الجامعة اللبنانية

كلية الحقوق والعلوم السياسية والادارية

إستراتيجية "إسرائيل" الأمنية في ظّل الحروب الإلكترونية بعد حرب تموز 2006

رسالة لنيل ماستر بحثي في العلاقات الدوليّة والدبلوماسيّة

إعداد

نهى شفيق مكي

لجنة المناقشة

الدكتور غسان العزي	**الأستاذ المشرف**	**رئيساً**
الدكتور جوزاف عيسى	**أستاذ مساعد**	**عضواً**
الدكتور كميل حبيب	**أستاذ**	**عضواً**

2017

الجامعة اللبنانية غير مسؤولة عن الآراء الواردة في هذه الرسالة وهي تعبّر عن رأي صاحبها فقط .

الجامعة اللبنانية

كلية الحقوق والعلوم السياسية والادارية

إستراتيجية "إسرائيل" الأمنية في ظل الحروب الإلكترونية بعد حرب تموز 2006

رسالة لنيل ماستر بحثي في العلاقات الدوليّة والدبلوماسيّة

إعداد

نهى شفيق مكي

لجنة المناقشة

الدكتور غسان العزي	**الأستاذ المشرف**	**رئيساً**
الدكتور جوزاف عيسى	**أستاذ مساعد**	**عضواً**
الدكتور كميل حبيب	**أستاذ**	**عضواً**

2017

الإهداء

الحمد لله رب العالمين على جميع نعمه وعطاياه ، ومنها توفيقي لإنجاز هذه الرسالة...

إلى والديّ وسّر وجودي...

إلى عائلتي المحبّة وأولادي أغلى ما أملك...

إلى زوجي ، إلى من شجّعني ودعمني وآمن بقدراتي...

وأخصّ بالشكر أستاذي المشرف الدكتور غسان العزي ، إلى توجيهاته ونصائحه القيّمة في إعداد هذه الرسالة ...

الشكر الأوّل والأخير إلى كل من ساهم في صنع نصر تموز 2006

إلى دمائهم الزكية الطاهرة التي روت تراب الوطن ...

إلى القدس وفلسطين ....

إلى صانعي الإنتصارات في زمن التخاذل ...

أهدي هذا العمل المتواضع .....

نهى مكي

المقدمة

يعيش العالم اليوم حرباً جديدة تعـرف بالحرب الرقميـة الالكترونية أو حرب الفضاء الالكتروني ، فقد شكلّت تكنولوجيا الاتصالات والمعلوماتية ثورة في ميدان الجيوش والحروب والاقتصاد والسياسة والإعلام ، ووسيلة فاعلة في خدمة التكتيكات العسكرية الهجومية والدفاعية ، واستخدام هذه العلوم أيضاً لمجابهة التدابير الالكترونية المعادية واحباط فاعليتها وأصبحت الحرب الالكترونية فى الفضاء السيبرانى الإفتراضى واقعاً ملموساً ومؤثراً ، دون إستخدام الاسلحة التقليدية القاتلة . وعليه أن تهديد الحروب الإلكترونية بات التهديد المركزي للقرن الجديد.

وقد استحدث حزب الله من خلال حرب تموز 2006 جبهة قتالية جديدة في مواجهة " إسرائيل " ، وسلاحاً أكثر شراسة وفتكًا من الطائرات والصواريخ والقاذفات ، ينتج عنه آثار مدّمرة وخسائر فادحة دون إطلاق رصاصة واحدة أو إراقة دماء، حرب عقول أبطالها القراصنة ، ووسيلتها أزرار الكيبورد وأجهزة الكمبيوتر، وتبدأ بضغطة زر واحدة لتنتهي بمئات الخسائر.(فقد حذّر العميد يارون روزين ، رئيس هيئة الفضاء السيبراني التابعة لرئاسة الأركان الإسرائيلية ، من المخاطر و التحديّات الكبرى التي تواجه" إسرائيل" **قائلاً إنّ "الدبابات والمقاتلات الأكثر حداثة قد تُشل بمجرد كبسة زر واحدة** ") .

تتمتّع" إسرائيل" حالياً بما يسمى " الإستقرار الإستراتيجي الشامل " ، كون هذا الإستقرار من وجهة نظر قادتها يستند من جهة أولى إلى قوة عسكرية وإلكترونية متفّوقة ، ومستمد من جهة ثانية من تراجع تهديد الجيوش العربية النظامية التي واصلت عملية التقهقر والتلاشي التدريجي على مدى السنوات الخمس الماضية ، لا سيما بعد تفكّك الجيشين العراقي والسوري ، وصمود السلام مع كل من مصر والأردن ، إن لم نقل إنه تعزّز أكثر.

وبما أنّ القدرة العسكرية لأية دولة تقوم على حسن تنظيم وتشغيل واستغلال مجموعة من العناصر أهمها : الموقع الجغرافي والقوى البشرية والموارد الطبيعية والاقتصادية والعلاقات الدولية والروح المعنوية والفكر التنظيمي وسلبيات وضعف الخصم .

وبالرغم من مواطن الضعف التي تتمّتع فيها " إسرائيل"، إستطاعت قيادتها العسكرية إستغلال الإمكانات المتاحة لها بشكل يخدم أهدافها . «قبة حديدية» جديدة من المزمع إنشاؤها، لكن من نوع آخر. فبحسب ما أورده المراسل العسكري لصحيفة «معاريف»، نوعام أمير، أن الجيش الإسرائيلي بصدد إقامة قبة حديدية إلكترونية ، من خلال "مقاتلين تقنيين" بهدف حماية مراكز المعلومات الأمنية الاسرائيلية ، والتي ستعمل بنظام فريد من نوعه .

فالإستراتيجية العسكرية الإسرائيلية تتصّف بأنها ثابتة في جوهرها، صهيونية بطبيعتها، عدوانية بوسائلها، إستعمارية توسعيّة في غاياتها. لذا فإن ما يطرأ عليها من تغييرات ، لا يعدو أن يكون تطويراً في الأسلوب وليس في الجوهر . وتستند "إسرائيل" في بناء إستراتيجيتها على عدة معطيات تعتبرها وقائع أولية خاصة بها. وأهم هذه المعطيات : الوضع الجغرافي العسكري، وقلة سكانها بالنسبة إلى العرب، وعدم القدرة على تحمل حرب طويلة الأمد، وبما أنّها ولدت نتيجة الغزو والاستيطان الإستعماري فإن "إرادة البقاء" هي التي تسيطر على جميع معطيات الاستراتيجية العسكرية الإسرائيلية وأغراضها وأسسها ومفاهيمها. وتتوّلد عن هذه الإرادة ثلاثة مفاهيم أساسية توّجه الإستراتيجية العسكرية الإسرائيلية وترسم لها سبل عملها ووسائل تنفيذها . وهذه المفاهيم هي:

1-الأمن : مشكلة " إسرائيل" الأولى هي في وجودها ونشأتها " تكون أو لا تكون". وغدت هذه المشكلة محور تفكيرها وسلوكها. وبالتالي نشأت الثنائية التي يتصف بها مفهوم الأمن فهو حركي – عدواني في آن معاً لأنه يجد مجاله الحيوي خارج " إسرائيل".

2-**العنف** : وهو وليد طبيعة الحركة الصهيونية ومبادئها ، والتي تعتنق مبادىء العنف والقتل والإبادة.

3-**حتمية الحرب:** وهو مفهوم ينبثق من طبيعة نشأة " إسرائيل" ، فقد خاضت حروباً أكثر من أي دولة أخرى في العالم ، وغيّرت حدودها الجغرافية ووسعّتها بأساليب وطرق لم تضاهيها أي دولة أخرى في العالم . وارتكزت النظرية الأمنية الإسرائيلية على ثلاث مبادىء : الضربة الإستباقية المفاجأة ، ونقل المعركة الى أراضي العدو وحماية عمقها الإستراتيجي ، وحسم المعركة بسرعة .

وعلى الرغم من تعدد أجهزة الاستخبارات والجمع الإسرائيلية وما تمتلكه من خبرة وتنظيم ، وعلى الرغم من النفوذ التكنولوجي والإلكتروني الواسع لتلك الأجهزة وما تمتلكه من قدرات رقمية وتقنية فائقة الدقة ، وعلى الرغم مّما تتلقاه من دعم وإسناد إستخباري من كبرى دول العالم وعلى رأسهم الولايات المتحدة الأمريكية ، وما يخصّص لها من ميزانيات ضخمة ؛ إلا إنها وعلى مدار التاريخ قد واجهت العديد من أوجه الفشل الاستخباري والقصور المعلوماتي وتعدّ حرب تموز 2006 خير مثال على ذلك والتي بفعلها لم تتضرر هيبة الردع الصهيونية فحسب ، بل تضررّت العقيدة الأمنية الاسرائيلية ، فقد تمّ نسف وزعزعة مرتكزاتها حيث استمر القتال 33 يوماً لم تتمّكن " إسرائيل" خلالها من حسم المعركة أو منع سقوط الصواريخ على العمق الداخلي الإسرائيلي .

بناء على ما تقّدم ، **تحاول الدراسة معالجة الإشكالية التالية : دور ومكانة الحرب الإلكترونية في الإستراتيجية الأمنية الإسرائيلية الجديدة ؟ ومستقبل هذه المكانة في ظل تطور الحروب الإلكترونية وصعود مكانة حزب الله إقليمياً ؟**

وخلال ذلك سيتّم الاجابة عن بعض أهداف الرسالة التي تدور في فلك التساؤلات التالية:

1- ما هو دور تكنولوجيا المعلومات في تحديد طبيعة العلاقات الدولية الجديدة ، من خلال حرب الإنترنت والشبكات وحروب السايبر؟

2- كيف أثّرت حماية المعلومات على واقع وسيادة الدول وخصوصية الحالة الاسرائيلية في ظلّ الهاجس الأمني والتهديد الوجودي؟

3- مكانة الحرب الإلكترونية في الإستراتيجية الأمنية الإسرائيلية الجديدة ؟

4- ما مدى قدرة وجهوزية حزب الله في الفضاء الالكتروني (دفاع وهجوم) من خلال حرب تموز 2006 ؟ وكيف يستعدّ للحرب المقبلة ؟

5- في ظل سباق تسّلح إلكتروني ، ما هو مستقبل " إسرائيل " في ظل تطور الحروب الإلكترونية و صعود حزب الله (العدو المركزّي الأول) إقليمياً ؟

لا بد من الاشارة الى **الأهمية العلميّة للدراسة لأنّها تتمحور حول القضية المحورية الأساسية في ما تبقى من الصراع العربي _ الاسرائيلي** ، التي تحولت من حروب بين "إسرائيل " ودول الطوق العربية الى حروب مع حركات المقاومة (حزب الله وحماس والجهاد..) غير أنّ الدراسة ستقتصر على حزب الله تحديداً من خلال حرب تموز 2006 لأسباب عدّة :

- يعدّ صمود وانتصار المقاومة الاسلامية في حرب تموز 2006 نقطة البداية في فشل مشروع (الشرق الأوسط الجديد) في المنطقة ، ولاحقاً لاعباً مهمّا في محور الممانعة الذي حققّ إنجازات تاريخية في هزيمة هذا المشروع وأدواته في لبنان وسوريا والعراق ..

- إقتصرت الدراسة على الجانب اللبناني نظراً لتعقيدات الحروب الإلكترونية وتشّعباتها الكثيرة ، فلم يتمّ تناول الجانب الفلسطيني بالرغم من الإنجازات الهامّة التي حققّتها حركات المقاومة في فلسطين في مجال حرب الشبكات الإلكترونية .

– تحوز الدراسة على قدر كبير من الأهمية لأنها من الدراسات الأولى التي تناولت موضوع الحروب الالكترونية في قسم العلوم السياسية والادارية ومرجع جديد يضاف لمكتبة الجامعة خاصّة أنّها تعدّ لغة المستقبل .

أمّا **الأهمية العمليّة** فتتّمثّل في الجوانب التالية :

– أدّى نصر تموز 2006 الى إرساء معادلة ردع جديدة في الصراع مع "إسرائيل" وأصبح الاعتداء على لبنان يحسب له ألف حساب .

– أصبح حزب الله قوة إقليمية ودولية مهمّة ، وورقة رابحة لدى النظام السياسي في لبنان يستثمرها عند الضرورة ، ويتعاون معها للصالح العام (معركة تحرير جرود عرسال من النصرة وداعش ...)

وقد واجهت مراحل اعداد هذه الدراسة **صعوبات عدّة** تتمثل في النقاط التالية:

- ✓ دقة وحساسيّة الموضوع وبالتالي صعوبة الحصول على معلومات دقيقة لكلا الطرفين ، فالمعلومات التي تمّ جمعها في الجانب الإسرائيلي تقتصر على بعض الدراسات التي أجراها ونشرها مركز أبحاث الأمن القومي الإسرائيلي ، وجامعاته من أجل تقييم حرب تموز 2006 وتداعياتها ، وما يترجم عن الصحف اليومية الإسرائيلية من قبل بعض مراكز الدراسات الفلسطينة .

في المقلب الآخر ينتهج حزب الله إستراتيجية الغموض البنّاء ، وتصنف هذه المعلومات ضمن الخطوط الحمراء التي يمنع التداول بها ، ولذلك تمّ الاستعانة ببعض الإنجازات الخاصة والمميزة في سيرة عمل المقاومة وتحليلها خاصة حرب تموز 2006 .

- ✓ شكّل فهم تفاصيل الحروب التكنولوجية الرقمية وتعقيداتها مزيداً من العوائق التي تضاف الى صعوبات الدراسة ، لذلك تمّت الاستعانة ببعض المصادر الأجنبية وترجمتها إلى اللغة العربية بهدف الاستفادة منها أكاديمياً .

أماّ **المنهجية المتبعّة** تمثّلت في المنهج التحليلي لأنه يختصر معظم المناهج حيث يصوّر الظاهرة ويعمل على وصفها وشرحها وتحليلها وصولا الى فهمها والاستفادة منها في الواقع . فالتفاصيل الدقيقة والمعقّدة لواقع الحروب الالكترونية كانت لها تداعياتها على سيادة الدول وأثّرت على الواقع الأمني للمجتمع الدولي ، ووسيلة جديدة للصراعات بين الدول .

التصميم

تقسّم هذه الدراسة الى قسمين كما يقسّم كل قسم الى فصلين .

الفصل الأول من القسم الأول يقّدم فكرة عن أنواع القوة وأهمّها القوة الالكترونية ، وتأثيرها في الدول والعلاقات الدولية كجزء من حماية أمنها القومي، حيث أصبح أمن المعلومات من صلب الأمن القومي. كما يشير الى أهمية الفضاء الالكتروني كمجال جديد للحروب ، وكيف يمكن استثماره في حروب المستقبل .

أما الفصل الثاني فيتحدث عن مفهوم جديد هو الحرب الالكترونية وأهميتها ومميزاتها في عصرنا الحالي وعلى صعيد المستقبل ، وأنواع الاستراتيجيات الأمنية التي تتخذها الدول للبقاء في الصدارة ولمواكبة الأحداث الأمنية التي تمّكنها بالتالي من الحفاظ على ثباتها واستقرارها ووجودها.

في حين الفصل الأول من القسم الثاني يتحدث عن أهمية الأمن لدى الكيان الصهيوني الذي خاض حروبا كثيرة للحفاظ على وجوده ، وكيف أثّر قيام هذا الكيان والواقع الجغرافي في نظريته الأمنية . كما يشير الى سعيه الدائم للتفوق والريادة كجزء من نظرية الردع . كما يشير الى مدى التفوق التي أحرزته في السيطرة على الفضاء السيبراني ، وحماية أمنها الوجودي والمعلوماتي.

وأخيراً يشرح الفصل الثاني الاستراتيجية التي اعتمدها "حزب الله" في مقاومة "إسرائيل " وتأثيرها الفاعل في الصراع العربي الإسرائيلي . ومدى جهوزيته في ميدان الإستخبارات والمعلومات من خلال حرب تموز 2006 ، وكيف يتحضر الطرفان اللبناني والإسرائيلي للحرب القادمة .

القسم الأول

الأمن القومي والمجتمع الدولي في ظل الحروب الإلكترونية

طرأت تحولات جديدة على مفهوم القوة، وظهر على الساحة مفهوم جديد أطلق عليه جوزف ناي[1] القوة الإلكترونية والتي أدت إلى توزيع القوة بين عدد أكبر من الفاعلين من غير الدول بمن فيهم الفاعلين العنيفين والأفراد، وذلك بعدما كانت الدولة هي المحتكر الوحيد للقوة ، ما جعل قدرة الدولة على الهيمنة على هذا المجال موضع شك، وخصوصاً مع زيادة تأثير الفاعلين من غير الدول على السياسة على المستويين الداخلي والدولي.

دفعت الثورة الرقمية والتطورات الجارية في الاتصالات والمعلومات إلى الساحة بالعديد من المتغيرات الجديدة في ما يتعلق بامن المعلومات حتى جعلت منه ركيزة أساسية من ركائز الأمن القومى، فبات الكثيرون حول العالم يعيدون النظر فى قضية أمن المعلومات، ويرون أنه من الضرورات القصوى الإرتقاء بها من مستوى الأمور التقنية التفصيلية التى تسند إلى فنيين وتكنوقراط داخل المنشآت والمؤسسات كل على حدة بشكل مجزأ، لتأخذ مكانها ضمن القضايا التى يتولاها سياسون واستراتيجيون وصناع قرار، ويترجمونها فى سياسات واستراتيجيات وطنية تعمل ضمن منظومة الأمن القومى الشاملة وتضبط العلاقة بين أمن المعلومات والأمن القومى وتوجهها فى مسارها الصحيح.

[1] Josph Neye، الابن (ولد في 19 يناير 1937) أمريكي وأستاذ العلوم السياسية وعميد سابق لمدرسة جون كينيدي الحكومية في جامعة هارفارد. أسس بالاشتراك مع روبرت كوهين، مركز الدراسات الليبرالية الجديدة في العلاقات الدولية وتولى عدة مناصب رسمية منها مساعد وزير الدفاع للشؤون الأمنية الدولية في حكومة بل كلينتون ورئيس مجلس الاستخبارات الوطني.

لقد دخلت حرب المعلومات في صلب الاقتصاد والثقافة والعسكر وتتعرض شبكات المعلوماتية في كل يوم الى هجوم القراصنة من الهواة أو العاملين لحساب شركات أو دول. والمشكلة الأساسية التي تواجهها الدول الكبرى غياب اليقين في معرفة العدو . كما أن حركة الرساميل والمعلومات السريعة والفورية العابرة للقارات والحدود تزيد من تفاقم المشاكل الأمنية .

إلاّ أنَّ العالم العربي بمعظمه لا يزال مغموساً في حروبه العرقية والمذهبية ومشاكله الداخلية وبالتالي فان أمن المعلومات بحكم المغيَّب عن الاهتمام في الساحة العربية في حين نشهد إهتماماً دولياً وعالمياً في علوم الحاسوب وتأمين الشبكات تتسابق فيه الدول المتقدمة إلى تحقيق الأفضلية ، لأن الفضاء الالكتروني يشكّل المستقبل في الصراعات والحروب ، وفي مقدمتها الولايات المتحدة الأميركية التي صرّحت علناً وبشكل رسمي بالتالي: " يشكّل الأمن السيبراني الآن واحداً من أهم وأخطر تحديات الأمن القومي الذي يواجه الولايات المتحدة الأميركية ، نحن معرضون للهجوم وتحَمل الخسائر ..." [2]

تشكل المستجدات العديدة في مجال تكنولوجيا الحرب السبرانية تحديّاً للمفاهيم السائدة حول الأمن القومي، وتفرض علينا مراجعة مفرداتها الأساسية . وهذا يرتب علينا إيلاء قضية الدفاع عن البنى التحتية الحيوية للدولة أهميّة قصوى ولا سيّما في مجالات الطاقة والمياه والحوسبة والإتصالات والمواصلات والاقتصاد، في القطاعين المدني والأمني. وبناءً عليه، ينبغي إجراء التعديلات اللازمة في مفهوم الأمن القومي بهدف الردّ على التهديدات المستجدة .[3]

---

[2] James.A Lewis ,**cyberse security recommendations for the next administration testimony**,center for strategic and international studies,september2008,Washington DC,subcommittee on emerging threats,cyber security, science and technology.
Kenneth J.Knapp,**cyber security and global information assurance**,information science reference ,2009,Newyork,preface xviii.

[3] شموئيل إيفن ودافيد سيمان طوف، "حرب في الفضاء السبراني: مفاهيم، واتجاهات، ودلالات لإسرائيل"، معهد دراسات الأمن القومي، مذكرة رقم 109 ، تل أبيب ، 2011، المقدمة .

بناء على ما تقدّم ما أهمية تكنولوجيا الحرب السبرانية في مفهوم الأمن القومي ، وتداعياتها على متغييرات القوة ، ومدى سعي الدول إلى إحراز التفّوق والسباق نحو التسلح لحجز مكانها على الساحة الدولية أو لحماية نفسها أمام المجتمع الدولي .

الفصل الأول

أثر الفضاء الالكتروني في المجتمع الدولي أمنياً .

حدثت تحولّات في مفهوم الأمن والمشهد الأمني العالمي، وأبرزها تحولات القوة ، التي لم تعد ترتبط إرتباطاً وثيقاً ووحيداً بالعامل العسكري . بل تعّدته إلى التكنولوجيا والتعليم ، والنمو الاقتصادي والاعتماد المتبادل والمعلومات. فالقوة العالمية اليوم تتأسس على مصادر هي من قبيل القوة اللينة ، كما تقوم على مصادر ملموسة : القوة الصلبة. وكما يلاحظ جوزف ناي فإن : "القوة أقل تحولية، وأقل قهرية، وأقل ملموسية"، ذلك أن تحويل المكاسب المحققة في مجال ما نحو مجال آخر يزداد صعوبة ، أما في ما يخص الأمن ، فإن الأمن اللين يعني التهديدات غير المباشرة أو التهديدات غير العسكرية ، مثل عدم الإستقرار، التطرف ، الإرهاب ، التهريب ، المخدرات ، الهجرة غير المشروعة ، الجريمة المنظمة ، بينما يقصد بالأمن الصلب : التهديدات المباشرة أي التهديدات العسكرية .[4]

يؤكّد هانز مورغانثو "Hans Morgenthau " مؤسس النظرية الواقعية في العلاقات الدولية على فكرة القوة في العلاقات الدولية بقوله: إنّ السياسة الدولية بمختلف أشكالها إنّما هي صراع من أجل القوة وتدخل الوسائل في إطار السياسة الدولية ويبدأ العمل للكفاح من أجل القوة [5] . وينطلق "نيكولا سبيكمان " في تحليله من أن مركز الدولة في إطار السياسة الدولية لا يتوقف من الناحية الجيوبوليتيكية ، على موقعها الثابت ، وإنما يعتمد أيضا وإلى حد بعيد

[4] خليل حسين ،**مفهوم الأمن في القانون الدولي العام** ، 2009/1/16.على الرابط الالكتروني :
http://drkhalilhussein.blogspot.com/2009/01/blog-post_16.html

[5] سيف الهرمزي، تحليل هانس مورغانثو لمفهوم لقوة وتطبيقها على وحدات النظا م الدولي ، **مجلة تكريت للعلوم السياسية**،م1،عدد1،السنة1،ص158. على الرابط التالي:
cpos.tu.edu.iq/images/cpos/2016/journal/no_one/تحليل_هانز_مورجانثو_للقوة.pdf

على علاقة هذا الموقع بمراكز القوى المؤثّرة في السياسة الدولية [6] وهكذا فالحدود ليست إلا تعبيراً عن موازين قوى في لحظة معينة . وعلى هذا الأساس فان الدول تسعى جاهدة لامتلاك القوة كوسيلة ردع ضد الاخرين.

