطة والمعارضة الهدامة التي لا تسعى إلى بناء الثقة والإستقرار داخل

[1] – مسعودة بايوسف،"**الطفل والانترنت المنزلي، مجالات الاستخدام والاشباعات المحققة**"، مجلة العلوم الإنسانية والاجتماعية ، العدد 27، (ديسمبر2016)، ص 44

[2] – حكيم غريب، "**مخاطر مواقع التواصل الاجتماعي على الأمن المجتمعي: الرهانات والاستراتيجيات**"، ندوة علمية دولية حول: "عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية"، الثلاثاء (11 أفرير 2017)، ص 08

المجتمع الجزائري وزعزعة الثقة بالمسؤولين، إن المعظلة الحقيقية التي يمكن أن تقف كتحدي للدولة، هي صعوبة التحكم في هذه الصفحات ما يطرح إشكالية مدى وحدود القدرات التي تتمتع بها الدولة الجزائرية سواء كان النظام القانوني الذي يشكل الردع لدى الأشخاص، أو القدرات التكنولوجية لتعقب الأثر الإلكتروني لهذه الصفحات خاصة في ظل تعدد الوسائط التكنولوجية وعدم ثباتها، بحيث يمكن إستخدامها من عدة حواسيب أو عدة هواتف نقالة.[1]

رابعا: تسريبات بكالوريا 2016

أكدت مصالح الأمن الوطني أن بكالوريا 2016 إنتهت على وقع توتر كبير عقب تسرب مواضيع الإمتحان على شبكات التواصل الإجتماعي، تم على إثره تحديد هوية 31 شخصا متورطا في هذه القضية. وفند الديوان الوطن للإمتحانات والمسابقات إلغاء الامتحانات عقب معلومات مشرت على الشبكات الإجتماعية (**الفيسبوك**)كما قامت مصالح الأمن باستجواب إمراة قد تكون المتورطة الرئيسة في تسريب مواضيع الإمتحان في مادتي التاريخ والجغرافيا والتي ظلت تحت الرقابة القضائية. وقد أكدت وزير العدل حافظ الأختام "**طيب لوح**" أن وكالاء الجمهورية ببعض ولايات الوطن أعطو تعليمات للشرطة القضائية والدرك الوطني لفتح تحقيق حول أسباب تسرب مواضيع البكالوريا.

و أوضحت المصالح أنه تم التعرف على صفحات التبادل المتورطة (أكثر من 15) وحسابات "**الفايسبوك**" المستعملة (ضبط 150حساب منه ماهو متمركزا بالخارج) وذلك بفضل التحريات والتدابير المتخذة وفق نظام محكم لمركز الوقاية من جرائم الاعلام الآلي وجرائم المعلوماتية ومكافحتها التابع للدرك الوطني.[2]

خامسا: لعبة الحوت الأزرق المميتة:

بدأت لعبة "**الحوت الأزرق**" سنة 2013 في روسيا، لتبدأ مرحلة الانتشار وتستهدف الأطفال والمراهقين على حد سواء في لعبة تحدي الموت. حيث تقوم اللعبة بالتحكم بهم من خلال تحديدهم على

---

[1] – شرف الدين بن إرث، "**إشاعات وآثارها على الاستقرار الأمني والسياسي للدولة، حقائق من صفحات التواصل الاجتماعي، صفحات الفيس بوك الجزائرية**"، ندوة علمية دولية حول: "عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية"، الثلاثاء (11 أفريل2017) ، ص 06

[2] – غنية توات،" **القرار الأخير بشأن مصير الامتحان يعود للحكومة، يومية إخبارية وطنية**"، جريدة الفجر، العدد 4778، 19 (جوان2016)، ص05

مستوى خمسين مرحلة، بأمرهم بمهمات خطيرة لتصل اللعبة في مرحلتها الأخيرة إلى أمرهم بالإنتحار، هذا وقد يكون أطفال الجزائر من ضحايا هذه اللعبة القاتلة.

فعن الجهاز الأمني الجزائري ومختصون في علم الإجتماع أنه دق ناقوس الخطر حول مخاطر إستعمال الأنترنت على الأطفال والقصر في الجزائر، وفي ظل انتشار ظاهرة "**الحوت الأزرق**" الذي قال عنه مختصون في ملتقى جهوي ضم رؤساء مديريات الأمن لولايات الشرق الجزائري، أنه يدخل ضمن الجرائم الالكترونية، حيث تم عرض النصوص التشريعية المتعلقة بالجرائم المعلوماتية وطرق مكافحتها، وستنظم في هذا الشأن قافلة توعية تشارك فيها مديرية النشاط الاجتماعي، مديرية التربية والتكوين المهني ومصالح الأمن، لتفعيل الجانب الوقائي من مخاطر الأنترنت.[1]

كما أعلنت وزارة العدل أن الهيئة الوطنية للوقاية من جرائم تكنولوجيات الاعلام والاتصال بالتنسيق مع النيابات العامة المختصة ، فتحت تحقيقا قصايا بخصوص هاته اللعبة المميتة التي تدفع الأطفال إلى الانتحار، وفي هذا السياق أطلقت المديرية العامة للأمن الوطني ووزارة التربية الوطنية ، حملة تحسيسية عبر المؤسسات التربوية لتوعية التلاميذ وأوليائهم بخطورة الألعاب على شبكة الانترنت في أعقاب ارتفاع عدد الضحايا ما يعرف بلعبة الحوت الأزرق الالكترونية .[2]

وأكدت وزيرة البريد وتكنولوجيا الاتصالات الجزائرية " هدى أيمان فرعون " أنه من الجانب التقني ، لا تملك تماما، لأنه لا يوجد موقع ألعاب يمكن حجبه ، وإنما تطبيقات يتم تحميلها مثل هذه اللعبة. ونقلت تقارير محلية عن مديرية الشرطة القضائية الجزائرية حول مخاطر الألعاب الالكترونية والاستخدام السيء للأنترنت على الأطفال بأنه يستحيل حجب هذه الألعاب الإلكترونية والسبب يعود إلى " التطور التكنولوجي " الذي يسمح بفتح الآلاف الصفحات في ثانية واحدة.[3]

---

[1]– علجية عيش، "**الحوت الأزرق من الجرائم الالكترونية التي يعاقب عليها القانون**"، جريدة الأحرار، العدد 6063، (25 ديسمبر 2017)، ص04

[2]– الإذاعة الجزائرية، "**فتح تحقيق قضائي في "انتحار" بعض الأطفال بسبب لعبة الحوت الأزرق**"،01 أفريل 2018/10:00 www.Radioalgerie.dg

[3]– عثمان لحياني، "**السلطات الجزائرة : تحجب "الحوت الأزرق" مستحيل ... وهذا بديلها**"، في: 01 أفريل 2018/10:22 www.altahrironlen.com

المبحث الثالث: رؤية إستشرافية للأمن السيبراني.

المطلب الأول: أوجه القوة السيبرانية في الجزائر.

تجتهد الجزائر في سبيل أجهوتها الأمنية ، حيث أشرف خبراء تكونية سنة2010 وكانت حول مكافحة الجريمة المعلوماتية لفائدة ضباط الشرطة القضائية والقضاة، وغيرها من الأجهزة الأمنية الأخرى، حيث تهدف هذه الأخيرة إلى إطلاعهم على آخر التكنولوجيات لمحاربة الجريمة وكيفية استخدام الأدلة الالكترونية في التحقيق والمقاضاة، وقد شارك في الاشراف على الورشة التدريبية خبراء في الجرائم الحاسوبية والملكية الفكرية، وقسم الجريمة المنظمة وإبتزاز الأموال التابعة لوزارة العدل الأمريكية ، وقد نصب التدريب على الجانب النظري والتطبيقي معا. كما تم التعرف على تقنيات إجراء التحري وإقامة الدليل على الجرائم المعلوماتية وكيفية استغلال الأنترنت والبريد الالكتروني ، وكذا التعاون في هذا المجال.[1]

[1] – عبد الحليم بوقرين، "**حتمية إنشاء ضبطية خاصة بالجرائم الالكترونية ، مجلة العلوم القانونية والسياسية**"، المجلد الخامس ، العدد الثاني ، 2016، ص 158

في مجال الدرك الوطني		
الولايات المتحدة الأمريكية	فرنسا	الجزائر
	*إنشاء قسم أنترنت تابع للمصلحة التقنية للبحوث القانونية سنة 1998 يتكون من (13)دركيا من بين مهندسين وتقنيين ويتولى هذا القسم مهمة معالجة المعلومات *إنشاء قسم معلوماتي تابع لمعهد البحوث الجنائية في الدرك الوطني سنة 1992 مهمته تقديم المساعدة التقنية على شكل خبرة	* إنشاء مركز الوقاية من الجرام الاعلام الالي سنة 2008 ببئر مراد رايس * إنشاء المعهد الوطني للأدلة الجنائية وعلم الاجرام الوطني ببوشاي بموجب مرسوم رئاسي رقم 04/133في جوان 2004 ودخل حيز الخدمة في جانفي 2009
في مجال الشرطة		
- إنشاء مكتب مركزي لمكافحة الجريمة المعلوماتية سنة 1991،و وصل عدد أعضائه إلى (20) وكيل نيابي سنة 2000	*إنشاء مكتب مركزي لمكافة الاجرام المعلوماتي بموجبمرسوم رقم(405/2000) سنة 2000 ويتواجد على مستوى المديرية المركزية للشرطة القضائية	*إنشاء ورشة تكوينية سنة 2001 حول مكافحة الجريمة المعلوماتية لفائدة الشرطة القضائية وتطويرها بالتعاون مع خبراء من الاستخبارات الأمريكية.
في مجال الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال		
	*إنشاء مكتب مركزي لمكافحة الجريمة المعلوماتية بموجب المرسوم (405/2000) على مستوى مديرية للشرطة القضائية	*إنشاء هيئة حسب المادة (13) من القانون (04/09)المؤرخ في 2009، متعلق بالوقاية من الجرائم المعلوماتية

جدول يوضح مقارنة بين الجزائر ودول أخرى للأجهزة الأمنية المختصة في الأمن السيبراني

