| | |
|---|---|
| العنوان: | الأمن المعلوماتي وعلاقته بالأمن القومي |
| المصدر: | مجلة الباحث للدراسات القانونية والقضائية |
| الناشر: | محمد قاسمي |
| المؤلف الرئيسي: | الطاهري، عبدالفتاح |
| المجلد/العدد: | ع10 |
| محكمة: | نعم |
| التاريخ الميلادي: | 2019 |
| الشهر: | فبراير |
| الصفحات: | 21 - 65 |
| رقم MD: | 998043 |
| نوع المحتوى: | بحوث ومقالات |
| اللغة: | Arabic |
| قواعد المعلومات: | IslamicInfo |
| مواضيع: | الأمن القومي، الأمن المعلوماتي، الحرب الإلكترونية |
| رابط: | http://search.mandumah.com/Record/998043 |

ذ عبد الفتاح الطاهري

باحث بسلك الدكتوراه بكلية الحقوق – القاضي عياض – مراكش

# الأمن المعلوماتي وعلاقته بالأمن القومي

**مقدمة:**

برزت في الفترة الأخيرة أهمية الأمن المعلوماتي، خاصة مع التحول إلى الطبيعة الرقمية في الاتصالات والتعاملات بين الأفراد والجماعات، حيث أصبح العالم أشبه بقرية صغيرة يستطيع أي شخص أن يصل للأخر مهما كانت المسافة بعيدة بينهم، فالمعلومات والأمن يمثلان وجهان لعملة واحدة.

فأداة هذا العصر هي وسائل الاتصال الالكتروني، حيث دخلت هذه الوسائل جميع مجالات الحياة الإنسانية بشكل قوي، وأصبحت أداة تستخدمها كافة شعوب العالم في شتى المجالات، كما أضحت وسيلة قوية تستخدم أيضا للأغراض التدميرية، الأمر الذي جعل من الاهتمام بأمن المعلومات الالكترونية والرقمية مطلبا امنيا نابعا من توجه سياسي، خصوصا

تلك الدول الحديثة التي ربطت جميع مرافق حياتها اليومية بقواعد الانترنت الضخمة، لتتحول إلى دول الكترونية بشكل شبه متكامل.

حيث تغيرت مفاهيم السيادة في دول العالم بفعل التطورات التّقنية والإلكترونية التي طرأت على حياة الأفراد والمؤسسات والحكومات والمجتمعات، لتوجد التطورات التكنولوجية الهائلة ساحاتٍ سياديةٍ جديدةٍ دفعت دول العالم لفرض رقابتها الأمنية عليها.

فلم يعد الأمر مقتصراً على المحيط الجغرافي أو المائي أو حتى الجوي للدول؛ بل عملت وسائل الاتصال الحديثة على خلق فضاءٍ جديدٍ يختلج كمياتٍ كبيرةٍ من المعلومات التي تخص الأمن القومي لدول العالم.

## 2_ تحديد المفاهيم:

بفعل مجموعة من التغيرات المتوالية لم يعد مفهوم الأمن[22] مقتصرا على الأمن الجوي و البري والبحري فحسب، بل بات الاهتمام بأمن المعلومات الإلكترونية والرقمية مطلبا امنيا نابعا من توجه سياسي، خصوصا تلك الدول التي حاولت أن تربط جميع مرافق حياتها اليومية، بقواعد الأنترنت الضخمة، لتتحول إلى دول إلكترونية بشكل شبه متكامل.

1 يعتبر مفهوم الأمن على انه في الغالب مرادفا للطمأنينة ومناقضا للخوف، إذ يجب التمييز بين مفهومين للأمن، مفهوم ضيق وهي تلك الإجراءات المتمثلة في تحقيق الأمن الداخلين والمفهوم الواسع ويتمثل في تامين سلامة الدولة ضد أخطار خارجية وداخلية.La sécurité est l'absence de danger, c'est-à-dire une situation dans laquelle quelqu'un (ou quelque chose) n'est pas exposé à des évènements critiques ou à des risques (défaillance, accident, agression physique,..).voir Jean-Philippe BAY,« tout sur la sécurité informatique », Dunod, 2005, p 48.

### أ- المقصود بالأمن القومي

أصبحت قضية الأمن القومي[23] هي القضية الأولى الأكثر أهمية بالنسبة لكل دول العالم في الوقت الحالي، بفعل عوامل متعددة، أهمها تلك المتغيرات الحادة التي يشهدها النظام الدولي[24].

فمفهوم الأمن القومي[25] ارتبط في بداية تعريفه بالبعد العسكري، حيث يرى والتر ليبمان[26] بأن مصطلح الأمن القومي يشير إلى" القوة العسكرية للدول، والتي تضمن لها عدم تضحيتها الكاملة بجميع مقدراتها تجنباً لويلات الحروب، مع قدرتها وإمكانيتها على حماية نفسها عسكرياً إن اقتضت الضرورة[27]".

لكن مفهوم الأمن تطور ليشمل إبعادا أخرى غير عسكرية، حيث عرفته دائرة معارف العلوم الاجتماعية العالمية على انه؛ " قدرة الدول على حماية نفسها من الأخطار و التهديدات الخارجية التي قد تعترضها."[28]

---

2 ظهر مصطلح الأمن القومي، كنتيجة لقيام الدولة القومية في القرن السادس عشر الميلادي ، و بدأ التداول بمفهوم الأمن القومي في نهاية الحرب الأوربية التى سميت بحرب الثلاثين سنة.

La **guerre de Trente Ans** est une succession de conflits armés dont les causes sont religieuses et politiques. Elle se déroule en Europe centrale surtout, de 1618 à 1648. La guerre est close par les traités de Westphalie qui consacrent la division religieuse et politique de l'Allemagne et l'affaiblissement de la puissance impérialeLa guerre de Trente ans est un tournant décisif dans les relations entre états européens. Article publié sur le site électronique « https://fr.vikidia.org/wiki/Guerre_de_Trente_Ans » sous le tire de '' guerre de trente ans''.

24 مفيد محمود شهاب، نحو مفهوم متطور للأمن القومي العربي ، مقال منشور بمجلة الأمن و القانون، كلية شرطة دبي، العدد الأول، يناير 1993، ص123.

25 La sécurité nationale est l'ensemble des moyens (institutions, doctrines, activités et ressources) de nature civile (politique, diplomatique, économique, juridique, ...) et de nature militaire mis en œuvre par un Etat pour protéger ses intérêts nationaux essentiels que ce soit en temps de guerre, de crise ou de paix. Article publié par Bertrand WARUSFEL, sur le site électronique http://www2.droit.parisdescartes.fr/warusfel/articles/Securite%CC%81Nationale_Warusfel2011 sous le titre de ''La sécurité nationale, nouveau concept du droit français ''.

26 والتر ليبمان، صحفي أمريكي، و يعد من أوائل واضعي أسس مفهوم الأمن القومي في تاريخ أمريكا الحديث. انظر الرابط https://fr.wikipedia.org/wiki/Walter_Lippmann

6La définition de Walter Lippmann, l'une des premières, reflète ainsi l'attachement à l'intérêt national. Selon lui, «une nation possède la sécurité lorsqu'elle n'est pas contrainte de sacrifier ses intérêts légitimes afin d'éviter la guerre, et est capable, s'il y a un obstacle, de les préserver à travers la guerre .»Voir Marcus G. Raskin, *The Politics of National Security,* New Brunswick ,1979, p. 32.

28رأفت الكمار، الحاسوب والأمن القومي العربي، القاهرة، دار الكتب العلمية للنشر والتوزيع، 2005، ص:22.

فمن خلال ما سبق يتضح أن مفهوم الأمن القومي هو تلك الإجراءات التي تتخذها الدولة وفي حدود طاقتها للحفاظ على كيانها في الحاضر والمستقبل، مع مراعاة المتغيرات الداخلية والخارجية التي قد تطرأ عليها مستقبلاً.

غير أن هناك من يخلط بين مفهومي الأمن القومي و الوطني، إذ أن مفهوم الأمن الوطني هو الأمن الذي يعني دولةً بعينها، وذلك لحصانة تأمينها الذاتي، ونظامها السياسي من ناحيةٍ عسكرية[29]، غير أن الأمن القومي لا يقاس بالقوة فقط، بل بمجموع قُدرات الدول وإمكانياتها في الحفاظ على مقدراتها الحاضرة والمستقبلية، حيث أن القوة العسكرية وحدها في عصرنا الحالي لا تكفي لتحقيق الأمن القومي.

**ب- المقصود بالأمن المعلوماتي:**

إن الأمن ألمعلوماتي[30] هو ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزونة في أجهزة الحاسوب إضافة إلى الأجهزة الملحقة و شبكات الاتصالات و التصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزونة أو تلك التي ترمي إلى نقل أو تغيير أو تخريب الخزين المعلوماتي لهذه القواعد[31].

غير انه من الصعوبة بمكانٍ وضع مفهوماً محدداً لأمن المعلومات الإلكترونية في عصرنا الحالي، نظراً لتعاظم وتيرة الابتكارات التّقنية والإلكترونية، حيث عرف حسن الطاهر، أمن

---

[29] حمد عبد الله اللحيدان، مفهوم الأمن الوطني ومقوماته، مقال منشور بالموقع:
http://www.alriyadh.com/625802

[30]La sécurité de l'information est l'ensemble des mesures adoptées pour empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le refus d'utilisation d'un ensemble de connaissances, de faits, de données ou de moyens. Le terme sécurité de l'information désigne donc les mesures préventives que nous mettons en place pour préserver nos informations et nos moyens .Voir « Stéphane Gill , La sécurité de l'information, Dalloz ,2009 p : 28.

[31]أمين أعزان، الحماية التقنية و الجنائية للنظم المعلوماتية، مقال منشور بالمجلة المغربية للقانون الجنائي و العلوم الجنائية، العدد الثالث، سنة 2006 ،ص59.

المعلومات الإلكترونية على أنه:" العمليات التي تؤمن حماية كافة الموارد والآليات المستخدمة والمتبعة في معالجة المعلومات أمنياً، بحيث يتم تأمين كافة الموارد البشرية وغير البشرية المختصة بجهةٍ معنيةٍ، بوسائل وإجراءاتٍ وعملياتٍ أمنيةٍ وتّقنيةٍ تُوفر لها سلامة محتواها المعلوماتي من أية مخاطر داخليةٍ أو خارجية"[32].

