دور جهاز الدفاع الوطني في تحقيق الأمن المعلوماتي في ظل تنامي الإجرام السيبراني

The role of the National Defense Agency in achieving information security in light of the growing cybercrime

إعداد

د. عائشة عبد الحميد

جامعة باجي مختارعنابة

Doi: 10.21608/jinfo.2020.114721

استلام البحث : ٥ / ٧ / ٢٠٢٠ قبول النشر: ٢٠ / ٨ / ٢٠٢٠

المستخلص:

بالرغم من الإيجابيات التي حملها الإنترنت ، إلا أنها حملت معها العديد من التهديدات و المخاطر التي ترجمت في شكل جرائم إلكترونية ، ناهيك عن التهديدات التي تطال أمن و استقرار الدول، إذ لا ينكر أحد الدور المتعاظم لشبكة الانترنت في الثورات العربية . وتشير الإحصائيات المسجلة في الجزائر أن الجريمة الإلكترونية أخذت منحا تصاعديا في الآونة الأخيرة ، و هو ما ينبأ بخطورة الوضع ، لاسيما في ظل توجه الجزائر نحو تبني مقاربة الحكومة الإلكترونية ، و من هذا المنطلق فإن السلطات الجزائرية ملزمة باتخاذ الاحتياطات الأمنية اللازمة لتفادي أي نوع من الجرائم الإلكترونية . و من المعلوم أن الدفاع الوطني منذ الاستقلال تولى مسؤولية الدفاع عن الوطن في جميع الميادين ، و توفير الأمن بمعناه الواسع ، الأمر الذي فرض عليه التعامل مع المتغيرات الحديثة و التكيف معها ، بغية تحقيق هدفه الأسمى. فقد قررت القيادة العليا للجيش ، استحداث مصلحة " الدفاع السيبرياني و مراقبة أمن الأنظمة " على مستوى دائرة الاستعمال و التحضير لأركان الجيش بهدف تأمين و حماية المنظومات و المنشآت الحيوية للبلاد ضد التهديدات و الإرهاب الإلكتروني و الجوسسة على أسرار الدولة الجزائرية.

الكلمة المفتاحية : الإجرام السيبرياني ، الدفاع الوطني ، الأمن المعلوماتي ، الجيش الوطني الشعبي).

Abstract :

Despite the positives that the Internet carried, it carried with it many threats and risks that were translated into the form of electronic crimes, not to mention the threats that affect the security and stability

of countries, as no one denies the growing role of the Internet in the Arab revolutions.Statistics recorded in Algeria indicate that cybercrime has taken an upward grant recently, which predicts the seriousness of the situation, especially in light of Algeria's move towards adopting an e-government approach, and from this point of view, the Algerian authorities are obliged to take the necessary security precautions to avoid any kind of Cybercrime.It is well known that since independence, the national defense has assumed the responsibility of defending the homeland in all fields, and providing security in its broadest sense, which forced him to deal with modern changes and adapt to them, in order to achieve his ultimate goal.
The Supreme Command of the army decided to introduce the interest of `` cyber defense and monitoring systems security " at the level of the department of use and preparing the staffs of the army with the aim of securing and protecting the country's vital systems and installations against threats, cyber terrorism and spying on the secrets of the Algerian state.
Key words: Cybercrime, National Defense, Information Security, National People's Army.

مقدمة :

إن التطـــور المتسارع الذي تشهده الجزائر في مجال التكنولوجيات الجديدة للإعلام و الاتصال و الاستخدام المتنامـــي للتطبيقات المتصلـــــة بالانترنت و الوسائط الإلكترونيـــــة و الرقمية الجديدة لحفظ الملفات و الصور و غيرها ، يستدعي إرساء قاعدة قانونية و توفير الأجهزة و الهياكل الضرورية لمكافحة الجريمة السيبريانية العابرة للأوطان.

حيث تواجه البشرية تهديدات رقمية جديدة أكثر تعقيدا و أشد فتكا و ضررا ، تتسبب في إتلاف منظومات شبكات الكمبيوتر لمؤسسات كبيرة و حساسة داخل الدول التي لا زالت غير آمنة ، بالإضافة إلى وجود هجمات إلكترونية موجهة و معقدة ، حيث ينتج تعقيد هذه الهجمات الإلكترونية من كون أنه قد لا يبرز أثرها على الفور ، فأغلبية ضحايا هذه الهجمات يجهلون بادئ الأمر تعرضهم للقرصنة و لا يكتشفوا ذلك إلا بعد مرور الوقت.

و حسب آخر الإحصائيات ، فإن ٤٠ % فقط من الدول الإفريقية هي التي تملك اليوم إطارا قانونيا يعاقب الأعمال المتعلقة بالجرائم السيبريانية ، و حتى و إن وجدت هذه

القوانين الساعية لتطوير مجال الأمن السيبرياني إلا أنها لا تواكب الوتيرة المتسارعة للابتكارات المتجددة في مجال التكنولوجيا الرقمية.

و تعد الجزائر من الدول التي تحارب الإجرام السيبراني حفاظا على مراسلاتها الإلكترونية و أمنها المعلوماتي. مع مرور الزمن و تسارع التطور التكنولوجي ، غلبت ثقافة العولمة في أرجاء المعمورة فتحول العالم إلى قرية صغيرة و أصبح تبادل المعلومات و الأفكار متاح بضغطة زر. و عليه : ما هو مفهوم الإجرام السيبراني ؟ و ما هو دور مرفق الدفاع الوطني في التصدي لهذا النوع و تحقيقي الأمن المعلوماتي.

من خلال هذه الإشكالية سنقسم هذه المداخلة إلى العناصر التالية :

أولا : الإطار المفاهيمي للإجرام السيبراني في نظر التشريع الجزائري .

ثانيا : سياسة جهاز الدفاع الوطني في تحقيق الأمن المعلوماتي.

أولا : الإطار المفاهيمي للإجرام السيبراني في نظر التشريع الجزائري :

١- **تعريف الجريمة السيبرانية (الإلكترونية):**

تعتبر الجريمة المعلوماتية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية ، لتطورها التي ارتبطت بتقنية المعلومات ، فقد اصطلح على تسميتها بداية بـ " إساءة استخدام الكمبيوتر" ثم " احتيال الكمبيوتر " ، "فالجريمة المعلوماتية" بعدها "جرائم الكمبيوتر" ، جرائم التقنية العالية إلى "جرائم الهاركز" " فجرائم الانترنت" و أخيرا " السيبركرايم" (مليكة عطوي ، ٢٠١٧ ، ص ٠٨).