نشر الاتحاد الدول للاتصال (ITU) تقريره السنوي لتصنيف دول العالم في مجال الأمن السيبراني ويقيس المؤشر التزام الدول في جميع أنحاء العالم بتفعيل وتطوير مختلف تقنيات الامن السيبراني ،ووفقا للاتحاد الدولي للاتصالات ،فإن حوالي نصف بلدان العالم لديها استراتيجية النظر في السياسات الوطنية الرامية إلى الحماية من الجرائم المعلوماتية والالكترونية ، وأظهر التقرير أن هناك مجالا للمزيد من التحسينات والتعاون على

كافة المستويات وفقا لما جاء في التقرير الذي يدعو إلى تشجيع الحكومات على الاهتمام بالسياسات الوطنية التي تأخذ في تأخذ في الاعتبار الأمن السيبراني، وكذلك زيادة وعي المواطنين حول استعمال الأنترنت .[1]

وتم تقسم الدول إلى ثلاث فئات في مجال الامن السيبراني : المتخلفة – الناضجة – المتقدمة ، وفيما يلي قائمة الدول التي تصدرت التصنيف المراتب العشرة في تحقيق الأمن السيبراني بما فيهم الجزائر التي تحتل المرتبة التتاسعة عربيا وافريقيا، والمرتبة ثمانية وستين عالميا :

	الدول الغربية	الدول العربية
المرتبة الأولى	سنغافورة	عمان – عالميا 04
المرتبة الثانية	ال وم	مصر- عالميا 14
المرتبة الثالثة	ماليزيا	قطر - عالميا 25
المرتبة الرابعة	رستونيا	تونس – عالميا40
المرة الخامسة	موريتشوس	المملكة العربية السعودية عالميا46
المرتبة السادسة	استراليا	الامارات العربية المتحدة عالميا 47
المرتبة السابعة	جورجيا	المغرب-عالميا 49
المرتبة الثامنة	فرنسا	البحرين – عالميا 65
المرتبة التاسعة	كندا	الجزائر – عالميا 68
المرتبة العاشرة	روسيا	الأردن – عالميا 93

جدول يوضح قامة الدول التي تصدرت المراتب العشرة الأولى في تحقيق الأمن السيبراني

البنية الأساسية لتكنولوجيا المعلومات ولاتصالات: شهدت البنية الأساسية في المنطقة العربية تطورا سريعا مع ظهور الأجيال الجديدة من الشبكات النقالة وسرعة الاتصال بالأنترنت عبر الشبكات الثابتة والنقالة على سواء، حيث احتلت الجزائر المرتبة الثانية بعد الأردن تحت مسؤولية (سلطة الضبط للبريد والموصلات السلكية واللاسلكية):[2]

1. الأردن (الهيئة التنظيم قطاع الاتصالات)

[1] – أماني جهاد، "**تصنيف الدول الغربية والعربية في مجال الأمن السيبراني لسنة 2017**"، في: 02 أفريل WWW.3ARABINSIDEE.COM11:18/2018

[2]– الاسكوا، **تقرير الملامح الإقليمية لمجتمع المعلومات في المنطقة العربية**، اللجنة الإقتصادية والاجتماعية لغربي آسيا،بيروت، لبنان، (2016)، ص 23

2. الجزائر (سلطة الضبط للبريد والمواصلات السلكية واللاسلكية)

3 . تونس (الهيئة الوطنية للاتصالات

4 . البحرين (هيئة تنظيم الاتصالات)

5 . الإمارات العربية المتحدة (هيئة تنظيم الاتصالات)

6 . سوريا (الهيئة الناظمة لقطاع الاتصالات)

المطلب الثاني: أوجه الضعف للأمن السيبراني في الجزائر:

1 . سياسات واستراتيجية تكنولوجيا المعلومات والاتصالات: دفعت القمة العالمية لمجتمع المعلومات عددا من الدول العربية إلى سياسات واستراتيجيات لبناء مجتمع المعلومات وتطويره (2007-2012)، والتي شارك في وضعها لجان وفرق عمل منبثقة عن مجلس الوزراء العرب والمعلومات، بالإضافة إلى الاسكوا ومنظمات إقليمية ودولية:

الدول	سنة إعتماد الاستراتيجية	تسمية الاستراتيجية الأولى	الجهة المسؤولة	تسمية الاستراتيجية 2	الجهة المسؤولة	تسمية أحداث إستراتيجية	الجهة المسؤولة
الأردن	2000	R E A CHريتش	القطاع الخاص لتكنولوجيا المعلومات	الاستراتيجية قطاع الاتصال (2007-2011)	وزارة الاتصالات والتكنولوجية المعلومات	الاستراتيجية الوطنية لقطاع الاتصالات وتكنولوجيا المعلومات (2011-2017)	وزارة الاتصالات وتكنولوجيا المعلومات
الامارات العربية المتحدة	-	تعتمد كل إمارة سياسة خاصة بها	الحكومة في كل إمارة	سياسة قطاع الاتصال(2006-2010)	هيئة تنظيم الاتصالات	السياسة العامة لقطاع الاتصالات (2011-2015)	هيئة تنظيم الاتصالات
البحرين	2001	الخطة الوطنية للاتصالات	الجهاز المركزي للمعلومات	الخطة الوطنية الثانية للاتصالات	الجهاز المركزي للمعلومات	الخطة الوطنية الثانية للاتصالات	هيئة تنظيم الاتصالات
تونس	-	-	-	-	-	استراتيجية قطاع الاتصال التكنولوجي (تونس الرقمية)	وزارة اتعليم العالي والبحث التكنولوجي
الجزائر	-	-	-	-	-	مشروع الجزائر الالكتروني	وزارة البريد والاتصال وتكنولوجيا المعلومات

جدول يوضح الإستراتيجيات الوطنية لتكنولوجيا المعلومات

- **تقييم حجم الخسائر المعلوماتية بالمقارنة بين الجزائر ونظيراتها فرنسا والولايات المتحدة:**

أولا: فرنسا

التقرير الذي نشرته الجمعية الفرنسية لأمن المعلومات عام 1991 تضمن الخسائر وصلت 10,4 مليار فرنك فرنسي 57% منها يرجع إلى أفعال إجرامية، وفي عام 96 انتهى التقرير الصادر عن الجمعية إلى اجمالي الخسائر الناجمة عن المعلوماتية قدر بحوالي 12,72 مليار فرنك فرنسي.

ومن جهة أخرى توصلت الإدارة العامة للشرطة القضائية باعتبارها إحدى الجهات التي يصل إلى علمها الجرائم المختلفة بما فيها الجرائم المعلوماتية إلى أن أكثر من يتعرض لهذا النمط من الاجرام المشروعات التي تتعلق بالمعلومات بنسبة 25% يليها البنوك بنسبة 21 % ثم المشروعات التجارية المختلفة بنسبة 18% وأخيرا الجهات الحكومية سنة 17.%

ثانيا: أمريكا

توضح إحصائيات مكتب التحقيقات الفدرالي أن متوسط الخسارة في الجريمة المعلوماتية الواردة حوالي 500 ألف دولار بينما في جريمة سرقة عادية فمتوسط الخسارة 2500 دولار ، أي متوسط الخسارة في الجريمة المعلوماتية أعلى ب 150 مرة عنه في الجرائم العادية .

كما بينت دراسة أخرى أجريت من قبل منظمة (institute ecurity the conputer) أن خسائر 163 شركة أمريكية من الجرائم المتعلقة بتقنية المعلومات قد بلغت أكثر من 125 مليون دولار سنة 2000، كما ورد في التقرير السنوي الثامن لمكتب التحقيقات الفدرالي الأمريكي الصادر عام 2003 بعنوان جرائم الحاسب بأن أكثر خسائر المؤسسات الولايات المتحدة الأمريكية أتى من الاستيلاء على المعلومات والتي كبدتها خسائر تتعدى 70 مليون دولار أمريكي ويأتي في المركز الثاني نشاط تعطيل نظم المعلومات محققا خسائر تتجاوز 65,5 مليون دولار.[1]

ثالثا: الجزائر

أما في الجزائر فإن المحيط الكمي لإجرام المعلوماتي غير واضح لعدم وجود دراسات وبحوث من شأنها كشف اللثام عن أرقام ومؤشرات للخسائر في بلادنا جراء هذا النمط الاجرامي. وإن كانت الجزائر ليست

[1]– نعيم سعيداني، "**آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**"، رسالة ماجستير، (جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم سياسية، تخصص : علوم جنائية، 2012–2013)، ص 68–69

بمنادى عن خطورة الجرائم المعلوماتية طالما أنها تحتل جزءا من الفضاء الالكتروني خاصة فيما يتعلق بالحاسوب المالية وبعض الهيئات الحكومية التي يعتبر اختراق مواقعها ضمن حجم الأضرار الناتجة عن الجريمة المعلوماتية

كشف دراسة حديثة حول "الأمن السيبراني" أجريت سنة 2017، عبر 1000 مؤسسة وطنية عمومية وخاصة، بأن نصف عدد المؤسسات الجزائرية غير محمي بنظم معلوماتية واقعية من خطر التهديدات السيبراني، حيث أشار السيد "**مهري زكريا** "، رئيس القمة الإفريقية للأمن السيبراني المنظمة بوهران، إلى أن تحقيق مستقلا تم إجراءه بالتعاون مع شركة "**ألجيريا ديجيتال تاندرس**" (Algeria Digital Taandras) للتوجيهات الرقمية والمدعم من طرف مؤسسة "**رابيد7**" (Rapide 7) الرائد العالمي في قطاع إدارة المخاطر، مس مديري وتقنيي المعلومات وكذا مديري أمن المعلومات ومديري الشركات الكبرى والمؤسسات الجزائرية ، حول تطور الهجمات الالكترونية واستخدام التدابير الأمنية، كشف بأن 50% من المؤسسات التي طالما التحقيق، غير مؤمنة في مجال التهديد المعلوماتي الذي يعرف تطورا كبيرا. وكشف التحقيق ن بأن 54% من المؤسسات تعتقد أن الهجمات الالكترونية تؤثر على تطورها، فيما لا تملك 16% من المؤسسات نظم أمن سيبراني، مقابل 12% من المؤسسات لا تعرف النظم الأمنية للمعلومات و17% من المؤسسات لا تفكر في إنشاء النظم الخاصة بالحماية، رغم أهميتها.