إذن، يمكن تعريف أمن المعلومات الإلكترونية، وبناء على التحول الذي طرأ على المجتمعات البشرية في عصورها الماضية، ووصولها إلى عصرها الجديد المتمثل بالثورة المعلوماتية، بأنه:" عمليات الحماية الأمنية والتّقنية للمجتمعات التي يتعامل أفرادها ومؤسساتها مع المعلومات ووسائل الاتصالات، خاصةً في تسيير أمور قطاعاتهم المختلقة، كالقطاعات الاقتصادية و الاجتماعية و الثقافية و الأمنية و السياسية..."[33].

### 3_ أهمية الموضوع:

تبرز أهمية هذه الدراسة من حيث المكانة التي بات يحتلها المجال الإلكتروني في دول العالم، حيث أصبح هذا المجال مجالاً مستهدفاً بشكلٍ كبير، وخُصوصاً مع ارتفاع وتيرة التقدم التكنولوجي والتّقني والإلكتروني، والذي أعطى الإمكانية لضرب أي دولةٍ أو منظمةٍ في وقتٍ قصيرٍ وتكلفةٍ قليلة، وذلك باستخدام الإنترنيت ووسائل الاتصال الإلكتروني الأخرى، مما حدا بالعديد من دول العالم إلى حماية فضائها الالكتروني، ومن جانبٍ آخر؛ أصبحت الحروب الإلكترونية أسلوباً جديداً من الأساليب التي أنتهجها العالم كنوع من وسائل المقاومة.

---

[32] طاهر حسن، الحاسب وأمن المعلومات، مكتبة الملك فهد الوطنية، الرياض 2000م، ص23.
[33] أمين أعزان، مرجع سابق، ص: 22.

## الإشكال الذي يطرحه الموضوع:

ما مدى تأثير الأمن المعلوماتي على الأمن القومي؟ وهذا الإشكال تتفرع عنه مجموعة من التساؤلات: هل غيرت التكنولوجيا الحديثة من مفهوم الأمن القومي؟ كذلك نتساءل عن أهم التجارب الدولية في مجال الأمن القومي والامن المعلوماتي؟

## خطة البحث

بناء على ما تقدم وفي سبيل الاتساق مع النهج الذي حددنا معالمه، ومن جانب الحرص على أن يتسم موضوعنا بالدقة المطلوبة، سنعمل على تناول ودراسة هذا الموضوع من خلال خطة البحث التالية؛ المطلب الأول: تأثير الأمن المعلوماتي على الأمن القومي. المطلب الثاني: تجارب دولية في التعامل مع الأمن المعلوماتي والأمن القومي

## المطلب الأول: تأثير الأمن المعلوماتي على الامن القومي

أصبحت المعلومات الالكترونية في وقتنا الحاضر ضرورة قومية ، وجب على جميع دول العالم احتضانها والعمل على إدراجها ضمن سياستها العامة، فغالبية المحتوى المعلوماتي لدول العالم أصبحت متوفرة على الشبكات الاتصال العالمية، يستطيع أي شخص الاطلاع عليها في أي وقت شاء ومن أي مكان شاء، لذلك أصبح لكل محتوى رقمي وجها معلوماتي لأي دولة وينبغي تبعا لذلك المحافظة عليه[34]، وهذا ما سوف يكون عنصر بحتنا في هذا المطلب وذلك عن طريق تقسيمه إلى فقرتين، الفقرة الأولى :التلازم بين الأمن المعلوماتي والأمن القومي، الفقرة الثانية : مخاطر الامن المعلوماتي على الامن القومي.

### الفقرة الأولى: التلازم بين الأمن المعلوماتي والأمن القومي

تكمن ذروة التفاعل بين الأمن المعلوماتي الالكتروني والأمن القومي في عقدنا الرقمي هذا في حماية العديد من المجالات الحيوية للدولة والتي يؤثر عدم أمنها على سلامة واستقرار آمن الدولة، بحيث يلعب الأمن المعلوماتي دورا مهم في توفير الأمن للعديد من المجالات سواء الداخلية منها أو الخارجية ونذكر منها.

#### أولا: الأمن القومي العسكري

تعمل مختلف الدول على ضمان أمنها سواء الداخلي أو الخارجي ، وذلك عن طريق الابتكارات التسلحية العسكرية في وقتنا الحاضر وربطها بوسائل الاتصال الحديثة و التحكم

[34]- وليد غسان سعيد جعلود، دور الحرب الالكترونية في الصراع العربي الاسرائيلي، رسالة ماجستير في التخطيط والتنمية السياسة بكلية الدراسات العليا في جامعة النجاح الوطنية نابلس، فلسطين2013، الصفحة: 54.

فيها عن بعد، ويعد المحتوى العسكري الحربي المعلوماتي الرقمي منه من أخطر الأبعاد تأثيرا على الأمن القومي لأي دولة في العالم، بحيث يلعب الأمن المعلوماتي دورا مهم في حماية تلك المعطيات التي تتسم في الغالب بالسرية وذلك عن طريق منع الوصول إليها أو الحصول عليها أو تغير محتويتها ، بحيث أن تلك المعلومات أصبحت في عصرنا الحالي تعرف تنافس و تسابق شديدين بين الدول سواء في الحصول عليها أو استغلالها الشيء الذي يضر بأمنها القومي إن استعملت تلك المعلومات الخاصة بها[35].

ويلعب الأمن المعلوماتي دورا مهم في تحقيق الأمن القومي، إذ بتحققه تتحقق مجموعة من الخدمات في المجال العسكري ومنها.

تحصين رأس الحربة والنواة المعلوماتية الأساسية للأمن القومي لأي دولة في العالم والمتلخصة بالمستوى الحربي والعسكري والتكتيكي التي تشكل رأس الهرم الأمني.

توفير الأمن المعلوماتي للمعلومات الحساسة ومن ضمان سريتها.

السرعة في تلبية الحاجات والتعامل مع المعلومات الطارئة.

سرعة انتقال المعلومة بين الأجهزة الاستخباراتية والعسكرية.

المرونة و سرعة اتخاذ القرارات[36].

[35]سليمان حسين مصطفى، نقل تقنيات المعلومات إلى الأقطار النامية، الإدارة العامة، العدد الرابع سنة 1987 الصفحة: 32.
[36] أبو زيد مرسي أبو زيد، تطور نظام الرقابة الالكترونية وتطورها لزيادة فاعلية الإدارة بالاستثناء، المجلة العربية للإدارة، العدد الثاني سنة 1987الصفحة: 57.

وفي هذا السياق نذكر إحدى الوقائع التي حددت أثناء قيام الحرب العالمية الثانية 37 (الحرب العمياء)، بحيث أن ألمانية كانت تتجسس على بريطانية بواسطة موجات الراديو واستطاعت قرأت تحركاتها وحجم قوتها وبناء على تلك المعلومات قامت بتوجيه ضربت جوية لها وتحقيق النصر لصالح السلاح الجوي الألماني.

## ثانيا: الأمن القومي الاقتصادي

يعد المجال الاقتصادي من أكتر القطاعات الوطنية عرضت للهجمات الإلكترونية، وذلك اعتبارا لطبيعة للمعلومات التي يحتويها، معلومات بنكية، معلومات في مجال البورصة، وحيث أن تعرض مثل هده المعلومات لأي هجوم قد يلحق الاقتصاد الوطني لتلك الدولة خسائر مادية كبيرة لا تعوض.

ويوفر الأمن المعلوماتي حماية مهمة لمجموعة من البرامج التطبيقية الالكترونية والتي تعتمد في طبيعة عملها على توفير مجموعة من البيانات والمعطيات المعالجة بشكل الالكتروني بحيث أن أي مساس بها تكون له أثار وخيمة، لذلك عملت مختلف الدول على تحصين هذه المعلومات سواء كانت تلك المعلومات تهم أشخاص (حسابات بنكية، معلومات شخصية)، أو شركات (عناوين الزبناء، مبلغ رأس المال،...) بكل الوسائل سواء التقني[38] منها أو القانوني[39].

وبتحقق الأمن المعلوماتي في المجال الاقتصادي تتحقق مجموعة من الأهداف والمزايا والتي منها.

---

[37] سنة 1944.
[38] التشفير مثلا.
[39] من خلال مجموعة من القوانين مثل القانون رقم 53.05.

تدعيم معلومات الاقتصاد المالي، وتوفير بيئة أمنة لتنظيم أعمالها خاصتا وأنه يحتوي جانبا كبيرا من العمليات القومية الاقتصادية لأي دولة في العالم، البورصات، بطائق الائتمان، قطاع البتروليات، سوق الأموال، الموازنة العامة، صناديق الاستثمار.

التشجيع على الاستثمار وجلب رؤوس الأموال الخارجية.

خلق تنافسية في السوق الوطنية و كذلك حتى الأسواق العالمية[40].

### ثالثا: الأمن القومي السياسي

يدخل في هدا المحتوى من البيانات الرقمية الالكترونية، المعلومات التي تخص الأحزاب السياسية وكذلك المعلومات البرلمانية ورئاسة الدولة، وأجهزتها السيادية والسياسية.

وتعتبر هذه المعلومات من أخطر البيانات الرقمية التي يجب توفير أمن معلوماتي لها لما تتصف به من حساسية، قد يؤدي المساس أو العبث بها إلى حرب أهلية أو دولية، وأن حمايتها أمر ضروري بحيث لا يمكن الحديث عن أمن قومي في غياب حماية معلوماتية لتلك البيانات.

ويحقق الأمن المعلوماتي مجموعة من الآليات السياسية داخل البلد.

تنظيم العمل السياسي والحزبي داخل الدولة.

المساهمة في تنظيم المصالح القومية الالكترونية [41].

[40] وليد غسان جعلود .م. س، ص: 58.
[41] وليد غسان جعلود .م. س، ص:55.

### رابعا: الأمن القومي البحثي

يتعلق هذا المحتوى الأمني القومي بالبيانات و المعلومات الخاصة بالمؤسسات البحثية والعمليات الجامعية والتي تشكل ثروة قومية مستقبلية تحتوي على العديد من الاكتشافات وبراءات الاختراع التي يجب حمايتها وصيانتها من كل الأساليب التي يمكن أن تتعرض لها من سرقة وقرصنة الالكترونية[42].