إنّ معطيات القوة المتغيّرة لدولة ما، هي العناصر التي يمكن تفعيلها في المدى القريب والمتوسط ، وهي العناصر التي تعكس مدى قدرة الدولة على استخدام القوى الكامنة فيها. وتعد كل من الموارد الاقتصادية للدولة ، وبنيتها التحتية التكنولوجية ، والتراكم العسكري لديها ، هي عناصر متغيّرة في معادلة القوة للدولة .[7]

وأصبحت الدول ساحة مكشوفة وسهلة الاختراق أمنياً حتى من خلال بعض الهواة . ويبحث أمن المعلومات في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها . ومن زاوية تقنية ، هو الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية . ومن زاوية قانونية ، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة ، وهذا هو هدف تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها. [8]

---

[6] نيكولاس سبيكمان **و نظرية الإطار**: 1893-1943 المدرسة الأمريكية ...
https://bohoht.blogspot.com/2016/04/1893-1943.htm

[7] بحث - النظرية الجيوسياسية - **الموسوعة الجزائرية للدراسات السياسية**
/https://www.politics-dz.com/threads/alnzri-algiusiasi.5981

[8] شريف اللبان، خبرة عربية منقوصة: أمن المعلومات في ظل تحديات البيئة الرقمية ،**المركز العربي للبحوث والدراسات** ، الأربعاء 04/مارس/2015 - 11:06 ، على الرابط التالي : http://www.acrseg.org/36712

المبحث الأول: ثورة المعلوماتية وتأثيرها في ميزان القوة في المجتمع الدولي.

أثرَت الحربان العالميتان في واقع العلاقات الدولية ، حيث تبلورت أفكار جديدة ومدارس نظرية أخذت تتَّحدد مفاهيمها بدءا بالمثالية أو الطوباوية ، مرورا بالواقعية ، وصولاً الى السلوكية أو البنائية . وبالرغم من إيجابيات كل من هذه المدارس وسلبياتها ، إلا أّن المنظرين في الولايات المتحدة الأميركية تبنوا المدرسة الواقعية التي تركز على قوة الدولة بل وعلى احتكارها لهذه القوة أيضا في سبيل الهيمنة على العالم . الا أنَ وجهة نظر الماركسية اللينينية مخالفة حيث تعتبر أن التنمية المتفاوتة للمجتمعات هي بمثابة مصادر للفتوحات الإستعمارية ، وفي الحقيقة أن عملية التنمية المتفاوتة تحفز النزاع السياسي لأنها تقوض الوضع السياسي الدولي ، وان انتقال مواقع الأنشطة الاقتصادية يغير توزيع الثروات والقوة بين الدول في النظام ، وإعادة توزيع القوة هذه وتأثيرها في مكانة الدول ورفاهها تبرز النزاع بين الدول الناهضة والدول الآفلة ، وإن عدم حل النزاع يمكن أن يؤدي الى حروب هيمنة .

وقد شهد العقد الأخير تطورات سريعة في مجالي الحوسبة وتكنولوجيا المعلومات بما أفضى إلى تغييرات بعيدة المدى في كل مجالات الحياة تقريباً ، ولا سيما في المجالين العسكري والأمني اللذين شهدا تغيرات عديدة تتعلق بطريقة القتال وأسلوب بناء قوة الجيوش. ويعزى ذلك جزئياً إلى المستجدات التي طرأت على أنماط التفكير الاستراتيجي .

أن أشكال القوة تتغير بتغير التكنولوجيا، وقد أثر الفضاء الإلكتروني في الأشكال التقليدية للقوة، وطرح مفهوماً وشكلاً جديداً هو القوة الإلكترونية ، وقد كان لهذا الشكل الجديد دور في بلورة مفهوم انتشار القوة ، وتعدد الفاعلين الممارسين لها سواء من الدول أو من غير الدول ما هدّد الدور التقليدي للدول وقلّل من سيادتها على إقليمها .

المطلب الأول: متغيّرات القوة وظهور مفهوم القوة الالكترونية .

مفهوم القوة هو أحد أهم المفاهيم في العلاقات الدولية والمفسر الأساسي الذي يمكن الاعتماد عليه في فهم التفاعلات الدولية والمواقف التي تتخذها الفواعل المختلفة. وتظهر أهميته كذلك في فهم الصراعات الدولية وكيفية تجاوب الأطراف فيها بناء على قوتها المادية والمعنوية . تطور مفهوم القوة وتعددت اتجاهاته على مر التاريخ فيما بين القوة العسكرية والقوة الاقتصادية والقوة على الإقناع والتأثير حتى العصر الحديث وبزوغ التكنولوجيا الحديثة وتأثيرها في مفهوم القوة سواء كانت المادية أو المعنوية .

إلتفت المفكرون السياسيون مبكراً لموضوع "**القوة**" و حاولوا تحليله وإبراز مكنوناته فكانت القوة تعني عند الاغريق مثلاً " المبادرة التي تمكن الرجل الموهوب من فرض إرادته ورغبته على الأخرين ".[9] وقد وقع خلاف بين بعض الكتاب و الباحثين على هذا الموضوع حين تناول كل واحد منهم جانباً جزئياً محدداً من الموضوع وأغفلوا الطبيعة المركبة المعقّدة والشمولية له، حيث نجد مثل هذه النظرة والتوجه لدى" **رايت مل**" الذي قال " إن كل السياسة صراع من أجل القوة والشكل النهائي للقوة هو العنف " [10].

ويعتبر"مورجانثو" و"سبيكمان" من أهمً المنظرين ل"الواقعية "، بعد ما كان هوبس ومكيافيللي من أوائل الداعين الى السعي الى امتلاك القوة وبكل الوسائل ، "الغاية تبرر الوسيلة " شعار مكيافيللي الخالد.

إنطلقت النظرية الواقعية من الواقع الانساني الذي تتحكّم به مجموعة من القوانين الطبيعية التي لا يمكن تغييرها إلّا اذا تمّت مراعاة المحددات التي تحدّد مجالات هذه القوانين ومن بين

---

[9] كاظم هاشم نعمة ، **العلاقات الدولية**،جامعة بغداد ، كلية العلوم السياسية ، شركة اياد للطباعة ، بغداد 1987، ص 156.
نفلا عن دراسة " تأثير مقومات قوة الدولة على سياستها الخارجية" ، بسمة خليل نامق .

[10] المصدر نفسه ص 157.

محددات الدولة أمنها وقوتها التي يساهم في وجودها تداخل العامل العسكري والاقتصادي والتكنولوجي والسكاني . وتؤخذ هذه القوّة كمعيار يتحدّد على ضوئه قياس قدرة الدولة على الحفاظ أو الدفاع عن مصالحها الحيوية ، وعليها تعتبر الدولة ، حسب هذه النظرية ، الهيئة الوحيدة المؤثرة في العلاقات الدولية لكونها ذات طبيعة حدودية وعقلانية ، تهدف الى الحفاظ وبأقصى حد على مصالحها القومية ، ما يدفعها وبشكل مستمر الى اللجوء للقوة بهدف الحفاظ على الأمن والقضايا السياسية اللذين يشكلان الأهداف الرئيسة للسياسة الخارجية .

وتعتبر الولايات المتحدة الأميركية من أهم المتبنين لهذه النظرية التي تركز على القوة واحتكارها حتى لا يقاسمها أحد عليها لضمان الهيمنة على العالم ، وقد أكدً هنري كيسنجر بعد أن أصبح وزيرا للخارجية أنً " القوة لا تزال الحكم الأخير في العالم ".[11]

1. **تعريف القوة .**

إنَ التغيير في العالم سمة رئيسية للدول في ظلً الفوضى التي تعًم النظام الدولي ، وامتلاك هذه القوة السياسية، أو الاقتصادية، أو العسكرية ليس هو المقياس الفعلي لنجاح سياسات التأثير في الآخرين، بل انّ فن إدارة هذه القوة يمثل العنصر الرئيسي الاخر لنجاح أي سياسة فعلية تأثيرية، وقوة ردع ضد الاخرين ، وبالتالي فقد تعددت التساؤلات حول القوة وأهميتها وتأثيرها وتحديدها ونسبيتها ... فما هي هذه القوة ؟ وكيف يمكن تعريفها ؟

يرى "مورجانثو" أن "القوة هي طبيعة غريزية في الشخصية الانسانية وفي السلوك الانساني عامة" .[12] ولكنه ربطها بفكرة التأثير والتحكم فى المكاسب ، فرأى أن القوة هى " القدرة على التأثير فى سلوك الآخرين"، بينما استفاد عالم الاجتماع ، روبرت دال، من تعريف مورجانثو

---

[11] غسان العزي ، **سياسة القوة مستقبل النظام الدولي والقوى العظمى** ، مركز الدراسات الاستراتيجية والبحوث والتوثيق ، بيروت ،2000، ص22.

[12] اسماعيل صبري مقلد،**العلاقات السياسية الدولية: دراسة في الأصول والنظريات**،(الكويت :كلية التجارة والاقتصاد والعلوم السياسية ، مطبوعات جامعة الكويت ،1984)، ص 19-20.

فقدم تعريفا أكثر وضوحا للقوة حيث اعتبرها " القدرة على جعل الآخرين يقومون بأشياء متناقضة مع أولوياتهم، ما كانوا ليقوموا بها لولا ممارسة تلك القدرة ". [13]

عرّف مولودسكي القوة بأنها " قابلية الدولة لاستخدام الوسائل المتوافرة لديها من أجل الحصول على سلوك ترغب في ان تتبعه الدول الأخرى "[14]. أو هي " القدرة و التأثير في الاخرين وقت الحرب والسلم ومن ثمَّ فالقوة والنفوذ مترادفان " .[15]

أما "سبيكمان" فيرى بأن القوة هي ما تعتمد عليه بالاقناع أو الإغراء أو الإكراه . كما يعتقد بأن "السياسة لايمكن ان تحدّدها الأخلاق ، وبالتالي فالمبادىء الأخلاقية لا يمكن تطبيقها على العمل السياسي ".[16]

في حين جادل الفن توفلر أن (المعرفة هي القوة، و أن امتلاك المعرفة هو أساس لامتلاك الثروة والقوة العسكرية).[17]

وبناء على ما تقدم يوجد ثلاثة اتجاهات رئيسة :

- الاتجاه الأول يعرّف القوة على أنها القدرة على التأثير في الغير .
- الاتجاه الثاني يعرّف القوة على أنها المشاركة في صنع القرارات المهمّة في المجتمع .
- الاتجاه الثالث يحاول أن يجمع جوانب كل من الاتجاهين السابقين .[18]

---

[13] صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية فى التفاعلات الدولية جزء 2،**المعهد المصري للدراسات الاستراتيجية**،نوفمبر 2016/5،على الرابط الالكتروني التالي:
http://www.eipss-eg.org/2/0/1224

[14]G.Modelski , **theory of foreign policy** , Newyork:pall MALL , 1962 , p23.

[15] H. Ferris Wayne **,the power capabilities of nations states** , (U.S.A laxington book , 1973) p.4-6

[16] أحمد جلال ، **صراع القوى المدنية-العسكرية وأثره على السياسة الخارجية التركية** ، المكتب العربي للمعارف للنشر والتوزيع والطباعة ، القاهرة ،2015 ، ص 75. على الرابط الالكتروني التالي:
https://books.google.com.lb/books?isbn=977276816X

[17]ايهاب توفيق،**القوة الالكترونية وأبعاد التحول في خصائص القوة**،نفلا عن ألفن توفلر،**تحول السلطة** ، ترجمة لبنى الريدي(د.م،الهيئة المصرية العامة للكتاب 1995) ، ص ،25.على الرابط الالكتروني التالي :
https://www.bibalex.org/Attachments/.../2014070311292451794_awrak12pdf.pdf

[18] غسان العزي، مرجع سبق ذكره ، ص 23.

وفي المحصلة تعدّ القوة مفهوماً شائعاً ومتداولاً كثيراً ولكن من الصعب قياسها نظراً إلى نسبيتها ، وليس هناك تعريف محدّد ، وكل واحد يختار التفسير الذي يوافق قيمه ومصالحه .[19]

فضلاً عن هذا هناك أيضاً تصنيفات عدة أخرى للقوة ، وهي تمثل الموارد العامة التي يمكن استخدامها على المدى الطويل لامتلاك قدرات معينة تستخدم في التأثير، وتتضمن بالنسبة الى الدول: الموقع الجغرافي، عدد السكان، الموارد الاقتصادية، القاعدة الصناعية، الإمكانات العلمية/التكنولوجية ، والقيم الثقافية، وطبيعة النظام السياسي/التنظيمي ومدى تجانسه واستقراره . وتتمثل أهمية تلك المصادر في كونها عاملًا أساسيًا في تحديد وزن الدولة ضمن هيكل القوى العالمية، كما أن الطبيعة الكمية والكيفية للموارد المتوفرة هي التي تحدد طبيعة ونوعية القدرات التي يمكن امتلاكها.وبالتالي يمكن تقسيم أشكال القوة الى عدة أنواع وكل منها يعتمد على موارد معينة تؤدي الى تحقيق غايته المنشودة في التاثير .

ونستنتج من ذلك أن معايير القوة وأدواتها نسبية ومتغيرة وهشة تبعاً للتطورات التي طرأت على الساحة الدولية فالمعلومات قوة ، والتكنولوجيا قوة والعولمة التي شبكت الدول بعضها ببعضها الآخر فأصبحت قرية عالمية واحدة قوة ، كل ذلك متغيّرات جديدة أثرّت في طبيعة القوة وأدخلت أشكال جديدة على الواقع الدولي . تتجلى هنا مشكلة أساسية وهي عملية تحويل القوة كما أشار لها ناي ، وتعني كيفية تحويل المصادر إلى قوة فعلية وقدرة الفواعل الدولية

[19] Joseph s.Nye,**"cyber power**"Harvard kennedy school,belfer center for science and internationalaffaires ,May 2010, page 2 . on the website: http:/belfercenter.ksg:Harvard.edu/files/cyber-power.pdf.

على ذلك ، وأن التفوق في القوة يعتمد على القدرة على تحويل هذه الموارد وليس فقط امتلاكها، وبذلك أصبح محدد القوة هو امتلاك الموارد والقدرة على تحويلها إلى قوة فعلية .[20]

2. أثر التكنولوجيا في تحوّلات القوة .

اعتبرت القوة العسكرية الشكل الرئيس للقوة ، والتي سيطرت و لفترة طويلة على السياسة الدولية بشكل عام ، غير أن كّلا من الثورتين الصناعية والمعلوماتية ألقت بآثارها ، حيث كان لها دورها في تغيير أشكال القوة ، ان ازدياد وزن التكنولوجيا قد أدى إلى تحولات كبرى على مفهوم القوة من أوجه عدة من أهمها تغير أشكال القوة بين القوة الصلبة والناعمة. ان أشكال القوة تتغير بتغير التكنولوجيا، وقد أثر الفضاء الإلكتروني في الأشكال التقليدية للقوة، وطرح مفهوماً وشكلاً جديداً هو القوة الإلكترونية، وقد كان لهذا الشكل الجديد دور في بلورة مفهوم انتشار القوة، وتعدد الفاعلين الممارسين لها سواء من الدول أو من غير الدول ، ما هدد الدور التقليدي للدول وقلل من سيادتها على إقليمها . غير أن تحويل الموارد الى قوة متحققة ، بمعنى الحصول على النتائج المرغوبة يتطلب خططاً استراتيجية جيدة التصميم ، أي ليس مهما امتلاك القوة بقدر ما يهم كيفية استعمالها حتى تصبح فاعلة ومؤثّرة . وقد قسم جوزف ناي أشكال القوة الى أربعة أقسام : القوة الصلبة ،القوة الناعمة ، القوة الالكترونية ، والقوة الذكية . وسوف نتناول تباعاً تاثير التكنولوجيا على كل منها.

2-1- القوة الصلبة: hard power

القوة الصلبة تعني القوة المشتركة السياسية والاقتصادية والعسكرية ،أي القوة في صورتها الخشنة التي تعني الحرب ، والتي تستخدم فيها الجيوش . وهذه القوة تعني الدخول في مزالق

[20] يمني سليمان ، القوة الذكية ـ المفهوم والأبعاد: دراسة تأصيلية،**المعهد المصري للدراسات السياسية والاستراتيجية** ، يناير 2016/12. على الرابط التالي: http://www.eipss-eg.org/A9/2/0/320

خطرة ، ونتائجها تكون في منتهى الخطورة على الدولة نفسها . وتتمثل القوة العسكرية في الامكانات والمقدرات العسكرية للدولة كحجم القوات المسلحة ومدى تفوق أسلحتها وتقدمها التكنولوجي والقوة الاقتصادية تشمل حجم الاقتصاد وحجم الدخل القومي وإجمالي الناتج القومي للدولة .

تتكون القوة الصلبة من عناصر القوة المادية : العسكرية والاقتصادية ، والتى يمكن توظيفها واستخدامها بطرائق مختلفة ، وهي النظرية التقليدية بينما تبنى " جوزف ناي" أحد رواد النظرية الليبرالية الجديدة ، تعريفا اوسع حيث تتركز القوة الصلبة على المغريات "**الجزرات** " أوعلى التهديدات "**العصي**" [21]. ويمكن تمييز أنماط عّدة لاستخدام القوة الصلبة والتي تراوح بين الاكراه والتخريب والتغيير وذلك من طريق تهديدهم بالقوة أو إغرائهم بها الردع و الدفاع وصولاً الى التدخل العسكري المباشر .[22]

أما بالنسبة الى القوة الصلبة (العسكرية) وعلاقتها بتكنولوجيا المعلومات ، فإن الأخيرة أدت إلى قيام ثورة فى النظم العسكرية وتطور نظام التسلح وطبيعة ونوعية الأسلحة وقدرتها التدميرية، وبالتالى التأثير في قوة الدول النسبية وقدرتها على التأثير والنفوذ والهيمنة على هيكل القوة داخل النظام الدولى .[23] ولكنها كانت بمثابة سلاح ذي حدين حيث أدت إلى اختلاف نوعية الأسلحة المستخدمة وزيادة قوتها التدميرية وتكاليفها المادية والبشرية ، ما أدى الى وجود رأي عام عالمي يسعى الى نبذ العنف والحروب فاتجهت الدول العظمى، وعلى رأسها الولايات المتحدة الأميركية ،الى نشر ثقافتها والوصول الى أهدافها المرجوة من طريق

---

[21] جوزف ناي، **القوة الناعمة وسيلة النجاح في السياسة الدولية** ، ترجمة محمد البجيرمي ، العبيكان ،2007، ص24.

[22] أحمد جلال، مرجع سبق ذكره ، ص 49-54.

[23] عادل عبد الصادق، **" أثر الإرهاب الإلكترونى على مبدأ استخدام القوة فى العلاقات الدولية "**، رسالة ماجيستير، جامعة القاهرة ، 2001-2007 ، ص 42.

الجذب والاستمالة ، وهو ما يعرف بالقوة الناعمة، وكانت هذه أبرز تحولات للقوة الصلبة الى الناعمة .

2-2- القوة الناعمة : soft power

لاحظ آدم سميث أن الناس تقودهم يد خفيّة عندما يتخذون قراراتهم، والتي كثيرا ما تشكّلها القوى الناعمة . فعلى سبيل المثال يمتلك الفاتيكان قوة ناعمة من طريق سلطته الدينية . وقد كان "كينيدي" من الرؤساء اللذين انتبهوا الى أهمية القوة الناعمة ، حيث كان يفهم بأنّها القدرة على اجتذاب الاخرين وهذا ما تشيره استطلاعات الرأي العام ، التي أظهرت أهمية الولايات المتحدة الأميركية وشعبيتها في العالم . وقد صَرح الرئيس السابق لمجلس النواب الأميركي نيوت غينفرتش :"إن المفتاح الحقيقي ليس في عدد الأعداء الذين أقتلهم، بل إنّ المفتاح الحقيقي هو عدد الحلفاء اللذين أكسبهم ، وهذا مؤشر مهم لا يفهمونه أبدا .[24]

ولقد عرّف جوزف ناي مخترع مفهوم "القوة الناعمة" أنها ببساطة " **القوة الجذّابة** "، وتمتلك ثلاثة أنماط : الجاذبية (Attraction) ، والاقناع (persuation) ، ووضع جدول للأعمال (Agenda Setting) . وترتكز القوة الناعمة لبلد ما على ثلاثة موارد : هي ثقافته حيث (الأماكن التي تكون فيها جّذابة للاخرين) ، وقيّمه السياسية (عندما يطبقها باخلاص في الداخل والخارج) ، وسياسته الخارجية (عندما يراها الاخرون مشروعة وذات سلطة معنوية)[25]. وتشكل القوة الناعمة أحد أشكال القوة التي تستخدمها الدول في سياستها الخارجية ، كما أنها تسلك اطارا عاما من الأنماط والسلوكيات الثقافية التي تسعى من خلالها الى تحقيق أهدافها ، وذلك عبر مجتمع المعلومات مثل نشر الأفكار والثقافة الأميركية من خلال الاعلام ومن

[24] جوزف ناي، مصدر سبق ذكره ، ص11.
[25] المصدر نفسه ، من ص26_32.

طريق دعم القنوات الاذاعية والتلفزيونية والفضائيات ، فعلى سبيل المثال : تظهر تجليات هذه القوة لدى الولايات المتحدة الأميركية من خلال الترويج لثقافتها وعولمتها عالمياً ، وهذا يبدو واضحاً وجلياً من رواج ثقافة " الجينز ، والمأكولات السريعة (fast food) او ما أصبح يدعى Junk food اضافة الى عالمية اللغة الانكليزية ....."

أما تأثير التكنولوجيا فقد تمّ من طريق استغلال مواقع التواصل الاجتماعي الفيسبوك وتوتير والواتس اب) من أجل دعم النظم المعارضة و التحكّم بالجماهير وتحريضها بالاساليب الاقناعية من دون اللجوء إلى العنف (منها تسريبات موقع ويكيليكس حول ثورات الربيع العربي) .

3-2- **القوة الالكترونية Electronic power .**

ترتبط القوة الالكترونية بامتلاك المعرفة التكنولوجية والقدرة على استخدامها، وهى القدرة على استخدام الفضاء الالكترونى والمعلومات للتأثير فى الأحداث على النحو الذى يحقق الأهداف المرجوة باستخدام الوسائل والأدوات الالكترونية .

أما جوزيف ناي فقد اعتبر أنها مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحواسيب والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل ، ويرى أن القوة الالكترونية فرضت تحديات على الأطراف الدولية وخاصة الكبرى والتى كانت تحتكر مصادر القوة مثل الولايات المتحدة الأمريكية ، وانتقال القوة وانتشارها بين أطراف متعددة سواء كانت دول أو غير دول يؤدي الى تهديد أمنها واستقرارها .

وقد حدد " **ناي** " ثلاثة أنواع من الفاعلين والذين يمتلكون القوة الالكترونية وهم : الدول والأفراد والفاعلين من غير الدول .

1. **الدولة:** وهي تمتلك القدرة على تنفيذ هجمات الكترونية ، وتطوير البنية التحتية وممارسة السلطة ضمن حدودها.
2. **الفاعلون من غير الدول:** وهم قادرون على احداث اختراقات لمواقع الكترونية ، واستهداف أنظمة الاتصالات الدفاعية وتنفيذ أعمال ارهابية . وهم لايمتلكون مقومات الدولة نفسها في الهجومات الافتراضية ، ولكنهم يشكلون خطراً كبيراً على البيئة الدولية لقيامهم بالأعمال التخريبية . وحسب ناي يمكن أن تكون القوة الافتراضية مصدرا للقوة الناعمة كما في حالة اتجاه الدولة لوضع معايير ملزمة للبرمجيات . او يمكن أن تستخدم كقوة صلبة من طريق الحرمان من خدمات الانترنت ، أو قطع الانترنت نهائيا عن الدولة .[26]
3. **الأفراد:** وهم الذين يمتلكون معرفة الكترونية ويستطيعون توظيفها ، ولكن تصعب ملاحقتهم والكشف عن هويتهم .