و قد وصفت هذه الجريمة بأنها مقاومة للتعريف، لكثرة ما تناولته الكتابات عنها شرحا و توضيحا، فمنهم من نظر إليها من خلال وسيلة ارتكابها، و منهم من خلال موضوعها، و منهم من خلال توافر المعرفة بتقنية المعلومات.

حيث يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها " الجريمة التي تلعب فيها البيانات الحاسوبية، و البرامج المعلوماتية دورا رئيسيا (محمد عبيد الكعبي ، د ، ت ، ش ، ص ٣٣) أو كل " فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه ، أو كسب يحققه الفاعل (نهلة عبد القادر المومني د،ت،ن، ص ٤٩) . و قد اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمـــــة التعاون الاقتصادي و التنمية (OCDE) للجريمة المعلوماتية في اجتماع باريس عام ١٩٨٣ بأنه :

" كل سلوك غير مشروع أو غير أخلاقي ، أو غير مصرح به يتعلق بالمعالجة الآتية للبيانات أو نقلها " (سميرة معاشي ، ٢٠١٠ ، ص ٢٧٨).

أ- **مراحل تطور الجريمة السيبرانية:**

مرت الجريمة السيبرانية بتطور تاريخي، بدأ من اختراع الحاسوب و إنشاء الشبكة العنكبوتية، وصولا إلى الثورة العالمية في الاتصالات و التكنولوجيا، و بحكم هذا التطور تطورت هذه الجريمة بشكل عام و خاص، و يمكن ملاحظة ثلاث مراحل لتطورها:

Doi: 10.21608/jinfo.2020.114721

- ✓ **مرحلة شيوع استخدام الكمبيوتر في الستينات ثم السبعينات :** بظهور استخدام الكمبيوتر و ربطه بالشبكات في الستينات إلى السبعينات ظهرت أول معالجة لنظام الكمبيوتر و تدمير أنظمة الكمبيوتر فبقيت محصورة في البداية في إطار السلوك الغير أخلاقي دون النطاق القانوني، و مع توسع الدراسات تدريجيا و خلال السبعينات بدأ الحديث عنها كظاهرة إجرامية جديدة (يونس عرب ، ٢٠٠٢ ، ص ٠٨).
- ✓ **مرحلة الثمانينات :** في هذه المرحلة ، ظهر نوع جديد من الجرائم ارتبط بعمليات اقتحام نظام الحاسوب عن بعد، و نشر الفيروسات عبر شبكات الكمبيوتر أين شاع إصطلاح "الهاركز" و كانوا مرتكبوها من العباقرة صغار السن لإظهار التفوق التقني ، و بعد ذلك تحولت الجريمة من مجرد مغامرة إلى أفعال تستهدف التحسس و الاستيلاء على البيانات الاقتصادية و الاجتماعية و السياسية و العسكرية. (عبد الفتاح مراد، د،ت،ن، ص ٤٣).
- ✓ **مرحلة التسعينات :** شهدت هذه المرحلة تناميا هائلا ، في حقل الجرائم التقنية و تغييرا في نطاقها و مفهومها ، فظهرت أنماط جديدة كأنشطة إنكار الخدمة، كما نشطت جرائم نشر الفيروسات عبر مواقع الانترنت، كما ظهرت أنشطة الرسائل و المواد الكتابية المنشورة على الانترنت، أو المراسلة عبر البريد الإلكتروني المنطوية على إثره الأحقاد أو المساس بالكرامة . (يونس عرب ، ص ٠٨) .

ب- **خصائص الجريمة السيبرانية**:

تعد الجرائم السيبرانية إفرازا و نتاجا لتقنية المعلومات و هذا ما أكسبتها طابعا قانونيا خاص يميزها عن غيرها من الجرائم التقليدية بمجموعة من الخصائص:

- ✓ **الجرائم السيبرانية هي جرائم عابرة للحدود :** إن الجريمة المعلوماتية هي شكل من أشكال الجرائم العابرة للحدود ، فمسح الجريمة لم يعد محليا بل أصبح عالميا، إذ أن العامل لا يتواجد ماديا على مسرح الجريمة، فالفاعل يستطيع القيام بجريمته بالدخول إلى ذاكرة الحاسوب الموجود في بلد آخر و هذا الفعل ليلقى شخصا ثالثا موجود في بد آخر.(معتوق عبد اللطيف ،٢٠١١، ص ٢٤.) و هذا ما يثير مسألة الاختصاص القضائي في محاكمة الجاني.
- ✓ **صعوبة اكتشاف و إثبات الجرائم السيبرانية:** تتميز هذه الجرائم بصعوبة الاكتشاف و الإثبات و ذلك لعدم ترك الجاني آثار تدل على إجرامه، فالجريمة تتم عن طريق إدخال رموز و أرقام دقيقة يصعب اكتشافها و إثباتها، لهذا عادة ما يتم اكتشافها بالصدفة، و غالبا ما يصعب معاقبة المجرم و ذلك لعدم وجود أدلة قائمة في حقه. (معتوق عبد اللطيف ، ص ٢٤).

فالجريمة المعلوماتية لا تترك آثار ملموسة ، و بذلك لا تترك شهود تمكن الاستدلال بأقوالهم، و لا أدلة مادية يمكن فحصها ، لأنها تقع في بيئة افتراضية ، يتم فيها نقل المعلومات و تناولها بواسطة نبضات الكترونية غير مرئية. (سعيد علي نعيم، ٢٠١٣، ص ٢٤).

- ✓ **ارتفاع الخسارة الناتجة عن الجريمة المعلوماتية :** و ذلك مقارنة بالجريمة التقليدية، فقطاعات الأعمال العالمية يتكبد خسائر تصل إلى ٤٠٠ مليار دولار أمريكي، و قد خسر مصرفين في الخليج ٤٥ مليون دولار في ساعات قليلة و أعلنت الهند عن تعرض ٣٠٨٣٧١ موقعا الكترونيا للاختراق بين عامي ٢٠١١ و ٢٠١٣ (سعيد علي نعيم ، ص ٣٤) ، قلة الإبلاغ عن وقوع الجريمة الإلكترونية راجع إلى الخشية و الخوف من التشهير و الإساءة للسمعة.