## الفقرة الثانية: مخاطر وتهديدات الأمن المعلوماتي على الامن القومي الحرب الالكترونية فنموذجا

أدت التطورات الحديثة في مجال تقنية المعلومات والاتصالات الى تبني التغير والتطوير في الادارة العامة والقطاع العام من خلال التحول الى تطبيق مفهوم الحكومة الالكترونية لكن هدة المتغيرات المتسارعة في مجال تقنية المعلومات والاتصالات وفرص التغير ترتبط بتأثيرات أو مخاطر محتملة[43] ومن بين الاخطار المحتملة ما أصبح يعرف في البيئة الرقمية بالحرب الالكترونية

### أولا: الحرب الالكترونية وآلية عملها

بفضل ثورة المعلومات ومع ظهور الإنترنت ومواقع الويب، ظهرت لدينا بيئة أخرى وهى الفضاء الإلكتروني، وعلى الرغم من أن هذه البيئة تختلف عن البيئات الثلاثة " الإقليم البرى، البحري، الجوي" ، ولكنها تشترك مع البيئات السابقة في بعض الخصائص، وأصبح

---

[42]وليد غسان جعلود .م. س، ص 56 .

[43]بركات بن مازن العتيبي، العوامل المؤثرة في زيادة المخاطر المحتملة لبرامج ومشروعات الحكومة الالكترونية، مقال منشور بمجلة الادارة العامة العدد 4 نونبر 2009الرياض الصفحة، 677.

الفضاء الإلكتروني أحد العناصر المؤثرة في النظام الدولي بما يحمل من أدوات تكنولوجية تلعب دور مهم في عملية التعبئة والحشد في العالم فضلا عن التأثير في القيم السياسية، والتأثير على نمط القوة، الحرب، الأمن[44].

## 1 مفهوم الحرب الالكترونية

لقد ادت الثورة التكنولوجيا الى تغير العديد من المفاهيم من بين هاته المفاهيم نجد مفهوم الحرب الالكترونية بحيث لم تعد الحرب كما كانت في السابق بمفهومها التقليدي القائمة في بيئة ملموسة وبأسلحة ملموسة بل اصبحت حربا من نوع اخر لها مجالها الخاص بها وبهذا فالحرب الالكترونية تعرف كالاتي:

تعرف الحرب الالكترونية بانها حرب تخيلية او افتراضية ذات طبيعة غير ملموسة تحاكي الواقع بشكل شبه تام وهي حرب بلا دماء بحيث تتلخص ادوات الصراع فيها بالموجهات الالكترونية والبرمجيات التقنية وجنود من برامج التخريب المحوسبة وطلقات من لوحات المفاتيح ونقرات المبرمجين في بيئة افتراضية تحاول ما امكن الوصول الى صورة حقيقية لملامح الحياة المادية والملموسة[45].

ويمكن تعريف الحرب الالكترونية كذلك بانها نظام قائم على الرعب المنتشر في الشبكة العنكبوتية والتي تهدف الى تنفيد العديد من الاعمال لترويع امن الافراد والجماعات

44-نسرين الشحات الصباحى على، الأبعاد العسكرية للقوة السيبرانية على الأمن القومي للدول دراسة حالة إسرائيل منذ عام 2010، مقال منشور بواسطة: المركز الديمقراطي العربى للدراسات الاستراتيجية والسياسية والاقتصادية بالموقع الالكتروني:
http://democraticac.de/?p=30962 تم الاطلاع عليه بتاريخ 2017/02/18 على الساعة 17.48
45 -كمال مساعد الحرب الافتراضية وسيناريوهات محكاة الواقع مقال منشور على شبكة الانترنت بالموقع الالكتروني
http://www.bebarmy.gov تم الاطلاع عليه بتاريخ 2017/02/17 على الساعة 17.07.

والمؤسسات والدول وارهاقهم اقتصاديا وادخالهم في ازمات نفسية واجتماعية ناتجة عما يعرف بالإرهاب الصامت[46].

كما تعرف الحرب الالكترونية كذلك بانها امتداد للحروب التقليدية المادية بحيث يتألف جندها من المدنيين والعسكريين في أن واحد كما انها حرب ادمغة بالدرجة الاولى كونها تستهدف في المقام الاول تدمير البينية المعلوماتية وتأخذ اشكالا عدة كشكل الاتصالات بين الجيوش وقيادتها واضعاف شبكات النقل والامدادات وضرب المعلومات والمعاملات الاقتصادية والعبث بالمحتويات الرقمية.

## 2 الية عمل الحرب الالكترونية

تتجه العديد من دول العالم لانتهاج سياسات تقنية ورقمية هادفة لإنشاء ادارات خاصة تعنى بهده الحروب العصرية كإنشاء مراكز متخصصة في ادارة شبكات الانترنيت تقوم الية عمل الحروب الالكترونية على عنصرين مهمين في صراع الكتروني قد ينشب في الفضاء الرقمي واول هدين العنصرين نجد المعلومات والتي ترتكز عليها الحروب الالكتروني بشكل كبير اما العنصر الثاني فيتمثل في القدرات العقلية والدهنية التي تكون مسؤولة عن تخطيط وتوجيه الضربات الالكترونية في عالم رقمي شديد التعقيد وزخم المعلومات[47].

فبتوفر كل من هدان العنصران للقيام الحرب الالكترونية تتم مجموعة من عمليات الحرب الالكترونية والتي تتمثل في:

[46] وليد غسان سعيد جعلود م س ص: 83.
[47] وليد غسان سعيد جعلود م س ص: 88.

### العمليات الهجوم الالكتروني

تنطلق هده الهجمات من قاعدة معلوماتية تقوم عليها معظم عمليات الحروب الالكترونية في العالم وهي العمليات المعلوماتية تهدف الى السيطرة على المعلومات الخصم، لمنعه من القيام بأي عمليات مسبقة، حيث يتم التركيز على ضرب معلوماته _ أي الخصم _ السياسية والاقتصادية والعسكرية لإلحاق الأضرار المادية والمعنوية النفسية به.

### ب: عمليات الدفاع الالكتروني

وتشمل الإجراءات والوسائل الوقائية وذلك للحد من ردة فعل الخصم المهاجم

وتتلخص هذه العمليات الدفاعية بالمنع والوقاية التي يهدف من خلالها حماية النظم المعلوماتية من الطرف المهاجم وتحدير هدا الاخير وتنبيهه وكشف الاختراقات الرقمية في حالة حدوتها ووضع الخطط الاستباقية الرامية لمنع وقوع اي اختراقات معلوماتية

### ج: عمليات استطلاع شبكات الحاسب الآلي

وهى القدرة على الدخول غير المشروع والتجسس على شبكات الخصم، دون تدمير البيانات بهدف الحصول عليها، وهى قد تشمل خطط دفاع عسكري، أسرار حرب عسكرية، معلومات استخباراتية، ويمتد أثرها إلى مدى بعيد مثل رسم خرائط لشبكات الحاسب الآلي واستخدامها مستقبلا في الهجوم الإلكتروني[48].

[48]نسرين الشحات الصباحي على م س (بدون ذكر الصفحة).

### ثانيا: أسلحة الحروب الإلكترونية

تتسلح الحروب الإلكترونية بالعديد من الأدوات والوسائل الّتقنية والرقمية، والتي يتم توظيفها في الصراعات الافتراضية الدائرة عبر الفضاء الإلكتروني، في صورةٍ مشابهةٍ للحروب التقليدية التي تندلع على أرض الواقع. تتنوع أدوات الحرب الإلكترونية باختلاف تأثيراتها، ومقدار قوتها، ومدى الآثار التي تخلفها، فمنها ما هو بسيط التأثير، ومنها ما هو أعلى من ذلك بكثير.

تبعًا لذلك، يمكن إجمال أهم أسلحة الحروب الإلكترونية وأساليبها وأدواتها، والتي يتم استخدامها عبر الفضاء الإلكتروني كوسائل للحرب الإلكترونية أو غير الإلكترونية، إلى ما يلي:

#### 1. التجسس المعلوماتي (Spyware Information)

تمثل وسائل التجسس الّتقني والمعلوماتي أحد أشهر وأقدم أسلحة الحروب الإلكترونية، فقد تم استخدام هذا السلاح منذ بداية الاستعمال الإنساني لوسائل الاتصال والتواصل[49]. تتخذ وسائل التجسس المعلوماتي عدة أشكال، منها ما يتم عبر التجسس والتنصت على المعلومات الصادرة من أجهزة الحواسيب، أو الصادرة عن المحطات الطرفية، أو اعتراض المراسلات الإلكترونية الصادرة عن الأقمار الصناعية، والهواتف المحمولة، وغيرها من وسائل التجسس المعلوماتي ذات الطابع القديم أو الحديث.

#### 2. الاختراق الإلكتروني (Penetration Mail):

وهي عبارة عن إنشاء نظامٍ أو برنامجٍ إلكتروني يهدف إلى استغلال معلومات الخصم وتدميرها، إضافة إلى إفساد نظامه الحاسوبي والآلي، وذلك بهدف التقدم عليه أمنيًا وعسكريًا

[49]- جاسم جعفر، مرجع سابق، ص171.

واقتصاديًا وسياسيًا، وقد تكون هذه المواجهة على المستوى الفردي، أو المؤسساتي، أو على مستوى الدول[50]. للاختراق الإلكتروني أشكالا عدة، لكن تتلخص جميعها بوظيفةٍ واحدة، وهي الدخول إلى قلب معلومات الخصم، والحصول عليها، مستخدمة لأجل ذلك، نظام محوسب يضرب البنية المعلوماتية للفئة المستهدفة.

### 3. زرع الفيروسات الّتقنية في البيئات المعلوماتية:

وهي عبارة عن برامج إلكترونية مدمرة، تعمل ضمن آلية معينة يحددها صانع هذه البرامج، ولها أشكال وأنواع متعددة .تهدف هذه الفيروسات الإلكترونية إلى إحداث فوضى في نظام تشغيل الضحية المنوي ضربه إلكترونيًا، وتلويث بيئتها لمعلوماتية، وذلك بغية تعطيل الوصول المعلوماتي للضحية، وفقدانه لغالبية مخزونه الرقمي، وربما ضرب الأجزاء المادية من أنظمة التشغيل الخاصة به.