كما تبين الدراسة أن 52% من المؤسسات لا تملك سياسة لحماية المنظومات المعلوماتية، ولا موظفين متخصصين ومؤهلين في مجال تقنيات الاعلام والإتصال، مع تأكيد سهولة ولوج نظم التخزين والتوثيق في هذه المؤسسات، حيث تؤكد الدراسة بأن معظم المؤسسات التي شملتها الدراسة يستطيع أي موظف فيها استخدام بطاقات ذكية وقارئ ذاكرة بسهولة ودون استشارة المصلحة المعينة، ما يجعلها عرضة للهجمات عن طريق الفيروسات أو القرصنة، فضلا عن السهولة في ولوج المواقع الالكترونية عبر أجهزة الاعلام الآلي لهذه المؤسسات.[1]

كما أن أماطت نتائج مقاييس الأمن السيبراني لعام 2018 اللثام عن واقع تسيير الشركات الجزائرية، باعتبار أن نسبة 45% من الشركات المستجوبة لا تملك أي استراتيجية لحماية نظامها المعلوماتي، من بينها نسبة 17% عبرت عن نيتها في إرساء هذه الاستراتيجية مستقبلا، فضلا عن إحصاء نسبة 42% من

[1]– رضوان قادة،"**50% من المؤسسات غير مؤمنة الكترونيا**"، جريدة المساء ، العدد 6462، (05 أفريل 2018)، ص6.

الشركات التي اعترفت بعدم إجراء أي خبرة داخلية دورية لحماية نظامها المعلوماتي، ونسبة 33% من الشركات التي تقر بعدم تصنيف وتحديد الوثائق والبيانات ، من بينها 13% تجهل هذا الاجرام أصلا.

فأهم العراقيل التي تعترض الأمن السيبراني تكمن في نقص الكفاءات المؤهلة بنسبة 52% ونقص الموارد المالية بنسبة 35%.[1]

المطلب الثالث: مستقبل الأمن السيبراني في الجزائر

لا يمكن مناقشة مستقبل "الأمن السيبراني" دون النظر في الاتجاهات الناشئة في مجال التكنولوجيا والتهديدات المرتبطة باستخدامها، إذ تقوم المنظمات المختصة بتطوير وإعتماد التكنولوجيات المتصلة بالبيانات الكبيرة والحوسبة الادراكية، مما يجعل الأبعاد السيبرانية تنمو في الحجم والتعقيد بصورة مطردة. ولقد طور المختصين نماذج وطرق حديثة ومناسبة للاستفادة من هذه المعلومات في حملات الدعاية والتسويق الذكي، لكن نظرة المختصين في أمن المعلومات كانت حتى فترة قريبة تركز على تكنولوجيا الأجهزة والابتكارات التي تشكل ترابط عالمنا، حتث تصدر كميات هائلة من البيانات بسرعة مع تزايد عدد الأجهزة المرتبطة بالقضاء السيبراني. ويبقى السباق إلى تأمين هذه الأنظمة والأجهزة من المحتالين والتهديدات الأمنية المحتملة وإساءة استغلالها تحديا قائما ومستمرا. وما يحدث في الوقت نفسه أن مجرمي الانترنت يسعون إلى وضع أيديهم على البيانات لاستغلالها بطرق غير مشروعة، بل سعى بعضهم إلى إبرام اتفاق مع بعض السلطات للتأثير على سلوك الجمهور، بما يمكن أن يعود بعواقب وخيمة على المجتمع، ويعكف العلماء على دراسة التفاعل مع هذا السيل من المعلومات الهائلة باستخدام أجهزة الاستشعار لفهم الكيفية التي يتفاعل بها الدماغ البشري مع المثيرات والعواطف باستخدام نماذج معينة

بينما تمثل البيانات الكبيرة واستخدامها أهداف محتملة للمحتالين، فإن هذه البيانات يمكن أن تساعد المختصين في أمن المعلومات على كشف النشاط الإجرامي الذي يترك دائما وراءه أدلة رقمية، إذ يقوم المحللون المعنيون باستخدام هذه البيانات للتنبؤ بالهجمات وتحديد الهجمات الفاعلة الخبيثة قبل وقوع الضرر بيد أن عملية تحليل الملايين من السجلات قد تستغرق أياما من العمل الحاسوبي، وهنا تأتي الاستفادة من منهجية

[1]– محمد درقي،" **النظام المعلوماتي للشركات الجزائرية غير مؤمن**"، جريدة الخبر، العدد 7638، (04 أفريل 2018)، ص 08

الأمن المعرفي التي ترتكز على مبدأ آلة التعلم، إذ يقوم محترفو تكنولوجيا المعلومات بصياغة نماذج ذكية يمكنها معالجة بيانات التهديد بصورة أكثر كفاءة وفاعلية ودقة للتنبؤ بالنشاط الاجرامي. [1]

وهذه أحدى الطرق التي تحظى باهتمام بالغ من الباحثين في أمن المعلومات والعاملين في المجال المعرفي للحوسبة، وستشكل قريبا إحدى أهم الأدوات لأمن المعلومات في الفضاء السيبراني الحاسوبي، إن مشاهد تهديد امن المعلومات باتت متطورة على نحو متزايد في حين تنفذ العديد من المؤسسات والوكالات الحكومية لوائح لحماية البيانات، مما يتطلب تغييرا جذريا في ثقافة العمل المؤسساتي عندما يتعلق الأمر بأمن المعلومات؛ إذ ينبغي أن يكون المستخدمون لبنة بناء أمن المعلومات بما في ذلك الحرص على عدم نشر معلومات حساسة عن أعمال ونشاطات المؤسسة في مواقع التوصل الإجتماعي، واعتماد الحلول الأمنية الأساسية مثل حماية كلمة السر، واستخدام جدران الحماية وبرامج الحماية من الفيروسات.

وثمة ضرورة للتصدي بشكل استباقي للتهديدات الجيوسياسية التي أدت إلى ظهور هجمات أمنية معلوماتية من نوع جديد ومعقد توجهه بعض الدول أو والأفراد، إذا تتصدى العديد من المؤسسات لذلك من خلال نشر أدوات متخصصة، مثل رصد المعلومات وتحليلها وتبادلها بشكل مباشر، إضافة إلى بناء ثقافة أمنية مقبولة، وكل ذلك بهدف الإسهام في خلق بيئة آمنة في المجتمع والأعمال المختلفة. [2]

كما أن التوجهات العالمية الجديدة تفرض تحقيق حطة التنمية لعام 2030 وأهداف القمة العالمية لمجتمع المعلومات للفترة ما بعد عام 2015(wsis+10) على الدول العربية والتي تعد الجزائر واحد منها عدة التزامات، منها تنفيذ الخطط العالمية التنموية، ومجابهة التحديات التي تحول دون تنفيذها. وذلك من خلال إبداء الإلتزام، السياسي اللازم وتحديث الإستراتيجيات، لاسيما تكنولوجيا المعلومات والإتصالات، بما يتلاءم مع الأهداف التنموية الجديدة ووفقا لأولويات الدول العربية بما فيهم الجزائر. [3]

بالإضافة إلى الجريمة السيبرانية، يجب أن تهتم الجزائر دول الجوار بالإرهاب السيبراني والحرب السيبرانية، ويجب أن تضمن إستراتيجية حقيقية شاملة للأبعاد الثلاثة في استراتيجية "**الدفاع السيبراني**" كما أنه من التحديات المستقبلية ستشمل على نحو متزايد صراعات في الفضاء السيبراني في جميع الأبعاد، وبما أن "**الفضاء**

[1] فواز العنزي،"**أمن المعلومات والقرصنة الإلكترونية، مجلة التقدم العلمي**"، العدد 99، (أكتوبر 2017)، ص 96

[2] – فواز العنزي، مرجع سابق، ص 98

[3] – الاسكوا ، **مرجع السابق**، ص 145

الإلكتروني" هو مسرح جديد للعمليات في القرن الحادي والعشرين، فإن القوات المسلحة الحديثة لا يمكنها ببساطة أن تعمل بفعالية دون وجود شبكة اتصالات ومعلومات مؤثرة بها ومرنة، لذلك من المهم أن تتمتع الدولة الجزائرية بقدرة على التحكم في الفضاء السيبراني ويعد إطلاق الجزائر أول قمر صناعي للإتصالات بالتعاون مع الصين خطوة مهمة نحو تأمين مؤسساتها وتحقيق الأمن السيبراني.[1]

[1]– عنترة بن مرزوق، محي الدين حرشاوي، مرجع سابق، ص 71

خلاصة الفصل الثالث:

وخلاصة القول أن الجزائر خاضت تجربة فريدة من نوعها في ظل التطور التكنولوجي والمعلوماتي، يتمثل في إنشاء مؤسسات أمنية مختصة في مكافحة التهديدات السيبرانية المحدقة بها، حيث تعمل على تطوير تلك المؤسسات لإستكمال إقامة منظومة إتصال آلية على شكل شبكة تربط مختلف وحداتها وهياكلها للاتصال الآلي للمعلومات أفقيا وعموديا مما يسهل عليها التحقق والتحري عن التهديدات والمخاطر السيبرانية التي تواجه أمن الدولة وممتلكاتها وأفرادها. فالأمن السيبراني يحتل مكانة عظيمة في منظومة الأمن الوطني الجزائري.

الـــخـــاتـــمـــة

الخاتمة.

ومن خلال التفصيل المتقدم يستنتج نتيجة مفادها أن التهديدات السيبرانية هي خطر الحاضر والمستقبل، والأخطبوط الذي أنتجه الحضارة التقنية والثورة المعلوماتية التكنولوجية، الذي امتدت أذرعه في جميع أنحاء العالم ، ولم تفلت من قبضته الدول الضعيفة والمتطورة على حد سواء ،واستشرى خطره المدمر على مختلف القطاعات الحياتية الاقتصادية منها والاجتماعية والسياسية ،وحتى الشخصية ،و أن جميع الأفراد في العالم مستهدفون بجميع فئاتهم وأعمارهم ، ومرجعياتهم الفكرية والدينية والثقافية، فأصبح العالم يعيش زمن "الاستعمار السيبراني" بكل أشكاله ومظاهره الذي يستهدف التأثير بشكل مباشر وغير مباشر على شكل سلوكيات الفواعل الدولاتية وغير الدولاتية .