٢- **موقف المشرع الجزائري من الإجرام السيبراني :**

بالموازاة مع منافعها و خدماتها الجمة ، أضحت التكنولوجيا و الانترنت بصفة خاصة تستخدم لارتكاب الجرائم و الإضرار بالأفراد و المؤسسات و ممتلكاتهم ، و بالتالي أصبح من واجب الدولة اتخاذ الإجراءات اللازمة لإحباط أي هجوم من شأنه تهديد سيادة الدولة و مؤسساتها و أمن مواطنيها.

لقد أبدت الجزائر التي تعتبر دولة رائدة إقليميا في مجال الأمن المعلوماتي استعدادها منذ سنوات لمكافحة الجرائم السيبريانية و المعلوماتية بشكل حازم، لذا عكفت على إعداد النصوص القانونية القادرة على إنشاء منظومة دفاعية وقائية يتم على أساسها مكافحة الأعمال الإجرامية المتعلقة بالانترنت و متابعة مرتكبيها قضائيا، كما تسمح بثقفي آثار المجرمين و الجناة الذين يستغلون التكنولوجيا و تطبيقاتها لارتكاب أعمالا إجرامية و غير قانونية. فكيف ساهمت النصوص المختلفة في مكافحة و محاربة الإجرام السبيراني أو الإجرام المعلوماتي ؟

و بعبارة أخرى كيف واجه التشريع الجزائري الجرائم السيبريانية ؟

حاول المشرع الجزائري إصدار قوانين عامة و خاصة و هياكل و أجهزة للجرائم الالكترونية و من بينها :

- كفل الدستور الجزائري الصادر في ٠٦ مارس ٢٠١٦ حماية الحقوق الأساسية و الحريات الفردية و على أن تضمن الدولة عدم انتهاك حرمة الإنسان منها المواد ٣٨، ٤٤ من الدستور.
- و قد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات و قانون الإجراءات الجزائية و التي تحظر كل مساس بهذه الحقوق.

أ- **قانون العقوبات :**

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي حيث عدل قانـــون العقوبات بموجب القانـــون رقم ٠٤-١٥ المؤرخ في ١٠ نوفمبر ٢٠٠٤

Doi: 10.21608/jinfo.2020.114721

المعدل و المتمم للأمر رقم ٦٦-١٥٦ المتضمن قانون العقوبات ، تحت عنوان : "المساس بأنظمة المعالجة الآلية للمعطيات، و يتضمن هذا القسم ثمانية مواد من المادة ٣٩٤ مكرر إلى ٣٩٤ مكرر ٧.

ب- **قانون الإجراءات الجزائية :**

قام المشرع الجزائري بتمديد الاختصاص المحلي لوكيل الجمهورية في مجال الجرائم الالكترونية ، طبقا للمادة ٣٧ فقرة ٠٢ من قانون الإجراءات الجزائية. (ق،إ،ج، الأمر ١٥-٠٢).

حيث يمتد الاختصاص المحلي إذا تعلق الأمر بجرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهـــاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف و جرائـــم الفساد و التهريب . (عبد الله اوهايبية ، ٢٠١٨، ص ٣٥٨).

كما تعد هذه الجرائم أيضا من الجرائم الموصوفة طبقا للتشريع الجنائي الجزائري.

كما نص على التفتيش في المادة ٤٥ فقرة ٧ من نفس القانون المعدل حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعرف عليه من حيث القواعد الإجرائية العامة و الشروط الشكلية و الموضوعية ، و بالتالي لا تطبق عليه المادة ٤٤ من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية و نص على توقيف النظر في جريمة المساس بأنظمة معالجة المعطيات طبقا للمادة ٥١ فقرة ٠٦ من القانون (قانون الإجراءات الجزائية).

كما نص أيضا قانون الإجراءات الجزائية بموجب المادة ٦٥ مكرر ٣ فقرة ٥ أنه في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإن وكيل الجمهورية المختص يقوم بوضع الترتيبات التقنية دون موافقة المعني، من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة .

و في عام ٢٠٠٦، أدخل المشرع تعديل آخر على قانون العقوبات بموجب القانون رقـــم ٠٦-٢٣ المؤرخ في ٢٠ ديسمبـــــر ٢٠٠٤، من هذا التعديل القســـــم السابــع مكـــــرر و الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و قد تم تشديد العقوبة المقررة لهذه الأفعال.

و بعد التعديل الأخير لقانون العقوبات الجزائري بموجب القانون رقم ١٦-٠٢ المؤرخ في ١٩ يونيو ٢٠١٦ (ج، ر، ج ، ج ، عدد ٢٠١٦/٣٧) ، ضمن القسم السابع مكرر من قانون العقوبات بموجب المواد من ٣٩٤ مكرر إلى المادة ٣٩٤ مكرر ٨. و ضمن نطاق الفصل الثالث الخاص بالجنايات و الجنح ضد الأموال .

من بين هذه الجرائم : الغش أو الشروع فيه في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات ، حذف أو تغير للمعطيات المنظمة، إدخال أو تعديل في نظام المعطيات،

تصميم أو بحث أو تجميع أو توفير أو نشر أو حيازة أو إفشاء أو نشر أو استعمال المعطيات ، تكوين جمعية الأشرار.

ج- **صدور قانون رقم ٠٩-٠٤ :**

عمليا ، سعت الجزائر إلى استدراك الفراغ القانوني من خلال تعزيز منظومتها التشريعية خاصة منذ ٢٠٠٩، بحيث سن المشرع الجزائري القانون رقم ٠٩-٠٤ المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها بتاريخ ٠٥ أوت ٢٠٠٩. (القانون رقم ٠٩-٠٤) .

يحتوي هذا القانون على ١٩ مادة موزعة على ٠٦ فصول مستمدة من الاتفاقيات الدولية (اتفاقية بودابست حول الجرائم المعلوماتية لسنة ٢٠٠١).

كما جاء مطابقا للتشريعات الوطنية لاسيما تلك المتعلقة بمحاربة الفساد و تبييض الأموال و تمويل الإرهاب.

حيث نص القانون رقم ٠٩-٠٤ و بموجب الفصل الخامس منه على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته.

و من مهام الهيئة الوطنية تفعيل التعاون القضائي و الأمني الدولي و إدارة و تنسيق العمليات و الوقاية و لمساعدة الجهات التقنية للجهات القضائية و الأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حالة الاعتداءات على المنظومة المعلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

و ذلك بالتعاون مع جهات قضائية أخرى منها المعهد الوطني للأدلة الجنائية و علم الإجرام و المديرية العامة للأمن الوطني مكافحة الجريمة الإلكترونية ذات البعد الدولي من خلال انضمامها للمنظمة الدولية للشرطة الجنائية .INTERPOL.