### 4. القرصنة الإلكترونية:

تعتبر_ القرصنة_، من أضخم وأشمل الأسلحة الإلكترونية المستخدمة عبر الفضاء الرقمي .يشتمل هذا السلاح الّتقني على غالبية وسائل الصراع الإلكتروني في يومنا هذا، وذلك لشمولية مفهوم هو مضمونه، حيث تقوم آلية عمله على تجنيد العديد من الأشخاص المؤهلين والقادرين على التعامل معا لحاسوب بخبرةٍ ودرايةٍ عاليةٍ جدًا، تمكنهم من اقتحام مختلف الوسائل الاتصالية، والُنظم التكنولوجية، من حواسيب، وهواتف، وموجات، وألياف

ضوئية وغيرها .كما ويطلق على هؤلاء الأشخاص المؤهلين للعمل الحاسوبي والإلكتروني في عالم البرمجيات والإلكترونيات اسم الهاكرز؛(Hackers).

### 5. الرسائل الصامتة (Messages silent):

عبارة عن برمجة تقنية مخصصة للهواتف المحمولة الذكية من فئة الجيل الثالث *Third Generation * وهي رسائل يتم برمجتها بشكلٍ لا يشعر حاملا لهاتف أو المحمول بوصولها، بحيث تساعد مرسلها على التحديد الدقيق لمكان تواجد الشخص، وذلك عبر استخدام معادلة تقوم باحتساب قوة إشارة الموجات المنبعثة من الجهاز المحمول تبعًا لأقرب ثلاث مراكز مستقبلة لهذه الموجات .أحدثت هذه التّقنية العديد من الأزمات في المجتمعات الغربية، كونها تحوي جانبا من التعدي على الخصوصية، وهو ما أثر على نسبة مبيعاتها في العالم، علمًا أنها لاقت قبولا ورواجًا من قبل رجال الأمن في بعض دول العالم.

### 6. وسائل الإعلام (Media)

تلقى هذه الوسائل إقبالا عاليًا من قبل الجمهور المتلقي، نظرًا لسرعة انتشارها، وكثرة متابعيها، وتأثيرها على النفس البشرية .دخلت هذه الوسائل عالم الحروب الإلكترونية عبر فضائيات التلفزة، ومحطات البث المحلي الملتقطة عبر الراديو، ومواقع الفيديو الاجتماعي كاليوتيوب(YouTube) ، وغيرها من وسائل الإعلام الأخرى .

تستخدم العديد من دول العالم هذه الوسائل بشكلٍ كبير، خاصَّة في توجيه الخطابات السياسية، وهي سلاح متعدد الأطراف، يتم توجيهه إلى دولةٍ أو نظامٍ أو مجموعةٍ بغية تهديدها أو تحذيرها أو التأثير عليها نفسيًا ومعنويًا[51].

### 7. شبكات التواصل الاجتماعي (Social Networks):

وهي تركيباتٌ اجتماعيةٌ تقنيةٌ ذات محتوى رقمي، تقوم بربط الحلقات الاجتماعية بعضها ببعض، كالعمل والدين وغيرها، والتي تضم في طياتها مختلف الفئات العمرية، وجميع المستويات الاجتماعية والاقتصادية، وكافة الدرجات الثقافية والتعليمية.

استخدم هتلر البث التلفزي إبان الحرب العالمية الثانية لنشر خطاباته، وتحميس جنوده وجماهيره، وهي الصورة نفسها التي ركز عليها الخميني إبان الثورة الإسلامية في إيران، مستخدمًا لأجل ذلك ما عرف (بِالشريط الإسلامي). اتجه كلٌّ من هتلر والخميني إلى البث التلفزي آنذاك، لمعرفتهما بفائدة هذه الصورة الجديدة من الإعلام لاجتماعي في تمرير أهدافهما نحو الجمهور .وهو نفس المشهد الذي ألقى بظلاله اليوم على الصراع الّتقني الناشب عبر الفضاء الإلكتروني العالمي، ولكن بسلاحٍ جديد، وهو شبكات التواصل الاجتماعي.

تضم شبكات التواصل الاجتماعي باقة من المواقع ذات النفوذ القوي عبر العالم، من أشهرها :الفيسبوك(Facebook) ، تويتر (Twitter) ، اليوتيوب (YouTube) المدونات الإلكترونية (Blogs)، وغيرها الكثير.

تعد هذه المواقع من أكثر البيئات تناسبًا وتناغمًا مع الحروب الإلكترونية، وأكثرها اصطدامًا وصراعًا، فلقد تكون هذه الشبكات هي وجها للصراع الإلكتروني القائم الآن في

[51]- اليحياوي يحيى، حرب الإعلام الوقائية، في موقع الكاتب يحيى اليحياوي على شبكة الإنترنيت، د.ت.
http://www.elyahyaoui.org/guerre-info.htm تم الاطلاع عليه بتاريخ 2017/02/19 على الساعة 20.00

عقدنا التّقني هذا، باعتبارها سهلة الوصول والاستخدام، وتفاعلية وشعبية بشكلٍ كبير، ومتطورة بوتيرةٍ مرتفعة .ومن المآخذ عليها أنها ذات طابع اصطيادي، أي يمكن من خلالها الإيقاع بالضحايا الإلكترونيين، إلا أنها وفي المقابل، منبرًا حاشدًا للتغيير السياسي.

### 8. الأقمار الاصطناعية (Satellites):

وهي أسلحةٌ ذات دلالاتٍ استحواذيه، هدفها السيطرة على أكبر قدرٍ ممكنٍ من المعلومات، وذلك عبر التقاط ملايين الصور للهدف، وإرسالها للقاعدة المعلوماتية الموجودة على الأرض.

تعتبرا لأقمار الاصطناعية من أكفئ الوسائل التّقنية، وأكثرها تعقيدًا في حسم المعارك، فهي قادرًة على توجيه الصواريخ والقاذفات النارية صوب أهدافها على الأرض، وقد بلغت ذروة استخدامها إبان الحرب الباردة، والتي هددت العالم باندلاع حربٍ كونيةٍ ثالثة. كما وُتستخدم اليوم في التشويش على المحطات الفضائية، ومنعها من البث، وذلك بأجندةٍ وأهداف سياسية، في تعبيرٍ جديدٍ عن الحرب الإلكترونية الدائرة في العالم الافتراضي، كالتشويش الذي تعرضت له بعض القنوات الفضائية العربية (العربية، الجزيرة) خلال الثورات العربية.

وكذلك تمكن الأقمار الصناعية من اعترض الرسائل وتشويش الاتصالات والتنصت على المكالمات[52].

[52]- ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، المطبعة والوراقة الوطنية، الطبعة الأولى، سنة 2011 ، ص263.

### 9. الحقيبة الكهروستاتيكية (Electrostatic bag):

أحد أنوع التكنولوجيات العسكرية وهي عبارة عن أجهزةٍ صناعيةٍ على شكل حقائب صغيرة، تقوم بتوليد نبضات كهرومغناطيسية فائقة الُقدرة، يمكن من خلالها تدمير الوحدات الالكترونية في أيةِ إدارةٍ أو محطة إرسال، مما يفقدها قدرتها العملية والإنتاجية والتشغيلية، هناك أبحاثًا جارية على هذه الحقيبة، وذلك بهدف تطوير نواتها الخاصة، والتي تسمى الميكروبات إلكترونية، بحيث يتم تصويبها ضد الّتقنيات السيليكونية، بغية تدمر المعدات الالكترونية الخاصة بها.

### 10: الخداع الإلكتروني (E-Deception):

وهو من أهم وسائل تأمين الصراعات الإلكترونية، وبه تحقق المعارك الإلكترونية عنصر المفاجأة .يشتمل هذا السلاح الرقمي على عدة وسائل، أهمها :التقليد الصوتي، التشويش الإلكتروني، التضليل المعلوماتي، الخداع ونشر الشائعات، انتحال الشخصيات افتراضيًا، الابتزاز الإلكتروني، وغيرها من أساليب الخداع الرقمية.

### 11: الطائرات الإلكترونية (دون طيار)

دخلت هذه الطائرات الحرب الإلكترونية، لُتشكل فوارق عديدةٍ في قدرات الجيوش، ومدى امتلاكها للمنظومات المعلوماتية، والتي تؤهلها لتحقيق ما بحوزتها من أهدافٍ موضوعةٍ في بنكها المعلوماتي .تمتلك هذه الطائرات قدراتٍ عاليةٍ على التصوير والمراقبة، وحتى القصف بشتى أنواع القنابل . كما وتشكل حلقات وصلٍ بين القاعدة المعلوماتية الموجودة على الأرض، وساحة العمليات الحربية الكامنة في المجال الجوي والافتراضي، عبر مختبرٍ للتحليل المعلوماتي، والذي يمكنها من تحديد نيرانها بدقة.

## 12: الارهاب الالكتروني

أصبح مفهوم الارهاب واضح الى حد ما فان الارهاب الالكتروني كمفهوم مستحدث لا يزال يكتنفه الغموض ذلك انه يعتمد على تقنية انظمة المعلومات من حيث وسيلة ارتكابه ومن حيث دور الفاعل فيه وطبيعة سلوكه وهو ايضا ووفقا لذلك يوقع نتائج تطال امن المعلومات وتقنية انظمة المعلومات بالإضافة الى ما يتسبب به من اضرار واسعة الانتشار عظيمة الاثر على المجتمع وافراده[53].

ويمكن أن يعرف الإرهاب الإلكتروني بأنه استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو أنه القيام بمهاجمة نظم المعلومات بدوافع سياسية أو عرقية أو دينية. وقد عرّفت الأمم المتحدة في أكتوبر 2012 الإرهاب الإلكتروني بأنه "استخدام الانترنت لنشر أعمال إرهابية."

ويمكن شرح مفهوم "الإرهاب الإلكتروني" بأنه العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول، أو الجماعات أو الأفراد على الإنسان، في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله ، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الإفساد.

لقد بات "الإرهاب الإلكتروني "CyberTerrorism" يُمثل تهديداً واضحاً للأمن القومي للدول، حيثُ أصبحت البنية التحتية لأغلب المُجتمعات الحديثة تُدار عن طريق أجهزة الحاسب الآلي

[53] جلال محمد الزعبي و اسامة احمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية دراسة مقارنة الطبعة الاولى دار الثقافة للنشر والتوزيع عمان سنة 2010 الصفحة: 276.

والإنترنت، وهو ما يُعرّضها لهجمات مُتعددة من"الهاكرز" و"المُخترقين" بشكل عام، ومن أجهزة المخابرات والمنظمات الإرهابية بشكل خاص.