فالأمن السيبراني مفهوم متعدد الأبعاد والمستويات، ومن ثم فهو مفهوم مركب متسع النطاق يبدأ بتحقيق النظام أمن الدولة ثم ممتلكاتهم مجتمعها وأفرادها، ليسع بعد ذلك كافة الدوائر التي يمكن أن تكون مصدرا للتهديد، سواء كانت في البيئة الداخلية أو الخارجية أو متداخلة بين الداخل والخارج، فالتطورات المعاصرة لثورة المعلومات أدت إلى اتساع نطاق مفهوم الأمن السيبراني، بحيث أصبحت المتغيرات الأمنية الالكترونية، متغيرات حاكمة بالنسبة للعديد من البيانات والقرارات بدرجة لم تكن معهودة من قبل.

ومع تصاعد التحول الجزائري نحو بناء مجتمع معلوماتي ، وإنشاء حكومة الكترونية، وتكثيف الاعتماد على أدوات تكنولوجيا المعلومات والاتصالات ، أدركت الأجهزة الأمينة الجزائرية المختصة في مكافحة المخاطر السيبرانية، أنه يتوجب عليها تأمين هذه المعلومات بشدة ، لأن تداولها وإدارتها إلكترونيا عبر شبكات المعلومات والاتصالات، التي ترابطت محليا وإقليميا وعلميا ، جعلها معرضة لخطر الاختراقات المعلوماتية، الأمر الذي يختلف الكثير من الآثار على الأمن على الأمن الوطني الجزائري المعتمد على شبكات المعلومات وأدوات الاتصال لقد كان الهدف من الدراسة معرفة أهم تأثيرات التهديدات السيبرانية على التسيير الاستراتيجي الأجهزة الأمنية المختصة في تلك التهديدات.

نتائج إختبار فرضيات الدراسة.

جاءت نتائج اختيار الفرضيات الدراسة التي تم وضعها في بداية الدراسة على نحو التالي:

إختبار الفرضية الأولى (الرئيسية): يعد التشخيص الاستراتيجي لمتغيرات البيئة الداخلية والخارجية، يمكن للأجهزة من تحديد نقاط القوة ومواطن القصور واقتناص الفرص وتجنب التهديدات السيبرانية إن كفاءة التسيير الاستراتيجي كأسلوب فعال مرتبط بمدى فعالية التشخيص الاستراتيجي لمتغيرات بيئة الأجهزة من حيث :

- تحليل ظروف العمل الداخلية للأجهزة للوقوف على نقاط القوى التي تمتلكها والعمل على تنميتها وتطويرها، ومعرفة نقاط الضعف التي تعاني منها للتقليل من حدتها على الأقل باستعمال نقاط قوتها في ذلك.
- فالتشخيص الخارجي يمكن المؤسسات الأمنية من استقراء المستقبل لمعرفة أهم الثغرات البيئية التي تمكن أن تشكل تهديدات مستقبلية بالنسبة لأهداف المنظمة، وإعداد الحلول والسيناريوهات اللازمة لتجنب هذه الأخيرة.
- إذن التسيير الاستراتيجي يساعد في إيجاد التوازن بين الفرص والتهديدات الخارجية وبين نقاط القوة ومواطن القوة القصوى في الموارد الداخلية للمنطقة ، أي إيجاد الموائمة بين نتائج تقييم البيئة الداخلية والخارجية في الأجهزة الأمنية بهدف تحقيق ميزة الكترونية، وهذا ما يثبت صحة الفرضية الأولى.

إختبار الفرضيات الجزئية:

الفرضية الأولى: تساهم تكنولوجيا المعلومات والاتصالات في تحقيق مزايا في المجال السيبراني للمؤسسات الأمنية الجزائرية في ظل اعتمادها على أسلوب التسيير يعيش المجتمع الجزائري اليوم بما يسمى ، مجتمع المعلومات، فمن يملك المعلومة يملك القدرة على المنافسة في المجال السيبراني ، حيث أصبحت هذه الأخيرة تملك موردا استراتيجيا وأصبحت المعلومة تستعمل في جميع عمليات وأنشطة المؤسسات الأمنية ، لتفعيل التسيير الاستراتيجي الذي يسمح للأجهزة الأمنية بتحديد صورتها المستقبلية وأهدافها الاستراتيجية والقدرة على اتخاذ القرارات على الفعالة بسبب دقة وجودة المعلومات التي توفرها لها تكنولوجيا المعلومات والاتصالات وبالتالي تحسين قدرة المؤسسات الأمنية على التكيف مع متغير بيئتها وتعزيز مركزها . وهو ما يثبت صحة الفرضية أعلاه

الفرضية الثانية: في إطار مواجهة تحديات التهديدات السيبرانية في الجزائر، تجد الأجهزة الأمنية نفسها مجبرة على اختيار البديل الاستراتيجي المناسب.

من خلال الدراسة وتحديدا في الأوار الاستراتيجية للأجهزة الأمنية في مجال الأمن السيبراني، تبين أنها تستعمل خليط من البدائل أو الخيارات الاستراتيجية، ما بين استراتيجية التنويع والتركيز والتمييز محاولة منها الاستفادة من إيجابيات المزج بين القضايا المختلفة في مجال التهديدات السيبرانية في الجزائر، وهذا ما ينفي صحة الفرضية المذكورة أعلاه .

الفرضية الثالثة: تعدد الأدوار الاستراتيجية لتحقيق الأهداف السيبراني من طرف المختصين في مجال مكافحة المخاطر السيبرانية في الجزائر، سمحت بتحقيق عدة نتائج منها:

- تحقيق مزيا أمنية من خلال اتباع استراتيجية فعالة.
- تفعيل التطوير التنظيمي من خلال التغيرات الهيكلية ، التي عرفتها المؤسسات الأمنية، والتعديلات الوظيفية المستحدثة.
- الاستفادة من الذكاء الاستراتيجي في تشخيص متغيرات البيئة الخارجية، ودراسة سلوكيات المجتمع المعلوماتي الجزائري كل هذه النتائج تثبت صحة الفرضية السابقة.
- نتائج الدراسة على ضوء الإشكالات التي أظهرتها الدراسة خلصت في الإجابة على جملة من النتائج: يلعب الأمن السيبراني دورا مهما في حماية الأمن الوطني الجزائري ، فهو قد يهدد أمنها كليا إذما تعرض للانكشاف، الأمر الذي قد يكلف الدولة الكثير من الخسائر الأمنية والاجتماعية والسياسية والاقتصادية وغيرها.
- تمتلك الجزائر فضاء سيراني محدود التطور والحصانة ،وحيث تبدل جهدها في تطوير إمكانياتها في المجال السيبراني والرقمي ، ولا تدخل جهدا أو ما لا في سبيل ذلك، فهي تواصل بناء قواعد ها الرقمية والتكنولوجية والمعلوماتية الهادفة لأحكام سيطرتها على كل يهدد أمنها.
- إن تكثيف نشاط القطاع المعلوماتي ، لا يكفي وحده لضمان دخول دولة الجزائر في طريق النمو إلى حلبة مجتمع المعلومات بنجاح ، فمن الضروري مواكبة التسارع التكنولوجي بتطوير الإنتاجية ، والتي لا يمكن تحقيقها بدون نشاطات منتجة ، وهياكل قاعدية للاتصال ، وأن يتمتع المجتمع بتعليم عال ، وهو شروط يغيب في الجزائر والذي يسير على طريق النمو، حيث نسبية الأمية مرتفعة نسبيا (26%) لمن يفوق سنهم 10 سنوات، ونسبة البطالة (36.6 %) وهذا يؤدي إلى تعطيل النشاط الاقتصادي، ومنه إلى استهلاك الصناعة المعلوماتية.
- ممارسة الأجهزة الأمنية لأسلوب التسيير الاستراتيجي بشكل جدي، أصبح ضرورة ملحة وحتمية، والذي أصبح الطريقة الوحيدة التي تعصف بها رياح التهديد السيبراني من كل جهة.
- توسيع استخدام تطبيقات تكنولوجيا المعلومات في الجزائر، شكل مجتمع معلوماتي، أدى إلى زيادة انتشار المخاطر والتهديدات السيبرانية بكل أنواعها على أمن المجتمع وأمن الدولة.

إقتراحات:

- يجب أن تقوم الأجهزة الأمنية باستمرار تشخيص دقيق وفعال لمتغيرات عمل بيئتها الداخلية لمعرفة ما هي نقاط قوتها وكيف تستفيد منها، وما هي نقاط ضعفها وكيفية معالجتها، وفي نفس الوقت دراسة وتشخيص بيئتها الخارجية للوقوف على الفرص الايجابية التي يمكن أن تعزز بها موقفها الأمني في المجال السيبراني، وكذلك تحضير السيناريوهات اللازمة للرد على المخاطر السيبرانية.
- ضرورة اقامة ندوات ومؤتمرات علمية وتشجيع الأبحاث والدراسات الهادفة إلى تعزيز الجانب التطبيقي للتسيير الاستراتيجي باستعمال تكنولوجيا المعلومات مع محاولة ترجمة نتائجها إلى واقع عملي للاستفادة منها.
- خلق أقسام خاصة للذكاء الاستراتيجي والتحكم في الجودة الشاملة والبحث والتطوير ز إعطائها المزيد من الحرية للابداع والتطوير.

قائمة المصادر والمراجع

قائمة المراجع:

الكتب:

1.أبو عامود، محمد سعد، المفهوم العام للأمن المعلوماتي، (مصر ، جامعة حلوان، 2013)

أوس مجيد غالب العوادي، الأمن المعلوماتي السيبراني، (بيروت، مركز البيان للدراسات والتخطيط، 2016)

2.البداينة ذياب موسى، الأمن الوطني في عصر العولمة، (الرياض، جامعة نايف العربية للعلوم الأمنية،20112

بربر، عزيز ملحم، أمن الشبكات والانترنت، (القاهرة، جامعة نايف العربية للعلوم الأمنية، 2008)3.