علاوة على ذلك يجب التنويه بالجهود التي تقوم بها الجزائر منذ جانفي ٢٠١٥ من أجل تكييف إطارها التشريعي و التنظيمي من خلال تبني مجموعة من القوانين الهامة منها الخاصة بالتوقيع و المصادقة الالكترونية التي من شأنها تطوير الخدمات المقدمة عبر الانترنت مثل الإدارة الالكترونية ، التجارة الالكترونية و كذا البنوك الالكترونية ، فضلا عن سعي الجزائر الحثيث إلى إرساء قاعدة قانونية لاستخدام التكنولوجيات الجديدة للإعلام و الاتصال في تطوير قطاع العدالة.

ثانيا : سياسة جهاز الدفاع الوطني في تحقيق الأمن المعلوماتي :

لقد وضعت قيادة الدفاع الوطني الأمن السيبراني أحد أولوياتها ، على غرار باقي دول العالم التي سارعت إلى مراجعة سياساتها الأمنية، و إدراجها لآليات و ميكانيزمات جديدة تعني بهذه المسائل بالموازاة مع تطوير البنايات الأساسية المتعلقة بتكنولوجيات العالم الرقمي . و يفرض مطلب الأمن مضاعفة أنظمة

Doi: 10.21608/jinfo.2020.114721

الرقابة التي قد تشكل تهديدا ممكنا للحريات الفردية ، و لهذا وجب مرافقة كل المقاربات الأمنية في مجال الأمن الرقمي للأطر القانونية و التكنولوجية الملائمة، و تأخذ بعين الاعتبار دقة الهجمات الالكترونيـــة و تعقيداتها و التـــــي يزداد خطرها مع التطـــور التكنولوجي و استخداماتها اليومية.

و تجسيدا لذلك باشرت الدولة الجزائرية و في مقدمتها مؤسسة الدفاع الوطني إلى إعداد برامج خاصة لمجابهة الجريمة الالكترونية و الحد من انتشارها ، و إنشاء أجهزة جديدة تنسجم في أدوارها و تجهيزاتها مع المتغيرات الحاصلة في هذا المجال ، إذ أصبحت الحماية السيبرانية جزء مهما في أي منظومة للدفاع ، و قد استطاع الجيش الشعبي الوطني المضي قدما و مسايرة التطورات التكنولوجية و الإعلامية الحاصلة في العالم ، و من ثمة تأمين و حماية نطاقه المعلوماتي ، و تأمين الفضاء المعلوماتي لكل الناشطين فيه. (دبارة سمر ، المجلة الجزائرية للأمن ..... ، ص ٢٦٢.)

١- **الهياكل المنشأة لتقصي الجريمة السيبرانية** :

أ- **مركز الوقاية من جرائم الإعلام الآلي و جرائم المعلوماتية للدرك الوطني :**

أنشئ هذا المركز في ٢٠٠٨، يوجد مقره ببئر مراد رايس ، أهدافه تأمين منظومة المعلومات لخدمـــــة الأمن العمومي ، و هو بمثابة مركز توثيق ، و يقوم بتحليل المعطيات و البيانات للجرائم المعلوماتية المرتكبة ، و محاولة تحديد هوية أصحابها ، مما يأمن الأنظمة المعلوماتية للمؤسسات و البنوك و البيوت و الشركات ... الخ ، و يعمل على التنسيق الأمني بين الأجهزة الأمنية الأخرى، و الجدير بالذكر أن المركز استطاع معالجة أزيد من ١٠٠ جريمة الكترونية سنة ٢٠١٤ ، و ما يفوق ٥٠٠ قضية رقمية خلال سنة ٢٠١٥ ، و هذا بفضل التركيبـــة البشرية المؤهلة التي اكتسبها الجهاز من التكوين المستمر و الملتقيات الوطنية و الدولية و تبادل الخبرات مع الدول الأخرى.

ب- **المعهد الوطني للأدلة الجنائية و علم الإجرام :**

أنشأ المعهد الوطني للأدلة الجنائية و علم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام و الاتصال الإلكتروني ، أنشأ بموجب المرسوم الرئاسي رقم ٠٤-١٨٣ المؤرخ في ٢٦ يونيو ٢٠٠٤ و عدل نظامه الأساسي بموجب المرسوم الرئاسي رقم ٠٩-١١٨ المؤرخ في ١٤ أفريل ٢٠٠٤.

يتكون هذا الجهاز من "١١" إحدى عشر دائرة متخصصة في عدة مجالات متباينة، تضمن جميعها الخبرة و التكوين و التعليم ، و تقديم جميع المساعدات التقنية ، تقوم دائرة الإعلام الآلي و الالكتروني المكلفة بمعالجة و تحليل و تقديم كل دليل رقمي يساعد العدالـــــة مع تقديم المساعدة للمحققيـــــن ، يتكون من عدة تجهيـــزات تتمثل في محطة ترميم و تصليح الأجهزة و الحوامل المعطلة ، الشبكات الإعلامية و التجهيزات البيانية ، محطة محمولة و ثابتة لإجراء خبرات الإعلام الآلي ، و يحتوي سبع قاعات ، هي: كتب

التوجيه، فصيلة الأنظمة المشحونة ، فصيلة تحليل المعطيات ، فصيلة الهواتف ، اقتناء المعطيات ، قاعة موزع و قاعات تخزين.

حيث يعد مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بالمهام التالية:

- إجراء الخبرات و الفحوص العلمية في إطار التحريات الأولية و التحقيقات القضائية و هذا بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات و الجنح.
- ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية.
- المشاركة في الدراسات و التحاليل المتعلقة بالوقاية و التقليل من كل أشكال الإجرام.
- تصميم و إنجاز بنوك المعطيات.
- المشاركة في تحديد سياسة جنائية مثلى لمكافحة الإجرام.
- المبادرة و إجراء بحوث متعلقة بالإجرام باللجوء إلى التكنولوجيات الدقيقة.
- العمل على ترقية البحوث التطبيقية و أساليب التحريات التي أثبتت فعاليتها في ميادين علمي الإجرام و الأدلة الجنائية على الصعيدين الوطني و الدولي.
- المشاركـــــة في كل الملتقيات و المحاضرات و الندوات على الصعيدين الوطني و الدولي لتطوير مستوى مستخدمي المعهد.
- المساهمة في تنظيم دورات الإتقان و التكوين ما بعد التدرج في تخصيص العلوم الجنائية.

و لتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية و علم الإجرام يحتوي على العديد من الأقسام و المصالح المختصة من أهمها:

- **مصلحة البصمات:** يتم على مستوى هذه المصلحة مقارنة البصمات للتعرف على الجثث و تجدر الإشارة إلى أن الدرك الجزائري مجهز بأنظمة التعرف الآلي على البصمات (THE AFIS Automated Fingerprint Identification System.
- **مصلحة الوثائق:** في هذه المصلحة يتم التأكد من صحة الوثائق و الإمضاءات و التحقق من النقود و كذلك التأكد من صحة الوثائق السرية .
- **مصلحة الإعلام الآلي:** على مستوى هذه المصلحة يتم رصد و مراقبة و تتبع عمليـــــات الاختراق و القرصنة المعلوماتية و كذا اكتشاف المعلومات المسروقة و تفكيك البرامج المعلوماتية.
- **مصلحة البيئة:** تشرف هذه المصلحة على عمليات البحث في أسباب تلوث المياه و التربة و كذا الكشف عن المواد السامة المتواجدة في المحيط أو أماكن العمل. (بارة سمير، ٢٠١٧، ص ٤٣٦).

Doi: 10.21608/jinfo.2020.114721

ج- **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:**

استجابة لمطلب الأمن المعلوماتي و محاربة التهديدات الأمنية الناجمة عن الجرائم الالكترونية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الالكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية ، و التي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني و التي أنشئت سنة ٢٠١١ ، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بقرار من المدير العام للأمن الوطني و أضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي ٢٠١٥.

د- **الهيئـــة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها:**

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم ١٥-٢٦١ و هي سلطة إدارية مستقلة لدى وزيـــر العدل ، تعمل تحت إشراف و مراقبـة لجنـــة مديريـــة يترأسها وزير العدل و تضم أساسا أعضاء من الحكومة معنيين بالموضوع و مسؤولي مصالح الأمن و قاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

و تضم الهيئة قضاة و ضباط و أعوانا من الشرطة القضائية تابعين لمصالح الاستعلامات العسكرية و الدرك الوطني و الأمن الوطني وفقا لأحكام القانون الإجراءات الجزائية .

و كلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصـــال و مكافحتها و تنشيط و تنسيق عمليـــات الوقايـــة منها ، و مساعدة السلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة هذه الجرائم ، من خلال جمع المعلومات و التزويد بها و من خلال الخبرات القضائية ، و ضمان المراقبة الوقائيـــة للاتصالات الالكترونيـــــة ، قصد الكشف عن الجرائم المتعلقـة بالأعمال الإرهابية و التخريبية و المساس بأمن الدولة.

و هي سلطة إدارية تشكلت بمرسوم رئاسي رقم ١٥-٢٦١ تعمل تحت إشراف لجنة يديرها وزير العدل ، تضم أعضاء من الحكومة و مسؤولي مصالح الأمن و قضاة و أعوان الشرطة القضائية تابعين للاستعلامات العسكرية و الدرك الوطني و الأمن الوطني . تعمل على الكشف عن الجرائم الإرهابية الالكترونية و جرائم المساس بأمن الدولة .(يوسف بوغرارة ، مجلة الدراسات الإفريقية ، ٢٠١٨، ص ١١٢).

٢- **دور الجيش الوطني الشعبي في تحقيق الأمن المعلوماتي :**

يقصد بالدفاع الالكتروني في الاستراتيجيات العسكرية : " مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثير الهجمات الالكترونية ، و التخفيف من حدتها و التعافي منها بسرعة" ، فقد اعتبرت الإستراتيجية النمساوية مصطلح الدفاع

الالكتروني " جميع التدابير اللازمة للدفاع عن الفضاء الالكتروني بالوسائل المناسبة لتحقيق الأهداف العسكرية الإستراتيجية " ، أما بخصوص الإستراتيجية العسكرية البلجيكية ، اعتبرت الدفاع الالكتروني " تطبيق التدابير الوقائية الفعالة للحصول على مستوى مناسب من الأمن الالكتروني ، و تقليل المخاطر الأمنية إلى مستوى مقبول ، " و فيما يتعلق بالإستراتيجية العسكرية الفرنسية : " مجموعة الوسائل الفنية و غير الفنية التي تسمح للدولة بالدفاع عن نظم المعلومات الحرجة في الفضاء الالكتروني " ، و فيما يتعلق بالإستراتيجية العسكرية الجزائرية ، فقد اعتبرت الدفاع الالكتروني "مراقبة الأنظمة التي تحمي الدولة من كافة التهديدات ، و متابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لضمان فعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات و منظومات الاتصال و كذا منظومة الأسلحة للجيش" (نوارة باشوش ، جريدة الشروق ، ٢٠١٩ ص ٠٣).

حيث أصبحت الحروب المستقبلية حروب الالكتروني ، كما أبرزت مجلة الجيش في العدد ٦٧٦ لشهر نوفمبر ٢٠١٩ على أهمية المركز الوطني للإشارة للجيش الوطني الشعبي (مجلة الجيش ، العدد ٦٧٦ لسنة ٢٠١٩).

أ- **الدفاع السيبراني في الجيش الوطني الشعبي :**

قررت القيادة العليا للجيش الوطني إحداث "مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة " على مستوى دائرة الاستعمال و التحضير لأركان الجيش الوطني الشعبي، بهدف تأمين و حماية المنظومات و المنشآت الحيوية لقواتنا المسلحة ضد التهديدات السيبرانية .

وعيا منها بالتحديات التي بات يحملها هذا الواقع الجديد و قصد الإلمام بكافة التهديدات التي يشكلها الدفاع السيبراني على الأمن و حتى على سيادة الدول و الحكومات . قامت قيادة الجيش الوطني الشعبي بوضع إستراتيجية دفاع سيبراني ، تغطي كل الجوانب التي لها صلة بتحقيق نظام دفاع سيبراني متكامل و فعال بهدف تأمين و حماية المنظومات و المنشآت الحيوية للدولة الجزائرية ، حيث تم في هذا الصدد و بتاريخ ٦ نوفمبر ٢٠١٥ إحداث على مستوى دائرة الاستعمال و التحضير لأركان الجيش الوطني الشعبي " مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة " ، تكلف أساسا بتخطيط و إدراج و متابعة حالة تقدم نشاطات تجسيد السياسة الشاملة للدفاع السيبراني الرامية لتحقيق بفعالية الحماية ضد التهديدات السيبرانية التي تستهدف أنظمة المعلومات و منظومات الاتصال و كذا منظومات الأسلحة للجيش الوطني الشعبي .