4-2- القوة الذكية Smart power

إن مفهوم القوة الذكية ليس مفهومًا جديداً أو مبتكرًا ، وإنّما هو نتاج الجمع بين القوة الصلبة والقوة الناعمة معاً ولكن وفقاً لاستراتيجية محددة تجمع بينها . ويعّرف ارنست ويلسون القوة الذكية على أنها قدرة الفاعل الدولي على مزج عناصر القوة الصلبة والقوة الناعمة بطريقة تضمن تدعيم تحقيق الأهداف بكفاءة وفعالية . ويحدّد هذا التعريف مجموعة من الشروط الإضافية التي يجب توافرها لتحقيق القوة الذكية .[27]

---

[26] Joseph s.Nye , reference previous seen.

[27] Ernest J. Wilson, III, "**Hard Power, Soft Power, Smart Power**", Annals of the American Academy of Political and Social Science, Vol. 616, Public Diplomacy in a Changing World (Mar., 2008), pp. 110-124, Published by: Sage Publications, Inc. in association with the American Academy of Political and Social Science, Article Stable URl,p.112-114.
: http://www.jstor.org/stable/25097997

وتعتبر القوة الناعمة، في نظر **ناي،** بأهمية القوة الصلبة نفسها كل منه يدعم الآخر، ففي حين أن القوة الصلبة تعد أساساً للقوة الناعمة حيث أنها تزيد من جاذبية الدولة وكذلك قدرتها على التأثير واستخدام مصادر القوة الناعمة وتوجهيها في الإتجاه المناسب ؛ فإن القوة الناعمة هي الأخرى توفر للقوة الصلبة غطاء الشرعية في عيون الأخرين ، وبالتالي تقابل مقاومة أقل لطموحاتها [28]. كما أكد ناي على :" أن القوتين الصلبة والناعمة مترابطتان لأنهما معا من جوانب قدرة المرء على تحقيق أغراضه بالتأثير على الاخرين . وما يميز بينهما هو الدرجة في طبيعة السلوك ". [29]

وفي المحصّلة أحدث التطور السريع لتكنولوجيا الكمبيوتر وخصوصاً في الشبكات تحولاً كبيراً في مفهوم القوة ترتب عليه دخول المجتمع الدولي في مرحلة جديدة تؤدي فيها هجمات الفضاء الإلكتروني دوراً أساسياً سواء في تعظيم القوة أو الاستحواذ على عناصرها الأساسية. وأصبح التفوق في مجال الفضاء الإلكتروني عنصراً حيوياً فى تنفيذ عمليات ذات فاعلية في الأرض وفي البحر والجو والفضاء واعتماد القدرة القتالية في الفضاء الإلكتروني على نظم التحكم والسيطرة . [30]

فبجانب قوة الدولة الصلبة والناعمة ، ظهر الفضاء الالكتروني أو القوة الإلكترونية والتي أصبح لها تأثيرها على المستويين المحلى والدولي ، حيث أدت إلى تعدد مستويات القوى بين الفاعلين ولم تعد استخدام القوة حكراً على الدولة ، كما مكنت صغار الفاعلين في السياسة الدولية من ممارسة كل من القوة الصلبة والناعمة عبر الفضاء الإلكتروني ، وهو ما يعنى

---

[28] JOSEPH. Nye, J**, "Soft Power" Foreign Policy**, No. 80, Twentieth Anniversary (Autumn, 1990), pp. 167, Published by: Washingtonpost.Newsweek Interactive, LLC, Article DOI: 10.2307/1148580, Article Stable URL: http://www.jstor.org/stable/1148580

[29] جوزف ناي، مرجع سبق ذكره ، ص 27.

[30] Arsenio T. Gumahad**, Cyber Troops and Net War: The Profession of Arms in the Information Age**. Maxwell AFB, AL: Air University, Air War College, April 1996. pp.57-156.

تغيراً في علاقات القوى في السياسة الدولية ومن هنا يمكن التمييز بين مستويين للتغير الذي طرأ على مفهوم القوى وهما: المستوى الخاص بالعناصر المكونة للقوة، والأشكال المختلفة للقوة، ومستوى الفاعلين الممتلكين للقوة وخصوصا الفاعلين من غير الدول .[31]

المطلب الثاني : أثر الفضاء الالكتروني في تغيير طبيعة العلاقات الدولية .

عكست عملية تغيير طبيعة القوة في العلاقات الدولية طبيعة التغيرات الأفقية والرأسية في النظام الدولي ، والتي كان فيها للبعد التكنولوجي والاتصالي دور مهم سواء على مستوى الثورة في الشؤون العسكرية أو في ما يتعلق ببروز مجال جديد للصراع الدولي أو ما يتعلق بانتشار القوة الاقتصادية وانتقال معايير القوة القومية من خصائص السكان والمساحة وعدد الجيش والموارد إلى ابعاد جديدة تتعلق بدور الدولة في الابتكار والإنتاج التكنولوجي .[32] وأصبح العالم يشهد تطورا في المخاطر الأمنية مع تطور مراحل النضج التكنولوجي ، ومع الانتقال من مرحلة النمو السريع إلى مرحلة الاستخدام الكثيف ، وأصبحت قضية أمن الفضاء الإلكتروني تلقى اهتماماً متصاعداً على أجندة الأمن الدولي وذلك في محاولة لمواجهة تصاعد التهديدات الإلكترونية ودورها في التأثير في الطابع السلمي للفضاء الإلكتروني ، وباتت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الإستراتيجية – ذات الطبيعة الإلكترونية – إلى أخطار إلكترونية ، وتهدد بتحول الفضاء الإلكتروني لوسيط ومصدر لأدوات جديدة للصراع الدولي المتعدد الطرف ودورها تغذية التوترات الدولية ، وهو ما يفرض تحديات تتعلق بإعادة تعريف الأمن والقوة والصراع . فما هو الفضاء الالكتروني ؟

---

[31] ايهاب توفيق، **مرجع سبق ذكره** .

[32] الفضاء الالكتروني واسلحة الدمار الشامل ، **مؤتمر الحرو ب السيبرانية**
https://seconf.wordpress.com/2015/05/15/الفضـــــاء-الإلكتروني-وأسلحـــة- ال/

1- الفضاء الالكتروني.

الفضاء الإلكتروني هو الوسط الذي تتواجد فيه شبكات الحاسوب ويحدث من خلالها التواصل الإلكتروني ، وقد استخدم ذلك "ويليام جيبسون" لأول مرة مصطلح الفضاء الإلكتروني وهو كاتب في الخيال العلمي وبالأخص في نوع الأدب الذي يعرف باسم الشر الإلكتروني .[33]

ويعمل الفضاء الإلكتروني تحت ظروف مادية غير تقليدية حيث يكون وسيطاً عبر العمل من خلال أجهزة الكمبيوتر وشبكات الاتصال ، حيث يختلف عن الجو أو الفضاء الخارجي في أن الفضاء الإلكتروني يعمل وفق قوانين فيزيائية مختلفة عن قوانين الفضاء الخارجي ، فمثلاً لا تزن المعلومات شيئاً ولا تمتلك كتلة مادية وبإمكان المعلومات أن تظهر للوجود وتختفي منه ويتم تعديل وتبادل المعلومات من خلال نظم مرتبطة بالبنية التحتية ، ويتطلب الفضاء الإلكتروني وجود هيكل مادي من أجهزة الكمبيوتر وخطوط الاتصالات ، ومن ثم فإن ما يعمل داخل هذه الأجهزة يمثل نمطاً من القوة والسيطرة ، وتصبح القيمة الحقيقة للفضاء الإلكتروني هي الاستفادة من كم المعلومات الموجودة داخله والمساهمة في التحكم بها في إطار وشكل إلكتروني .[34]

تعريف قاموس اوكسفورد لمصطلح الفضاء السيبرانى انه :" البيئة الافتراضية التى يتم عبرها اتمام عملية الاتصال عبر شبكات الكمبيوتر". و استنادا الى التعريف البسيط والواضح هذا يمكن اعتبار الحروب السيبرانية هى أشكال الصراع ذات الاهداف السياسية الحادثة داخل هذه البيئة الافتراضية والذى أعتقد أنّه تعريف كافي لتحديد مجال الحروب السيبرانية لا طبيعتها و أهدافها الاستراتيجية .[35]

---

[33] **الفضاء الإلكتروني** ، http://www.arabic-military.com/t117864-topic

[34] ايهاب خليفة ، مرجع سبق ذكره ، ص11.

[35] محمود فخر الدين، **حدودالمجال الخامس** ،مايو2015/150 ،على الرابط الالكتروني:

" الفضاء الالكتروني يتمّ في اطار المجال الالكتروني لاستخراج المعلومات من خلال الشبكات السلكية للحاسوب ". [36]

و أيضا " الفضاء الإلكتروني هو المجال الذي تطير به وتحارب القوات الجوية ".[37]

و الفضاء الإلكتروني عبارة عن مجال طبيعي ومادي ويرى آخرون أنه ذا طابع افتراضي حيث يرونه بأنه تلك البيئة الإفتراضية التي تعمل بها المعلومات الإلكترونية والتي تتصل عن طريق شبكات الكمبيوتر، كما يُعرف بأنه " **ذلك المجال الذي يتميز بإستخدام الإلكترونيات والمجال الكهرومغناطيسي لتخزين وتعديل أو تغيير البيانات من طريق النُظم المُتصلة والمُرتبطة بالبنية التحتية الطبيعية** ". ومن ثم فانّه يشمل عملية الاندماج ما بين الإنترنت والمحمول وأجهزة الاتصالات والاقمار الصناعية . [38]

هناك ثلاثة عناصر أفرزتها ثورة المعلومات ، هي المعلومة ، Information ، والطابع الالكتروني Digital ، والفضاء الالكتروني Cyberspace المقتبسة من علم Cybernetics . وهو عبارة عن نظرية الاتصالات والتحكم في المنظم في التغذية المرتدة التي تعتمد عليها دراسات الاتصالات والتحكم في الحياة وفي الاليات التي صنعها الانسان أي علم دراسات الاتصالات والتحكم الالي في النظم العصبية للكائنات الحية ومحاكاة الالات لها . وتستخدم كلمة Cyber المرتبطة بكلمة Space لتعبر عن الفضاء السيبراني لتضم كل الاتصالات والشبكات وقواعد المعلومات والبيانات ومصادر المعلومات .[39]

---

https://seconf.wordpress.com/2015/05/15

[36] Daniel T. Kuehl, "**From Cyberspace to Cyberpower: Defining the Problem**," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., Cyberpower and National Security (Washington, D.C.: National Defense UP, 2009) "joseph neye"

[37] Michael Wynne in 2006, . هو رئيس القولت الجوية الأميركية

[38] Joseph s.Nye,"**cyber power**, p.3-5.

[39] عادل عبد الصادق، **الإرهاب الإلكتروني: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة** ،(مركز الأهرام للدراسات السياسية والاستراتيجية،)، القاهرة ، 2009، ص 30 - 40 .

القوة السايبيرية هي القدرة على استخدام الفضاء الالكتروني لخلق مزايا والتأثير على الأحداث في البيئات التشغيلية الأخرى وعبر أدوات القوة .[40]

2- خصائص الفضاء الالكتروني

فالفضاء الالكتروني يعتمد على مجموعة من الموارد التي تتعلق بانشاء مواقع والتحكم والتواصل الالكتروني والكومبيوتر ، بناء على قاعدة من المعلومات والبيانات والبنية التحتية والشبكات والبرمجيات والمهارات البشرية "الموارد المادية " ويشمل شبكة الانترنت من أجهزة الكومبيوتر المتصلة بالشبكات ولكن أيضا الشبكات الداخلية والتقنيات الخلوية والفضاء والأقمار الصناعية "البيئة الافتراضية" ، والقدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء الإلكتروني وتتميز بالتالي بخصائص عدة ومن أهمها:

- يختلف الفضاء الإلكتروني عن الغلاف الجوي والفضاء الخارجي ايضاً يعملان وفق قوانين فيزيائية ، فالمعلومات لا تزن شيئا ، ولا تمتلك كتلة مادية وبامكانها أن تظهر وتختفي من الوجود فهي متقلبة وغير ثابتة ويمكن التحكم بها بكبسة زر .
- لقد جعلت الانترنت العالم قرية واحدة منفتحة بعضها على بعض ، ما أدى الى موت المسافات ، وسهّل عملية وحرية تبادل المعلومات والتواصل والتعارف ، وألغى حدود الزمان والمكان، وأصبح سوقا مفتوحا لجميع أنواع التبادلات التجارية منها أو المعلوماتية ، وملعبا مفتوحاً امام الجميع.

[40] Joseph s.Nye,**"cyber power"**, p.4 .

- أثبتت أنها وسيلة سريعة ورخيصة ويسهل التحكم بها ، كما أنها جعلت المعلومات بمتناول. الجميع ما انعكس سلباً على أمن الدول وحدّ من سيادتها ، وفرض تغييرات جذرية على مفهوم الأمن القومي .[41]
- والفضاء الالكتروني شأنه شأن ظاهرة الفضاء التقليدية التي تتألف من أربعة مكونات رئيسية هي المكان والمسافة والحجم والمسار ويعبر محتواها عن طبيعة وجود هذا المحتوى ويتميز هذا الفضاء الالكتروني بغياب الحدود الجغرافية وغياب الحكم القاهر لعنصر الزمن .[42] اذن فالفضاء الالكتروني هو ذلك المكان الذي اوجدته تكنولوجيا المعلومات والاتصالات وفي مقدمتها الانترنت ، ويرتبط ارتباطاً وثيقاً بالعالم المادي عبر البنى التحتية المختلفة للاتصالات والأنظمة المعلوماتية وعبر العديد من الخدمات التي لم يكن بالامكان الحصول عليها من دونه.

ويعتبر الفضاء الالكتروني هو السمة التي تميز الحياة العصرية والمكون الاساسي للبنية التحتية لمؤسسات الدولة المختلفة القطاعين العام والخاص فضلا عن أهمية حمايتها لما تنطوي عليه في صميمها على الحريات الاساسية للتعبير والتجمع والخصوصية الفردية والتدفق الحر للمعلومات والاتصالات الالكترونية ، ومعالجة البيانات ذات الطابع الشخصي والجرائم السيبرانية والمعاملات الالكترونية والتواقيع الإلكترونية والإثبات الإلكتروني والتجارة الإلكترونية وحماية المستهلك وحقوق الملكية الفكرية في المجال المعلوماتي والسيبراني والاسس الضرورية للفرص والنمو التي بدورها تدفع الى قطاع عالمي مزدهر .[43]

---

[41] ايهاب توفيق ، مرجع سبق ذكره ، ص 20-24.

[42] عادل عبد الصادق، **الارهاب الالكتروني ،: القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة** ، ض 40.

[43] أمن الفضاء الالكتروني ، **اعداد لجنة الفضاء الالكتروني** ، الشركة العامة لخدمات الشبكة الدولية للمعلومات ،ص6 .على الرابط الالكتروني التالي :https://www.scis.gov.iq/upload/upfile/ar/security.doc

3- علاقة الفضاء الالكتروني بالتغييرات في العلاقات الدولية

أسفر تطور التكنولوجيا والفضاء السيبراني عن مجموعة من المتغييرات ، التي انعكست بدورها على طبيعة الدولة وتراجع مكانتها ، وعلى تعدد الفواعل من غير الدول ، اضافة الى تحولات القوة . وتمت عولمة المشكلات والقضايا التي تواجهها الجموع البشرية: مثل الفقر والتخلف والتلوث البيئي والانفجارات السكانية وتغير طبيعة النمو والناتج الاقتصادي وغيرها الكثير الكثير ، حيث لم تعد تقتصر نتائج هذه المشكلات على دولة محددة أو مجموعة دول ، وإنّما تعّدت ذلك الى المجتمع الدولي ككل . شغلت المعلومات حيّزاً مهّماً ورئيساً في النظام العالمي ، لما تمثّل من قيمة اقتصادية وميدانية بالنسبة الى الجهات العسكرية ، و أصبحت مجالا للصراع والسيطرة وبرز مفهوم الحروب الالكترونية (وقد شكّل الفضاء مجالاً و ميداناً جديداً للمواجهة، حيث يمكن ضرب أهداف واسعة تتعلق بالبنية التحتية وتحقيق أهداف مباشرة وخسائر فادحة من دون اراقة الدماء) . ما انعكس على الدول التي أصبحت مكشوفة امنيا واستخباراتيا. أما بالنسبة الى تراجع مكانة الدولة في العلاقات الدولية برزت مجموعة من التحديات أبرزها:

أ- **بروز فاعلين أقوياء من غير الدول في شبكة التفاعلات الدولية:** الشركات المتعددة الجنسية، المنظمات الإقليمية والدولية ، المنظمات غير الحكومية ، رجال الأعمال، الأسواق التجارية ، الجماعات المتمردة والانفصالية والتنظيمات الارهابية ...الخ.

ب- **تراجع دور الدولة القومية** ، وظهور مفهوم الأمن الجماعي والتدخل الانساني المعارض لقوانين الأمم المتحدة والمحافظة على سيادة الدول .

ت- **التجسس :** وساعد الفضاء الإلكتروني على أن تكون دولة ما مكاناً لانطلاق عمل الاعتداء ضد دولة أخرى خارجية مع عملية الربط بين شبكات الكمبيوتر والإنترنت بين دول العالم، وتجاوزها للحدود التقليدية وسيادة الدول، ولم تعد الدول المعتدية في حاجة إلى إرسال عصابات أو جماعات مسلحة أو الدفع بمجالات التجسس وتجنيد العملاء عبر الفضاء الإلكتروني بهدف اختراق الدول الأخرى.

ث- **الانكشاف الأمني :** أصبحت الدول مكشوفة من الناحية الأمنية والمعلوماتية والاستخباراتية .

ج- **الارهاب أو التطرف :** تم توظيف التطرف ذي الخلفيات الدينية أو القومية لتحويل استخدام التكنولوجيا من أداة مدنية إلى أداة عسكرية وذات ابعاد تخريبية.[44]

ح- **بروز ظاهرة الحروب الالكترونية :** حيث كشف استخدام الفضاء الإلكتروني عن حال التعارض الحقيقي أو المتخيل للاحتياجات والقيم والمصالح بين العديد من الأفرقاء سواء أكانوا دولاً أو أفراداً أو جماعات أوشركات ، وبما ساعد على بلورة أساليب للصراع الدولي ذات الطابع التقني والتجاري والاقتصادي والعسكري ، إلى جانب ظهور طرائق بديلة عن الحرب المباشرة بين الدول أو بين الخصوم عبر شبكات الاتصال والمعلومات . [45]

---

[44] Martin C. Libicki **, Conquest in Cyberspace:National Security and Information Warfare** , Cambridge University Press , 2007 ,pp1-14.

[45] Myriam A. Dunn**," The Internet and the Changing Face of International Relations and Security**", Vol. 7, Issue number: 1, ProCon Ltd., Sofia, Bulgaria, 2001.

المطلب الثالث : الفضاء الالكتروني وأهميته في حروب المستقبل .

شهدت السنوات الأخيرة تحولات وتغيرات جذرية في مفاهيم الأمن والحرب ونظرياتها ، ومن ثم لحقت هذه التغييرات بالعقائد القتالية للجيوش . وظهرت مفاهيم ونظريات عسكرية جديدة ولدت من رحم التهديدات الأمنية غير التقليدية التي برزت على الساحة العالمية في العقدين الأخيرين ، وباتت مصطلحات مثل :" الحروب اللامتماثلة " [46] أو الهجينة [47]، واقعا خاضته العديد من الجيوش الكبرى في مناطق شتى من العالم . كما تجلّت "الحروب الالكترونية "[48]، على أرض الواقع وهبطت من الفضاء النظري الذي رسم سيناريوهاتها وتأثيراتها المحتملة طوال سنوات مضت ، ما يعكس عمق الخطر الاستراتيجي الذي يترتب على حروب الفضاء الالكتروني ، التي دفعت الأمن المعلوماتي الى ان يشغل صدارة الأمن في القرن الحادي والعشرين ، بناء على التهديدات المعاصرة والطبيعة المتغيرة للحرب ، والتهديدات الجديدة للأمن القومي، والدور المستقبلي للتكنولوجيا في الاستخدام العسكري ، وكذلك الجوانب السياسية والمدنية المؤثرة في الحروب المستقبلية ، بالإضافة إلى العلاقة بين شركات تصنيع الأسلحة والمؤسسة العسكرية، والأبعاد الاستراتيجية لتلك العلاقة ، ومستقبل الحرب والاستقرار في الشرق الأوسط .

أن هناك متغيرات مؤثرة في أنماط حروب المستقبل وخططها ، أهمها التوجه العالمي نحو تقليص الإنفاق العسكري، بصورة غير مسبوقة ، بحيث يصبح أكثر تركيزاً على الكيف ، إلى

---

[46]"الحرب اللامتماثلة": هي محاولة طرف يعادي الولايات المتحدة الأمريكية أن يلتف من حول قوتها ويستغل نقط ضعفها , معتمداً في ذلك على وسائل تختلف بطريقة كاملة عن نوع العمليات التي يمكن توقعها. وعدم التوازي في الامكانيات والتكتيك

[47] Jérôme Maire**, Stratégie hybride, le côté obscure de l'approche globale** ?,tribune n0 811,sur website: www.defnat.fr - 02 septembre 2016.

[48] هي مجموعة الاجراءات التي تقوم بها القيادة العامة والافرع الرئيسية للقوات المسلحة والاسلحة والتشكيلات لخرق النظم الالكترونية التي يستخدمها العدو في القيادة والسيطرة على قواته واسلحته ومعداته، ومقاومة استطلاع العدو اللاسلكي والراداري وتحقيق استقرار عمل النظم الالكترونية التي تستخدمها قواتنا في القيادة والسيطرة وذلك تحت ظروف استخدام العدو لاعمال الاعاقة الالكترونية.

جانب ظاهرة الإرهاب ، والحرب المعلوماتية التي تغري بشن هجمات إلكترونية ذات تكلفة اقتصادية باهظة . انّ الواقع الدولي العام يشير الى أن تكنولوجيا المعلومات هي عصب حروب المستقبل ومحور ارتكازها ، فالعالم الذي يمر بأول إرهاصات عصر المعلوماتية، ويشهد موجاتها الأولى في تجليات مختلفة، باتت تؤثر أشد التأثير في المجالات كافة ، يمر أيضاً بفورة هائلة في مجال التصنيع الدفاعي، اعتماداً على تكنولوجيا المعلومات .