4.جبور، منى الأشقر، السيبرانية هاجس العصر، (بيروت، المركز العربي للبحوث القانونية والقضائية، 2013)

5.الحاج، ميلود عامر، الأمن القومي العربي وتحدياته المستقبلية، (المملكة العربية السعودية، مركز الدراسات والبحوث، جامعة نايف للنشر، 2017)

6.الزبيدي، فوزي حسن، منهجية تقييم مخاطر الأمن القومي، دراسة تحليلية لمنهجية تقييم مخاطر الأمن القومي، (دبي، رؤى استراتيجية، 2015)

7.زرواطي، اليمين، التجربة الجزائرية في مكافحة الإرهاب- 1978-2008، (لندن، مطبوعات إيبي، 2014)

الشقحاء، فهد بن محمد، الأمن الوطني: تصور شامل، (الرياض، جامعة نايف العربية للعلوم الأمنية، 2004)

8.عباس، علي مراد، الأمن والأمن القومي، مقاربات نظرية، (بيروت، دار الروافد الثقافية – ناشرون، 2017)

عباس، مصطفى صادق، الإعلام الجديد، دراسة في مداخلة النظرية وخصائصه العامة، (القاهرة، دار العلم، 2012)

9.غيطاس، جمال محمد، الأمن المعلوماتي والجرائم الالكترونية.. أدوات جديدة للصراع، (القاهرة، مركز الجزيرة للدراسات، 2012)

10.المعوش، سالم، مجتمع المعرفة وتعزيز الأمن القومي، المشهد العالمي الجديد، (لبنان، مركز الأبحاث العلمية، 2011)

11.المنيف، أمجد، الإرهاب الالكتروني- معركة حديثة، المجلة العربية العربية، العدد07، (يوليو2015)

12.نوران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني، (القاهرة، المكتب العربي للمعارف، 2014)

13.نيوف، صلاح، مدخل للفكر الاستراتيجي، (الدنمارك، المركز الأكاديمي المفتوح للعلوم السياسية)

المراجع باللغة الإنجليزية:

3.CERT-UK. Common Cyber Attaks Reducing The Impact.the Informatio Cecurity Arm of GCHQ. 2015

2.Timothy Franz.TheCyber Warfare professionnel Realization for Devloping the Next Generation. Summer 2011

3.Josepf S.Nye. the Future of Power. Newyork. 2011

الدوريات والمجلات:

1.شاهد، إلياس، الحاج عرابة، عبد النعيم دفرو، تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر، المجلة الجزائرية للدراسات المحاسبية والمالية، العدد الثالث، (2016)

2.غريب، حكيم، مخاطر مواقع التواصل الاجتماعي على الأمن المجتمعي: الرهانات والاستراتيجيات، ندوة علمية دولية حول: "عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية"، الثلاثاء (11 أفرير 2017)

3.آر كريدين، مادلين، الفضاء والفضاء الالكتروني: التحديات المشتركة، مجلة الفضاء والفضاء الالكتروني التابعة للقيادة الاستراتيجية الامريكية، (يناير 2012)

4.الاسكوا، تقرير الملامح الإقليمية لمجتمع المعلومات في المنطقة العربية، اللجنة الإقتصادية والاجتماعية لغربي آسيا،بيروت، لبنان، (2016)

5.إلياس شاهد، الحاج عرابة، عبد النعيم دفرو، تقييم تجربة تطبيق الحكومة الإلكترونية في الجزائر، المجلة الجزائرية للدراسات المحاسبية والمالية، العدد الثالث، (2016)

6.بارة، سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني (Cyber Security) في الجزائر: الدور والتحديات، جامعة قاصدي مرباح، ورقلة

7.بايوسف، مسعودة، الطفل والانترنت المنزلي، مجالات الاستخدام والاشباعات المحققة، مجلة العلوم الإنسانية والاجتماعية ، العدد 27، (ديسمبر2016)

8.البداينة، ذياب موسى، الجرائم الالكترونية: المفهوم والأسباب، ملتقى علمي حول: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، عمان، المملكة الأردنية الهاشمية، (2014)

9.بكري، سعد علي الحاج، "الأمن السيبراني" ومعضلة حمايته.. عولمة التعليم العالي.. الرقمي، جريدة العرب الإقتصادية الدولية، العدد 25، (24 أوت 2017)

1.بن إرث، شرف الدين، إشاعات وآثارها على الاستقرار الأمني والسياسي للدولة، حقائق من صفحات التواصل الاجتماعي، "صفحات الفيس بوك الجزائرية"، ندوة علمية دولية حول: "عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية"، الثلاثاء (11 أفريل2017)

11.بن بريكة، عبد الوهاب، بن التركي زينب، أثر تكنولوجيا الاعلام والاتصال في دفع عجلة التنمية، مجلة الباحث، العدد07، بسكرة، (جوان 2010)

12.بن حمادي، عبد الرحمان، الفضاء الأزرق أصبح مكانا مثاليا للقيام بأعمال غير مشروعة، معرض الصحافة، تجزئة سعيد بن حداد، الشراقة ، الجزائر (25 ماي 2016)

13.بن سعيد، مراد، صالح زياني، النخب والسلطة والأيدولوجيا في الجزائر: بيمن بناء الدولة والتغيير السياسي، جامعة باتنة الجزائر، قسم العلوم السياسية

14.بن عاتق، حنان، توفيق حجماوي، واقع التطور التكنولوجي وتأثيره على آداء المنظمة في الجزائر، ملتقى دولي حول: الإبداع والتغيير التنظيمي في المنظمات الحديثة، جامعة سعد دحلب، البليدة، كلية العلوم الاقتصادية، وعلوم التسيير، (2013)

15.بن عائشة، محمد الأمين، الدبلوماسية الجزائرية والمعضلة الأمنية في مالي: بين الاستمرار والتغير، ملخص أطروحة دكتوراه في العلوم السياسية والعلاقات دولية، جامعة الجزائر-3-، المجلة العربية للعلوم السياسية

16.بن مرزوق، عنترة، محي الدين حرشاوي، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، كلية الحقوق والعلوم السياسية، المركز الجامعي آفلوا

17.بوعموشة، سهام، الفضاء السبراني يتميز بانفتاح شبكة المعلوماتية وانعدام الحواجز الجغرافية، جريدة الشعب ، العدد 17345،24 ماي (2017)

18.بيبيمون، كلثوم، السياقات الثقافية الموجهة للهوية الرقمية في ضوء تحديات المجتمع الشبكي من التداول الافتراضي إلى الممارسات الواقعية، مجلة "إضافات" العدد 23، (ربيع2016)

19.توريه، حمدون، "الأمن السيبراني" في لبلدان النامية، الاتحاد الدولي للاتصالات، (2006)

20.جبر، دنيا محمد، ابتسام حاتم علوان، الاستراتيجية الشاملة للأمن القومي العراقي بعد عام2003، (رؤية لمبادئ العمل اللازمة وأليات التفعيل)، مجلة الأهرام، (مارس 2007)

21.جبور، منى الأشقر، الأمن السيبراني: التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، (مايو2012)

22.الجريدة الرسمية، القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال وطرق مكافحتها، الفترة التشريعية السادسة، السنة الثالثة، الدورة الرابعة، رقم 122، (27 يونيو 2009)

23.عبد الصبور، سماح، "اصراع السيبراني".. طبيعة المفهوم وملامح الفاعلين، مجلة السياسة الدولية، البنك العربي الافريقي الدولي،(9 أفريل2017)

24.جنة، إسماعيل، حماية منظومتنا الوطنية للمعلومات من خلال تطبيق القانون، مجلة الجيش،العدد 599، (جوان 2013)

25.الجهيني، دعاء، طريق محتمل لمواجهة تهديدات الفضاء الالكتروني؟ اتجاهات الأحداث، العدد 06، (يناير 2015)

26.حسن بن أحمد الشهري، الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس، مركز النور للأبحاث الإلكترونية، (2010)

27.خليفة، إيهاب، إمكانيات تحقيق الردع في الصراعات الفضاء الالكتروني، مجلة تحليلات المستقبل، العدد 13، (أوت 2015)

28.خليفة، إيهاب، نمط جديد لممارسة التأثيرات غير التقليدية في العلاقات الدولية، اتجاهات الأحداث، العدد 06، (يناير 2015)

29.دخان، نور الدين، عيدون الحامدي، مسار تأمين الحدود الجزائرية: بين الإدارة الأحادية والصيغ التعاونية الإقليمية، دفاتر السياسة والقانون، العدد الرابع عشر، (جانفي 2016)

30.درقي، محمد، النظام المعلوماتي للشركات الجزائرية غير مؤمن، جريدة الخبر، العدد 7638، (04 أفريل 2018)

31.ركاش، جهيدة، قسايسية إلياس، التحديات الثقافية والاجتماعية لتنمية السياسية في الجزائر وآليات تفعيلها، جامعة حسيبة بن بوعلي، شلف

32.زياني، صالح، تحولات العقيدة الأمنية الجزائرية في ظل تنامي تهديدات العولمة، جامعة محمد خيضر، بسكرة كلية الحقوق والعلوم السياسية

33.زين عبد الهادي، الحكومة الالكترونية في العالم العربي بين النماذج الناجحة ونماذج تطلع للنجاح، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية،

34.سعداوي، عمر، عقيدة الأمن القومي الجزائري من منظور جيواستراتيجي : قراءة في عملية تيقنتورين، مجلة الرائد المغاربي للدراسات السياسية والبحوث ، العدد الرابع ، (سبتمبر2014)

35.سعود، الطاهر، أدوار الجيش في المراحل الانتقال في الجزائر، سياسات عربية، مركز دبي للأبحاث العلمية (يناير 2017)

36.سويقات، أحمد، دور الجيش الوطني الشعبي من خلال التجربة الدستورية في الجزائر، جامعة قاصدي مرباح، ورقلة