تتمحور إستراتيجية الدفاع السيبراني للجيش الوطني الشعبي حول سبعة محاور و هي :

Doi: 10.21608/jinfo.2020.114721

- ✓ **جانب وظيفي و تنظيمي :** تكون أعمال الدفاع السيبراني ضمن الجيش الوطني الشعبي موجهة و منفذة في إطار وظيفة و / أو تنظيمية مكرسة لضمان تجانس و فعالية هذه الأعمال .
- ✓ **جانب قانوني :** تحيين و تعزيز باستمرار الإطار القانوني المتعلق باستعمال تكنولوجيات الإعلام و الاتصال عموما و تأمين منظومات الإعلام خصوصا.
- ✓ **جانب الموارد البشرية :** تعد جاهزية مورد بشري تقني معتبر و ذوي كفاءة عالية في مجال الدفاع السيبراني هدفا أساسيا لكي تضمن نجاح إدخال هذا المجال في النشاطات العملياتية و التسيير للجيش الوطني الشعبي.
- ✓ **جانب تقني :** تقوية و تكييف القدرات التقنية للحماية ، الكشف و الرد على الهجمات السيبرانية باستمرار ، مع ضمان يقظة دائمة فيما يخص الطرق و الوسائل المستعملة من طرف المهاجمين
- ✓ **جانب الوقاية و التحسيس :** الوقاية و تحسيس مستخدمي الجيش الوطني الشعبي من المخاطر و التهديدات التي تنجز عن استعمال تكنولوجيات الإعلام و الاتصال في الإطار المهني أو الشخصي بطريقة مستمرة
- ✓ **جانب البحث و التطوير:** تعد درجة معتبرة من الاستقلالية التكنولوجية، باستعمال وسائل تقنية خاصة أو مشخصة من طرف هياكل البحث و التطوير للجيش الوطني الشعبي ، لاسيما تلك المستعملة للحماية ضد التهديدات السيبرانية ، عنصرا حاسما في إستراتيجية الدفاع السيبراني
- ✓ **جانب التعاون :** تعزيز التعاون في مجال الدفاع السيبراني مع جيوش الدول الشريكة من أجل السماح للجيش الوطني الشعبي من الاستفادة من الخبرات و الوسائل التكنولوجية المتقدمة جدا

في سياق ذي صلة و تعزيزا لإستراتيجية الدفاع الوطني لمكافحة التهديدات السيبرانية ، و قصد الإلمام بكافة المستجدات في هذا المجال ، و بخاصة تلك التي تعالج موضوع الأمن السيبراني و الدفاع كرهان للأمن و الدفاع الوطنيين و حماية المنشآت الحساسة ضد الهجمات السيبرانية ، تعكف مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة لدائرة الاستعمال و التحضير لأركان الجيش الوطني الشعبي دوريا على تنظيم ملتقيات محاضرات و ورش عمل تطبيقية ، كان آخرها ملتقى بعنوان : " الدفاع السيبراني : مكون أساسي للأمن و الدفاع الوطني " يومي ١٥ و ١٦ ماي ٢٠١٧ ، و الذي أكد من خلاله رئيس دائرة الاستعمال و التحضير لأركان الجيش الوطني الشعبي اللواء شريف زراد في كلمة افتتاحه ، أن تنظيم مثل هذا الملتقى يأتي من أجل خلق فضاء نقاش بين مختلف الفاعلين في الفضاء السيبراني على المستوى الوطني ، لفهم أفضل لرهانات الأمن و الدفاع السيبرانين، و

لتحسيـــن و إثراء المعارف فـــي مجال الوقايـــة و مكافحة التهديدات السيبرانية و كذا تحديد أثرها على الأمن الوطني. (مجلة الجيش ، العدد ٦٥١ لسنة ٢٠١٧).

مهام مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة : مصلحة الدفاع السيبراني و مراقبة أمن الأنظمة هي تركيبة ملحقة بدائرة التحضير و الاستعمال لأركان الجيش الوطني الشعبي ، فاستحداثها في نوفمبر ٢٠١٥ ، يندرج ضمن نهج إرساء السياسة الشاملة المسطرة من قبل القيادة العليا و الهادفة إلى حمايـــــة مؤسستنا ضد المخاطـــــر و التهديدات السيبرانية ، و باعتبارها جهاز للتوجيه و الخبرة من المستوى الاستراتيجي ، تحرص هذه المصلحة أساسا على وضع و تطبيق السياسة العامة للدفاع السيبراني في الجيش الوطني الشعبي و أيضا إلى تقييم و تعزيز مستوى أمن الأنظمة المستغلة و كذا إلى تحيين و تطبيق الإطار التنظيمي المسير لمجال الدفاع السيبراني .

على الصعيد العملياتي : تتمثل مهام المصلحة التي تعد طرفا فاعلا في العمليات العسكرية في تعزيز قدراتنا في مجال الدفاع السيبراني ، على نحو يسمح بتأمين أنظمة السلاح و الإعلام و الاتصال .

طبقا لتوجيهات القيادة العليا ، و باعتبارها هيئة تابعة لوزارة الدفاع تساهم هذه المصلحة مع الهيئات الوطنية المعنية في إعداد و وضع السياسة الوطنية المتعلقة بالدفاع السيبراني ، مع ضمان التنسيق مع مختلف الهيئات في مجال تأمين المنشآت الرقمية الحساسة.

ب- **الأمن و الدفاع السيبراني للجيش الوطني الشعبي :**

تحت تأثير الفضاء الالكتروني أو ما أصبح يعرف بالقوة السيبرانية ، دفعت العديد من الدول إلى تبني استراتيجيات في مجال دفاعها السيبراني و تدعيم مراكز قوتها بطريقة تشابه الاستراتيجيات الدفاعية التقليدية ، خاصة في ظل توزع القوة السيبرانية بين عدد من الفاعلين من غير الدول و بروز التهديدات التي أصبحت تطال أمن و استقرار الدول موازاة مع تغيير منطق الحروب حاليا نحو الاتجاه اللاتماثلي.