كما إن ظاهرة الإرهاب ستظل ، أحدى أهم التحديات المستقبلية التي تهدد الأمن والاستقرار العالميين، كما أن الأجيال المقبلة من الإرهابيين تمثل تحدياً يفوق من سبقهم على المستويات التنظيمية والتنفيذية وطبيعة الأهداف والأدوات، في ظل نزعة التنظيمات الإرهابية إلى بناء هياكل هلامية عابرة للجغرافيا والقوميات ، بحيث أصبحت القضايا الإيديولوجية والسياسية هي المحرك الأساسي ، وشبكات التواصل الاجتماعي هي المراكز الافتراضية لإدارة العمليات ،ما يدفعنا إلى بناء توقعات بشأن تطور الخبرات القتالية للإرهابيين ، مع تنامي صعوبات ملاحقتهم ورصد تحركاتهم . إذ إن حالات التدخل العسكري ، سواء لأغراض إنسانية أو لحماية المدنيين أو لغير ذلك ، ربما تفرض بدورها تحالفات وقتية تتطلب أنماطاً تسليحية محددة تختلف باختلاف حالات التدخل ومتطلباته العسكرية واللوجستية .[49]

كما أن التطوّرات الراهنة سلطت الضوء على بنى تحتية استراتيجية جديدة يكاد الأثر الناجم عن استهدافها يضاهي تأثيرات التعرض لهجمات بأسلحة الدمار الشامل ، مثل البنى التحتية المعلوماتية، التي قد يؤدي استهدافها بهجمات إلكترونية إلى خسائر هائلة ، قد ترتقي إلى شل قدرات الدول على الحركة ، كالأنظمة المعلوماتية الخاصة بالتحكم في المواصلات

[49] جمال سند السويدي ،عسكريون: تكنولوجيا المعلومات عصب حروب المستقبل ، **مجلة الاتحاد** ، المؤتمر السنوي الثامن عشر ،مركزالامارات للدراسات والبحوث الاستراتيجية، على الرابط الالكتروني التالي: http://www.alittihad.ae/details.php?id=35263&y=2013&article=ful

والمصارف ، وأسواق المال وشركات النفط وغير ذلك من أمور تعكس بروز التهديدات الإلكترونية ، كأحد أبرز التحديات التي تواجه الأمن القومي للدول في القرن الحادي والعشرين، وبروز حماية المجال المعلوماتي للدول كإحدى أولويات التخطيط الأمني والعسكري .[50]

وقد أصبح هذا البعد حاضراً منذ أن أوجدت الثورة المعلوماتية ما يسمى المجال المعلوماتي العالمي الموحد. وحول خطورة هذا البعد في الصراع نشير إلى تأكيد الخبراء والمحللين العسكريين الأميركيين والروس والصينيين على حجم الضرر الذي قد يلحق باقتصاد البلد ، جراء حدوث خلل جوهري في الأداء الوظيفي لمنظومة الحواسيب الموجودة بكثافة في كل التنظيمات القيادية الحكومية والمؤسسات المالية والمصرفية . ضرر يمكن مقارنته من حيث العواقب باستخدام السلاح النووي، الأمر الذي يؤدي إلى نتائج كارثية في بعض الحالات على مستوى حياة السكان. وهو قد يؤدي بدوره إلى الاستياء العام والثورة الاجتماعية وسقوط الدولة أحياناً .

1- حروب المستقبل على شبكة الإنترنت .

انَّ الحروب المقبلة قد تبدأ بهجوم سيبراني من أجل شل فاعليَّة النُظُم الإلكترونيَّة للمنشآت الحيويَّة، العسكريَّة والمدنيَّة (مثل الكهرباء والمياه والطاقة والاتِّصالات والمواصلات والبنوك)، فتنهار لاحقًا، ما يُفضي إلى وَيْلات أعظم من المُنازعات المُسلَّحة التقليديَّة . ويُمكن أنْ تكون هذه الحرب إمَّا مُباشرة (بين دولتين أو أكثر) أو من خلال وكيل – أو طرف ثالث . ويبدو أّن الصراع المسلح غير التقليدي أصبح أكثر انتشاراً اليوم من أي وقت مضى ، وقد تلجأ أطراف فاعلة من غير الدول الى أساليب الحرب المسلحة لتحقيق أهدافها ولهذا التطور

[50] **جمال سند السويدي** ، المصدر نفسه .

آثار قوية تنعكس على العلاقات المدنية – العسكرية في سياق الصراع . كما ان انتشار الأسلحة على نطاق واسع ، ووجود دول ضعيفة وفاشلة ، وظهور (أو عودة ظهور) أيديولوجيات أكثر من أي وقت مضى ، يوّفر أرضا خصبة ،لحالات طوارىء معقّدة ، قد لا تنطبق عليا صفة الحرب التقليدية ، ولكنها تتطلب مع ذلك ردود فعل دبلوماسية واقتصادية وعسكرية .

" كشفت صحيفة نيويورك تايمز أنّ الدول الكبرى تتعرض على مستوى دوائر القرار والشركات الضخمة الى اختراقات تَتَداخل فيها الأهداف العسكريَّة بالأهداف الاقتصاديَّة، أو ما يُعرَف بالتجسُّس الصناعي. وقدرة هائلة قادرة على اختراق الحواجز الأمنيَّة للمعلومات السريَّة لدى الخصم أو المُنافس، وقرصنتها. وقد أشارت إلى التحليلات الجنائيَّة السيبريَّة والتي بَرْهَنت أنَّ وحدة المُحاربين السيبريّين في الجيش الصيني هي المسؤولة، مع مستوى طفيف من الشك ، عن غالبيَّة الهجمات التي تعرَّضت لها الشركات الأميركيَّة وحتى الوزارات" .[51]

لذا من المرجح أن تبقى الحرب اللامتماثلة , asymmetric warfare , والارهاب الدولي من المميزات المحددة للقرن الحادي والعشرين ، وهاتان الظاهرتان غير جديدتين ، لأنهما تشكلان جزءا من المنظومة الدولية منذ أواخر القرن التاسع عشر على الأقل . ولذلك فانّ فهم الحرب اللامتماثلة والارهاب الدولي يعدّ أمراً أساسياً لفهم مستقبل العنف بين الدول والعنف داخل الدول. وقد التقت الجيوسياسية والتكنولوجيا في أحداث 11 أيلول 2011 وتداعياتها حيث استغل تنظيم القاعدة البنية التحتية العالمية للاتصالات والمواصلات لشن الهجمات ، وسرعان ما أصبح الرد الأميركي المدّمر في الحملات التقليدية الأولى ضد أفغانستان والعراق

[51]معمر عطوي ونزار عبود حول "الوحدة 61398» تتَّخِذ من شنغهاي مُنطلقًا لهجماتها"، **صحيفة الأخبار اللبنانيَّة** في 21/ 02/ 2013.

غارقا في حرب غير متكافئة [52]. وبالتوازي مع الحملات الأميركية برزت نماذج من الحروب غير المتكاقئة مثل المواجهات بين "إسرائيل" وحركات المقاومة أمثال "حماس" و "حزب الله" وأيضا السعودية والعدوان على اليمن كما الحرب الكونية على سوريا .

وقد تسبب هذا في قيام الكثير من الجيوش لا سيما الجيش الأميركي بالنظر الى هذا الموضوع بطريقة سلبية ، بحيث يعتبرها تحدّيا لتفوقه العسكري . وفي الخطاب الذي ألقاه الجنرال مارتن ديمبسي ، رئيس هيئة الأركان الأمريكية المشتركة في أوكتوبر 2012 ، أشار الى هذا التحدي وقال الاتي: " لطالما كان هناك نوع من التباين في الحرب، ولكنه أكثر انتشاراً حيث أن خصومنا سيسعون وسيجدون الأساليب لمواجهة جوانب التفوق الذي نتمتع به ، وتعزيز بعض مزاياهم من خلال الحرب اللامتماثلة " . [53]

وبالمحصلة تعد حرب الطائرات بدون طيار من أهم وسائل هذه الحروب ذات القدرة المالية الهائلة والعلاقات السياسية والتي من أبرز سماتها المرونة ، حربا مفتوحة أمام الولايات المتحدة وحلفائها في المستقبل المنظور ، ما سيجعلها قدرة لامتماثلة للغاية . كما أن في الحروب المستقبلية اللامتماثلة لا تنفع معها قوة نيران ولا سيطرة مطلقة على الجوّ والبرّ والبحر، لأنّها ببساطة حروب استنزاف طويلة الأمد تقاتل خلالها "أشباحاً" ، لا جيوشاً نظامية تعتمد تكتيكات لا علاقة لها بالحروب التقليدية . كما أن الاستراتيجية العسكرية للحرب المستقبلية ، انتقلت من الاستراتيجية التقليدية إلى الاستراتيجية الفضائية ، كما تغيّرت طبيعة الحرب بتغيير وسائل الصراع المسلح الى الحرب الالكترونية ، ميدانها الشبكات والانترنت

---

[52] أوستن لونج ، الحروب اللامتماثلة في القرن الواحد والعشرين الارهاب الدولي والتمرد وحرب الطائرات من دون طيار، **الحروب المستقبلية في القرن الواحد والعشرين** ، مركز الامارات للدراسات والبحوث الاستراتيجية. على الرابط الالكتروني التالي: ecssr.com/ECSSR/print/pb.jsp?lang=ar&publicationId=/Publications/Books

[53] U S Joint Chlefs of Staff ,"**Gen.Dempsey s Remarks at Kansas State University s landon lecture series,"**General Martin E. Dempsey,octobre 1,2012(http://www.jcs.mil/speech.aspx?id=1731).

كما يتجلَّى تأثير استخدام الفضاء السيبراني في خمسة أمور مهمَّة: إضعاف المفهوم التقليدي للدولة العسكريَّة ، تَغيير في مضمون الجندي (أو المُقاتل أو المُحارب) والسلاح ومدلول الدولة الصغيرة ، وتَقييد مبدأ سيادة الدولة، وتَشَتُّت المسؤوليَّة الدوليَّة ، وتَغْييب مبدأي الضرورة والإنسانيَّة .[54]

[54] راجع ما أورده الموقع الإلكتروني للجنة الدوليَّة للصليب الأحمر حول موضوع "Cyber warfare" في 29/ 10/ 2010، وهذا ثَبْت بالجملة الإنكليزيّة:

"Cyber warfare adds a new level of complexity to armed conflict that may pose novel questions for IHL. (…). The norms in international humanitarian law covering such issues as the use of indiscriminate weapons, distinction between military targets and civilians, proportionality and perfidy, can and must be applied also to cyber warfare.(تصفُّح بتاريخ 9/ 04/ 2014) ,"

المبحث الثاني : العلاقة بين أمن المعلومات والأمن القومي.

بعد أحداث 11 سبتمبر 2001 بدأ التركيز على الفضاء الإلكتروني كتهديد أمني جديد بفعل أحداث دولية ، كان أبرزها استخدام تنظيم القاعدة له كساحة قتال ضد الولايات المتحدة وفي عام 2007 برز بوضوح دور الفضاء الإلكتروني كمجال جديد في العمليات العدائية في الصراع بين استونيا وروسيا وفي 2008 في الحرب بين روسيا و جورجيا، وجاء الهجوم الإلكتروني بفيروس "**ستاكسنت**" على برنامج إيران النووي عام 2010 ليمثل نقلة مهمة في مجال تطور الاسلحة الإلكترونية . وعلى الرغم من الدور السياسي الذي لعبته شبكات التواصل الاجتماعي في الثورات العربية مطلع عام 2011 إلا انها مثلت نقطة مهمة لمضاعفة الاهتمام الدولي بأمن الفضاء الإلكتروني ، وبرزت محاولات للسيطرة عليها بعد تصاعد الاحتجاجات في أكثر البلدان المتقدمة لا سيما بريطانيا والولايات المتحدة .[55]

وفي خلال العقد الأخير شهد المجتمع الدولي صعود قضايا الأمن الإنساني المشترك . والتغير في المجال الاقتصادي والاعتماد المتبادل وضعف دور الدولة وبروز الفاعلين من غير الدول .[56]

في ظل التطور الحاصل بالتكنلوجيا الحديثة والاتصال والانتشار الكبير للشبكات الالكترونية والسرعة التي توفرها جعل منها موردا مهما للعديد من الدول في بناء منظوماتها المالية والحكومية والعسكرية وبناء مجتمعاتها المعلوماتية حيث قدرت الزيادة الحاصلة في استخدام الانترنت من 360 مليون نسمة لعام 2000 الى نحو 2 مليار نسمة لعام 2010 اضافة

---

[55] الفضاء الالكتروني وأسلحة الدمار الشامل،**مؤتمر الحروب السيبرانية**، الانتشـــار الشـــامـــل بين ... https://seconf.wordpress.com/2015/05/15/الفضـــــاء-الإلكتروني-وأسلحـــة-ال/

[56] مصطفي علوي ،"**مفهوم الأمن في مرحلة مابعد الحرب الباردة**"، قضايا الأمن في أسيا ، مركز الدراسات الأسيوية ، كلية الإقتصاد والعلوم السياسية ، القاهرة،2004 ، ص 14.

الى الزيادة المتوقعة في ظل الانتشار الذي يشهده الفضاء الالكتروني وتشعبه في نسيج الحياة والأموال والأفراد بين دول العالم .[57] ما استدعى احداث تغييرات على مستوى أمن المعلومات سيّما في عصر المعلومات ، وتضم مستويين :

الأول: مستوى تعقب المعلومات وجمعها ، ويشمل الوسائل التقليدية لجمع المعلومات التى تعتمد بشكل كبير على العناصر البشرية من الجواسيس أو ما يعرف بالطابور الخامس ، ووسائل الاستطلاع الحديثة وفى مقدمها الأقمار الصناعية التي تطورت في شكل كبير, حيث بلغت الصور والمعلومات الواردة منها حدا فائقا من الجودة والدقة لم تبلغها من قبل .

الثاني: مستوى يستهدف إفساد المعلومات وتعطيلها، ويستخدم فيه العديد من الأدوات كفيروسات الحاسب والاختراق المباشر لشبكات المعلومات والهجوم بفيض الرسائل والطلبات وهجمات الاختناق المروري الإلكتروني على نطاق واسع وغيرها.

المطلب الأول: الأمن القومي وعصر المعلومات.

على الرغم من حداثة الدراسات في موضوع الأمن فإن مفاهيم الأمن قد أصبحت محددة وواضحة في فكر وعقل القيادات السياسية والفكرية في الكثير من الدول.. وقد برزت كتابات متعددة في هذا المجال ، وشاعت مفاهيم بعينها في إطاره لعل أبرزها "الأمن القومي الأمريكي" و"الأمن الأوروبي" و"الأمن الإسرائيلي" .

[57] أمن الفضاء الالكتروني ،**اعداد لجنة الفضاء الالكتروني** ، الشركة العامة لخدمات الشبكة الدولية للمعلومات ، ص6. على الرابط الالكتروني :https://www.scis.gov.iq/upload/upfile/ar/security.doc

1- الأمن القومي

في مجال التوصل إلى مفهوم متفق عليه "للأمن"، فإنه يجدر بنا التعرف على ذلك المدلول في إطار المدارس الفكرية المعاصرة . تعرف دائرة معارف العلوم الاجتماعية "الأمن الوطني " بأنه "مقدرة الدولة على حماية قيمها الداخلية من التهديدات الخارجية".

الأمن من وجهة نظر دائرة المعارف البريطانية يعني "حماية الأمة من خطر القهر على يد قوة أجنبية". وهناك اتجاه آخر لتعريف الأمن، حيث يعرف لورنس كروز، وجوزيف ناي الأمن بأنّه " غياب التهديد بالحرمان الشديد من الرفاهية الاقتصادية " .

ولعل أدق مفهوم "للأمن" هو ما ورد في القرآن الكريم في قوله – سبحانه وتعالى –: "فَلْيَعْبُدُوا رَبَّ هَذَا الْبَيْتِ * الَّذِي أَطْعَمَهُم مِنْ جُوعٍ وآمَنَهُمْ مِنْ خَوْفٍ". ومن هنا نؤكد أن الأمن هو ضد الخوف ، والخوف بالمفهوم الحديث يعني التهديد الشامل، سواء منه الاقتصادي أو الاجتماعي أو السياسي، الداخلي منه والخارجي .

ورد في قاموس وزارة الدفاع الأميركية:" ان الأمن القومي هو مصطلح كلي يشمل كلا من الدفاع الوطني والعلاقات الخارجية للولايات المتحدة ، وهو على وجه التحديد ، الذي يحقق التميز العسكري أو الدفاعي على أي دولة أجنبية أو مجموعة من الدول ، وهو الذي يوفر المواقف المؤاتية للعلاقات الخارجية ، ويحقق الموقف الدفاعي القادر على المقاومة بنجاح ضد أي عمل عدائي أو مدمر سواء من الداخل أو الخارج سواء ان كان ذلك في شكل معلن أو سري .[58]

ومن وجهة نظر هنري كسينجر، وزير الخارجية الأمريكي السابق يعني أي تصرفات يسعى المجتمع من طريقها إلى حفظ حقه في البقاء . غير أن الاتجاه الأهم الذي يربط الأمن

[58] http://www.dtic.mil/doctrine/dod_dictionary/data/n/646.html

بالاقتصاد هو تعريف روبرت ماكنمارا الذي يقول: "إنّ الأمن هو التنمية ، ومن دون التنمية لا يمكن أن يكون هناك أمن " . ويرتبط بهذه التعريفات أبعاد الأمن القومي ، التي تمثل بدورها مجموعة العناصر التي يؤدي وجودها أو غيابها إلى استقرار الأمن القومي للدول أو تدنّيه ، وهو ما يرتبط أصلاً بوجودها وقدرتها على حماية الشعب ضد أي اعتداءات داخلية أو خارجية، ويضمن سلامة الدولة ضد المعتدين الخارجيين أو من الداخل، ومنها البعد العسكري، والسياسي ، والاقتصادي، والاجتماعي، والثقافي، الجيوبوليتيكي، والديموغرافي.

ويقول مكنمارا " الأمن يعني ،التطور والتنمية، سواء منها الاقتصادية أو الاجتماعية أو السياسية في ظل حماية مضمونة ".[59]

إنّ الأمن الحقيقي للدولة ينبع من معرفتها العميقة للمصادر التي تهدد مختلف قدراتها ومواجهتها؛ لإعطاء الفرصة لتنمية تلك القدرات تنمية حقيقية في كل المجالات سواء في الحاضر أو المستقبل . ويمكن إرجاع مفهوم الأمن القومي National Security ، إلى فكرة سيادة الدولة [60]، تلك الفكرة التي أسست معالمها معاهدة ويستفاليا عام 1648 في أوروبا، والتي أعلنت نظاماً دولياً جديداً يقوم على أساس الدولة القومية [61] ، أما المحاولات الأكاديمية لتعريف الأمن القومي، فقد بدأت بعد الحرب العالمية الثانية 1939 – 1945

---

[59] شيرين الضاني، " الأمن القومي ومشروعيته في الإسلا م "، في: **شبكة الحوار المتمدن** _ محور الإرها ب، الحرب والسلام ، 20 تشرين الأول/ أكتوبر 2010 م ، ع: 3160 على الرابط التالي:
http://www.ahewar.org/debat/show.art.asp?aid=232581

[60] السيادة نوعان: السيادة الخارجية والسيادة الداخلية، فالسيادة الخارجية تعني قدرة الدولة على اتخاذ قرارات السياسة الخارجية من دون إملاءات خارجية، أما السيادة الداخلية فتعني قدرة الدولة على بسط قوانينها ونفوذها على جميع أقاليم الدولة، والأمن القومي ارتبط بمفهوم السيادة للحفاظ على حرية اتخاذ القرار خارجياً وداخلياً، كما ذهب إلى ذلك هارولدلاسويل، لمزيد من التفاصيل انظر:
Jens Bartelson, "**The Concept of Sovereignty Revisited**", The European Journal of International Law, vol17 ,no.2,2006.

[61] النظام الدولي الجديد الذي أرسته معاهدة صلح ويستفاليا عام 1648 التي ركزت على مبدأ احترام سيادة الدول ليكون هذا المبدأ ركيزة للقانون الدولي والنظام العالمي الذي كان سائداً آنذاك.

كمفاهيم ترتبط بسياسات الدول للتغلب على التهديدات الداخلية والخارجية التي كانت تحدق بها آنذاك.[62]

وبناء على ما تقدم فان الأمن القومي هو حماية الدولة من أي خطر يهدد وجودها وبقائها ،ويؤدي بالتالي الى استخدامها لكل مقومات القوة التي تمتلكها وفي كافة المجالات كقوة ردع من أجل ضمان بقائها والحفاظ على استمراريتها .

ويرى زكريا حسين أستاذ الدراسات الإستراتيجية، والمدير الأسبق لأكاديمية ناصرالعسكرية بمصر أن الأمن هو "القدرة التي تتمكن بها الدولة من تأمين انطلاق مصادر قوتها الداخلية والخارجية، الاقتصادية والعسكرية ، في شتَّي المجالات في مواجهة المصادر التي تتهدَّدُها في الداخل والخارج، في السلم وفي الحرب ، مع استمرار الانطلاق المؤمَّن لتلك القوى في المستقبل تخطيطاً للأهداف المخططة". وفي رأيه ، للأمن أربعة مستويات :

أولاً : أمن الفرد ضد أي أخطار تهدد حياته أو ممتلكاته أو أسرته.

ثانيًا : أمن الوطن ضد أي أخطار خارجية أو داخلية للدولة وهو ما يُعبَّر عنه "بالأمن الوطني".

ثالثًا : الأمن القُطري أو الجماعي، ويعني اتفاق دول عدة في إطار إقليم واحد على التخطيط لمواجهة التهديدات التي تواجهها داخليًّا وخارجيًّا، وهو ما يعبر عنه "بالأمن القومي".

رابعًا: الأمن الدولي .. وهو الذي تتولاه المنظمات الدولية سواء منها الجمعية العمومية للأمم المتحدة أو مجلس الأمن الدولي ودورهما في الحفاظ على الأمن والسلم الدوليين.[63]

---

[62] إسماعيل صبري مقلد، مرجع سبق ذكره ،.ص 130.

[63] زكريا حسين ،" الأمن القومي"، **موقع إسلام أونلاين دوت نت**. مفاهيم ومصطلحات ،2004، http://www.islamonline.net/arabic/mafaheem/index.shtml

2- الأمن القومي في عصر المعلومات

اعتمد مفهوم الأمن القومي في السابق على القوة العسكرية وقدرتها في حماية الدولة ، ولكن تغير هذا المفهوم في شكل كبير في الأونة الأخيرة حيث أصبح ما يؤثر في أمن الدولة مختلفاً نظراً لتغير البيئة الدولية. فهناك قضايا داخلية لها مردود دولي وقضايا دولية لها مردود داخلي وبالتالي صعب التمييز بين الداخل والخارج. وفي هذا السياق أصبح قصر مفهوم الأمن القومي على القوة العسكرية غير مقبول فهناك العديد من القضايا التي تؤثر في الأمن القومي للدولة منها ما هو سياسي وثقافي واقتصادي وبيئي. [64]

ولقد باتت كثافة المعلومات وسرعتها تخلق مناخًا مختلفًا من العلاقات الدولية بحيث أضحت المعلومات هي القوة فمن يملكها ويوظفها هو القادر على أن يفرض سيطرته فظهر ما عرف بحرب الشبكات والحروب الإلكترونية كنتيجة لذلك .[65]

وأصبح للعالم أوجه رقمية إلكترونية غير مسبوقة في شمولها وعمقها واختلافها واتساع نطاق تغطيتها وتعاظم أضرارها وذكاء منفذيها وتعقد آلياتها وتواصل هجماتها . [66]

فالبيئة الدافعة والداعية للتطور والتقدم، والتي تتمتع بدرجةٍ عاليةٍ من استخدام الّتقنيات الحديثة؛ هي نفسها البيئة التي تعج بالكثير من المشاكل الأمنية. فالفضاء الإلكتروني لأي دولةٍ في العالم يحوي الكثير من البيانات والمعلومات الأمنية والسياسية والاقتصادية والاجتماعية التي تخصها، والتي قد تصيبها بالانهيار أو الشلل الكامل إذا ما تم الاطلاع على فحواها من قِبل خصومها. وبالتالي برز نوع جديد من الأمن هو الأمن المعلوماتي Information Security

---

[64] سماح عبد الصبور، **"القوة الذكية في السياسة الخارجية: دراسة في أدوات السياسة الخارجية الإيرانية تجاه لبنان منذ 2005"**، رسالة مقدمة لنيل درجة الماجستير، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة ، 2013، ص 44.

[65] المصدر نفسه ،ص44.

[66] الأمن الوطني ، **مجلة درع الوطن** ، اعداد هيئة التحرير ، على الرابط الالكتروني التالي:
http://www.nationshield.ae/home/details/files/WMLzSVWGPIU

ولكن لتقريب الصورة سوف نتطرق الى تعريف المعلومات والميدان الذي تتوافر فيه ، ومن ثم تبسيط مفهوم الأمن المعلوماتي لتمكن القارىء من متابعة الأحداث تباعاً .