37.صويلح، آمال، الهية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام خطوة هامة نحو مكافحة الارهاب الالكتروني بالجزائر، الملتقى الدولي حول "الاجرام السيبراني"، المفاهيم والتحديدات يومي: 11-12 أفريل 2017، جامعة 8 ماي 1945، قالمة . الجزائر

38.طاجين، فريدة، "سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية: واقع وتحديات"، جامعة قاصدي مرباح، ورقلة، كلية الحقوق والعلوم السياسية

39.طيب، أسامة بن صادق، محمد نور بن ياسين فطاني، عصام بن يحي الفيلالي، الحكومة الالكترونية، نحو مجتمع المعرفة، معهد البحوث والاستشارات، العدد التاسع، جامعة الملك عبد العزيز، جدة، السعودية، (2013)

40.ظريف، شاكر، البعد الأمني الجزائري في منطقة الساحل والصحراء الإرفيقية، التحديات والرهانات، رسالة ماجستير، (جامعة الحاج لخضر- باتنة، كلية العلوم السياسية، 2009-2010)

41.عايد، عبد الجواد بشار ناجح، المسؤولية المجتمعية الني يتبناها جهاز الامن الوطني الفلسطيني وأثرها على الصورة النمطية للسلطة الفلسطينية، رسالة ماجستير، (جامعة النجاح الوطنية، نابلس، فلسطين، كلية الدراسات العليا لتلخطيط والتنمية السياسية، 2017)

42.عباني، مصطفى، التدابير الأخرى في مجال نزع السلاح والأمن الدولي، اللجنة الأولى للدورة الـ 71 الجمعية العامة للأمم المتحدة، بعثة الجزائر الدائمة لدى الأمم المتحدة، نيويورك، (24 أكتوبر2016)

43.عبد الصادق، عادل، أسلحة الفضاء الالكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، سلسلة أوراق، مكتبة الإسكندرية، العدد 23، (يناير2015)

44.عبد الصادق، عادل، الفضاء الالكتروني وتهديدات جديدة للأمن القومي، المركز العربي للأبحاث الالكترونية، (2012)

45.عبد الصادق، عادل، أنماط "الحرب السيبرانية" وتداعياتها على الأمن العالمي، مجلة الاتجاهات النظرية، البنك العربي الافريقي، (14 ماي 2017)

46.عبد الصادق، عادل، خطر الحروب "السيبرانية" عبر الفضاء الالكتروني، مجلة الأهرام لكمبيوتر الانترنت والاتصالات، (مارس2017)

47.عطية، إدريس الطيب، الظاهرة الإرهابية في زمن ما بعد الحداثة، دراسة تحليلية في الأشكال والأساليب والإجراءات المضادة، المجلة العربية للدراسات الأمنية والتدريب، المجلد 31، العدد 63، الرياض، (2015)

48.عطية، أيسر محمد، دور الآليات الحديثة للحد من الجرائم المستحدثة، الإرهاب الالكتروني وطرق مواجهته، الملتقى العلمي، الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، المملكة الأردنية الهاشمية، عمان، الأردن، 2014

49.العنزي، فواز، أمن المعلومات والقرصنة الإلكترونية، مجلة التقدم العلمي، العدد 99، (أكتوبر 2017)

50.عيش، علجية، "الحوت الأزرق" من الجرائم الالكترونية التي يعاقب عليها القانون، جريدة الأحرار، العدد 6063، (25 ديسمبر 2017)

51.غزال، عادل، مشاريع الحكومة الإلكترونية من الاستراتيجية إلى التطليق، مشروع الجزائر: الحكومة الإلكترونية 2013 – أنموذجا-، مجلة المكتبات والمعلومات، العدد34، (مارس 2014)

52.غشير، بوجمعة، تطور خطاب حقوق الانسان في الجزائر والوضع الراهن، معهد السياسات بالجامعة والمواطنة، تقرير بحثي، (2010)

53.غنية توات، القرارالأخير بشأن مصير الامتحان يعود للحكومة، يومية إخبارية وطنية، جريدة الفجر، العدد 4778، 19 (جوان2016)

54.الفتلاوي، أحمد عبيس نعمة، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، (السنة الثامنة، 2016)

55.قادة، رضوان، 50% من المؤسسات غير مؤمنة الكترونيا ،جريدة المساء ، العدد 6462، (05 أفريل 2018)

56.قادير، اسماعيل، إدارة الحروب النفسية في الفضاء الالكتروني: الاستراتيجية الأمريكية الجديدة في الشرق الأوسط، الندوة الدولية: عولمة الاعلام السياسي وتحديات الأمن القومي للدول النامية، جامعة الجزائر -3 -

57.قصعة، خديجة، جمال بن مرزوق، تفعيل آليات الحماية القانونية للحد من انتشار الجريمة الالكترونية في العالم والجزائر، مجلة تاريخ العلوم، العدد السادس، (جانفي 2010)

58.قطب، محمد علي، الجرائم المعلومات وطرق مواجهتها، مركز الاعلام الأمني، الأكاديمية الملكية للشرطة، (2009)

59.قندور، طارق، السعيد قاسمي، تحديات ورهانات استراتيجية ترقية الصادرات الجزائرية خارج المحروقات (مقاربات وصفية تحليلية)، جامعة محمد بوضياف، المسيلة، الجزائر.

60.ليتيم، فتيحة، نادية ليتيم، الأمن المعلوماتي للحكومة الالكترونية وإرهاب القرصنة، مجلة الفكر، العدد الثاني عشر، (سبتمبر 2016)

61.المجذوب، طارق، ساحة "خفية" لحرب "ناعمة" قادمة !، منشورات الدفاع الوطني اللبناني، العدد 89، (تموز 2014)

62.مجيد، نجاة معلا، تعزيز وحماية جميع حقوق الانسان، بما في ذلك الحق في التنمية ، الجمعية العامة، الأمم المتحدة، الدورة الثانية عشر، البند 03 من جدول الأعمال

63.محمد، إبراهيم عبد القادر، التحديات الداخلية والخارجية المؤثرة على الأمن الوطني الأردني في الفترة (1999-2013) دراسة حالة، رسالة ماجستير، (جامعة الشرق الأوسط، الأردن، كلية العلوم السياسية والاقتصاد، قسم العلوم السياسية، 2012-2013)

64.مختار، محمد، هل يمكن أن تتجنب الدول مخاطر الهجمات الالكترونية؟، اتجاهات الأحداث، العدد 06، (يناير2015)

65.مزيود، سليم، الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها، جامعة المدية، الجزائر، (2015)

مصنوعة، أحمد، بركتو نصيرة، الأمن الاقتصادي العربي الواقع والتحديات، مجلة الزيادة لاقتصاديات الأعمال، المجلد 02، العدد03، (2016)

66.مقبل، ريهام، كيف يمكن أن تمارس الدول نفوذها في العلاقات الدولية؟، إتجاهات الأحداث، العدد 06، (يناير 2015)

67.ميهوبي، صالح، جرائم الانترنت تنخر المجتمع الجزائري، جريدة البلاد ، العدد 18،5369 (جويلية2017)

68.ناصر، مراد، التنمية المستدامة وتحدياتها في الجزائر، مجلة التواصل، العدد 26، (جوان 2010)

69.النجار، أحمد السيد، محمد عبد الهادي علام، حروب المعلومات... من يواجهها ؟ مجلة الأهرام، العدد 139، (13يوليو2015)

67.نورين، بومدين، زيدان محمد، دور السوق المالي في تمويل التنمية الاقتصادية بالجزائر"معوقات وآفاق"، الملتقى الدولي حول سياسات التمويل وآثارها على الاقتصاديات والمؤسسات، دراسة حالة الجزائر والدول النامية، يومي 22/21 نوفمبر ، (2006)

68.يحي، سارة، بعد غير تقليدي في العلاقات غير الرسمية بين الدول، اتجاهات الأحداث، العدد 06، (يناير 2015)

المذكرات:

1.روابحي، خيرة، ثقافة الأنترنت: دراسة ميدانية لاستعلامات الشبكة بمدينة تيهيرت، رسالة ماجستير، (جامعة وهران، كلية العلوم الإنسانية والحضارة الإسلامية، قسم علم المكتبات والعلوم الوثائقية، 2009-2010)

2.الأبرش، محمود، السياسة البيئية في الجزائر في ظل الاتجاهات البيئية العالمية، أطروحة دكتوراه، (جامعة محمد خيضر، بسكرة، كلية العلوم الإنسانية والاجتماعية، تخصص: علم اجتماع البيئة، 2016-2017)

3.أبو تمور، إنعام عبد الكريم، مفهوم الأمن الإنساني في حقل نظريات العلاقات الدولية، مقاربة معرفية، رسالة ماجستير في العلوم السياسية، (جامعة الأزهر، غزة، فلسطين، كلية الإقتصاد والعلوم الإدارية، 2013)

4.آكلي، نعيمة، استراتيجيات التنمية في الجزائر، أطروحة دكتوراه، (جامعة مولود معمري، تيزي وزو، الجزائر، كلية العلوم السياسية، 2010)

5.باسط، سميرة، الاستراتيجية الجزائرية لمكافحة الإرهاب 1999-2014، رسالة ماجستير، (جامعة الجزائر-3-، كلية العلوم السياسية والعلاقات الدولية، تخصص: دارسات استراتيجية وأمنية، 2013-2014)

6.بتقة، خديجة، السياسة الأمنية الأوروبية في مواجهة الهجرة غير الشرعية، رسالة ماجيستير، (جامعة محمد خيضر، بسكرة، كلية العلوم السياسية والعلاقات الدولية، تخصص: علاقات دولية استراتيجية، 2013-2014)

7.براهمي، حنان، جريمة تزوير الوثيقة الرسمية الإدارية، ذات الطبيعة المعلوماتية، أطروحة دكتوراه علوم، (جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، تخصص قانون جنائي، 2015)

8.براهيم، أحمد، الدولة العالمية والنظام الدولي الجديد، أطروحة دكتوراه، (جامعة السانيا، وهران ، كلية العلوم الاجتماعية، 2009-2010)