## المطلب الثاني: تجارب دولية في التعامل مع الامن المعلوماتي القومي

سارت دول العالم بعد الثورة الّتقنية نحو إدراج الابتكارات الإلكترونية ضمن سياساتها الأمنية لحماية أمنها القومي، وهو أمر لم توفره غالبية دول العالم في خططها الإستراتيجية والمستقبلية، مما أدخلها في مستنقع التبعية التكنولوجية.

سنحاول من خلال هذا المطلب التطرق الى تجارب بعض الدول العربية وكذلك سنتطرق الى تجارب بعض الدول الأجنبية الرائدة في المجال المعلوماتي وذلك على الشكل التالي

### الفقرة الألى: التجربة العربية في التعامل مع الأمن المعلوماتي القومي

يعتبر الامن المعلوماتي ركيزة من الركائز التي يقوم عليها الامن القومي لكل بلد فالأمن المعلوماتي يمكن ان يؤثر سلبا او ايجابا على الامن القومي

سنحاول من خلال هذه الفقرة رصد كل من التجربة المغربية والفلسطينية في مجال الامن المعلوماتي والقومي

## أولا: التجربة المغربية في التعامل مع الأمن المعلوماتي القومي

تعتبر التجربة المغربية في مجال الامن المعلوماتي تجربة رائدة سواء في شقها القانوني او التقني او المؤسساتي.

سنحاول من خلال هذا الفقرة رصد كل من الشق القانوني والتقني والمؤسساتي وذلك على الشكل التالي:

### 1 الحماية القانونية للأمن المعلوماتي القومي

توفر الترسانة التشريعية المغربية حماية جد اساسية للأمن المعلوماتي القومي وذلك من خلال زجر كل من تسول له نفسه ارتكاب جرائم تمس نظم المعلومات المغربي

سنحاول التطرق للحماية القانونية من خلال كل من القانون 07.03 المتعلق بالمس بنظم المعالجة الالية للمعطيات وكدلك من خلال القانون 03.03 المتعلق بمكافحة الارهاب ودلك على الشكل التالي:

#### أ: على مستوى القانون رقم 07.03 المتعلق بالمس بنظم المعالجة الالية للمعطيات [54]

ينص الفصل 607-4 من مجموعة القانون الجنائي على ما يلي:

[54]-اضيف هذا الفرع بمقتضى الفصل الثاني من الظهير الشريف بمثابة قانون رقم 1.74.232 بتاريخ 28من ربيع الثاني 1394الموافق ل 21ماي 1974 يغير ويتمم بموجبه الفرع الرابع من الكتاب الثالث من القانون الجنائي.

دون الإخلال بالمقتضيات الجنائية الأشد، يعاقب بالحبس من ستة أشهر إلى سنتين وبالغرامة من 10.000 إلى 100.000 درهم كل من ارتكب الأفعال المشار إليها في الفصل السابق [55]في حق مجموع أو بعض نظام للمعالجة الآلية للمعطيات يفترض أنه يتضمن معلومات تخص الأمن الداخلي أو الخارجي للدولة أو أسرارا تهم الاقتصاد الوطني.

دون الإخلال بالمقتضيات الجنائية الأشد، ترفع العقوبة إلى الحبس من سنتين إلى خمس سنوات وبالغرامة من 100.000 إلى 200.000 درهم إذا نتج عن الأفعال المعاقب عليها في الفقرة الأولى من هذا الفصل تغيير المعطيات المدرجة في نظام للمعالجة الآلية للمعطيات أو حذفها أو اضطراب في سير النظام، أو إذا ارتكبت الأفعال من طرف موظف أو مستخدم أثناء مزاولة مهامه أو بسببها، أو إذا سهل للغير القيام بها

ما يمكن ملاحظته عن هذا الفصل هو أن المشرع المغربي وفر حماية قانونية للأمن المعلوماتي القومي وذلك من خلال تنصيصه على ان العقوبة تشدد في حالة ارتكاب الافعال المجرمة المنصوص عليها في الفصل 607-3 في حق مجموع أو بعض نظام للمعالجة الآلية للمعطيات يفترض أنه يتضمن معلومات تخص الأمن الداخلي أو الخارجي للدولة أو أسرارا تهم الاقتصاد الوطني.

[55]الفصل 607 -3 يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من 2.000 إلى 10.000 درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام للمعالجة الآلية للمعطيات عن طريق الاحتيال.
ويعاقب بنفس العقوبة من بقي في نظام للمعالجة الآلية للمعطيات أو في جزء منه، كان قد دخله عن طريق الخطأ وهو غير مخول له حق دخوله.
تضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام للمعالجة الآلية للمعطيات أو اضطراب في سيره.

كما نلاحظ أن العقوبة المنصوص عليها في الفقرة الأولى رهينة بإتيان الفعل المجرم دون إن تترتب عنه أية نتائج. اما في الحالة التي يترتب عن الافعال الاجرامية التي تمس نظم المعالجة الالية للمعطيات نتائج حددها المشرع المغربي في الفقرة الثانية من الفصل 607-4 والتي تتمثل في تغيير المعطيات المدرجة في نظام للمعالجة الآلية للمعطيات أو حذفها أو اضطراب في سير النظام، أو إذا ارتكبت الأفعال من طرف موظف أو مستخدم أثناء مزاولة مهامه أو بسببها، أو إذا سهل للغير القيام بها فان العقوبة ترفع إلى الحبس من سنتين إلى خمس سنوات وبالغرامة من 100.000 إلى 200.000 درهم.

كما نجد ان المشرع المغربي لم يكتف برفع العقوبة في حالة ارتكاب الافعال فيما يمكن أن يهدد الامن القومي بل جرم افعال اخرى من شانها ان تهدد الامن القومي وهو ما نص عليه الفصل 607-10.

يعاقب بالحبس من سنتين إلى خمس سنوات وبالغرامة من 50.000 إلى 2.000.000 درهم كل من صنع تجهيزات أو أدوات أو أعد برامج للمعلوماتيات أو أية معطيات أعدت أو اعتمدت خصيصا لأجل ارتكاب الجرائم المعاقب عليها في هذا الباب أو تملكها أو حازها أو تخلى عنها للغير أو عرضها أو وضعها رهن إشارة الغير.

وفي الاخير نود الاشارة الى ملاحظتين وهما كالاتي:

المشرع المغربي عاقب على مجرد المحاولة إذا ارتكبت في إطار الفصل 607-4 وهذا ما نص عليه الفصل 607-8 رغم خطورة هده الافعال التي تهدد الامن القومي المغربي إلا أن المشرع

عاقب عليها كحد اقصى بعقوبة تتراوح بين سنتين وخمس سنوات ما يجعلها جنحة تأديبية في حين إذا ما رجعنا إلى نفس الجريمة في صورتها التقليدية نجد ان المشرع شدد العقوبة واعتبرها جناية وهذا ما يستشف من الفصل 181 الذي ينص على ما يلي يؤاخذ بجناية الخيانة، ويعاقب بالإعدام، كل مغربي ارتكب، في وقت السلم أو في وقت الحرب، أحد الأفعال الآتية:

4 - سلم إلى سلطة أجنبية أو إلى عملائها، بأي شكل كان وبأية وسيلة كانت، سرا من أسرار الدفاع الوطني أو تمكن بأية وسيلة كانت، من الحصول على سر من هذا النوع، بقصد تسليمه إلى سلطة أجنبية أو إلى عملائها.

قام المشرع المغربي بتحديد المقصود بسر من اسرار الدفاع الوطني من خلال الفصل187.

تعتبر من أسرار الدفاع الوطني في تطبيق هذا القانون:

1 - المعلومات العسكرية أو الدبلوماسية أو الاقتصادية أو الصناعية التي توجب طبيعتها أن لا يطلع عليها إلا الأشخاص المختصون بالمحافظة عليها، وتستلزم مصلحة الدفاع الوطني أن تبقى مكتومة السر بالنسبة إلى أي شخص آخر.

2 - الأشياء والأدوات والمحررات والرسوم والتصميمات والخرائط والنسخ والصور الفوتوغرافية أو أي صور أخرى أو أي وثائق كيفما كانت، التي توجب طبيعتها أن لا يطلع عليها

إلا الأشخاص المختصون باستعمالها أو المحافظة عليها وأن تبقى مكتومة السر بالنسبة إلى أي شخص آخر لكونها يمكن أن تؤدي إلى كشف معلومات من أحد الأنواع المبينة في الفقرة السابقة.

3 - المعلومات العسكرية، من أية طبيعة كانت التي لم تنشر من طرف الحكومة ولا تدخل ضمن ما سبق والتي منع نشرها أو إذاعتها أو إفشاؤها أو أخذ صور منها إما بظهير وإما بمرسوم متخذ في مجلس الوزراء.

4 - المعلومات المتعلقة إما بالإجراءات المتخذة للكشف عن الفاعلين أو المشاركين في جنايات أو جنح ضد أمن الدولة الخارجي، أو القبض عليهم، وإما بسير المتابعات والتحقيقات وإما بالمناقشات أمام محكمة الموضوع.

وهذا ما يعني بان المعلومات التي يمكن الحصول عليها من خلال الدخول الى مجموع أو بعض نظام للمعالجة الآلية للمعطيات او البقاء فيه والتي اعتبرها المشرع جنحة تأديبه في صورتها التقليدية تعتبر جناية ويعاقب عليها بالإعدام. فقط الاختلاف يكمن في الوسيلة التي تم بها الحصول على المعلومات التي يمكن ان تكون سر من اسرار الدفاع الوطني اما النتيجة فهي واحدة.

### ب على مستوى القانون رقم 03.03 المتعلق بالإرهاب[56]

حدد المشرع المغربي مجموعة من الافعال التي اعتبرها افعال ارهابية بمقتضى الفصل 218-1 من القانون الجنائي بحيث نص على ما يلي:"

تعتبر الجرائم الآتية أفعالا إرهابية، إذا كانت لها علاقة عمدا بمشروع فردي أو جماعي يهدف إلى المس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف.

### 7. الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات

وبهذا فان المشرع المغربي تكريسا للأمن المعلوماتي القومي جعل من جريمة المس بنظم المعالجة الالية للمعطيات ادا ما ارتكبت عمدا وكانت لها علاقة بمشروع فردي أو جماعي يهدف إلى المس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف جريمة ارهابية. تطبق عليها مقتضيات القانون رقم 03.03 التعلق بمكافحة الإرهاب.