3- أمن المعلومات

تشكل المعلومات دورا حيويا في حياة الأفراد والمجتمعات ، فهي عنصر لا غنى عنه في أي نشاط نمارسه ، فهي المادة الخام للبحوث العلمية ، والمحك الرئيس لاتخاذ القرارات الصحيحة ومن يملك المعلومات الصحيحة في الوقت المناسب ،يملك عناصر القوة والسيطرة في عالم متغير يستند الى العلم في كل شيء ولا يسمح بالارتجال والعشوائية .

وتتجسَّد المعلومة الإلكترونيَّة ماديًّا، على سبيل المثال ، عَبْر الأمور الآتية : الشاشة (Screen)، أو الطابعة (Printer) ، أو الإسطوانة الضوئيَّة الرقميَّة أو القرص المُدمَج ، أو الناقل التَّسَلْسُلي العام أو الذاكرة الوَميضِيَّة أو الهاتف الذكي.

وتعد المعلومات في عصرنا الحالي من أهم وسائل القوة وهذا ما يؤكده جوزف ناي " فالمعلومات قوة "[67] . والمعلومات أيضا هي مصادر حيوية واستراتيجية للأمن القومي . وتعتبر بيئة المعلومات المكان الذي يستطيع فيه الناس والنظم الالية أو التلقائية أن يراقبوا، ويوجهوا ، ويقرروا ، ويتصرفوا بناء على المعطيات الموجودة ، وتعد هذه البيئة الأساسية لصانعي القرار.[68]

تَسْتَنِد التعريفات المُتعلِّقة بالمعلومة الإلكترونيَّة (Electronic information) إلى فكرة واحدة هي جَمْع المعطيات (Data) بطريقة إلكترونيَّة. فلُغة الحاسوب هي لُغة رقميَّة .[69] تَخْتَلِف عن لُغة الأحرف الأبجديَّة المُستعملة على الورق مباشرة. فالمعلومة الإلكترونيَّة هي المعلومة

---

[67] جوزف ناي، **مرجع سبق ذكره** ، ص 158.

[68] JP3-13,(2006,february13)joint,publication..3-13,information operationsU.S.(**DEPARTEMANT OF DEFFENSE**) .Kenneth J.Knapp,**cyber security global information**,p.115.

[69] تَتَشكَّل اللُّغة الرقميَّة من سلسلة من أصفار (أي الرقم 0) وآحاد (أي الرقم 1).

المخلوقة، المُرسلة، المُتلقَّاة أو المحفوظة، من دون أي مستند ورقي، إنَّما بوسائل إلكترونيَّة أو ضوئيَّة (Optical) . [70]

والحاسوب بحاجة إلى برامج تطبيقيَّة، نموذجيَّة أو مُتخصِّصة، من أجل إمكان حفظ هذه المعطيات والعودة إليها لقراءتها والتعاطي معها ، مثال على ذلك برنامجا Excel وWord ولو أَلْقَيْنا نظرة عاجلة على التواصل بين البشر، الذي أصبح يتمُّ اليوم بواسطة الحاسوب، ووسائل الاتصال من بعد، كالفاكس والإنْتَرْنَتْ والهواتف الذكيَّة (**Smart phones**) [71] ، لأمْكَننا استخلاص أشكال عدَّة قد تأخذها المعلومة الإلكترونيَّة، منها:

- تبادل المُعطيات الإلكترونيَّة (**Exchange of electronic data**) من حاسوب إلى آخر أو هاتف ذكي إلى آخر، بواسطة شبكة مُعيَّنة من طريق استخدام قاعدة مُتَّفق عليها لمُعالجة المعلومة (كالحَوْسَبَة السحابيَّة **Cloud computing**).[72]
- التبادل الحاصل من دون شبكة، مثلاً حين يتم نَسْخ المعلومات على الإسطوانة الضوئيَّة الرقميَّة أو القرص المُدمَج (CD) أو الناقل التَّسَلْسُلي العام (USB) أو الذاكرة الوَميضِيَّة (Flash memory) ونقلها إلى حاسوب أو هاتف ذكي آخر.

---

[70] Linant de Bellefonds et A. Hollande**, Droit de l'informatique et de la télématique**, J. Delmas et cie, 2ème édition, p. 141.
"Il est important d'opérer une distinction entre états informatiques de sortie et états informatiques de stockage. Les premiers (hard- copy, listes d'imprimantes, microfilm) constituent une visualisation stabilisée de l'information. Les matérialisations sont évidement celles qu'on produira le moment venu. Mais la plupart du temps, ces visualisations auront été préparées de manière extemporanée à partir d'une information normalement stockée sous la forme magnétique. C'est donc, en fin de compte, la valeur de l'enregistrement magnétique en tant que mode de preuve, qui doit être appréciée" .

[71] أضحى الهاتف الذكي جزءًا لا يتجزأ من الحياة العصريَّة، حيث يُمكن معرفة كل ما يدور حول حامله من خلال الحصول على بياناته وصوره المُخزَّنة في الهاتف.

[72] هي عمليَّة تخزين المعلومات على سَحابَة وليس في حاسوب المُستخدِم مِمَّا يُسْهِّل عليه استرجاعها أنَّى كان، من دون أنْ يَتَجشَّم عناء حمل الحاسوب معه في حِلِّه وتِرْحالِه. وصارت تُعدُّ الحَوْسَبة السحابيَّة مَنْفَعَة عامَّة كالغاز والكهرباء.

- التسجيل، أي المعطيات المسجَّلة على حاسوب أو الهاتف الذكي أو الحَوْسَبَة السحابيَّة والتي لا تكون مُخصَّصة للتبادُل .

وبناء على ما تقدم ، لم يحظ مفهوم الأمن المعلوماتي بالاهتمام والضوء بمثل ما حظي به مع التوسع في أنشطة معالجة البيانات ونقلها بواسطة وسائل الحوسبة والاتصال والتحول إلى أنظمة الحكومة الإلكترونية؛ إذ مع شيوع الوسائل التقنية لمعالجة البيانات وتخزينها وتداولها والتفاعل معها عبر شبكات المعلومات– وتحديداً الإنترنت احتلت بحوث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين بحوث تقنية المعلومات المختلفة ؛ بل ربما أمست إحدى الاهتمامات التي تؤرق مختلف الجهات وذلك نظراً الى ما عانته بعض الدول والجهات الأمنية والاستخباراتية من هجوم على مواقعها او استراق لخزائن ملفاتها السرية من قبل بعض الجهات أو الدول المناظرة أو الأفراد المعروفين باسم "الهاكرز Hackers " . ويمكن تعريف أمن المعلومات بأنّه " **العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن انشطة الاعتداء عليها** ". ومن الناحية الفنية ، يمكن تعريف الأمن المعلوماتي بأنّه "**هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الخارجية والداخلية** . ومن زاوية قانونية ، **فإن أمن المعلومات هو محل الاخطار الداخلية والخارجية**" وهو يوفر دراسات وتدابير حماية سرية وسلامة محتوى المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها مثل جرائم الكمبيوتر والإنترنت أو.e–crime ما يعرف اصطلاحاً بالجريمة الإلكترونية.

والأمن المعلوماتي هو أيضاً حماية أنظمة المعلومات من أي وصول غير مسموح به أو مخول فاعله بما يتسبب في تعديلات في المعلومات سواء بالتخزين أو المعالجة أو النقل أوعدم السماح للأشخاص المخولين الوصول إلى الخدمات المعلوماتية التي يشتغلون فيها، ويشمل ذلك في ما يشمل الإجراءات الضرورية لحماية وتوثيق ومجابهة الأخطار الخارجية. يعني إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر من دون إذن منك وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة.

ومن الواضح أن معظم الأشخاص يرغبون في الحفاظ على خصوصية معلوماتهم الحساسة مثل كلمات المرور ومعلومات البطاقة الائتمانية وعدم تمكين الآخرين من الوصول إليها والكثير من الأشخاص لا يدركون أن بعض المعلومات التي قد تبدو تافهة أو لا معنى لها بالنسبة اليهم فإنها قد تعني الكثير لأناس آخرين وخصوصاً إذا ما تم تجميعها مع أجزاء أخرى من المعلومات .[73]

خلاصة القول ، أنه بات على دول العالم حماية أمن معلوماتها الإلكترونية، والذي بات يمثل خطراً كبيراً على أمنها القومي ، وبالتالي تهديد وجودها في عالمٍ تكنولوجي ومعرفي تسوده المخاطر من كل حدبٍ وصوب.

حيث يشكل أمن المعلومات الإلكترونية بالنسبة الى المجتمعات المعاصرة حالة الوجود أو اللاوجود . فهي تنظر إلى أمن معلوماتها بأنها : " البنية التحتية الآمنة سياسيًا واقتصاديًا

[73] امن الفضاء الالكتروني، مرجع سبق ذكره ، ص 1.

واجتماعيًا وّتقنيًا، والقادرة على استيعاب تدفق المعلومات من جميع أطياف المجتمع داخليًا وخارجيًا " .[74]

المطلب الثاني : الأمن السيبراني وأهميته بالنسبة الى الدول .

قبل ظهور الأدوات الحديثة المعتمدة على تكنولوجيا المعلومات والإلكترونيات والاتصالات كانت هناك الوسائل التقليدية لجمع المعلومات التي تعتمد بشكل كبير على العناصر البشرية من الجواسيس ومجموعات الاستطلاع من عناصر المخابرات الذين يعملون داخل صفوف العدو من أجل نقل المعلومات اللازمة هي السائدة ، ومع تطور تكنولوجيا المعلومات أصبح العملاء يقومون ليس بإرسال معلومات تجسس ، ولكن بمهام أخرى منها مثلاً وضع مستشعرات وأجهزة متقدمة جداً في الأماكن الحيوية والاستراتيجية ، كما تساهم في تحديد الأهداف ، والتصويب اتجاهها بشكل أدق ، كما أن هناك أيضاً تتبع المعلومات العلنية المتاحة من قبل العدو، وهي أداة تقوم على عناصر بشرية مدربة تستعين بالحواسيب وتكنولوجيا المعلومات في رصد ما تنشره هيئاته ومؤسساته المختلفة .

وأدت علاقة الفضاء الالكتروني بعمل عدد من المنشآت الحيوية سواء أكانت مدنية أو عسكرية في الوقت نفسه لإمكانية تعرضها لهجوم من خلاله إما يستهدفه كوسيط وحامل للخدمات أو بشلّ عمل أنظمتها المعلوماتية ، ويكون من شأنه التأثير على القيام بوظيفتها ومن ثم فإن التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ إستراتيجية بالغة الأهمية سواء في زمن السلم أو الحرب؛ هذه العلاقة التي تمزقها قوى الشد والجذب هي سلاح ذو حدين ، فمن جهة تحتاج الدول إلى الانخراط في عالم التكنولوجيا والمعلوماتية نتيجة تحولات العولمة والثورة الرقمية وهي مضطرة لإشباع هذا الاحتياج . وفي المقلب الاخر هي بحاجة إلى

[74] طارق عباس ، **مجتمع المعلومات الرقمي** ، ط 1، القاهرة: المركز الأصيل للطبع والنشر والتوزيع ، 2004 م ، ص 121.

حماية أمنها القومي من الاختراق نتيجة عمليات التجسس الإلكتروني التي قد تؤدي إلى خسائر بالغة عسكرياً واقتصادياً وسياسياً ما لم تكن هناك أنظمة حماية وأمن معلوماتي صلبة تصد محاولات الاختراق والتجسس من قبل أفراد أو أجهزة استخباراتية أجنبية .

بالتالي رفعت هذه التطورات الاتصالية الهائلة من شأن المعلومات في حياة المجتمعات المعاصرة ، وحولتها إلى مصدرٍ للثروة البشرية اللازمة للانطلاق نحو عصر المعرفة. ساهم هذا التحول، وبشكلٍ ضخمٍ، في جعل المعلومات الإلكترونية والرقمية السارية في القنوات التكنولوجية رأس مالٍ مهمًا يفوق الأهمية التي تتحلى بها رؤوس الأموال الاقتصادية والمالية في وقتنا الحالي [75]، ما دعا إلى ضرورة التفكير في حمايتها _ أي المعلومات الإلكترونية _ من أي هجومٍ قد يعترض سير عملها في بيئتها الرقمية والتكنولوجية المليئة بالمخاطر والتهديدات. فتعالت المطالبة بالحماية ضد الجرائم الالكترونية أو السيبرانية. وسعت الدول الى تطوير منظومتها الأمنية في ظل تعدد الجرائم السيبرانية وتعاظم شأنها ودورها في المجتمع الدولي ، وذلك في ظل غياب القوانين الدولية المعتمدة . فما هو الأمن السيبراني ؟ وما هي الوسيلة الأمثل لحماية أمن الدول ؟

1- الأمن السيبراني

أصبحت قضية الأمن المعلوماتي السيبراني من التحديات الكبرى على الصعيدين الإقليمي والعالمي ، لا سيما في ظل تنامي التهديدات الأمنية الإلكترونية سواء من جهة ارتفاع عدد الهجمات أو الأضرار الناجمة عنها. وقد شهدت بلدان العالم كافة اختراقات أمنية مقلقة استهدفت مؤسسات وشركات وأدت إلى سرقة بيانات حساسة وأسرار الدول أو حجب الخدمات الإلكترونية الحيوية أو السطو الإلكتروني على البنوك أو تشويه مواقع الويب ، أو شن

[75] طارق عباس ، مصدر سبق ذكره ، ص 76.

الهجمات الإلكترونية على البنية التحتية ووسائل الإعلام . والاخطر من ذلك سرقة المعلومات المصرفية .

ف" الأمن السيبراني هو عبارة عن مجموع الوسائل التقنيَّة والتنظيميَّة والإداريَّة التي يتمُّ استخدامها لمنع الإستخدام غير المُصرَّح به وسوء الإستغلال واستعادة المعلومات الإلكترونيَّة ونُظُم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرار عمل نُظُم المعلومات وتعزيز حماية سريَّة البيانات الشخصيَّة وخصوصيَّتها واتِّخاذ جميع التدابير اللازمة لحماية المواطنين والمُستهلكين من المخاطِر في الفضاء السيبراني . إذًا فالأمن السيبراني هو سلاح استراتيجي بيد الحكومات والأفراد ، لاسيَّما أنَّ الحرب السيبرانيَّة أصبحت جزءًا لا يتجزَّأ من التكتيكات الحديثة للحروب والهجمات بين الدول ".[76]

ويشمل الأمن السيبراني أمن المعلومات على أجهزة وشبكات الحاسوب الآلي ، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسوب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث .[77]

ولعلَّ أفضل تعريف مُبسَّط للحرب السيبرانيَّة هو ذلك الذي يَعتبرها مجموعة الأعمال العدائيَّة المُوجَّهة ضدَّ مُعطيات الدولة الإلكترونيَّة المُخزَّنة أو المُعالجة أو المُتبادلة من حاسوب إلى آخر بهدف كَشْفِها أو نَسْخِها أو تعديلها أو إتْلافِها أو عرقلة تدفُّقها (كالهجوم على أنظمة المُراقبة الجويَّة ، وأنابيب نقل الغاز والنفط ، والمفاعلات النوويَّة) .[78]

---

[76] **موقع الهيئة المُنظِّمة للاتصالات في لبنان** حول "الأمن السيبراني"، (تصفُّح بتاريخ 9/ 04/ 2014). على الموقع الإلكتروني التالي: http:/ / www.tra.gov.lb/ Cybersecurity-AR

[77] الأمن السيبراني، **وزارة الاتصالات في جمهورية مصر العربية** ،على الرابط الالكتروني:
www.mcit.gov.eg/Ar/TeleCommunications/Cyber_Security

[78] طارق المجذوب، السَّايْبِر ساحة "خَفِيَّة" لحربٍ "ناعِمَة" قادِمة! | **الموقع الرسمي للجيش** ...
https://www.lebarmy.gov.lb/ar/.../السَّايْبِر-ساحة-خَفِيَّة-لحربٍ-ناعِمَة-قاد

ويشكل الأمن السيبراني واحدا من أهم التحديات التي تؤرق الدول وتضعه في سلم أولوياتها وهاجسها اليومي ، بما في ذلك الدول المتقدمة تكنولوجيا ، لا سيّما الولايات المتحدة الأميركية والتي صرحت مرارا وبشكل جدي وصريح حول أهمية الأمن السيبراني في سياستها المستقبلية حيث أعلنت : " يشكّل الأمن السيبراني الآن واحداً من أهم وأخطر تحديات الأمن القومي الذي يواجه الولايات المتحدة الأميركية ، نحن معرّضون للهجوم وتحَمل الخسائر ..."[79] " إن اقتصادنا وأمننا القومي الآن ، يعتمد بالكامل على تكنولوجيا المعلومات والمعلوماتية ..."[80]

ففي عامي 2007 و2008 قُدرت كلفة الإجرام السيبيري في العالم بنحو 8 مليارات دولار أميركي ، أما فيما يخص التجسس السيبيري على الشركات فقد بلغت قيمة ما استولى عليه المجرمون السيبيريون من ملكية فكرية لشركات تجارية 1 تريليون دولار أميركي وعليه يقوم برنامج الإنتربول لمكافحة الإجرام السيبيري على التدريب والعمليات ويعمل على مواكبة التهديدات الناشئة مبادرات على مستوى العالم .[81]

وذكرت صحيفة "نيويورك تايمز" أن التحليلات الجنائيَّة السيبرية والتي بَرْهَنت أنَّ وحدة المُحاربين السيبريين في الجيش الصيني هي المسؤولة، مع مستوى طفيف من الشك، عن غالبيَّة الهجمات التي تعرَّضت لها الشركات الأميركيَّة وحتى الوزارات"[82].

---

[79] Kenneth J. Knapp , **cyber security global information assurance** , information science reference , Newyork , 2009 , preface xviii. by James.A Lewis **, cyberse security recommendations for the next administration testimony** , center for strategic and international studies , september2008 ,Washington DC , subcommittee on emerging threats , cyber security, science and technology..

[80] Same reference , p.9.

[81] أمن الفضاء الالكتروني ، مرجع سبق ذكره ، ص8-9.

[82] معمر عطوي ونزار عبود حول "الوحدة 61398» تتَّخِذ من شنغهاي مُنطلقًا لهجماتها"، صحيفة الأخبار اللبنانيَّة في 21/ 02/ 2013.

"وقد طالب بنيامين نتنياهو في مؤتمر "سايبر تيك 2014" الدولي الأول، الذي عُقِد في تل أبيب بإنشاء "منظمة أمم متحدة للسايبر" ، لتحويل الإنترنت من "نَقمة إلى نِعمة"بسبب حاجة الجميع إليه ". [83] كما أَعلن رئيس هيئة الأركان العامة في الجيش الإسرائيلي [84]، بَني غانْتْس (Benny Gantz)، بأنَّ "الحرب المُقبلة قد تبدأ بصاروخ يَستهدف هيئة الأركان أو بهجوم سايبر واسع على أجهزة الحواسيب المدنيَّة والعسكريَّة. (...) وفي مجال السايبر تدور اليوم حرب حتى بين دول لا توجَد في حال حرب مع بعضها" . [85]

2- أين تكمن الخطورة ؟

بعد ثورة المعلومات والتكنولوجيا التي اجتاحت العالم ، قلّصت دول العالم من اعتمادها على العنصر البشري رغم أهميته، لمصلحة هذه التقنية . ما أدى الى أرشفة المعلومات والبيانات واعتماد الدول على نظام الحكومة الالكترونية وهذا أدى الى ظهور سلبيات عدة أهمها **التجسس وزيادة التبعية للخارج وشلل الادارات** .

انّ مصدر الخطورة لا يأتي من تطبيق الحكومة الالكترونية ، بل بالعكس ان الحكومة الالكترونية ضرورية لتسهيل عمل الدول وتواكب التطور التكنولوجي ولكنها تحتوي على سلبيات ، ولعل أهمها يكمن في عدم تحصين الجانب الأمني للادارة الالكترونية ، والذي يعدّ أولوية في مجال تطبيق استراتيجية الادارة الالكترونية ، فاهمال هذه الناحية يؤدي الى كارثة وطنية يحدثها التجسس الالكتروني ومصدر الخطر هذا يتأتى من ثلاث فئات :

---

[83] حلمي موسى حول "حرب السايبر" تُشغِل إسرائيل: البحث في تحويل "النقمة إلى نعمة"، **صحيفة السفير اللبنانيَّة** في 31/ 01/ 2014، تصفُّح بتاريخ 9/ 04/ 2014). على الموقع الإلكتروني التالي: http:/ / www.assafir.com/ Windows/ PrintArticle.aspx?ChannelID=62&ArticleID=336185&ref=Toolbar

[84] محمد المجذوب ، **"التنظيم الدولي: النظريّة العامّة والمنظمّات العالميّة والإقليميّة والمُتخصّصة"**، الطبعة الثامنة ، منشورات الحلبي الحقوقيّة، بيروت، 2006، ص 220-225. حيث اعتبرأن إسرائيل، في هذا البحث، تجاوزًا، دولة من دول العالم التي انضمّت إلى عضويّة الأمم المتحدة في 11 أيّار/ مايو 1949، وصدَّقت، منذ ذلك التاريخ، على بعض المواثيق والمعاهدات والاتفاقيات الدوليّة، وذلك على الرغم من إيماننا بأنّ ليس لإنشاء إسرائيل أي أساس أو سند قانوني، لا في صكّ الانتداب، الذي صدَّق عليه مجلس عصبة الأمم في 24/ 07/ 1922 ووُضِع موضع التنفيذ في 29/ 09/ 1923، ولا في قرار التقسيم 181 (II) تاريخ 29/ 11/ 1947.

[85] حلمي موسى حول "حرب السايبر تُشغِل إسرائيل: البحث في تحويل النقمة إلى نعمة"، المرجع سبق ذكره .

الفئة الأولى هي الأفراد العاديون .

الفئة الثانية هي الهاكرز (القراصنة) .

الفئة الثالثة هي أجهزة الاستخبارات العالمية للدول .

ويقتصر تخريب الفئتين الأولى والثانية على تخريب الموقع أو اعاقة عمله أو اتلافه ، ويمكن تلافي الضرر بطرائق وقائية أو اعداد نسخة احتياطية . أما الفئة الثالثة فيتعدى ذلك بكثير حيث يتّم الاطلاع الكامل على الوثائق الحكومية ووثائق المؤسسات والادارات والأفراد والأموال كافة . ما يشكل تهديداً فعليا للأمن القومي والاستراتيجي للدولة المعنية .

ومن المعلوم أنّ الدول العربية ليست دولاً رائدةً في مجال التكنولوجيا والمعلومات ، بل هي دول مستهلكة ومستعملة لهذه التكنولوجيا . وبما أنّ الادارة الالكترونية تعتمد بمعظمها على التكنولوجيا الغربية ، فان ذلك سيزيد من مظاهر تبعية الدول المستهلكة للدول الكبرى الصناعية ، وهذا يتضمن انعكاسات سلبية كثيرة وخصوصا في المجال الأمني . ولا يقتصر على الجانب العسكري فحسب بل يتعدى ذلك الى الأسرار التجارية والمصرفية ، والتحكم بالثروات الطبيعية من نفط وغاز .... ويؤّدي الى شلل الأعمال في هذه المنشآت والادارات متى دعت الحاجة وهذا يشكّل خطراً على الأمن القومي للدول المستهلكة .[86]

لذلك لجأت الدول عامّة الى اتخاذ تدابير واجراءات خاصة من أجل حماية أمنها وأمن معلوماتها وأسرارها الخاصة والقومية .