9.برنيس، نعيمة، الوظيفة الإعلامية لشبكة الأنترنت في عصر ثورة المعلومات، رسالة ماجستير، (جامعة منتوري قسنطينة، كلية العلوم الإنسانية والإجتماعية، فرع: صحافة مكتوبة وسمعية بصري، 2009-2010)

10.بن عبد الرزاق، حنان، تأثير المأزق الأمني الاثني على الاستقرار الداخلي لدولة. دراسة للنموذج الاسباني، أطروحة دكتوراه، (جامعة محمد خيضر، بسكرة، كلية العلوم السياسية، تخصص: علاقات دولية ودراسات استراتيجية، 2016-2017)

11.بوجليطة، احميدي، سياسات مكافحة لإرهاب في الوطن العربي، دراسة مقارنة بين الجزائر ومصر، رسالة ماجستير، (جامعة دالي براهيم -2-، كلية العلوم السياسية، تخصص: دبلوماسية وتعاون دولي، 2009-2010)

12.بوحادة، سارة، أثر الإرهاب الالكتروني على أمن واستقرار الدول، أطروحة دكتوراه، (جامعة الجزائر-3- ، المدرسة الوطنية العليا للعلوم السياسية، تخصص: دراسات دولية، 2014)

13.بودن، زكرياء، أثر التهديدات الإرهابية في شمال مالي على الأمن الوطني الجزائري واستراتيجيات مواجهتها 2010-2014، رسالة ماجستير، كلية العلوم السياسة والعلاقات الدولية، تخصص: علاقات دولية ودراسات استراتيجية، 2014-2015)

14.بوسبعين، تسعديت، آثار التغيرات المناخية على التنمية المستدامة في الجزائ- دراسة إستشرافية-، أطروحة الدكتوراه، (جامعة امحمد بوقرة، بومرداس، كلية العلوم السياسية، تخصص: تسيير منظمات، 2014-2015)

15بوسكين، سليم، تحولات البيئة الإقليمية وانعكاساتها على الامن الوطني الجزائري 2010-2011، رسالة ماجستير، (جامعة محمد خيضر- بسكرة الجزائر كلية العلوم السياسية والعلاقات الدولية، تخصص: علاقات دولية واستراتيجية، 2014-2015)

16.بوضياف، محمد، مستقبل النظام السياسي الجزائري، أطروحة دكتوراه، (جامعة الجزائر، العلوم السياسية والعلاقات الدولية، 2007-2008)

17.تباني، وهيبة، الأمن المتوسطي في استراتيجية الحلف الأطلسي، دراسة حالة: ظاهرة الإرهاب، رسالة ماجستير، (جامعة مولود معمري، تيزي وزو، الجزائر، كلية الحقوق والعلوم السياسية، تخصص: دراسات متوسطية ومغاربية، 2014)

18.حفصي، عباس، جرائم التزوير الالكتروني، دراسة مقارنة، أطروحة دكتوراه، (جامعة وهران -1-، أحمد بن بلة، كلية العلوم الإسلامية، تخصص شريعة وقانون، 2015)

19.حمزة، حسام، الدوائر الجيوسياسية للأمن القومي الجزائر، رسالة ماجستير، (جامعة الحاج لخضر- باتنة كلية الحقوق والعلوم السياسية، تخصص: علاقات دولية، 2010-2011)

20.خلوط، زهوة، التسويق الإبتكاري وأثره على بناء ولاء الزبائن، دراسة حالة: مؤسسة اتصالات الجزائر، رسالة ماجيستير، (جامعة امحمد بوقرة، بومرداس، كلية العلوم الإقتصادية تجارة وعلوم التسيير، 2013-2014)

21.سايح، بوزيد، دور الحكم الراشد في تحقيق التنمية المستدامة بالدول العربية حالة الجزائر، أطروحة دكتوراه، (جامعة بلقايد، آبي بكر، تلمسان، كلية العلوم السياسية والعلوم الاقتصادية، 2011)

22.سعيدي، ياسين، التحدبات الأمنية الجديدة في المغرب العربي، رسالة ماجستير، (جامعة وهران -2- ، كلية العلوم السياسية والعلاقات الدولية،2016،2015)

23.صراع، كريمة، واقع وآفاق التجارة الإلكترونية في الجزائر، رسالة ماجستير، (جامعة وهران، كلية العلوم الإقتصادية وعلوم التسيير، تخصص: إستراتيجية، 2013-2014)

24.صغير، يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجيستير، (جامعة مولود معمري، تيزي وزو، كلية الحقوق، تخصص: قانون دولي للأعمال، 2014)

25.طبوش، سفيان، الشراكة الأورو متوسطية في ظل التحديات الأمنية الراهنة، أطروحة دكتوراه، (جامعة حسيبة بن بوعلي، الشلف، كلية العلوم السياسية، تخصص: دراسات أورو متوسطية،2016-2017)

26.طويل، نسيمة، الاستراتيجية الأمنية الأمريكية في منطقة شمال شرق آسيا: دراسة لمرحلة ما بعد الحرب الباردة، أطروحة دكتوراه علوم، (جامعة الحاج لخضر، باتنة كلية العلوم السياسية: تخصص علاقات دولية، 2009-2010)

27.عبان، عبد القادر، تحديات الإدارة الإلكترونية في الجزائر، دراسة سوسيولوجية ببلدية الكاليتوس العاصمة، أطروحة دكتوراه (ل م د)، (جامعة محمد خيضر – بسكرة، كلية العلوم الإنسانية والاجتماعية، 2015 تخصص: إدارة وعمل 2016)

28.عبد ربه، آمنة بن، النظام الإقتصادي الجديد المبني على المعرفة وتطور مجتمع المعلومات والتكنولوجيا الحديثة للإتصال، الحلول المقترحة لإرساء مجتمع معلومات ناجح ومتكامل في الجزائر، رسالة ماجستير، (جامعة الجزائر كلية العلوم السياسية والإعلام، قسم علوم الإعلام والإتصال، 2005-2006)

29.عطية، إدريس، الإرهاب في إفريقيا: دراسة في الظاهرة وآليات مواجهتها، رسالة ماجيستير، (جامعة الجزائر-3-، كلية الحقوق والعلوم السياسية، والعلاقات الدولية، تخصص: دراسات إفريقية، 2011)

30.علوي، هند، المرصد الوطني لمجتمع المعلومات بالجزائ، قياس النفاذ إلى تكنولوجيا المعلومات والاتصالات بقطاع التعليم بالشرق الجزائري، أطروحة دكتوراه، (جامعة منتوري–قسنطينة، كلية العلوم الانسانية، تخصص: علم المكتبات 2007-2008)

31.غنام، فايزة، (التعاون)؟ الأمني الأورو-مغاربي: دراسة حالة حوار 5+5 (2001-2011)، رسالة ماجستير، (جامعة مولود معمري، تيزي وزو، الجزائر، كلية العلوم السياسية، 2011-2012)

32.فريمش، مليكة، دور الدولة في التنمية: دراسة حالة الجزائر، بحيث مقدم لنيل شهادة دكتوراه علوم السياسية والعلاقات الدولية، تخصص تنظيمات سياسية وإدارية، 2012

34.قط، سمير، البعد الافريقي في سياسة الأمن والدفاع الوطني الجزائري، أطروحة دكتوراه في العلوم السياسية، (جامعة محمد خيضر، بسكرة، تخصص: علاقات دولية واستراتيجية، 2016-2017)

35.قنوفي، وسيلة، حق الانسان في الأمن: بين مقاربة الأمن الإنساني ومبادئ القانون الدولي، أطروحة دكتوراه، (جامعة محمد لمين دباغين، سطيف-2-، كلية الحقوق والعلوم السياسية، 2016-2017)

36.كريم، مراد، مجتمع المعلومات أثره في المكتبات الجامعية، مدينة قسنطينة-أنموذجا-، أطروحة دكتوراه، (جامعة منتوري–قسنطينة، كلية العلوم الإنسانية والاجتماعية، قسم علم المكتبات، 2007-2008)

37.لخضاري، منصور، تطور"ظاهرة الإرهاب "في الجزائر من الصعيد الوطني إلى الصعيد غير الوطني ن مركز الامارات لدراسات والبحوث الاستراتيجية، أبو ظبي، العدد 194، (مايو 2014)

38.لونيس، باديس، جمهور الطلبة الجزائريين والأنترنت، دراسة في إستخدامات إشباعات طلبة جامعة منتوري قسنطينة، رسالة ماجستير، (جامعة منتوري- قسنطينة، كلية العلوم الإنسانية والعلوم الإجتماعية، قسم علوم الإعلام والاتصال 2007-2008)

39.مدوني، علي، قصور متطلبات بناء الدولة في إفريقيا وانعكاساتها على الأمن والاستقرار فيها، أطروحة دكتوراه، (جامعة محمد خيضر، بسكرة، كلية العلوم السياسية والعلاقات الدولية، 2013 -2014)

مريبعي، سوسن، التنمية البشرية في الجزائر – واقع وآفاق .، رسالة ماجستير، (جامعة منتوري -02- ، كلية علوم سياسية وعلوم التسيير، 2012-2013)

40.مريم، أحمد مسعود، آليات مكافحة جرائم تكنولوجيا الاعلام والاتصال في ضوء القانون رقم 04/09 ، رسالة ماجستير، (جامعة قاصدي مرباح- ورقلة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013)

41.نصر، بوعلام، دور الجزائر الإقليمي في ظل تنامي التهديدات في منطقة الساحل (2006-2014)، مذكرة رسالة ماجستير، (جامعة ملود معمري تيزي وزو، الجزائر، كلية العلوم السياسية،تخصص في: دراسات متوسطية ومغاربية، 2015-2016)

42.نعيم، سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري ، رسالة ماجستير، (جامعة الحاج لخضر، باتنة، كلية الحقوق والعلوم سياسية، تخصص : علوم جنائية، 2012-2013)

المواقع الإلكترونية:

1.الإذاعة الجزائرية، فتح تحقيق قضائي في "انتحار" بعض الأطفال بسبب لعبة الحوت الأزرق،01 أفريل www.Radioalgerie.dg 10:00/2018

2.آسر، تولاي، ما هي السيبرانية؟ وما دورها في صناعة القرار؟ 20 جانفي 17:53/2018، http//Zeitgeistarrabia.com