والملاحظ ان المشرع المغربي لم يكتف بجعل المس بنظم المعالجة الية المعطيات فعلا ارهابيا بل جعل كدلك الاشادة بالأفعال الارهابية عبر الوسائط الالكترونية فعلا مجرما وهذا ما يستشف من مقتضيات الفصل 218-2 من مجموعة القانون الجنائي الذي نص على ما يلي:

[56] اضيف هذا الباب بمقتضى المادة الاولى من الباب الاول من القانون رقم 03.03 المتعلق بمكافحة الإرهاب.

يعاقب بالحبس من سنتين إلى ست سنوات وبغرامة تتراوح بين 10.000 و200.000 درهم كل من أشاد بأفعال تكون جريمة إرهابية بواسطة الخطب أو الصياح أو التهديدات المفوه بها في الأماكن أو الاجتماعات العمومية أو بواسطة المكتوبات والمطبوعات المبيعة أو الموزعة أو المعروضة للبيع أو المعروضة في الأماكن أو الاجتماعات العمومية أو بواسطة الملصقات المعروضة على أنظار العموم بواسطة مختلف وسائل الإعلام السمعية البصرية والإلكترونية.

## 2 الحماية التقنية للأمن المعلوماتي القومي

لقد ازدادت اهمية ضمان سرية المعطيات المتبادلة بشكل الكتروني في العصر الحالي وذلك بفعل تطور وسائل التكنولوجيا الحديثة للاتصال الشيء الذي أدى الى اتباع طرق عديدة لضمان امن وسرية تلك المعطيات سواء بالنسبة لطرق تبادلها أو تخزينها عبر الوسائط الالكترونية، ومن بين اهم هذه الوسائل الحديثة المستعملة في حماية تلك المعطيات، التشفير المعلوماتي، التوقيع الالكتروني، المصادقة الالكترونية

### أ: التشفير المعلوماتي

يعد التشفير من أقدم الوسائل الحمائية التي استخدمها الانسان في ضمان حماية رسائله وتمام سريتها، وبلغ التشفير دروته خلال الحرب العالمية الثانية، وذلك عبر ادخال التقنية المعلوماتية عليه، بحيث اصبحت تستخدم لإرسال رسائل مشفرة عبر الوسائط الالكترونية دون إمكانية اضطلاع الغير على محتوياتها، وتعتمد تقنية التشفير المعلوماتي في عملها على مجموعة من الطرق والاليات و التي من بينها.

**التشفير المتماثل:** ويطلق عليه كذلك التشفير بواسطة المفتاح الخاص، وتقوم هذه العملية من التشفير على استخدام كل من المرسل والمرسل اليه المفتاح الذي تم اعداده خصيصا لتشفير الرسالة وفك الشفرة بنفس المفتاح.

التشفير اللا متماثل: وتقوم هذه العملية على مفتاحين مختلفين تربط بينهما علاقة رياضية متينة، أحدهما يسمى المفتاح العام والاخر يسمى المفتاح الخاص.

ومن خلال هذين المفتاحين يمكن تشفير الرسالة بالمفتاح وفك شفرتها بمفتاح اخر، مثلا تم تشفير الرسالة بواسطة المفتاح العام فانه يلزم لفك شفرتها المفتاح الخاص، وهذا النوع من التشفير لا يتطلب ارسال المفتاح العام لان كل من المرسل والمرسل والمرسل إليه يبقى محتفظا بمفتاحه الخاص [57].

## ب: التوقيع الالكتروني

لم يعرف المشرع المغربي عكس قانون الاونسترال النموذجي التوقيع الالكتروني ويعرف هذا الاخير بأنه بيانات في شكل الالكتروني مدرجة في رسالة بيانات أو مضافة اليها او مرتبطة بها منطقيا يجوز أن تستخدم لتعين هوية الموقع بالنسبة الى رسالة البيانات و لبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات[58] و للتوقيع عدة أنواع :

[57] عبد الحكيم زروق، تنظيم التبادل الالكتروني للمعطيات القانونية عبر الانترنيت، سلسلة الشؤون القانونية والمنازعات رقم7، دار الامان الرباط، الطبعة الاولى 2016 ص 416 - 417.

58 عبد الرحيم بن بوعيدة ضياء علي احمد نعمان موسوعة التشريعات الالكترونية المدنية والجنائية الجزء الثاني المطبعة والوراقة الوطنية مراكش الطبعة الأولى، 2010الصفحة 392.

التوقيع الرقمي: وهو عبارة عن مجموعة الارقام تقوم على معادلة رياضية من شأنها تحويل المعلومات الموجودة في رسالة البيانات الى رموز مشفرة لا يمكن لا شخص قراءتها ما لم يفك التشفير، بمعنى ان قراءتها تبقى مقصورة على الشخص الذي يمتلك المفتاح الذي يفتح هذا التشفير ويحتفظ بها لنفسه دون غيره.

إدن المعاملات الالكترونية التي تتم عن طريق تبادل رسائل بيانات بين الاطراف بشكل مشفر تضمن لها درجة عالية من المصداقية والثقة بفضل التوقيع الرقمي خاصتا عندما نعلم بوجود جهة مختصة تقوم بتوثيق التوقيعات الالكترونية و تصديقها[59] .

التوقيع البيومتري: يعتمد هدا النوع من التوقيع على الخصائص البيولوجية لجسم الانسان بصمة صوت ، بصمة معالم الوجه ، بصمة العين، بصمة الاصابع ، وبدلك تختلف من شخص لا اخر تطابقها لذى شخصين الشيء الذي يمنح هذا النوع من التوقيع درجة عالية من الموثوقية التي تدفع المتعامل الكترونيا باعتماده[60].

التوقيع بالرقم السري : يتم هذا النوع من التوقيع بإدخال رقمه السري فتتم المطابقة بين رقم سري مخزن في ذاكرة الحاسب الالي لمقدمي الخدمة المعلوماتية لتحقق من وجود المطابقة بين الرقمين للقول بصحة التوقيع من عدمه[61] .

[59]سكينة بن الشيخ الامن القانوني المعلوماتي رسالة لنيل دبلوم الماستر في العلوم الجنائية جامعة القاضي عياض كلية الحقوق مراكش 2015/2014 الصفحة: 97.

[60] احمد برادة غزيول قراءة في القانون المتعلق بالتبادل الالكتروني للمعطيات القانونية مجلة المعيار العدد31 يونيو 2008 الصفحة: 16.

[61]سكينة بن الشيخ، م س، ص: 98.

### ج: المصادقة الالكترونية

استنادا الى المادة 20 من القانون 53.05 المتعلق بالتبادل الالكتروني للمعطيات القانونية حدد المشرع المغربي الجهة المعتمدة من طرف الدولة والمختصة دون غيرها بإصدار الشهادات الالكترونية وتسليمها وتدبير الخدمات المتعلقة بها وفقا لما هو منصوص عليه قانونا وتتمثل هذه الجهة في مقدم خدمة المصادقة الالكترونية

وحسب المشرع المغربي يكون مقدم خدمات المصادقة الالكترونية في شكل شركة يوجد مقرها الاجتماعي في تراب المملكة، مع امكانية اعتماد من يوجد مقرهم بالخارج شرط ان تكون الدولة التي يمارسون نشاطهم بترابها تجمعها بالمغرب اتفاقية للاعتراف المتبادل بمقدمي خدمات المصادق الالكترونية

علاوة على دلك ينبغي ان يتوفر في مقدم خدمة المصادقة الشروط التالية

_الوثوق بخدمة المصادقة التي يقدمها

_سرية المعطيات المتعلقة بإنشاء التوقيع الالكتروني

_السيطرة على اداة التوقيع

وامام تنامي الارهابية الامن المغربي فقد اعطى المشرع المغربي الحق في منح الاعتماد لإصدار شواهد المصادقة الى الادارة العامة الدفاع الوطني بعد ان كان الامر مخولا الى الوكالة الوطنية لتقنين المواصلات

بهدف ضمان المتعاملين بشكل الكتروني بصفة خاصة ويحمي مصالحهم ومن جهة ثانية الحفاض على امن الدولة الداخلي و الخارجي[62].

### 3 الحماية المؤسساتية للأمن المعلوماتي القومي

بالإضافة الى الحماية القانونية والتقنية للامنا لقومن المعلوماتي فلقد قام المشرع المغربي بإحداث مؤسسات تعنى بالبحث والتحقيق عن الجريمة المعلوماتية ومتابعة مرتكبيها وهده المؤسسات هي كالاتي:

#### أ- وحدة الجرائم المعلوماتية التابعة للفرقة الوطنية لشرطة القضائية

تعمل هذه الوحدة تحت اشراف مهندسين وتقنين مختصون في الهندسة المعلوماتية لشبكة الانترنت جهزت هذه الوحدة بإحداث تقنيات الرصد والبحث المعلوماتي، وتتلخص مهام هذه الوحدة في تقديم الدعم المعلوماتي لعناصر الشرطة القضائية، معالجة الجرائم المعلوماتية، توفير الدعم التكتيكي للمصالح الخارجية لشرطة القضائية في الابحاث المنجزة

[62] خليهنا فتوح المصادقة الالكترونية مقال منشور على الموقع الالكتروني التالي:
http://www.marocdroit.com تم الاطلاع عليه بتاريخ 18/02/2017 على الساعة 20.12.

من هذا النوع من الجرائم، وقد جاء احداث هذه الوحدة لمواكبة تطورات الجرائم الالكترونية[63].

### ب- وحدة الجرائم المعلوماتية التابعة للمديرية العامة للأمن الوطني على الصعيد المركزي

تختص هذه الوحدة بتجميع وتحليل جميع انواع الجرائم المعلوماتية المرتكبة على الصعيد الوطني والدولي ومساعدة المصالح الخارجية في الامور التقنية المرتبطة بالتحقيقات وتتبع ورصد مرتكبي الجرائم المعلوماتية [64]

### ج- المديرية العامة لأمن نظم المعلومات التابعة لإدارة الدفاع الوطني

تتولى هذه المديرية مهام تسليم التراخيص وتدبير التصاريح المتعلقة بوسائل وخدمات التشفير والمصادقة على انظمة احداث وتأكيد سلامة التوقيع الالكتروني وقد تم اسناد هذه المهام الى المديرية العامة لأمن نظم المعلومات نظرا للعلاقة الوثيقة لهذه مع امن وسلامة نظم المعلومات[65].