[86] محمد مدحت محمد، الحكومة الالكترونية ، **المجموعة العربية للتدريب والنشر** ،2016، ص 99-102 .على الرابط التالي: https://books.google.com.lb/books?isbn=9796500185453

3- تأثير الأمن السيبراني في استراتيجيات الدول.

إن الحفاظ على أمن قواعد المعلومات في عالم الحوسبة المترابط (Interconnected Computing Environment) يشكل تحدّيًا حقيقيًا ، وهو يصبح أكثر حدّة مع توافر أي منتج إلكتروني جديد (New E-product) أو تدخل أي جهاز (Intruder Tool) . وقد أدركت المؤسسات على اختلافها أنه ليس هناك من حلّ متكامل لضمان أمن المنظومات وقواعد المعلومات، كما أدركت أنّه لا بد من اعتماد استراتيجية متعددة المستوى (Multi-Layered Security Strategy) .[87]

وفي سبيل ضمان حماية البنى التحتية للاتصالات وتكنولوجيا المعلومات ، سعت الدول بمساعدة المؤسسات التابعة لها في تكنولوجيا المعلومات وكل الميادين الأخرى ، من أجل السعي الى وضع إستراتيجية وطنية للدفاع عن الأمن السيبراني والإشراف عليها . حيث أَعْلَنَت أكثر من 130 دولة حول العالم عن تخصيص أقسام وسيناريوهات خاصَّة بالحرب السيبرانيَّة ضمن فرق الأمن الوطني .[88]

وكَشَفت تسريبات أنَّ الحكومة الأميركيَّة تُنفِق 4,3 مليار دولار سنويًا على العمليَّات السيبرانيَّة، حيث وَرَد أنَّه في العام 2011 شنَّت وكالات الإستخبارات الأميركيَّة 231 عمليَّة إلكترونيَّة هجوميَّة. فالولايات المتَّحدة ، على ما يبدو ، تستعدُّ للقتال السيبراني .[89]

كما " كَشَف القائد العسكري الروسي الميجور جنرال يوري كوزينتسوف (...) أنَّ بلاده تعتزِم إنشاء وحدات دفاع "سيبراني"خاصَّة لحماية البلاد ضد الحرب على الإنترنت في خلال

---

[87] نينا عقل - ندين البلعة خيرالله، **مجلة الجيش**، الأمن السيبراني ،العدد 350-351، 2014.على الرابط الالكتروني: https://www.lebarmy.gov.lb/ar/content

[88] **موقع الهيئة المُنظِّمة للاتصالات في لبنان** حول "المحة عامة حول الأمن السيبراني"، على الموقع الإلكتروني التالي: http:/ / www.tra.gov.lb/ Cybersecurity-AR

[89] **"كيف سيكون شكل الحرب الإلكترونيَّة الحقيقيَّة؟"**، 17/ 09/ 2013. على الموقع الإلكتروني الآتي: http:/ / www.slabnews.com/ article/ 38744

السنوات المقبلة، وذلك بحلول العام 2017 " .[90] وأكَّد رئيس الحكومة الإسرائيليَّة ، بنيامين نتنياهو، في كلمة ألقاها بمُناسبة تأهّل الشبَّان المُتفوّقين في مجال مُكافحة الحرب السيبرانيَّة في مدينة عسقلان: " انَّ الخطر النووي الإيراني وتهديد الصواريخ لا يُشكِّلان التهديدين الوحيدين اللذين نُواجههما، ذلك أنَّنا نُواجه أيضًا خطر الاعتداءات السيبرانيَّة على إسرائيل والتي تأتي من إيران وجهات أُخرى . ونحن نستعدُّ للتعامل مع هذا الخطر بشكل ما ولكن بطرائق أُخرى . إنَّ منظوماتنا الحيويَّة تُعتبر أهدافًا لهذه الاعتداءات، وسيزداد الأمر خطورة كلَّما تسارع الانتقال إلى العصر الرقمي. إنَّنا نُعزِّز قدراتنا على التعامل مع هذا الخطر من خلال هيئة السايبر الوطنيَّة التي أَقَمْناها، ومن خلال إنشاء قُبَّة حديد رقميَّة ل "إسرائيل". ونحن أيضا إحدى الدول الرائدة في العالم في مجال السايبر، وعلينا أنْ نُحافظ على مكانتنا هذه في المُستقبل " .[91] أما بالنسبة الى المحاولات العربية فما زالت هزيلة ودون المستوى وذلك لعدم تطور هذة الدول من الناحية التكنولوجيا ، فهي ما زالت مستهلكة وتعتمد على التكنولوجيا الغربية .

---

[90] **"روسيا تُنشئ وحدات للحرب "السيبرانيَّة"** بحلول العام 2017"، اليوم السابع، 30/ 01/ 2014. على الموقع الإلكتروني التالي:
http:/ / www.youm7.com/ News.asp?NewsID=1481858

[91] صحيفة يسرائيل هيوم العبريَّة، في 1/ 01/ 2013.**تَتْبَع هيئة السايبر الوطنيَّة تساهل** (أي جيش الدفاع الإسرائيلي بالتسمية العبريَّة). أُطلقت إسرائيل في العام 2009 برنامج القبَّة الحديديَّة الرقميَّة التابع لمكتب الحرب الافتراضيَّة في إسرائيل. ويُركِّز البرنامج على تطوير قدرات إسرائيل التكنولوجيَّة، الدفاعيَّة والهجوميَّة، في مجال الهجمات الإلكترونيَّة المُحتملة. راجع ما كتبته صحيفة فلسطين حول الموضوع "الإمكانات الإسرائيليَّة في حرب السايبر"، في 21/ 11/ 2013.على موقع فلسطين أون لاين الإلكتروني التالي:http:/ / www.felesteen.ps/ prints/ news/ 104454

إستنتاج الفصل الأول

بقي الأمن الالكتروني حتى وقت قريب ، حِكراً على مجموعة صغيرة من خبراء الحاسوب ، لكن تنامي عدد مستخدمي الانترنت بشكل هائل، بلغ أكثر من ثلاث مليارات حاليا ، [92] أبرز الاستخدامات الواسعة للانترنت ، بوجهيها السلبي والايجابي ، وجعل الاهتمام بالأمن الالكتروني ينتقل إلى سلم الأولويات ، في سياسات الدول .

وشكّلت السيبرانية هاجس عصر المعلومات ، وأصبح الخطر يتربص بالأفراد والشركات أو المؤسسات والدول على حد سواء . فالخطر يكمن في أمن الشبكات و أمن الانترنت في مختلف النواحي ، في ظل عدم قدرة الجميع على تحمل تكلفة كشف ومعالجة تحديات أمن المعلومات، وتأثيرها في استراتيجياتها واستدامتها على المدى الطويل . ومن جهة أخرى ، جعلت القوة الالكترونية بعض الفاعلين الأصغر (من الهواة أو الارهابيين وأصحاب الجريمة المنظمة) في السياسة الدولية لكون لديهم قدرة أكبر على ممارسة كلّ من القوة الصلبة والقوة الناعمة عبر الفضاء الإلكتروني ، وهو ما يعني تغيرًا في علاقات القوى في السياسة الدولية .[93] ما شكّل تحدياّت جديدة أمام الدول التي سعت بمختلف الوسائل الى حماية أمنها ومعلوماتها بل وأدخلتها في ضمن خططها الاستراتيجية المستقبلية .

---

[92] http://www.internetlivestats.com/internet-users/

[93] سعاد محمود أبو ليلة ، «دورة القوة: ديناميكيات الانتقال من "الصلبة" إلى "الناعمة" إلى "الافتراضية" »، **مجلة السياسة الدولية** ، ملحق اتجاهات نظرية القوة :كيف يمكن فهم تحولات القوة في السياسة الدولية ؟ العدد 188، 2012/16.

الفصل الثاني: الحروب الالكترونية وآلية عملها.

لم يعتقد الكثيرون أن نبوءة "ونستون تشرشل" رئيس الوزراء البريطاني السابق، وهو في نشوة النصر إبانّ الحرب العالمية الثانية ، حول " الحرب الالكترونية " ستتحقق ، وسوف تتسابق الدول على امتلاكها في المستقبل القريب . وقد لخصّها بكلمتين وهي " **الدرع والسيف** " [94] ، أي أنّها تستخدم كوسيلة دفاعية حيث تساعد على الحماية من أقسى صور التدمير المعادي، وهجومية كالسيف القاطع حيث تثبت فاعلية التدمير المؤثرة لأنظمة العدو.

أصبح المجال الإلكتروني منافساً لمجالات البث والاتصال البرية والبحرية والجوية والفضائية بل أصبح أحد ميادين الحرب بين الأمم وخصوصاً أن هيئات إستراتيجية مثل الجيوش والمصارف والشركات وغيرها صارت تعتمد على المجال الإلكتروني في تخزين بنياتها التحتية ما يجعلها عرضة لهجمات إلكترونية .

في كانون الثاني 2012، أعلنت وزارة الدفاع الأميركية من ضمن خططها العسكرية للقوات الأميركية ، " أنّ الفضاء السايبيري هو المجال الخامس في الحروب " [95] ، وأنّ العمليات العسكرية تجري في كل المجالات البرية الجوية ، البحرية ، الفضاء النووي والفضاء السيبراني. تلعب الحرب الإلكترونية دوراّ رئيساّ فى تغيير إستراتيجية الحرب التقليدية حيث تمثّل المجال الحقيقى لتطبيق وإستخدام التكنولوجيا الحديثة نظراً الى التطور الهائل لطرائق إستخدام القوات الجوية وأساليبها فى إستخدام الحرب الإلكترونية والمتمثل فى إستخدام الإعاقة الإلكترونية

---

[94] ابراهيم اسماعيل كاخيا ، **الحرب الالكترونية** ، مجلة الدفاع العربي ، قراءة استراتيجية في يوم الاربعاء ، 22 مارش ، على الرابط الالكتروني التالي : arabdefencejournal.com/article.php?categoryID=9&articleID=552

[95] Departement of Defense ,"**Defense Strategique Guidance**",Washington ,D.C. , Jan.2012 , p.4.

والحرارية فى أعمال القتال وكذلك التطوير المستمر فى نظم الإعاقة سواء المحمولة جواً أو الأرضية .

" تعتبر شبكات الانترنت إحدى الوسائل الاستراتيجية " [96]. فهي سلاح إستراتيجي فعّال لجميع أنواع الهجمات في الحروب ، ولكنّها في الوقت عينه تشكل هدفاً سهلاً أيضا. فهي تطلق بالتالي نقاشاً حول كفاءة نظم الأمن وكيفية تنيفذ الاستراتيجيات وتثير مسألة البيانات الرقمية وجود ثغر أمنية والتي تنعكس على الصراعات السياسية والعسكرية في المستقبل .

ويحفل واقع اليوم بالعديد من المتغيرات التي تدفعنا إلى تسليط الضوء على تلك الآلة العسكرية الجديدة ، التي فرضت نفسها بقّوة على واقع الصراعات المسلحّة وغير المسلّحة في عالم اليوم . ولذلك فإنّ هذا الفصل سوف يرّكز على أهمية الحروب السيبرانية و فعاليتها وخطورتها و مميزاتها وخصائصها وأنواعها الصلبة " الشديدة التأثير"، والناعمة " الخفيفة التأثير" إضافة إلى الحروب الاعلامية التي تهدف إلى طمس الحقائق وسلب هوية الشعوب .

المبحث الأول: مفهوم الحروب الالكترونية : خصائصها ومميزاتها .

لا تزال الدول الكبرى تعيش خلافات عقدية أو منازعات إقليمية ، فروسيا على سبيل المثال تسعى لاستعادة أمجادها بصفتها وريثة للاتحاد السوفياتي (سابقاً)، لتكون النّد للولايات المتحدة الأمريكية ، والصين في خلاف أيديولوجي حاد مع الولايات المتحدة الأمريكية ، وبريطانيا في صدد الخروج من الاتحاد الأوروبي وفرنسا ليست على اتفاق تام مع الولايات المتحدة الأمريكية...

[96] Sabrine Saad, **Asymmetric Cyber-warfare between Israel and Hezbollah**, Saint-Joseph University, Beirut, Lebanon, page 5.

لذا، فإّن كل دولة تحاول تحقيق التفوّق على الدول الأخرى ، ومع بروز الثورة التكنولوجية فإنّ عصراً جديداً من الحروب قد بدأ أو أوشك على البدء هو عصر الحروب الالكترونية مع ما يعنيه من عسكرة الفضاء، والإستعداد لإستخدام أسلحة مضادة للأقمار الصناعية لتدميرها أو أسرها أو حرفها عن مدارها أو سرقة تقنياتها...

وقد يعتقد البعض أنّ مصطلح الحرب الإلكترونية هو أحد المصطلحات التي تتحدث عن مفهوم إفتراضي تدور تفاعلاته في فضاء الإنترنت ، ولكن هذا التصور يعتبر تصوراً خاطئاً إلى حّد بعيد، فالإنترنت وشبكات الحاسوب في وجه عام تعدّ أحد ميادين الحرب الإلكترونية التي فاقت أسلحتها في القوة التدميرية قدرة الأسلحة التقليدية وفوق التقليدية . فالحرب الالكترونية هي الأعمال المتخذة لتحقيق السبق والأفضلية المعلوماتية في طريق التأثير في معلومات العدو وأنظمتها والدفاع عن المعلومات الخاصة وأنظمتها. وتعزّز هذه القدرات مجتمعة قوة الدولة وتوطّد أمنها القومي ، وتنطوي تكنولوجيا الحرب السبرانية على مزايا كامنة هائلة ، وكذلك على مخاطر جديدة وغير معروفة نظراً إلى حداثة هذا المجال ، فإن معرفة طبيعته وتأثيراته لا تزال في بداياتها. ويؤكد سيفر (General Siffre) أّن من يريد أن يسود العالم ويتحكم به ، لا بّد له من امتلاك القدرة على السيطرة على الفضاء السيبراني والموجات الكهرومغناطيسية .

(MAITRE DES ONDES, MAITRE DU MONDE) [97] .

لقد زادت التقنيات الرقمية من فاعلية الحروب الالكترونية ، فالبعض يقول أنّ أول إعلان عن دخول التقنيات الرقمية ميادين الحروب في حرب البلقان في نهايات القرن الفائت على

[97] Jean-Paul Siffre **, LA GUERRE ELECTRONIQUE,. MAÎTRE DES ONDES, MAÎTRE DU MONDE**., Éditions Lavauzelle , 2003.

يد حلف شمال الأطلسي ضد الصرب فيما سمي " القنابل المعتمة "، والذي أدّى إلى توقف شبكة الحاسوب الرئيسة ما أصاب نظم الكمبيوتر الخاصة بوزارة الدفاع اليوغسلافية بالشلل التام . إلّا إنّ التطوّر الأهم الذي أحدث انقلاباً في الموازين هو فيروس "ستكسنت" ، الذي أصاب المفاعلات الايرانية وكان تأثيره كبيراً في مفاعل بوشهر الإيراني وساهم في تضرّره بشكل كبير. " ستكسنت هو بمثابة هيروشيما الحرب السيبيرية ". [98] ويرى جايسون هايلي ، وهو مسؤول سابق في البيت الأبيض، ويدير الآن "مبادرة فنون الإدارة السيبرانية " ، Cyber Statecraft Initiative، في المجلس الأطلسي أن "ستكسنت" كان : " أول سلاح مستقل يضغط على الزناد بواسطة معادلة خوارزمية ، وليس يد بشرية " [99] ، الا أن رالف لانجنر " الخبير الأمني في مجال الحاسوب "، هو أول من كشف "ستكسنت" للعالم ، ووصف السلاح الجديد المذهل بقوله :

[....يمكن أن نعتبره نموذجا لنهج "حرب عادلة" ، فلم يقتل أحدا ، وهذا شيء جيد ، غير أنني أخشى أن يكون هذا على المدى القصير فقط ، فعلى المدى الطويل سيفتح صندوق باندورا (صندوق الشرور) ...] [100]

كما أنّ البرنامج كبير ومشفّر جداً ومعقد جداً ويوظّف تقنيات ذكيّة وجديدة ، ولا يلزمه للعمل أي تدخل بشري في أي مرحلة من المراحل ، ويكفي أن يكون هناك بطاقة ذاكرة تخزين إلكترونية مصابة به حتى يبدأ عمله . [101]

---

[98] Michael Joseph Gross, **"a declaration of cyber –war"**, vanity fair, Apr. 2011.

[99] بيتر سينجر، الحروب المستقبلية في القرن الواحد والعشرين ، ط1، مركز الامارات للدراسات والبحوث الاستراتيجية ،2014، ص88 نقلا عن : Silent war,vanity fair,july2013(http://www.vanityfair.com/culture/2013/07/new- cyberwar-victims-american-business.

[100] المصدر نفسه ، ص 88 .

[101] Mark clayton ," **from the man who discovered stuxnet,Dire wamings one year later** ", the Christian science monitor , September22, 2011.

وهذا يشير الى أنّ الحروب الالكترونية تمتلك كمّاً كبيراً من الشر والخداع ، قد تخرج عن السيطرة في بعض الأحيان ، ويمكن أن تنفّذ بمعزل عن اليد ، كما أن ما بعد "ستكسنت" ليس كما قبله ، فقد اكتشف العالم سلالة جديدة وذكية من السلاح الرقمي تستهدف أنظمة التحكم في المنشآت والمصانع والبنية التحتية ، و لا تحتاج لأن تكون موصولة بالانترنت ، بل يكفي أن يقوم شخص مجهول بادخال شريحة USB في أحد الأجهزة المتصلة بنظام التحكم حتى ينتقل آلية الفيروس بكامل خطته الالكترونية وينتظر ساعة الصفر . ببساطة لقد انتقلنا الى المستوى التالي من ذلك النوع من الحروب [102]. ممّا يعني أن هذه الحرب وأدواتها في تطور مستمر ، وقد تكون بمثابة قنبلة موقوتة إذا ما تّم استخدامها من قبل تنظيمات إرهابية وفقدت السيطرة عليها ، وهذا يبدو جلياً من خلال ماحصل مع تنظيم القاعدة وفروعه المتعددة النصّرة وداعش وجيش الفتح ..... ممّا يستدعي تنظيم قوانين امتلاكها وإستخدامها قبل أن تنشر ويلاتها وشرورها على العالم .

المطلب الأول: تطّور الحروب وبروز ظاهرة الحروب الالكترونية .

وجدت الحرب مع وجود الإنسان لأنّها مرتبطة بوجوده ، وهي قديمة كقدم هذا الوجود على هذه الأرض، وهذا ما عّبر عنه إبن خلدون بقوله : " إن الحرب وأنواع المقاتلة لم تزل واقعة في الخليقة منذ برأها الله ، وأصلها إرادة انتقام بعض البشر من بعض ، ويتعّصب لكل منها أهل عصبيته " [103]. ويستنتج من كلام إبن خلدون أّن الحرب هي الأصل في السلوك الإنساني، وأنّ السلام والمسالمة هي الاستثناء .

(http:/www.csmonitor.com/USA/2011/0922/from-the –man-who-discovered-stuxnet-dire-wamings-one-year-later).

[102] عباس بدران ، **"الحرب الإلكترونية: الاشتباك في عالم المعلوما ت"**، بيرو ت: مركز دراسات الحكومة الإلكترونية ، 2010، ص 56 .على الرابط الالكتروني التالي:-http://www.slideshare.net/abadran/cyberwar-book-in

[103]ابن خلدون: **المقدمة** ، دار مكتبة الهلال ، بيروت ، 1983، ص175.

و تعاظمت عمليات التنافس والتصادم البشري على مر العصور وعبر تطور التاريخ البشري، فشهدت تلك الفترات قيام حضارات وتجمعات بشرية ، واندثار حضارات أخرى. فمثلاً ، انهارت إمبراطورياتُ كبرى كالرومانية واليونانية القديمة والبيزنطية والعثمانية .

ومن ثمّ اندلعت الحربان العالميتان الأولى والثانية ، وتحّول العالم من الثنائية القطبية الى الأحادية القطبية بعد انهيار الإتحاد السوفياتي ، وجرت أحداث جمّة أثّرت على نوعية الأسلحة وفعاليتها ومدى قدرتها على إلحاق الأذى بالأعداء . وكان للثورة الصناعية أثرها في تطور الأسلحة والدبابات والطيارات وتصنيعها، ومن بعدها تطوير القنبلة النووية والكيميائية والبيولوجية ، كما تسابقت الدول لغزو الفضاء والتفوق في مختلف المجالات العسكرية والاقتصادية ... وتبين أنّ لكل وقت وعصر سلاحه وأدواته ، وكان الهدف واضح وهو امتلاك القّوة والتأثير وتدمير الخصم وإخضاعه . ف"الحرب هي فعل من أفعال القوّة لإجبار الخصم على تنفيذ إرادتنا ، كما تعتبر الحروب إحدى الوسائل السياسية للتعامل بين الدول ، وهي استمرار للسياسة بوسائل أخرى " [104].

ولكن الحدث الأبرز يكمن في الثورة المعلوماتية ، التي قلبت الأمور رأسا على عقب ، حيث ظهرت التكنولوجيا الرقمية والالكترونية والتي انعكست بدورها على كل المجالات العسكرية والاقتصادية والسياسية ، وأحدثت ثورة عالمية في عالم المعلومات والاعلام والتجسس والحروب . من هنا يتبادر السؤال التالي : **ما هو مفهوم الحروب الالكترونية ؟**

إنّ للحرب الإلكترونية مسميّات عددية في عالمنا المعاصر، منها على سبيل المثال : حرب الفضاء (space war) ، الحرب المعلوماتية (Information Warfare) ، حرب الفضاء الإلكتروني ، (Cyber War) ، القرصنة الإلكترونية (Electronic piracy) ،

[104] THOMAS RID **, cyber war will not took place** , Hurst&Company , London, tome 2 , 2013, p.1.

حرب الإنترنيت ، (Digital War) الحرب الرقمية ، (War hackers) حرب الهاكرز ، (Cyber War) حرب السايبر وغيرها من المسميّات التي ُتشير إلى ، (Dark War) حرب الظلام (Silent War) الحرب الصامتة ، (Internet War) والتي تشير في مضمونها إلى نفس مفهوم الحرب الإلكترونية . [105]

وهناك تعريفات عدّة للحروب الالكترونية فقد نصّ القانون الدولي فى مجالات الصراع والحروب السيبرانية على : " إنّها كل العمليات السيبرانية سواء كانت دفاعية أو هجومية والتى يعتقد أنها قد تسبب إصابات أو وفيات للبشر أو تلف وضرر للاشياء المادية ".

تنبع أزمة التعريف من أهمية التمييز بين أشكال الحرب السيبرانية و أشكال أخرى مثل الحروب النفسية وحروب المعلومات والحروب الالكترونية وأيضا أشكال الجريمة الالكترونية والإرهاب الالكترونى و الحدود الفاصلة بينها ومتى تنتهي حدود إحدى هذه الافرع لتبدأ حدود فرع اخر لتحديد إمكانات وأشكال التنسيق و مهام عناصر القيادة وعمليات التّحكم بمختلف القطاعات العسكرية وحتى الاقتصادية والمدنية منها. و يمكن الاستقرار على التعريف المبسط لمجال الحرب المذكور سابقاً حتى تستقر الحكومات والدول على تعريفاتها الخاصة بها و لطبيعة أهدافها الإستراتيجية ومن ثم تحديد المشتركات بينها للوصول إلى تعريف أشمل وأعّم أو ربما الإنتظار حتى اندلاع الحروب المقبلة لتحديد تعريف أكثر واقعية . [106]

وحاول كل من "ريتشارك كلارك" و"روبرت كناكي" تعريف الحرب الإلكترونية على أنّها : "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الحاسوب والشبكات التابعة لدولة أخرى

---

[105] وليد غسان جلعود ، **دورالحرب الالكترونية في الصراع العربي الاسرائيلي** ، أطروحة في جامعة النجاح الوطنية ، فلسطين،2003، ص 110 على الرابط الالكتروني التالي:
https://scholar.najah.edu/sites/default/files/وليد%20جلعود.pdf

[106] محمد فخر الدين، **حدود المجال الخامس – ما هى الحروب السيبرانية ؟**،على الرابط الالكتروني التالي:
https://seconf.wordpress.com/2015/05/15

بهدف تحقيق أضرار بالغة أو تعطيلها ، إن الحرب الالكترونية تحمل طابعاً مركبّاً حيث يشارك في خوضها قوى ووسائط كل أنواع القوى و صنوف القوات و المصالح ، حيث تتحول من شكل من أشكال التأمين القتالي (ألعملياتي) شكل العملية الخاصة لتدمير قيادة القوات (القوى) و أسلحة العدو و في المستقبل القريب لتدمير النظم المعلوماتية " [107].