3.باشوش، نوارة، الجيش يدخل الحرب "الفضاء الالكتروني" في: 07 مارس www.ehoroukonline.com،20:17/2018

4.بن عائشة، محمد الأمين، مفهوم الأمن الوطني الجزائري، في: 03 فيفري 21:33/2018 www.maqualaty.com

5.البنا، نانسي، الأمن السيبراني.. بيئة تكنولوجية أكثر أمنا، 20 جانفي 21:14/2018
http//boutiqueceena.eg
6.بيطار، ليال، ماذا يعني الأمن السيبراني؟ 20 جانفي 2018 ، الوقيت 17:58،
http//anbaaoline.com
7.جهاد، أماني، تصنيف الدول الغربية والعربية في مجال الأمن السيبراني لسنة 2017، في: 02 أفريل
WWW.3ARABINSIDEE.COM 11:18/2018
8.خليفة، إيهاب، القوة الالكترونية والصراع الدولي، المركز العربي لأبحاث الفضاء الالكتروني، 20 جانفي
http//alaeabycyberspace.com 20:32:/2018
9.سحواذ، نسيمة، الطموح لتوسيع دائرة الاعتماد المتبادل بإدراج طرق تحليلية لفائدة مخابر أخرى، في: 02
مارس 13:63/2018 http//Dikanews.com
10.سعيدي، عبد القادر، المصلحة المركزية الالكترونية في مواجهة مجرمي العالم الافتراضي، في: 03
www.essalamonline.com مارس17:42/2018
11.غاي، أحمد، تكييف الشرطة القضائية مع متطلبات إصلاح العدالة، تقييم وآفاق، في: 03 مارس
www.mjustice.dg 14:13/2018
12.قوي، بوحنيه، استراتيجية الجزائر تجاه التطورات الأمنية في الساحل الافريقي، مركز الجزيرة للدراسات في:
27 فيفري Studies.aljageera.net 22:17/2018
13.لحياني، عثمان، السلطات الجزائرة: تحجب "الحوت الأزرق" مستحيل ... وهذا بديلها،في: 01 أفريل
www.altahrironlen.com 10:22/2018
14.مقراني، سليمة، الجيش الوطني الشعبي : ملتقى حول "الدفاع السيبراني، مكون أساسي للأمن والدفاع
الوطني". في: 07 مارس 17:51/2018،hltps :www.eljoumhouria.dg
15.مناد، راضية، تطوير قدرات الشرطة في مواجهة الجريمة الالكترونية ، أمن واستراتيجية، 03 مارس
www.dgayerinfo.com .21:19/2018

قائمة المحتويات

الفهرس

ملخص: .....

جدول لأهم المصطلحات: .....

جدول المختصرات: .....

مقدمة .....أ

الإطار المنهجي والمفاهيمي والنظري

أولا : مشكلة الدراسة: .....ج

الإشكالية الرئيسية: .....ج

الإشكاليات الجزئية: .....ج

ثانيا: مجالات الدراسة: .....ج

ثالثا: أهمية الدراسة: .....ج

رابعا : فرضيات الدراسة ..... د

خامسا: مناهج وإقترابات الدراسة: ..... د

سادسا: تحديد مصطلحات الدراسة: ..... و

سابعا: المدخل النظري للدراسة: ..... ز

ثامنا: أدبيات الدراسة: .....ح

تاسعا: هيكل الدراسة: ..... ط

الفصل الأوّل: البناء الإيتومولوجي للأمن السيبيراني.

تمهيد الفصل الأول: 1

المطلب الأول: مفهوم الأمن السيبراني 2

المطلب الثاني: أبعاد الأمن السيبراني.....3

أولا: الأبعاد العسكرية:.....3

ثانيا: الأبعاد الاقتصادية: 4

ثالثا: الأبعاد الإجتماعية:.....4

رابعا: الأبعاد السياسية: 5

خامسا: الأبعاد القانونية:.....5

المطلب الثالث: الفواعل الأساسية في الفضاء السيبراني 6

أولا: الدولة: 6

ثانيا: الفواعل من غير الدول: 6

ثالثا: الفرد: 7
رابعا: المجموعات الإفتراضية (Virtual Community): 8
المبحثت الثاني: التهديدات الأمنية السيبرانية. 9
المطلب الأول: مفهوم التهديد السيبراني. 9
جدول يوضح: طرق استخدام التهديدات السبرانية وكيفية التعامل معها 10
المطلب الثاني: أنماط التهديدات السيبرانية 11
أولا: خطر الكوارث الطبيعية أو (العرضية للكابلات البحرية): 11
ثانيا: التجسس الإلكتروني: (Cyber Espionage): 11
ثالثا: الجريمة السيبرانية: (Cyber Crime): 12
خامسا: الحروب السيبرانية: (Cyber Warfare): 15
المطلب الثالث: تأثير التهديد السيبراني على الأمن القومي 15
المبحث الثالث: آليات إستخدام القوة السيبرية. 18
المطلب الأول: مفهوم القوة السيبرانية 18
المطلب الثاني: التحول في إستخدام القوة السيبرانية 19
أولا: القوة السيبرانية والقوة الصلبة: 19
ثانيا: القوة السيبرانية والقوة الناعمة: 20
ثالثا: القوة السيبرانية والصراع الدولي: 20
رابعا: القوة السيبرانية والردع السيبراني: 21
المطلب الثالث: القوة السيبرانية في الشؤون الدولية 21
أولا: الدبلوماسية السيبرانية (Cyber Deplomatcy): 21
ثانيا: الإستخبارات السيبرية (Cyber Intelligence): 22
ثالثا: التحالف السيبري (Cyber Allies): 22
رابعا: الإعلام السيبراني (Cyber Informating): 23
خلاصة الفصل الأول: 24

الفصل الثاني: الإدراكات الجزائرية الأمنية.

تمهيد الفصل الأول: 25
المبحث الأول: التصور الجزائري للأمن 26
المطلب الأول: تحولات في مفهوم الأمن 26
أولا: مفهوم الأمن 26

ثانيا: أسباب تحول مفهوم الأمن..... 27
ثالثا: التحول في الوسائل والأدوات. 28
رابعا: التحول في مصادر التهديد: 28
المطلب الثاني: الأمن الوطني الجزائري..... 29
أولا: مفهوم الأمن القومي: (Nationalist Security). 29
ثالثا: الأمن الوطني الجزائري. 30
المطلب الثالث: علاقة التنمية بالأمن الوطني الجزائري. 31
المبحث الثاني: العقيدة الأمنية الجزائرية 33
المطلب الأول: عقيدة الأمن الوطني الجزائري 33
أولا: مفهوم العقيدة الأمنية: 33
ثانيا: عقيدة الأمن الجزائري: 34
المطلب الثاني: مرتكزات عقيدة الأمن الوطني الجزائرية 34
أولا: العامل التاريخي: 34
ثانيا: العامل الجغرافي: 34
ثالثا: العامل الأيديولوجي:..... 35
المطلب الثالث: مراحل تطوير العقيدة الأمنية الجزائرية. 35
المبحث الثالث: التحديات الأمنية الجزائرية. 39
المطلب الأول: التحديات السياسية والأمنية. 39
أولا: التحديات الداخلية. 39
ثانيا: التحديات الخارجية: 40
المطلب الثالث: التحديات الإقتصادية والإجتماعية..... 41
أولا التحديات الإقتصادية: 41
ثانيا: التحديات الإجتماعية. 43
المطلب الثالث: التحديات البيئية والتكنولوجية 44
أولا: التحديات البيئية..... 44
ثانيا: التحديات التكنولوجية. 45
خلاصة الفصل الثاني: 47
الفصل الثالث: اليقظة الإستراتيجية الجزائرية لإرساء الأمن السيبيراني
تمهيد الفصل الثالث:..... 48

المبحث الأول: إستخدامات الأنترنت في الجزائر. 49
المطلب الأول: تطوير الأنترنت في الجزائر. 49
المطلب الثاني: ظهور مجتمع المعلومات في الجزائر: 50
ثانيا: إصلاح قطاع الاتصالات: 51
ثالثا: إتصالات الجزائر: 51
المطلب الثالث: مشروع الجزائر الإلكتروني 2013. 52
المبحث الثاني: دور المؤسسات الأمنية في تحقيق الأمن السيبراني 54
المطلب الأول: الأجهزة العملياتية المختصة في الأمن السيبراني 54
أولا: على المستوى الوطني 54
3: المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني: 55
4: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها. 56
ثانيا: على المستوى الدولي: 57
المطلب الثاني : الإستراتيجيات الأمنية لمكافحة التهديدات السيبرانية 58
أولا: اليقضة الإسراتيجية التابعة لمركز الوقاية 58
ثانيا: الندوة الدولية حول الأمن السيبراني في الجزائر 59
ثالثا: إستراتيجية حفظ النظام والأمن العموميين 60
رابعا: إستراتيجية إنشاء تشريعات جديدة متعلقة بالتهديدات السيبرانية: 60
خامسا: إستراتيجية التعاون الدولي للوقاية من الجرائم السيبرانية: 61
سادسا: إستراتيجيات الدفاع السيبراني ومراقبة الأنظمة: 61
سابعا: إستراتيجيات المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني 63
المطلب الثالث: نماذج تطبيقة عن أهم المخاطر السيبرانية في الجزائر 63
أولا: خطر الإرهاب السيبراني على الأمن الوطني الجزائري : 64
ثانيا: مخاطر الألعاب الإلكترونية على أطفال الجزائر 65
ثالثا: مخاطر مواقع التواصل الاجتماعي الهدامة: 66
رابعا: تسريبات بكالوريا 2016 67
خامسا: لعبة الحوت الأزرق المميتة: 67
المبحث الثالث: رؤية إستشرافية للأمن السيبراني. 69
المطلب الأول: أوجه القوة السيبرانية في الجزائر. 69
المطلب الثاني: أوجه الضعف للأمن السيبراني في الجزائر: 72

خلاصة الفصل الثالث: 78
الخاتمة. 79
قائمة المصادر والمراجع..... 83
قائمة المحتويات 97