## ثانيا: التجربة الفلسطينية للأمن المعلوماتي القومي

يحتل الصراع الفلسطيني الإسرائيلي المشهد العام والرئيسي للعصر الحديث، وأخذ هذا الصراع يواكب التطورات التسلحية المتمثلة في الحرب المعلوماتية بين فلسطين وإسرائيل، وفي

---

[63]سكينة بن الشيخ، م س، الصفحة: 153.
[64]سكينة بن الشيخ، مرجع سابق، الصفحة: 154.
[65]سكينة بن الشيخ، م س، ص: 154.

تبادل الهجمات الالكترونية نحو الأمن المعلوماتي لكل من الطرفين، مما دفعهم إلى اعتماد الوسائل الممكنة للتصدي للهجمات من أجل تحقيق الأمن القومي المعلوماتي.

تعيش فلسطين كباقي الدول العربية ونتيجة للاحتلال الإسرائيلي وما يفرضه من قيود على جميع المقدرات المادية والمعنوية تعيش حالة من الفراغ التكنولوجي والتي قامت عليها اتفاقية أوسلو[66] في عام 1993، لذلك يمكن إلقاء نظرة على الوضع التقني والمعلوماتي الفلسطيني قبل الاتفاقية وبعدها[67].

### 1: قبل الاتفاقية اوسلو

خضعت قطاعات الاتصال بكافة أشكالها إلى سيطرة الاحتلال الإسرائيلي والذي عمل على إبقاء الشعب بعيدا عن تحقيق أمنه القومي حيث احتكرت إسرائيل شركات بيع الحاسوب والتكنولوجيات الأخرى وفرض رقابة شديدة على شبكات الأنترنت العاملة في فلسطين، حيث كانت الشركات التي تعمل على تزويد الجماعات والبلديات الفلسطينية والمؤسسات التجارية بالحواسيب الالكترونية يسمح لها بذلك بتصريح إسرائيلي.

### 2 : بعد اتفاقية أوسلو

تسلمت السلطة الفلسطينية قطاع المعلومات والاتصالات التي أدارته شركة إسرائيلية ينرك كانت الخدمات التي تقدمها هذه الشركة دون المستوى المطلوب، لتكون هناك محاولات فلسطينية أكثر تطورا فيما يخص قطاع المعلومات والاتصالات الفلسطيني، كإنشاء وزارة

[66] اتفاقية اسلوا لسنة 1994.
[67] وليد غسان جعلود، م س، ص 67.

للقطاع التكنولوجي في فلسطين، ومعهدا وطنيا لتكنولوجيا المعلومات وشركات للاتصال الفلسطينية بال تل وشركة أنظمة الحاسبات والاتصالات وغيرها من الشركات، إلا أنها لم تكترث بعد توقيع الاتفاقية إلى أهمية ربط أمنية معلوماتها بالأمن القومي الفلسطيني، بل ظلت معتمدة عليها في تزويدها بالتطورات التقنية .

ونتيجة للتبعية الاقتصادية والتكنولوجية للعالم العربي للدول المتقدمة اقتصاديا وعسكريا وتكنولوجيا مما جعلها دولا استهلاكية بامتياز لجميع المنتجات ومن بينها الوسائل والبرامج المعلوماتية في شتى المجالات ومن بينها المؤسسات السياسية العسكرية و دون أن تدرك خطر ذلك على أسرار الدولة وأمنها القومي.[68]

### 3 الفضاء الالكتروني الفلسطيني الرسمي

مع دخول السلطة الفلسطينية عام 1994 إلى مناطق حكمها الذاتي المتفق عليها ضمن اتفاقية أوسلو، وبداية العمل في المؤسسات الفلسطينية بشكل رسمي شكلت مؤسسات خاصة لتكنولوجيا المعلومات في فلسطين، كوزارة الاتصالات وتكنولوجيا المعلومات الفلسطينية، وتسخير وسائل تكنولوجية الاتصالات والمعلومات لدعم التنمية الشاملة والمستدامة في فلسطين، إلا أن هذه الرؤية التي اعلنت حالت دون تكوين فضاء الكتروني فلسطيني مستقل أو منافس لإسرائيل، أهمها التغلغل الاسرائيلي التقني في فلسطين، عبر الشركات الإسرائيلية العاملة في مجالات تكنولوجيا المعلومات وأجهزة المحمول ومحطات البث الإذاعي والتلفزي ومحطات التزويد بخدمات الأنترنت والهاتف، بحيث يمكن لأي جندي

[68] وليد غسان جعلود، م س، ص 141.

إسرائيلي معرفة كافة بيانات أي مواطن فلسطيني مما يجعل الفضاء الالكتروني الفلسطيني يعيش حالة شبه الفوضى، وسهل الاختراق من قبل الهجمات الإسرائيلية.

وأمام ضعف الأمن المعلوماتي الفلسطيني، عملت إسرائيل على تطوير نظريتها الأمنية ضمانا لأمنها في المنطقة العربية من المقاومة الفلسطينية، والهجمات العربية، وترتكز النظرية الأمنية الإسرائيلية على مجموعة من المرتكزات البشرية والتقنية والتنظيمية، حيث عملت على إنتاج العديد من الأقمار الاصطناعية، أهمها الأقمار الاصطناعية آفاق، مجموعة تكسات، ايروسا، للتجسس على المقاومة الفلسطينية والعالم العربي الإسلامي بالإضافة إلى الأجهزة المخابراتية المعلوماتية الإسرائيلية وهي جهاز الأمن الداخلي الإسرائيلي الشاباك، وشعبة الاستخبارات العسكرية الإسرائيلية أمان، وجهاز الأمن الخارجي الإسرائيلي الموساد، وتقوم هذه الأجهزة باختراق الانظمة المعلوماتية الفلسطينية و بجمع المعلومات الاستخباراتية وتحليلها بشكل معلوماتي وأمني ومن تم تقديمها للجهات المختصة بالأمن الاسرائيلي وردا على هذه الهجمات تشكل فضاء معلوماتي غير رسمي للدفاع عن فلسطين.

### 4 الفضاء الالكتروني غير الرسمي

يضم الفضاء الالكتروني غير الرسمي الفضاء الالكتروني الفلسطيني والفضاء الالكتروني العربي.

هذا الفضاء الالكتروني يفضح ممارسات الإسرائيلية وينشرها في الساحة الإعلامية الدولية، عبر صفحات ومواقع التواصل الاجتماعي والمواقع الإعلامية عبر شبكة الأنترنت ايضا تمكن الشباب الفلسطيني وباقي شباب الدول العربية من استعمال الاختراقات الالكترونية

كسلاح رقمي ضد المواقع والصفحات الاسرائيلية، وكشف معلوماتها السرية وإلحاق الأذى النفسي والمعنوي والمادي بأي تواجد رقمي يخضع للسيطرة الإسرائيلية.

## الفقرة الثانية: التجربة الاجنبية في التعامل مع الامن المعلوماتي القومي

في كل مرحلة من مراحل التطورات النظام الدولي تسود منظومة فكرية مهيمنة التي تشكل اساس تفسير واقع العلاقات الدولية فالعصر الوسيط شهد هيمنة فكرة الدين ثم جاء عصر التنوير ليشهد هيمنة فكرة العقل بعد ذلك جاءت مرحلة القرنين التاسع عشر و العشرين ليشهد هيمنة النزاعة القومي إلى ان وصلنا الألفية الثالثة لتهيمن عليها فكرة العلم و التكنولوجيا التي تمتلك نسقين الاول ينصب نحوى خدمة البشرية و الثاني ينصب في تطوير الأسلحة غير المألوفة بما يؤدي الى دمار البشرية[69]

فالعصر الدي نعيش فيه هو عصر الفضاء المعلوماتي الدي غير كل المفاهيم التقليدية حتى على مستوى الامن القومي لدول[70]

وبعد التقديم البسيط سنعرض الي بعض تجارب الاجنبية في مجال الأمن المعلوماتي وحماية الأمن القومي باتخاذ الولايات المتحدة الأمريكية وإسرائيل كنموذجين باعتبارهم دول رائدة في المجال المعلوماتي من جهة وكونهما تشكل بؤر التوتر مما يجعل امنهما القومي معرض لتهديد

[69]- فوزي حسن الزبيدي منهجية تقيم المخاطر الأمن القومي دراسة تحليلية رؤى استراتيجية مجلة القانون، لعدد 8، ص: 38.
[70]- ربيع محمد يحيي إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط دراسة حول الاستعداد ومحاور عمل الدولة العبرية في عصر الأنترنت المجلة رأى إستراتجية العدد 3، 2003.

### 1.الولايات المتحدة الأمريكية

التفت الولايات المتحدة الامريكية الى ضرورة حماية المعلومات الالكترونية القومية منذ وقت مبكر والاستفادة من توفير منظومة امنية لمعلوماتها الرقمية لتشرع بتطبيق سلسلة من الاجراءات القانونية والتقنية والرقابية التي تتناسب وحجم محتواها المعلوماتي واتساع رقعتها الجغرافية وتوجهها السياسي والاقتصادي والثقافة الداخلية والخارجية نحوى جعلها أكثر البلدان امننا[71].

تقوم التجربة الامنية المعلوماتية الامريكية على ثلاثة منظومات سياسية وبنائية متشابكة بشكل متسلسل ومتداخل بطريقة متينة فما ان ينتهي اعداد وتطبيق المنظومة الأولى حتى تتدخل في الأعداد وتطبيق المنظومة الثانية لينصل الي الثالثة بشكل متكامل وسريع يتوافق مع سرعة و تطور الأنظمة المعلوماتية في العالم[72] والمنظومات الثالثة هي :

المنظومة القانونية :تظم سلسلة من القوانين الفيدرالية التي تنظم التعامل مع المعلومات الالكترونية من منظور امني كمنظومة القوانين الفيدرالية المسؤولة عن إدارة امن المعلومات و التي تهتم بقضايا الأمن المعلوماتي في الولايات المتحدة الامريكية[73]وقانون اصلاح إدارة قطاع التكنولوجيا المعلومات والاصلاح الاستحواذي الذي يهدف الى تقييم وتوفير الارشادات الخاصة بممارسة الوكالات والشركات الرأسمالية الكبرى للمعلومات الرقمية القومية و قانون الحرية الالكترونية و غيرها من القوانين

3- غيطاس جمال أمن المعلومات والأمن القومي طبعة الأولى، شركة نهضة لطباعة والنشر وتوزيع، مصر (القاهرة) 2007 ص: 27.