فهى حرب تقوم باتخاذ إجراءات إلكترونية التى تستخدم النظم والوسائل الالكترونية الصديقة فى استطلاع الإشعاع الكهرومغناطيسى الصادر من النظام ويتم استخدام الطاقة الكهرومغناطيسية فى التأثير في هذه الانظمة ومنع العدو أو تقليل استخدامه للمجال الكهرومغناطيسى .[108].

ولعل أبرز أشكال ذلك النمط الجديد من الهجوم هو القرصنة الإلكترونية والجريمة الإلكترونية والتجسس الإلكتروني والإرهاب والحرب عبر الفضاء الإلكتروني وغيرها مما يمكن تصنيفه ضمن الاستخدامات غير السلمية للفضاء الإلكتروني . كما أنّ الحرب السيبرانية تشكّل مجموعة من الهجمات والدفاعات السيبيرية بقيادة مجموعة أو حكومة [109]. وبناء على ما تقدّم **فما هو معيار تصنيف الحروب الالكترونية ؟**

يشير بعض الباحثين إلى أنّ مصطلح الحرب الإلكترونية هو "مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي " . ولأنّ مثل هذه التعريفات فضفاضة ولا تعبّر بدقّة عن فحوى الموضوع ، فسوف يتم التركيز بدلاً من ذلك على المعيار الذي من خلاله يتم ّ تصنيف أي هجوم ضمن خانة الحروب الالكترونية .

---

[107] علي حسين باكير، **"المجال الخامس.. الحروب الإلكترونية في القرن الـ21"** ، مركز الجزيرة للدراسات.،على الرابط الالكتروني التالي: 12 2011/01/studies.aljazeera.net/ar/issues/2010/20117212274346868.html

[108] defense-arab.com › ... › قسم القوات الجوية AIR FORCE › الـــــدفاع الجوي Air defence، 8/11/2015

[109] Dictionnaire.cordial-enligne.Fr/definition/cyberguerre

يصنف ضمن الحروب الالكترونية " أي أسلوب يعتمد للحصول على البيانات والمعارف وحرمان الخصم لغرض استراتيجيي " [110] . بمعنى الحصول على معلومات وأسرار تخص الدول الأخرى من دون رضاها ، أو الحؤول دون حصولها على معلومات أخرى لأغراض معينة .

"ويعتبر غزو الفضاء الكهرومغناطيسي لأي بلد عمل عدواني ، وفقا لنظريات الحرب الالكترونية المطبقة في أوقات السلم وفي زمن الحرب . ووفقاً للجيش الأميركي " أنّ الهجوم الالكتروني يشمل أي تدبير يتخذ لمنع العدو ، كلياً أو جزئياً ، من استخدام الطيف الكهرومغناطيسي مثل التدخل المعتمد أو خيبة الأمل " [111].

كما يتضمن الهجوم على الشبكات من وجهة نظر" الجيش الأميركي " أي عملية من شأنها تعطيل أو الحاق الضرر أو تخريب أو تدمير أجهزة وشبكات الكمبيوتر أو البيانات المخزنة " [112]

وفي المحصلة ، فإنّ كل تشويش ، أوتجسس أوسحب للمعلومات أو البينات المخزنة أو تخريبها والتلاعب بها أو احداث الفوضى أو تدمير الأجهزة والشبكات الالكترونية أو قطع الاتصالات أو منعها من تنفيذ أعمالها اليومية أو إرباكها يدخل ضمن نطاق الحروب الالكترونية .

---

[110] Francois-Bernard Huygue, "**Cyberguerre et guerre de l'information, stratégies, règles et enjeux**", under Daniel Ventre's supervision, 2010, introduction». Lavoisier, p. 13.

[111] **Joint Doctrine for Electronic Warfare**, Joint Publication 3-51, le 7 avril 2000. [TCO] www.iwar.org.uk/iwar/resources/ew/jp3-51.pdf

[112] Same reference .

المطلب الثاني: الحروب الالكترونية : الخصائص والأهداف والمخاطر .

من وجهة نظر عقيدة الحرب الإلكترونية هي قدرة وذروة الهجوم والحماية والدعم ، وتشمل أنواع مختلفة من الأنشطة . فقياسات الهجوم غير المدمرة (التشويش والتضليل) ، والمدمرة (الكهرومغناطيسية وأسلحة الطاقة الموجهة) ، كما تشمل الحماية الوسائل السلبية والترددات وزعزعة الاستقرار و قدرة فعّالة ضد العدو في إعداد البرمجة والتمويه . ويشمل الدعم الكشف عن التهديد والتوجيه للحقائق وجمع المعلومات . كما أن الحرب الإلكترونية لا تمّيز بين الهجوم والدفاع ، ولا يبدو هذا التمييز فعّالاً إلاّ في سياق عمليات جمع المعلومات باستخدام الحرب الإلكترونية.

ويمكن تقسيم الحروب الالكترونية الى مجالات عدة : أولّها مجال الدفاع الالكتروني والذي يعنى بالدفاع عن أنظمة وأجهزة معلومات الدولة والجيش والاستخبارات والمجتمع ، وثانيها الهجوم الالكتروني وهو المجال الذي يتمثل بالعمليات الالكترونية التي تهدف إلى التشويش على مصادر المعلومات وتدميرها وحرمان العدو من استخدامها لمصلحته في خلال أوقات الأزمات أو الحروب العسكرية ، والمجال الثالث هو مجال التجسس الرقمي . [113]

1- خصائص الحروب الالكترونية .

ينظر ذوو الاختصاص إلى الحرب الإلكترونية على أنها : حرب العصر الحقيقية ، مسارها الرئيس الشبكات الرقمية والإلكترونية ، كذلك الوسائل التكنولوجية الأخرى ، والأدوات الإعلامية، وكل ما يتعلق بعالم المعلوماتية والحداثة . الغاية الرئيسية لهذه الحرب هي الأضرار النفسية والمعنوية بالدرجة الأولى، ثُم تتبعها الأضرار المادية وهي حرب ناعمةٌ،

[113] عباس بدران ، مرجع سبق ذكره ، ص 30.

صامتةٌ، مظلمةٌ، بعيدةٌ عن الوسائل الحربية الخشنة، لكنها لا ُتمانع في امتطاء الترسانات المسلحة والعسكرية الضخمة.[114]

هي حرب أدمغةٍ بالدرجة الأولى ، كونها تستهدف في المقام الأول تدمير البنية العلمية والمعلوماتية للهدف ، وتأخذ أشكالًا عدة ، كشكل الإتصالات بين الجيوش وقياداتها وإضعاف شبكات النقل والإمدادات اللوجستية ، [115] وضرب المعلومات الإقتصادية وإحراج الساسة والعبث بالمحتوى الّتقني والرقمي وغيرها . وتتميّز الحروب الإلكترونية بأنّها تحتوي على تدمير لا تصاحبه دماء وأشلاء بالضرورة ، تتضمن التجسس والتسلل ثم النسف لكن لا دخان ولا أنقاض ولا غبار.كما أنّها حروب تتسم بالصمت والظلام وقلة التكاليف ومرونة الوقت وسرعة الأداء وقوة التأثير وشبه انعداميةٍ لمعرفة هوية المهاجم والخلفية الأيديولوجية ، وغيرها من الصفات التي تجعل منها حرباً شديدة الخطورة [116].

كما أنّها تجري في بيئة إستراتيجية بلا حدود؛ كما ينطبق هذا أيضا على شبكات الحاسوب. فيما يتعلق بحرب المعلومات أو تلك الخاصة بشبكات الحاسوب ، فهي ترتبط بقدرات خمسة وهي : الهجوم على الشبكات و الدفاع عن الشبكات و إدارة الشبكات وأمن المعلومات وأمن الحاسوب .[117]

كما أن هذه الحروب لا متماثلة أو لا تناظرية (Asymmetric) ، بمعنى يمكن أن تجري بين جماعات مستقلة بهدف الارهاب والجريمة المنظمة أو الانفصال والانقلاب أو المقاومة

---

[114] يحيى اليحياوي ، **" حرب المعلومات "**، موقع الكاتب يحيى اليحياوي على شبكة الإنترنيت، 13 كانون الأو ل ، 2010، على الموقع الالكتروني التالي:http://www.elyahyaoui.org/medias_war.htm

[115] عبد الجليل المرهون ، **" عصر الردع الإلكتروني"**، موقع قناة الجزيرة ، 26 تشرين الأو ل 2012، على الرابط الالكتروني التالي: http://www.aljazeera.net/analysis/pages/7bf0ab16-7011-4e73-b8ee-b756385c8a78?GoogleStatID=1#1

[116] وليد غسان جلعود ،**دور الحرب الالكترونية في الصراع العربي الاسرائيلي**، جامعة النجاح الوطنية،فلسطين،2003، ص76.على الرابط الالكتروني التالي: https://scholar.najah.edu/sites/default/files/وليد%20جلعود.pdf

[117] Ron Smith et Scott Knight , **L'APPLICATION DES SOLUTIONS DE LA GUERRE ÉLECTRONIQUE À LA SÉCURITÉ DES RÉSEAUX**,r evue militaire canadienne , Automne 2005 on website: www.journal.forces.gc.ca/vo6/no3/doc/electron-fra.pdf.

والتحرر. فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب تعني أنّه ليس هناك حاجة لدولة ما مثلا أن تقوم بتصنيع أسلحة مكلفة جدا كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا وحقيقيا على دولة مثل الولايات المتّحدة الأمريكية على سبيل المثال [118].

كما أن حرب المعلومات يمكن أن تستخدم في ثلاثة مستويات مختلفة:

1-1- **المستوى الأول يستهدف الفرد:** وفق هذا المستوى فإن أي فرد مذنب حتى تثبت براءته (وذلك بعكس القاعدة الحقوقية السائدة) , وفي هذا المستوى تكون أسرار الأشخاص غير محمية , وكذلك الأسماء والرموز التي تمارس بشكل اعتيادي و تصبح مجال متاجرة. وبهذا الشكل فعند نشوب نزاع لا شيء يمنع الخصم من تهديد زعماء حلف شمال الأطلسي (أو أي من الجنود في المعركة) , عبر استهداف عائلاتهم , مستخدماً محتويات الحواسب والمعلومات التي توفرها لتنفيذ اعتداءات.

1-2- **المستوى الثاني ويشمل حرب المعلومات من خلال التجسس الصناعي والاقتصادي على الدول والمنظمات غير الحكومية:**

ووفقاً لمعلومات مكتب التحقيقات الفيدرالية الأميركية هناك (122) بلداً يمارس تجسساً مستمراً على الولايات المتحدة في المجال الصناعي والاقتصادي , وتقدر الخسائر الناجمة عن هذا الموضوع ب(300) مليار دولار سنوياً.

---

[118] علي حسين باكير، **"المجال الخامس.. الحروب الإلكترونية في القرن الـ21"**، 2011/1. مركز الجزيرة للدراسات.،على الرابط الالكتروني التالي: studies.aljazeera.net/ar/issues/2010/20117212274346868.html 12

3-1- **المستوى الثالث , حرب معلومات موجه من أمة ضد أمة :** ويمكن أن يتضمن التجسس على المجموعات المنظمة في إطار الحكومات ، أو مجموعات الحرس الوطني ، أو التشكيلات "الإرهابية" التي تمتلك نفس أدوات الحكومة .[119]

2- **التمايز بين الحروب الالكترونية والتقليدية .**

عندما نذكر الحروب بشكل عام يتبادر إلى الأذهان تلقائيا صور الدمار والعنف والقتل والتدمير. فكل الحروب تهدف إلى إلحاق أشدّ الأذى بالطرف الآخر، فما بالك بالحروب الالكترونية والتي تعدّ أشد فتكاً وذات قدرة تدميرية بالغة الدقة . وتعتبر الحروب وسيلة أخرى من وسائل السياسة فعندما لا تنفع الدبلوماسية تلجأ الدول الى الحروب لفرض رغباتها بالقوة " فالعصا لمن عصا " ، وقد لجأت معظم الدول حالياً للحروب الإلكترونية لأنها تتميز عن الحروب التقليدية بسهولتها وشّدة فتكها ، ولأنّها تمثل حروب المستقبل وتحدّد المنتصر إذا استعملت بذكاء وحنكة .

" فمن مميّزات الحرب أنها عنيفة وتفترض وجود أدوات (صواريخ ، دبابات ، طيارات) ودافع أو غاية سياسية ، وبالتالي لا توجد حرب أو هدف أو هجوم سايبيري يمتلك هذه الصفات الثلاث ".[120]

وتعتمد الحروب التقليدية على الإستراتيجية التالية : التجسس و التخريب ومن ثم تأتي الضربة العسكرية ، لكن عندما تتعلق الأمور بالحروب الالكترونية فالمشاكل تبدأ، فعلى

---

[119] **الحرب اللامتماثلة ونظرية الأمن الاسرائيلي،** على الرابط الالكتروني: http://alma3raka.net/spip.php?page=imprimir_articulo&id_article=106&lang=a نقلا عن بلال مازن ، **الحرب غير المتوازية"الإرهاب"** , مطبعة اليازجي , ط 1: شباط 2002، ص56-57.

[120] THOMAS RID , reference previous seen , p. 4.

سبيل المثال في كازاخستان تمّ قطع الانترنت لعدة ساعات وأصبحت بالتالي معزولة عن العالم [121].

فا"الفرق بين الحرب العادية والسايبيرية ، أنّ الحرب العادية يتم استعمال العنف فيها ، في حين أن العنف هو ما ينتج من الحرب السايبيرية [122]". فالحرب التقليدية تفترض وجود جيوش جرارة وتدّخل العنصر البشري والآليات العسكرية في حين تتّم الحروب الالكترونية من دون تدخل الاثنين." معادلة خوارزمية أو فيروس ..." [123]

إضافة الى ذلك تختلف الأسلحة التقليدية عن الأسلحة الالكترونية ، فالسلاح المستعمل في الحروب التقليدية : " هو أداة مصممة لكي يتم استخدامها ، بهدف التهديد أو التسبب بالضرر المادي أو الفني أو العقلي للكائنات الحية أو النظم والمنشات " [124].

بينما الأسلحة المستعملة في الحروب السايبيرية عبارة عن رمز أو كود أو فيروس : "هو رمز على الحاسوب مصمّم بهدف التهديد أو التسبب بالضرر الفني والمادي ، للأجهزة الالكترونية والنظم والمنشآت والكائنات الحية " [125].

أضف الى ذلك لا توجد قوانين خاصة تتناول الحرب السايبيرية ، نظراً إلى حداثتها ، حتى أنّ الأمم المتحدة والمعاهدات والعهود والبروتوكولات الخاصة باتفاقات جنيف لم تتناول سوى الحروب التقليدية إجمالاً . كما أنه يوجد أهداف عديدة للحروب السايبيرية أهمها: التخريب والتجسس و إحداث الفوضى [126].

---

[121] Pierre Caron**, LA GUERRE ELECTRONIQUE N'AURA PAS LIEU**, assossiation ege, p.6. on the websitebdc.aege.fr/public/La_guerre_electronique_n_aura_pas_lieu.pdf :

[122] Mathew c. Waxman ,"**Cyber-Attacks and the use of force**", the yale journal of International law,vol 36,2011,pp.421-59

[123] بيتر سينجر، مرجع سبق ذكره ، ص 22.

[124] THOMAS RID , same reference , p. 37.

[125] Same reference.

[126] THOMAS RID,p.10.

3- **المخاطر والتهديدات .**

مع الاعتماد المتزايد ، في حياتنا اليومية ، على الأنظمة المعلوماتية ، والأجهزة المتصلة بالشبكة العالمية للمعلومات ، وتشعب طبيعة هذه الأجهزة ، من هواتف خليوية ، وأجهزة حوسبة شخصية يزدادعدد المتصلين بالفضاء السيبراني ، وتزداد إحتمالات الاعتداءات والجريمة . فقد أشار تقرير صادر عن ماكينزي ، إلى توقع زيادة المعلومات الرقمية ، بمعدل 44 % ، خلال الأعوام الممتدة من 2009 إلى2020 .[127]

فالمعلومات التي تضخ ، وتنساب ، وتحفظ في الفضاء السيبراني وعبره ، من أهم الموجودات التي يسعى إليها جميع المعنيين بهذا الفضاء ، من دون استثناء . فالشركات ، والحكومات، ومستخدمو الانترنت ، يلاحقون المعلومات كل بحسب أهدافه . وتصدر الأخطار والتهديدات السيبرانية ، عن أعمال قصدية كالإختراقات والإعتداءات ، وأعمال غير قصدية كالإهمال وقلة الوعي والادراك .

فالخطر يتناول أمن الشبكات و أمن الانترنت ، لناحيتين: الأولى ، هي البنية التحتية ، وما عليها من نقاط دخول وخروج وتخزين ، واعتراض للمعلومات . والثانية ، عمليات التخريب والتدمير والتعطيل التي تطاولها وتطاول الأموال والاشخاص من خلالها .[128]

إضافة الى خطر استيراد التكنولوجيا من الخارج مع فيروسات خاصة تضمن الخضوع والبقاء تحت السيطرة ، وبذلك تؤمّن الدول الكبرى والمصدرة للتكنولوجيا ، إخضاع مثيلاتها لسيطرتها والتبيعة لها عبر التجسس الدائم والتلاعب بمنظومتها الأمنية والمعلوماتية .

---

[127] Mckinsey noted in its july 2011 report.

[128]منى الأشقر جبور، **السيبرانية هاجس العصر** ، المركز العربي للبحوث القانونية ، بيروت ،2016 ، ص 25.
https://carjj.org/node/4595 2016

إنّ الامريكيين على سبيل المثال لا يبيعون العالم طائرات ليست فيها رادارات من إنتاج الولايات المتحدة . فالرادار ليس عيني الطائرة فحسب ، بل له أيضاً تأثيرات في جدوى استعمال السلاح الجوي ، وشل الرادار يمكن أن يشل الطائرة أو يشوش على الأقل على عملها بصورة لا تُمكّنها من الاستمرار في المهمة . واذا لم تكن تريد أن تكشف عن حقيقة أنك دخلت الى الرادار فانك تستطيع أنّ تهتم بألا تصيب الصواريخ التي تطلق منها أهدافها حتى لو كانت الأشد تطوراً. ويمكن أنّ يُغرس حصان طروادي في برنامج الرادار وينتظر يوم الأمر. ويحظّر الأمريكيون على المستهلك أنّ ينّقب في باطن الرادار من إنتاجهم . وإذا وقعت تطويرات على البرنامج فإّنهم يهتمون بأن تتلقاها وبألا تفعل أنت أي شيء بنفسك . [129]

وتتنوع المخاطر بتنوع أهدافها والجهات التي تعتمد عليها ونذكر على سبيل المثال :

أ- الجرائم العادية التي تستخدم الانترنت في تنفيذها كالسرقة والغش والخداع والتغرير بالقاصرين، وتسهيل الدعارة ، والترويج لنشاطات مخالفة للقانون ، والاعتداء على الملكية الفكرية .

ب- التعرض لسلامة المواقع : التلاعب بالمعلومات الموجودة في نظام معين ، وتشويهها أو إتلافها ، سواء عبر الاقتحام اليدوي ، أو عبر إرسال برامج وفيروسات متخصصة بذلك.

ت- جرائم الاعتداء على الحقوق الشخصية : كالتعرض لسرية الاتصالات التي تطاول البريد الإلكتروني ، والدردشة ، ونقل الملفات والدخول إلى الأنظمة للإطلّاع على

---

[129] **الحرب الالكترونية و أخر تطوراتها على الساحة الدولية** , مقال مهم
http://muha-hacker.blogspot.com/2012/01/blog-post.html

المعلومات . ويشابه هذا التنصت على المخابرات الهاتفية والاطلاع على البريد الشخصي .[130]

و أما الطّامة الكبرى فتكمن في أن الهجمات الالكترونية التي كانت تتّم من قبل الدول أصبح العامل الأساسي المحرك لها هو الجهاد السايبيري « cyber–jihad »، وهو المعتمد من قبل القاعدة بمختلف فروعها . كما أن الهجمات الوهمية التي تمت على المصارف الأميركية أثبتت قدرة القطاع المصرفي على تلافي الهجمات ، وتحييدها عن دائرة الصراعات [131].

[130] منى الأشقر جبور ، مرجع سبق ذكره ، ص35.

[131] Pierre Caron**, LA GUERRE ELECTRONIQUE N'AURA PAS LIEU**, assossiation ege, p.9. on the websitebdc.aege.fr/public/La_guerre_electronique_n_aura_pas_lieu.pdf

المبحث الثاني: العمليلت الأمنية في البيئة الاستراتيجية الإلكترونية .

إنّ حرب الظلال التي تجري اليوم بين الجيوش في عالم السايبر ، في عمق قلب معلومات العدو هي جبهة دينامية ، تستخدم فيها الأسلحة الثقيلة ، في ظل الحديث عن رقعة شطرنج ضخمة عالمية تتحارب فيها أفضل العقول . وفي كل يوم تدور معارك دفاع وهجوم وتقع أضرار واضحة وغير واضحة . إنّ الجميع هناك والجميع يستعملون السلاح على الجميع بدءاً بجيوش حديثة وانتقالاً الى منظمات إرهابية لا شأن لها بل وانتهاءً إلى قراصنة حواسيب أفراد . وفي هذه الحرب لا يوجد للصاروخ وللطائرة الحربية المتطورة أي تمّيز، فهي حرب العقل للعقل .

ومن أهم أشكال الصراع في عصر المعلومات والثورة التكنولوجية حرب الشبكات وحرب الفضاء الإلكتروني Cyber war & Net war ، وعلى الرغم من زيادة معدلات استخدام هذه الأشكال إلا أنّ ذلك لا يعني بالضرورة إعتمادها وسائل تكنولوجيا الاتصال والمعلومات حتى أنها تأتي مواكبة أو معبرة عن استخدام الآليات التقليدية للصراع ولكن بوجه تكنولوجي يتواكب مع عصر المعلومات [132].

يعتبر الإستعلام والإستخبار والتجسس وقطع إتصالات العدو والتشويش عليها والتنصت من المبادئ في العمليات العسكرية كمكّمل للحرب الإلكترونية وأمن المعلومات ، وعمليات الاستعلام . بل ويتحكم أيضا بالسياسة لأنه يشكّل ركيزة رئيسة لصنّاع القرار . ونلاحظ ثلاثة مجالات من نشاطات العمليات الأمنية ضد الخصوم في البيئة الاستراتيجية الالكترونية:

[132] Athina Karatzogianni,(ed), "**Cyber-Conflict and Global Politics**'", Routledge and Taylor & Francis Group. , 11th September 2008, pp. 240- 272 .

أولا: الدخول لنظم تكنولوجيا المعلومات والاتصالات للعدو لغرض التجسس وهذه ليست بحدود الحرب الالكترونية بل تهدف الى سرقة الأسرار الصناعية والتجارية .

ثانيا: الحرب الالكترونية الناعمة ، (Soft Cyber Warfare) نشاطات في الفضاء الالكتروني تهدف الى عرقلة سير عمل العدو ، مثل الحرب النفسية وعدم التسبب مباشرة بالدمار .