شهد القرن الحالي ثورة منفردة في عالم تكنولوجيا الإعلام و الاتصال ، إلى الحد الذي أعدها بعض الخبراء و المختصين الميدان الخامس للنزاعات ، بعد الأرض ، البحر ، الجو و الفضاء ، و يعود ذلك إلى درجة الانتشار و التطور السريعين لهذه التقنية ، حيث يكاد لا يخلو مجال من مجالات الحياة إلا و ارتكز عليها ، و بالخصوص مع ارتباط معظم الخدمات و قواعد البيانات و البنى التحتية و الأنظمة المالية و المصرفية بشبكة الانترنت ، و كذا اتجاه معظم الدول و الحكومات لتبني نماذج الحكومات الذكية و التحول نحو الخدمات الالكترونية التي قلصت الجهد ، الوقت و التكلفة ، و ساهمت بسرعتها و مرونتها في تلبية الاحتياجات ، و لذا فإن الحفاظ على هذا البنى من أي هجمات الكترونية يدخل في صميم الأمن القومي للدول ، لأن تعرض أحد هذه الأنظمة لهجوم الكتروني يمكن أن يولد آلاف

Doi: 10.21608/jinfo.2020.114721

الضحايا في دقائق معدودة ، فمثلا قد يؤدي اختراق نظام المواصلات كأنظمة ملاحة الطيران و السفن و سكك الحديد إلى تصادمها ، و عليه فإن خلق نظام دفاع الكتروني فعال يعمل بمثابة حائط صد للهجمات الالكترونية يعد أمرا حيويا للأمن القومي للدول.

على الرغم من الايجابيات التي حملتها الانترنت و التي جعلت من عصرنا الحالي عصر فضاء الكتروني بامتياز ، و أضحت فيه (الانترنت) الإطار العام الحاكم لتفاعلاته كافة ، سواء كانت شخصية أو عامة ، عسكرية أو سياسية ، اقتصادية أو اجتماعية ، إلا أنها جلبت معها العديد من التهديدات و المخاطر و الأخص على الأمن القومي للدول ، فإذا كان العدو في عهد الحرب الباردة معروفا و واضحا ، و يمكن تعقبه و التنبؤ بسلوكه ، فإن الأمر يختلف تماما في حالة العصر السيبراني ، فالعدو ليس بالضرورة دولة ، و لا يتقاسم بالضرورة جوارا جغرافيا ، كما أن استهداف المناطق و الخدمات الإستراتيجية قد يكلف أقل من الحرب التقليدية ، و في أحيان أخرى قد يكون أكثر تدميرا إذا كان الأمر يتعلق بالسيطرة على البنى التحتية و الخدمات اللوجستية ، سواء كانت مدنية أو عسكرية .

طبيعة و أشكال التهديدات السيبرانية :

هناك العديد من أنواع الهجمات السيبرانية ، نذكر منها على سبيل المثال لا الحصر :

- ✓ **تخريب المواقع:** الهجمات التي تشوه صفحات على الانترنت أو تدمرها أو تغير طبيعتها، و هذا النوع من الهجمات عادة ما يرد بسرعة و يكون ضرره محدودا.
- ✓ **الدعاية السلبية:** رسائل سياسية يمكن نشرها لأي شخص يستخدم الانترنت.
- ✓ **جمع البيانات:** بمعنى أن المعلومات السرية غير المحفوظة بأمان يمكن اعتراضها و التقاطها، بل و تعديلها، مما يجعل التآمر في هذه الحالة ممكنا.
- ✓ **تعطيل المعدات العسكريـــــة :** الأنشطــة العسكريـــــة التي تستعمل الحواسب و الأقمار الاصطناعية للتنسيق هي في خطر من هذا النوع من الهجمات ، حيث يمكن اعتراض الأوامر و الاتصالات أو استبدالها ، مما يعرض حياة الجنود للخطر.
- ✓ **مهاجمة البنى التحتيـــة الحساســـــة :** شبكات الكهرباء و الماء و الوقود و الاتصالات و المواصلات كلها معرضة لحروب الانترنت ، و يمثل هذا التدمير الاقتصادي الأشد وطأة في الحالات القصوى .

و يمكن لهذه الهجمات السيبرانية ، أن تستعمل بالموازاة مع أعمال أخرى غير تقنية مثل الاستعلام و الاستغلال و التخريب .

نتيجة لهذا التطور التكنولوجي أصبحت الدول في حاجة إلى استراتجيات جديدة لإدارة أمن الفضاء الالكتروني تنطلق من مبدأ رئيسي هو القابلية للاختراق خاصة أن الفضاء الالكتروني مجال عام لا يعترف بالحدود ، و عليه فإن منطلق الأمن "السيبراني" لأي دولة يبدأ بتطوير سياسة وطنية لرفع الوعي حول قضايا الأمن "السيبراني" و الحاجة

لإجراءات وطنية و إلى التعاون الدولي ، بل و يتعدى ذلك إلى تطوير مخطط وطني لتحفيز الأمن السيبراني بهدف تقليص مخاطر و أثار التهديدات السيبرانية و كذا المشاركة في الجهود الدولية و الإقليمية لتحفيز الوقاية الوطنية و التحضير و الاستجابة للتعافي من الحوادث السيبرانية ، فعلى سبيل المثال سنت الولايات المتحدة الأمريكية على مدار السنوات الخمسة الماضية فقط و لوحدها ٣٤ قانونا و ٥ أوامر تنفيذية لتحسين الأمن السيبراني.

وفقا للمؤشر العالمي للأمن السيبراني GCI في نسخته الثانية الذي أصدرته وكالة الأمم المتحدة للإتصالات في ٥ جويلية ٢٠١٧ ، فإنه لا يزال هناك حاجة إلى بذل المزيد من الجهود في هذا المجال الحرج ، خاصة أن الحكومات تعتبر المخاطر الرقمية ذات أولوية عالية ، كما أصبح الأمن السيبراني مصدر قلق كبير للدفاع القومي ، و أظهرت الدراسة وجود فجوات كبيرة في الأمن السيبراني بين الدول الأكثر قوة في العالم .

يعتمد الأمن السيبراني بناء على توصيات الإتحاد الدولي للاتصالات على مزيج مركب من التحديات التقنية و السياسية ، الاجتماعية و الثقافية ، و حصر المختصون صلاحياته في :

- تطوير استراتيجية وطنية للأمن السيبراني و حماية البنية التحتية للمعلومات الحساسة .
- إنشاء تعاون وطني بين الحكومة و مجتمع صناعة الاتصالات و المعلومات.
- ردع الجريمة السيبرانية .
- خلق قدرات وطنية لإدارة حوادث الحواسب الآلية.
- تحفيز ثقافة وطنية للأمن السيبراني. (بوكبشة محمد ، مجلة الجيش ، ٢٠١٧).