[72]- منصور بن سعيد الفحطاني الأمن المعلوماتي وسبل موجهتها رسالة النيل شاهدة الماجستير، جامعة نايف العربية للعلوم كلية الدراسات لعليا قسم لعلوم الإدراية 2008 ص: 140.

[73]-ابراهيم خالد، أمن العلومات الالكترونية، طبعة الاولى الاسكندرية الدار الجامعية لنشر 2008 ص: 27.

المنظومة الفنية : هي التي تحدد المعايير الفنية والتقنية الموحدة لتعامل مع أمن المعلومات الرقمية بشكل امني [74] وتتشكل هده المنظومة من جهات مختصة بأمن المعلومات القومية نذكر منها على سبيل المثال المعهد القومي لتكنولوجيا ولجنة السياسية القومية لتشفير المعلومات التي تهدف الى تشفير و ترميز البيانات المتداولة في الفضاء الالكتروني وحمايتها من التداول اللاسلمي.

المنظومة التنفيذية والتطبيقية والرقابية: هي مجموعة من الهيئات والوكالات الفيدرالية المسؤولة عن تطبيق سياسات امن المعلومات في الولايات المتحدة الامريكية و لها ارتباط مع باقي الوزارات القومية داخل الولايات المتحدة الامريكية تقدم لها الاستشارات وتطبيقات المعلوماتية المؤمنة[75].

وتقوم بتنسيق مع عشرات الوكالات الامريكية على راسها المخابرات الامريكية ووزارة الدفاع ومكاتب الاستطلاع الداخلية والخارجية ووكالات الامن القومي وذلك بهدف إبقاء الوضع المعلوماتي متزن.

## 2. التجربة الإسرائيلية (عملية استشراف المستقبل لحماية الأمن القومي الإسرائيلي)

يشكل تطوير قدرة إسرائيل في مجال الحرب الالكتروني مكوننا أساسيا في منازعتها القومية

[74]- عليان ريحي مجتمع المعلومات والواقع الأوربي طبعة الأولى، عمان دار التحرير لنشر توزيع2006 ص: 24.
[75]- منصور بن سعيد الفحطاني، م . س، ص: 155.

بحيث أنه لا شك ان الاقتصاد اسرائيل و صناعتها و مؤسساتها التربوية و الحرص على وجودها كمجتمع ديمقراطي منفتح على المعرفة رهين بخلق منظومة امنية في مجال التعامل الافتراضي لاسيما ان الاعتماد المتزايد على انظمة الحواسيب في اسرائيل افز تحدي جديد يستوجب الرد الفوري سوء على المستوى الوطني اي الجرائم المعلوماتية الداخلية أو الجرائم التي قد تهدد امنها القومي[76].

حيث إن من بين اهم الانجازات اسرائيل في مجال القوة السيبرانية وحروب المعلوماتية المستقبلية وحماية امنها القومي هي:

الوحدة 8200[77]: منذ ثلاثة عقود دشن جهاز "امان" الذي يعتبر اكبر جهاز الاستخبارات الصهيوني قسما متخصصا في مجال التجسس الالكتروني اطلق عليه اسم الوحدة "8200" ويطلق عليها كذلك "سغنيت" الاسرائيلية هي فيلق وحدة الاستخبارات الاسرائيلية المسؤول عن تجسس الالكتروني عن طريق جمع الاشارات و فك التشفير و ايضا هي المسؤولة عن قيادة الحرب الالكترونية[78].

أهدافها: هو المساهمة في تقديم رؤية استخباراتية متكاملة مع المعلومات التي توفرها المصادر البشرية القائمة العملاء وتعتمد هده الأخيرة على الرصد التصنت التصوير والتشويش مثلا التصنت ورصد أجهزة الاتصال السلكية ولا سلكية والتقاط المكالمات.

76- مع جميع القدرات والمزايا الكامنة في الفضاء الإلكتروني في شتى مناحي الحياة، إلا أنه في الوقت نفسه يفتح المجال لمخاطر هائلة، ودائما ما تتحدث إسرائيل عن قدرات جيشها على القتال في أكثر من جهة في آن واحد، إلا أنها قد تصاب بالشلل مع الهجمات السيبرانية المتكررة.

77- مروة الشامي، ماهي "8200" و ما هو دورها على موقع التواصل الاجتماعي، منشور على الموقع الالكتروني http://janoubia.com تم الاطلاع عليه بتاريخ 2017/02/17 على الساعة 20.00.

78- مع جميع القدرات والمزايا الكامنة في الفضاء الإلكتروني في شتى مناحي الحياة، إلا أنه في الوقت نفسه يفتح المجال لمخاطر هائلة، ودائما ما تتحدث إسرائيل عن قدرات جيشها على القتال في أكثر من جهة في آن واحد، إلا أنها قد تصاب بالشلل مع الهجمات السيبرانية المتكررة.

البنية التحتية الحكومية لعصر الانترنت:

قامت اسرائيل مشروع البنية التحتية لعصر الانترنيت داخل وزارة المالية و هدف هدا المشروع هو حماية و تأمين في استعمال الانترنت داخل الوزارات و المؤسسات الحكومية وأقيم داخل هدا المشروع مركز الحماية المعلومات الحكومية الاسرائيلية[79].

السلطة الرسمية لحماية المعلومات:

أنشأت عام داخل جهاز المخابرات العامة "الشباك" ومن مهامها حماية البنية التحتية في إسرائيل من المخاطر تهديدات الإرهابية أو عمليات تخريب نشاطات التجسس[80].

هيئة الأركان السيرانية القومية:

الغاية الرئيسية من تشكليها تعزيز قدرات حماية البنى التحتية الحيوية للدول من الهجمات الارهابية الالكترونية التي قد تشنها دول أجنبية أو مجموعات إرهابية[81] وتضم الهيئة أربع شعب.

1الشعبة الامنية.

2. الشعبة المدنية.

3. شعبة الاستخبارات وتقيم الوضع.

4. شعبة التنظيم السياسي.

[79]- غيطاس جمال، م س، ص:42.

[81]-jaysonspalechma s cyber power and amiraca national securtyu .sarrmywaarlcollege 2012 pp 55.

## خاتمة:

فرضت التكنولوجيا الرقمية سيطرتها على منافذ الحياة الإنسانية الخاصة والعامة، واكتسحت جميع مجالات الحياة السياسية والاقتصادية والثقافية والإعلامية والأمنية.

الشيء الذي ساهم في توطيد تلك العلاقة ما بين الأمن المعلوماتي والأمن القومي، فلم يعد الأمن القومي بالنسبة لدول العالم مقتصرا على مدى توفر القوى العسكرية فحسب، بل إن التطورات الاتصالية الحديثة والتي رافقتها أساليب جديدة كالتجسس والاختراقات وصراعات العالم الالكتروني وغيرها.

لهذا ارتأينا للوقوف على مجموعة من الملاحظات التالية؛

_ خلقت التطورات التّقنية والتكنولوجية الحديثة العديد من التهديدات الأمنية والمعلوماتية، خاصةً على مستوى الأمن القومي، والذي أصبح أكثر عرضةً وخطراً نظراً لسهولة الانكشاف المعلوماتي الذي وفرته وسائل الاتصال والتواصل الحديثة، وانتشار مختلف أنواع المعلومات بزخمٍ كبيرٍ على شبكات الإنترنيت، تُرافقها العديد من أساليب الاقتناص الأمني والمعلوماتي الرامية للاستحواذ على المعلومات المنتشرة عبر الفضاء الإلكتروني بكافة الطرق والأساليب.

_ دفعت هذه المخاطر دول العالم لاتخاذ العديد من سبل حماية أمنها القومي من مخاطر الانفتاح التّقني والمعلوماتي، وذلك عبر ربط أمن معلوماتها الرقمية باستراتيجياتٍ

شاملةٍ تندرج تحت منظومة أمنها القومي، وذلك بغية الحفاظ على معلوماتها القومية والوطنية والعسكرية والسياسية والاجتماعية والاقتصادية من الانكشاف الأمني.

كما أننا ومن خلال النقط التي عملنا على تحليلها في ذات الموضوع فإننا نؤكد على الاستنتاجات التالية؛

_ يلعب الأمن الإلكتروني المعلوماتي دوراً مهماً في حماية الأمن القومي للدول، فهو قد يهدد أمن الدولة كُلياً إذا ما تعرض للانكشاف أو الاختراق، الأمر الذي قد يكلف الدولة الكثير من الخسائر الأمنية والاجتماعية والسياسية والاقتصادية وغيرها.

_ مستقبل الحروب الإلكترونية مرهون بمدى التطورات التّقنية والمعلوماتية التي تواكب عصرنا الحالي والعصور التي ستليه، فعالم الاتصالات وتكنولوجيا المعلومات مستمر في إنتاج وطرح كل ما هو جديد، لتُجنده البشرية جمعاء في صراعاتها الرقمية والتّقنية المستقبلية.

ومن خلال ما سلف ذكره من ملاحظات واستنتاجات فإننا نود الإشارة إلى الاقتراحات التالية؛

_ يجب العمل على رفع مكانة وثقافة امن المعلومات الالكترونية، من خلال التحرر من التبعية التقنية، وتوظيف جميع الطاقات التكنولوجية، وذلك من خلال الاستفادة من التجارب المعلوماتية العالمية.

_ تأمين هذه المعلومات بشدة لتلك الدول المتعمدة على شبكات المعلومات وأدوات الاتصال الحديثة، لأن تداولها وإدارتها إلكترونياً وعبر شبكات المعلومات والاتصالات التي ترابطت محلياً وإقليمياً وعالمياً جعلها معرضةً لخطر الاختراقات الأمر الذي يخلف العديد من الآثار على أمنها القومي.

_ اتخاذ العديد من سبل حماية الأمن القومي لدول العالم من مخاطر الانفتاح التّقني والمعلوماتي، وذلك عبر ربط أمن معلوماتها الرقمية باستراتيجياتٍ شاملةٍ تندرج تحت منظومة أمنها القومي، وذلك بغية الحفاظ على معلوماتها القومية والوطنية والعسكرية والسياسية والاجتماعية والاقتصادية.

**تم بحول الله**