خاتمة :

يحظى الدفاع السيبراني باهتمام بالغ من قبل السلطات العليا للبلاد ، التي يجب أن تشرك كل الفاعلين المعنيين .

فمن الضـــروري إرساء إطار مناسب يتضمن كل العناصـر التنظيمية و القانونية و التقنية يسمح بتبادل المعلومات بين مختلف المؤسسات و الهيئات لصالح الدفاع السيبراني.

في هذا الخصوص ، لا يمكن أن يقتصر العمل على نشاط للتعاون أحادي الجانب، بل يجب أن يندرج ضمن مقاربة شاملة و دائمة تسعى إلى تحقيق التنسيق و التجانس بين مختلف مؤسسات الدولة المعنية .

في هذا السياق بادرت وزارة الدفاع الوطني بوضع آلية لتنسيق و تبادل المعلومات المتعلقة بالدفاع السيبرياني ، و هي محل مشاورات بين مختلف الأطراف المعنية.

الحقيقة أنه في عالم الأمن السيبراني لا يمكن الحديث عن ضمان تأمين مطلق للأنظمة ، لأن الأمر يتعلق باتباع مسار للتطوير المستمر للأم ، و عليه فإن كسب رهان

Doi: 10.21608/jinfo.2020.114721

الأمـــن السيبراني يستلزم تحديـــد مقاربة استباقية و تفاعلية ، تهدف إلى تعزيز و تدعيم أمن و سلامة أنظمتنا الأمنية لمواجهة أي تهديد سيبراني محتمل .

و من هذا المنطلق نحن بصدد تكثيف الجهود لتحقيق الأهداف المرجوة.

في هذا الخصوص ، يجب التنويه بالدعم الدائم و المستمر للقيادة العليا للجيش الوطني الشعبي من خلال تسخيرها كل الإمكانات المادية و البشرية الضرورية لإنجاز هذه المهمة بفعالية و نجاعة و من ثم التحكم في التكنولوجيا المستعملة في هذا المجال.

قائمة الهوامش :

١- أنظر مليكة عطوي ، الجريمة المعلوماتية ، حوليات جامعة الجزائر ، عدد ٢١ ، ص ٠٨.
٢- أنظر المادة ٣٧ من قانون الإجراءات الجزائية ، بموجب الأمر ١٥-٠٢ المؤرخ في ٢٣ يوليو سنة ٢٠١٥.
٣- أنظر الجريدة الرسمية عدد ٣٧ المؤرخ في ٢٢ يونيو ٢٠١٦.
٤- أنظر المادة نص القانون رقم ٠٩-٠٤ ، الجريدة الرسمية ، عدد ٤٧ الصادرة في ٠٥ أوت ٢٠٠٩ ، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها .
٥- بوكبشة محمد ، الأمن و الدفاع السيبراني أولوية قصوى ، مجلة الجيش ، العدد ٦٥١ ، أكتوبر ٢٠١٧.
٦- سميرة معاشي ، ماهية الجريمة المعلوماتية ، مجلة المنتدى القانوني ، عدد ٧ ، جامعة محمد خيضر ، بسكرة ، أفريل ٢٠١٠ ، ص ٢٧٨.
٧- سعيد علي نعيم ، آليات البحث و التحري عن الجرائم المعلوماتية في القانون الجزائري ، مذكرة ماستير ، جامعة العقيد الحاد لخضر ، باتنة ، كلية الحقوق ، ٢٠١٣ ، ٢٠١٢ ، ص ٢٤.
٨- سمير بارة ، الأمن السيبراني في الجزائر ، السياسات و المؤسسات ، المجلة الجزائرية للأمن الانساني ، العدد الرابع ، جويلية ٢٠١٧ .
٩- سمير بارة ، الدفاع الوطني و السياسات الوطنية للأمن السيبراني في الجزائر ، الدور و التحديات الملتقى الدولي حول سياسات الدفاع الوطني ، جامعة قاصدي مرباح ، ورقلة ، كلية الحقوق ، ٢٠١٧/٠١/٣١.
١٠- عبد الفتاح مراد ، د.ت.ن ، دور الكمبيوتر في مجال ارتكاب الجرائم الالكترونية بشرح جرائم الكمبيوتر و الانترنت ، مصر ، دار الكتب و الوثائق المصرية ، ص ٤٣.
١١- عبد الله اوهايبية ، ٢٠١٨ ، شرح قانون الإجراءات الجزائية ، الجزء الأول ، الجزائر ، دار هومة ، ص ٣٥٨.
١٢- عزارمي عبد الغني ، الفريق أحمد قايد صالح يدشن المركز الوطني للإشارة ، الحروب المستقبلية هي بالأساس حروب الكترونية ، مجلة الجيش ، العدد ٦٧٦ لشهر نوفمبر ٢٠١٩.
١٣- محمد عبيد الكعبي ، ٢٠٠٩ ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت ، القاهرة ، دار النهضة العربية ، ط٢ ، ص ٣٣.

١٤- معتوق عبد اللطيف ، ٢٠١١ ، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن ، مذكرة ماجستير جامعة العقيد الحاج لخضر ، باتنة ، كلية الحقوق ، ٢٠١٢ ، ٢٠١١ ، ص ٢٤.
١٥- نهلة عبد القادر المومني ، الجرائم المعلوماتية ، الأردن ، دار الثقافة للنشر و التوزيع ، ط١ ، ص ٤٩.
١٦- نوارة باشوش ، الجيش يدخل حرب القضاء الالكتروني و مكافحة الجوسسة ، على الموقع التالي : www.echoronkonlire.com/arar/articles/536554.html تاريخ دخول الموقع ٢٠١٩/١١/٢٥.
١٧- يوسف بوغرارة ، الأمن السيبراني ، الإستراتيجية الجزائرية للأمن و الدفاع في القضاء السيبراني ، مجلة الدراسات الإفريقية و حوض النيل ، المركز الديمقراطي العربي ، المجلد الأول ، العدد الثالث ، سبتمبر ٢٠١٨.
١٨- يونس عرب، جرائم الكمبيوتر و الانترنت، إيجاز في المفهوم و النطاق و الخصائص و الصور و القواعد الإجرائية للملاحظة و الإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي ٢٠٠٢، تنظيم المركز العربي للدراسات و البحوث الجنائية، أبو ظبي، ٢٠٠٢، ص ٠٨.