ثالثا: حرب السايبر Cyber War النشاطات التي تشتمل على هجمات في الفضاء الالكتروني التي تهدف الى الضرر بصورة مباشرة أو دمار للعدو[133].

بما في ذلك الأضرار التي ستلحق بالنظم المحوسبة أو أهداف بمساحات مادية ، من خلال إستهداف المساحات الخاضعة للسيطرة من الفضاء الالكتروني أو تفعيلها بشكل يلحق الضرر.

المطلب الأول: الدخول لنظم المعلومات أو الهاكرز.

المعلومات ؛ هي قيمة وقوة ، هدف ووسيلة في آن . فالحصول على المعلومة هو السلاح المشترك في كل الحروب وهو يعتبر الخطوة الأولى للنجاح ، نعم سلاح يستخدم في حرب باتت تعرف ب "حرب المعلومات" ، هذا المصطلح الآخذ في التردد ويملأ ما نطالعه من أخبار وقضايا في مختلف المجالات ، وهو لا يقتصر على المجال العسكري بل يواكب الاعلام والثقافة والمجتمع والاقتصاد ، فالحصول على المعلومات مهم جداً ويعتبر مصدر قوة . ومع تطور االتكنولوجيا تطورت طريقة التجسس وجمع المعلومات فأصبحت أسهل وأخطر في آن ، حيث من الممكن جمعها من طريق القرصنة الالكترونية أو الهاكرز ، لأن

133 Shmuel Even and David Siman-Tov**, Cyber Warfare:Concepts and Strategic Trends**,INSS-Institute for National Security Studies Memorandum No. 117, May 2012,p.20. on website: https://www.files.ethz.ch/isn/152953/INSS%20Memorandum_MAY2012_Nr117.pdf

كل الأسرار لدى الدول والحكومات أصبحت محفوظة ومخزنة على أجهزة الحاسوب ، ويكفي أن تخترق سرية هذه الحواسيب لتحصل على ما تريد من بيانات . فما هي أهم أدواته؟

1- القرصنة أو التجسس الالكتروني (الهاكنغ).

يرتبط التجسس الإلكتروني بالتطورات التي تحدث في مجتمع المعلومات ، فهو يزداد خطورة كلما زاد التقدم في المجال المعلوماتي ، فالاكتشاف والتطور والبنّاء يقابله التجسس والتخلّف والهدم، فالدمار الذي قد يلحقه التجسس الالكتروني بأنظمة المعلومات التي تتحكم في كل مرافق الحياة في هذه المجتمعات التي تعتمد على الحاسوب والإنترنت إعتماداً مطلقاً قد يعطّل حياة مجتمع بأكمله ، والخسائر التي قد تنجم عن مثل هذا التجسسم هي أكبر بكثير ممّا قد يتصوره العقل . ويمكن أن نعرف التجسس الالكتروني بأنه شكل آخر من الإرهاب يقوم باستخدام التكنولوجيا الضارة بشكل سلبي من أجل إحداث آثار مدمرّة وأضرار بالغة وكبيرة لمحطات التحكم وأجهزة الحاسوب وشبكات الاتصال بدوافع سياسية أو عرقية أو دينية..... الخ[134]

وتعدّ " اسرائيل من الدول الرائدة في هذا المجال ، خصوصا برنامج " بيغاسوس" حيث يعدّ بأنه البرنامج الهجومي الأكثر تطوراً ، بسبب قدرته على التسلل خلسة في أجهزة الهاتف التي يخترقها إلى المكالمات والكاميرات والبريد الإلكتروني ونظام تحديد الموقع الجغرافي وكلمات المرور والتطبيقات ، مثل فيسبوك وسكايب وواتساب وفايبر. وتقدر منظمة برايفيسي إنترناشونال البريطانية غير الحكومية ، أن هناك 27 شركة إسرائيلية على الأقل ناشطة في هذا المجال .[135]

---

[134] Real Estate Al Khal | Facebook
https://www.facebook.com/realestateKhal/posts/597750626955720

[135] **التجسس الإلكتروني.. تخصص إسرائيلي بامتياز**، موقع الجزيرة الالكتروني.
www.aljazeera.net/.../التجسس-الإلكتروني-تخصص-إسرائيلي-بام.

وقد يستهدف هذا البرنامج أفراداً أو مؤسسات خاصة بغرض التجسس الصناعي وسرقة الأسرار الصناعية والفنية والتجارية أو دولاً لأغراض أمنية أو سياسية أو إستيعاب أصول الانترنت للخصم عن طريق سرقة البرمجيات وقواعد البيانات مع نية استخدامها من دون إذن.

المطلب الثاني : التجسس والحرب الفضائية الناعمة (الاعلام ومواقع التواصل الاجتماعي).

تعتبر ملكية المعلومات جزءا لا يتجزأ من ثروات الأمة، ويمكن ربط تأثيرها بالسياسة الخارجية والأمن القومي . وذلك من خلال جمع وصيانة واستغلال الأسرار الخاصة بالحكومات ، والتي يمكن أن تنعكس اثارها على الخصوم أو الحلفاء في آن ، سواء السياسية منها أو العسكرية أو حتى الاقتصادية والثقافية .

وتعتمد الحرب النفسية على كسب "القلوب والعقول" وتحويل الرأي العام للجانب الخاص بك . عبر الدعاية ", propaganda وذلك من طريق استغلال مواقع التواصل وتكنولوجيا الاتصالات والانترنت ، عبر استخدام الفضائيات الاعلامية والصور وأشرطة الفيديو المفبركة والموجهة لزعزعة ثقة عامة الشعب بالسلطة وتدمير ثقة و دعم المجتمع المدني للعدو وكسب جمهوره لصالحه الخاص [136] ، وحرب المعلومات هذه هي شكل من أشكال الحرب الناعمة [137]، وعنصراً من عناصر الجيل الرابع من الحروب (GW4) ، والذي يستهدف القوة المدنية الداعمة للعدو كجزء من أجزاء الحرب [138]. فالحرب الناعمة تبدأ بالدعاية (propaganda) ، حيث تستحضر الايديولوجيات الشمولية [139]، وتقوم بممارسة الخداع

---

[136] Lawrence Freedman, "**Strategic Communications**," 76-77.

[137] Joseph S. Nye, Jr. "**Cyber Power**," p. 1.

[138] William S. Lind et al. **"The Changing Face of War: Into the Fourth Generation**," Marine Corps Gazette (October 1989),p. 23.

[139] الشمولية هي سيطرة حزب واحد على المجتمع ، كما كان الحال في الاتحاد السوفياتي السابق ، حيث يكون للحزب مكانة قيادية يضمنها الدستور الذي يضعه قادة الحزب بعد أن يتسلموا السلطة ، ويجعلونه قائداً أو (مالكاً) للدولة والمجتمع.

من طريق نشر الأكاذيب والأباطيل حول الدولة المستهدفة ، ويعود السبب الرئيس في كذب القادة على جمهور أجنبي الى كسب تفوق إستراتيجي عليه [140]. وذلك في سبيل تنفيذ الحرب الاعلامية والنفسية ، التي تستهدف النظام والسلطة الحاكمة والتي تشنها الفضائيات بشكل منظم ومبرمج وهدفها تفتيت وزعزعة القوة المدنية والتأثير على الرأي العام . ويترتب على هذة الميزة عواقب وخيمة كما حدث مع "ويكيليكس" ، حيث أدّت هذه االتسريبات الى تآكل ثقة الحكومات الأجنبية بالولايات المتحدة الأميركية ، و فضحت ما يحصل وراء الأبواب المغلقة ، وأثرّت على ميزة التأثير والجذب التي تمارسها الولايات المتحدة الأميركية في حربها الناعمة . وسوف نستعرض تباعاً أدواتها وأهدافها.

1 – أدوات الحرب الناعمة.

إنّ الحرب الناعمة لا تعد منهجاً جديداً في مناهج الحرب النفسية والدعاية ، بل هي تطور في الوظائف ناجم عن التطور الكمي والنوعي الهائل في وسائل ووسائط الاتصال والإعلام بل يمكن إعتبار الحرب الناعمة إفرازاً طبيعياً وحتمياً مرتبطاً بسعة إنتشار وتوسع الجيل الرابع من وسائط تكنولوجيا الاتصال والإعلام (الفضائيات / أجهزة الإتصال الخليوية الرقمية / مواقع وصفحات الإنترنت / شبكات التواصل الاجتماعي) .[141]

1-1- الإنترنت ومواقع التواصل الإجتماعي.

تعدّ شبكات التواصل الاجتماعيّ أضخم عملية تجسس عرفها التاريخ ، ويصرّح "جوليان أسانج" مُسرِّب وثائق ويكيليكس: " **إنّ شبكات التواصل الاجتماعيّ أضخم وأخطر جهاز**

[140]جون جي.ميرشيمر، لماذا يكذب القادة ؟ حقيقة الكذب في السياسة الدولية ، **مجلة عالم المعرفة**، العدد443 ترجمة غانم النجار ،المجلس الوطني للثقافة والفنون والاداب ، الكويت ،ديسمبر2016، ص 48.

[141] حادي عشر: **تكنولوجيا الإتصال والإعلام حولت الحرب النفسية الى ناعمة**
https://www.almaaref.org/books/...fe...alharb.../lesson11.htm

تجسّس واستخبارات ابتكره الإنسان وعرفته البشرية منذ فجر التاريخ؛ لأنّ المستخدم للشبكة يتبرّع مجّاناً بوضع المعلومات والصور والفيديو والتعليقات والآراء عن ذاته ودائرة زملائه ومحيطه الاجتماعيّ، وهي معطيات غالباً ما تكون مهمّة ومفيدة وموثوقة "[142].

تُعدُّ مواقع التواصل الاجتماعيّ في الولايات المتحدة ثمرة تحالف وتقاطع مصالح ، بين وزارة الخارجية الأميركية ووزارة الدفاع (البنتاغون) وجهاز الأمن القوميّ الأميركيّ (NSA) في إطار شراكات مختلطة مع القطاع الخاص الصناعيّ الأميركيّ، الذي يبلغ عديده حوالي 17 مليون موظفٍ من نخبة مجمع الابتكار العلميّ والهندسيّ والتقنيّ .[143] ويتّخذون من "وادي السيليكون" في كاليفورنيا مقرّاً لشركاتهم، مع توظيف ألمع العقول والخبرات الآسيوية : الهندية والكورية والصينية .[144]

2-1- **الفضائيات .**

تعتبر الفضائيات من أخطر الوسائل تأثيرا على المجتمعات والجماهير، فهي من المؤثرات التي توليها الحكومات والجماعات أهمية قصوى؛ نظرًا الى سُهولة وصول هذا الوسائل إلى قطاعاتٍ عريضة جدًّا من المجتمع، حيث تؤثر في عقول النَّاس ونفوسهم ، ومِن ثم تؤثر في اتجاهاتهم ومواقفهم التي يتَّخذونها حيال كثير مِن القضايا . فهي تشكل وسيلة الاتصال الأكثر انتشارا والأوسع مدى ، والأكثر جذباً واغراء ؛ لجمعها بين الصَّوت والصورة، والضَّوء واللَّون والحركة، وقد حوَّلتِ الفضائياتُ الإعلامَ اليوميَّ من مجرَّد نقل المعلومات والأفكار إلى المساهمة الفعلية في تكوين الحياة في أبعادها السِّياسيَّة، والثَّقافيَّة، والاجتماعيَّة، والاقتصاديَّة؛

---

[142] مقابلة مع "أسانج": www.it-scoop.com/2011/05/facebook-spying-machine-assange-wikileaks

[143] داليا قانصو، "لماذا خسر دونالد ترامب وادي السيليكون" ،**جريدة السفير** 2016/11/04م.

[144] وادي السيلكيون أو Silicon valley هو أهم منطقة للصناعات التكنولوجية العالمية لأجهزة الكومبيوتر والاتصالات جنوب كاليفورنيا.

لِمَا لها من قُدرة على التَّأثير في الاتِّجاهات لدى الأفراد والجماعات ، أو تعديلها ، أو تغييرها .[145]

3-1- أجهزة الاتصال الخلوية الرقمية.

تحولّت الهواتف المحمولة الذكية إلى «**مراكز تجسس**» في أيدي الأنظمة الاستخباراتية ، التي يبدو أنها تمكنت من استثمار التكنولوجيا الحديثة من أجل الوصول إلى المعلومات وجمعها بسهولة أكبر من أي وقت مضى ما ازداد إعتماد المستخدمين على هذه الأجهزة وأصبحوا يخزنون عليها صورهم ووثائقهم وملفاتهم ، فضلاً عن أنها تضم مراسلاتهم التي تتم عبر البريد الالكتروني ، وغير ذلك من الرسائل النصية والاتصالات الصوتية ، وهو ما يعني في النهاية أن اختراق الهاتف المحمول لأي مستخدم يعني الإطلاع على كل تفاصيل حياته سواء الشخصية أو المهنية [146]. أصبحت تطبيقات الهواتف الأكثر انتشاراً في العالم. فعلى سبيل المثال تؤكّد الإحصاءات أنّ 86% من اللبنانيين يملكون هواتف خلويّة ، ويحمل 45% منهم هواتف ذكيّة ، وتشكّل نسبة الذين تراوح أعمارهم بين 18 و29 عاماً ولديهم هواتف ذكية 62% منها .[147]

---

[145] منيرة الحوشاني، الفضائيات بين الايجابيات والسلبيات ، **شبكة الألوكةالثقافية** ،2012/5/23،على الرابط التالي:
http://www.alukah.net/culture/0/41242

[146] وثائق تؤكد: الهواتف الذكية أصبحت «مراكز تجسس» تخدم أجهزة الأمن ... **جريدة القدس العربي** ،على الرابط التالي:
www.alquds.co.uk/?p=374079

[147] تقرير: **"مركز بيو للدراسات"** نشرته جريدة النهار متوفر على الرابط:
http://newspaper.annahar.com/article/116498

2 - أهداف الحرب الناعمة .

تعتبر القوة المرنة الوسيلة الأمثل لكسب الحروب بالخديعة والاحتيال ، فهي تنتهج سياسات إعلامية مضللة وتقلب الحقائق بفبركة الدعاية الكاذبة . وهي ساحة مفتوحة أمام الجميع ، تتميز بالحرية ولكن لديها أهدافها الخاصة والتي تركز على استمالة القوة المدنية والتأثير على الجماهير ، إضافة الى الحفاظ على كسب الرأي العام بالمطلق ، لما تشكله هذه الأدوات من أهمية كبرى في شن الحروب النفسية ووسيلة دبلوماسية مهمة في العلاقات الدولية . وسوف نتعرض الى أمثلة عملية لأزمات من أرض الواقع .

2-1- السيطرة على القوة المدنية .

وتعتبر الأزمة السورية حالياً ،" الصراع المدني الأبرز في التاريخ بوساطة تكنولوجيا التواصل الاجتماعي " [148] ، والذي تنبأ به ويليام ماكنيل William H. McNeill في العام 1982، حيث أكد بأن تكنولوجيا وسائل الاتصال الجماهيري سوف تحدّ من قدرة الحكومات في البلدان

النامية على استخدام القوة للبقاء في السلطة [149]. ولقد تحققت مقولة ماكنيل في "الربيع العربي" والصراع في سوريا ، فبمجرد اندلاع الأعمال العدائية بدأ كل جانب باستغلال قدرات مواقع التواصل لدعم قضيته وشرح وجهة نظره والدفاع عنها .

[148] Marc Lynch et al., "**Syria's Socially Mediated Civil War**," Blogs and Bullets III (Washington DC : United States Institute of Peace, 2014),p. 5.

[149] William H. McNeill**, The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000**
(Chicago: University of Chicago Press, 1982), 378-381

فأميركا شجعت ودعمت النزاع في سوريا بحجة الحرية والديمقراطية ، وحاربت نظام الأسد من طريق استغلال أدواتها الناعمة الإعلامية الموالية لسياستها ، وتحديداً الفضائيات كالعربية و الجزيرة ، وتلفزيون الشرقBBC News [150] لكسب الرأي العام والمجتمع المدني وربح الحرب النفسية مسبقا واستمالة جمهورها المؤيد .

وتستخدم الاستخبارات الإسرائيلية تكنولوجيا المعلومات والإنترنت وكل أدوات الفضاء السيبراني للانتقال من مرحلة التجسس وجمع المعلومات حول أنشطة الدول والمنظمات التي تعتبرها معادية إلى مرحلة أخرى تتضمن زراعة معلومات مضللة أو نوعية لتحقيق غرض ما، وهو أمر خصصت له طاقات هائلة منذ بداية ما يعرف باسم "الربيع العربي" [151].

مثال آخر حول القوة المرنة والناعمة في إطار المواجهة بين إيران وإسرائيل والولايات المتحدة ، والتي استخدمت فيها الولايات المتحدة الأميركية مواقع التواصل الاجتماعي ، من أجل دعم الاحتجاجات في عام 2009، وتقديم دعم فني للمعارضة عقب الانتخابات الرئاسية ففي نهاية 2011 دشنت الولايات المتحدة "سفارة إلكترونية" لتزويد الإيرانيين بالمعلومات حول التأشيرات عبر الإنترنت، وتواصلت مع الطلاب الإيرانيين لتشجيع وتأجيجها التحركات وهو ما يلائم عملية قطع العلاقات الدبلوماسية بين إيران والولايات المتحدة منذ ثلاثين عاما [152]. وهو ما دفع إيران إلى حجب موقع السفارة وتجريم محاولة الدخول عليها على أنها تمثل تهديداً للأمن القومي لديها .[153]

---

[150] Edwin Grohe, "**The Cyber Dimensions of the Syrian Civil War**,"p. 135.

[151] ربيع محمد يحي ، اسرائيل وخطوات السيطرة على الفضاء السيبراني ، **رؤى استراتيجية** ، يونيو 2013 ، ص 75.

[152] U.S. launches 'virtual' embassy for Iran, **us today**, 12/6/2011 http://www.usatoday.com/news/washington/story/2011-12-06/us-embassy-iran/51673966/1

[153] Iran Blocks American 'Virtual Embassy,**the new York times**, December 7, 2011http://thelede.blogs.nytimes.com/2011/12/07/iran-blocks-american-virtual-embassy

2-2- الأيدي الخفية والتلاعب بالرأي العام .

ليس هدف التغطية الاعلامية تطور الوعي العام في العالم ، بل تدعيم مصالح الدول الشخصية والخاصة من طريق حشد التأييد لوحداتها العسكرية ، و تعزيز معنويات أسرهم وأقاربهم بالترويج والدعاية للأنشطة التي يمارسونها . ووسائل الإعلام هي في الواقع عامل "مضاعف للقوة " كما أنه يبني الرأي العام. ويقول أبراهام لينكولن في هذا الصدد :

" Public opinion is everything,with it nothing can fail,without it nothing can succeed ."

"الرأي العام هو كل شيء ، معه لا شيء يمكن أن يفشل ، وبدونه لا شيء يمكن أن ينجح. " [154]

كما إن أهمية الرأي العام بدأت تتصدر أولويات الدول ، والدليل ما أحدثته وثائق منظمة ويكيليكس التي تسربت إلى الرأي العام ، لُتحدث أزماتٍ عديدةٍ لبعض دول العالم، وصلت حد المساس بأمنها القومي. فقد سعت الولايات المتحدة الاميركية الى أن تبدو دائما رائدة الحضارات والحامية للقانون وللحريات العامة ،في حين أن هدفها الحقيقي السيطرة على موارد الثروات من نفط وغاز واستنزاف ثروات الشعوب وتحقيق الهيمنة المطلقة على القوة والعالم في آن معاً.

وتكمن المشكلة الرئيسية التي يقع فيها مستخدمو الانترنت من خلال محاولتهم تحقيق أهدافهم أنهم لا يعرفون من يدخل على الخط ويقف معهم أو ضدهم . فهم يتعاملون مع أناس لا يرونهم ولا يعرفونهم وبإمكانهم الإدّعاء بأنهم أي شيء أو أي كان من خلف ستار

[154] Gen Patrick Brady**, The Role of Media in War**, 1990,on website: http://www.defencejournal.com/2000/aug/role-media-war.htm

الانترنت [155]. أي أنه **الأيدي الخفية** التي يسهل عليها التلاعب بالجماهير وتسّييرهم في الاتجاه الذي يناسب غاياتها ، ما سهّل المهمة على المتلاعبون بالعقول .

المطلب الثالث: حرب السايبر .

في زمن تكنولوجيا المعلومات والإتصالات ، إختلف مفهوم العمليات العسكرية ، فقد تبدل ميدان المواجهة ، وبات يمكن إصابة الهدف من أي نقطة في العالم ، وفي أي وقت ، وتبدّلت مع ذلك، قدرة الرد والدفاع ، التي تفترض هي الاخرى ، تحديداً لنقطة انطلاق الهجوم ، وكذلك مراكز العدو. كما تأثرت القدرة على الرد السريع ، وعلى إدارة النتائج ، واثبات مصدر الاعتداء والمسؤولية . وانصبت الجهود على حيازة الأسلحة الذكية ، والأسلحة العاملة من بعد ، بحيث أصبح السلاح الذكي والمطور معلوماتيا ، والموصول بشبكة معلومات ، أساسيا في ترجيح الكفة في الحروب . ويأتي بعدها العنصر البشري، الذي يتطلب هو الآخر، مجهودا لبنائه، وتمكينه. كذلك، فقد اختلف مجال العمليات العسكرية، وانتقل النشاط العسكري كما النشاط الاجتماعي والتجاري والاقتصادي إلى المجال السيبراني . وهكذا ، تحتوي ترسانة العديد من الجيوش على الأنظمة المعلوماتية ، والمعدات الإلكترونية ، التي تستخدم ، سواء في إدارة الموارد البشرية، أ م اللوجستية، أم في خلال العمليات [156].

ويمكن استخدامها في عمل تخريبي عبر قطع كابلات الاتصالات أو تدمير أنظمة الاتصالات أو الاقمار الصناعية أو استخدام الأسلحة الإلكترونية المتقدمة كالفيروسات في تدمير الانظمة المعلوماتية لمنشآت حيوية بشكل يؤثر في وظيفتها ويهدد أمن الدولة والسكان .

---

[155] عباس بدران، مرجع سبق ذكره ، ص 57.

[156] منى جبور ، **مرجع سبق ذكره** ، ص73.

كما يمكن استخدامها لتخريب القدرات العسكرية للعدو من دون التسبب في الأضرار المادية فاستخدام الطيف الكهرومغناطيسي في الحروب ، يؤدي الى تعطيل الاتصالات عند العدو ويسبب فشلاً في معداتهم وخللاً في ساحة المعركة [157].

1- أدواتها وأسلحتها.

تشكل الفيروسات الأسلحة الأساسية في الحروب الالكترونية او السايبر ، حيث تؤدّي إلى تعطيل عمل الشبكات الإلكترونية، والخوادم الرئيسة ،Servers ، ويعتبر" ستكنست " الأنموذج الأمثل في هذا المجال ، حيث أدى الى تخريب أجهزة الطرد المركزي الايراني النووي وأحدث أضرار مادية "شديدة التأثير" من دون أية طلقة .

ويوجد الكثير من أنواع الأسلحة ونذكر أهمها :

1-1- **الفيروسات أو"البرمجيات الخبيثة":** والتي أصبحت أسلحة الفضاء الالكترونية في السياق العسكري ، وهي غالباً عبارة عن هجوم برمجي software، من خلال شبكة القرصنة "hacking. ومن المفيد تقسيم أسلحة الفضاء الالكتروني الى أسلحة معقدة" شديدة التأثير" تهدف الى احداث تأثير استراتيجي، وأسلحة أبسط كثيرا" منخفضة التأثير " تهدف الى الحاق ضرر محدود ، ولكن بقصد احداث ارتباك والاضرار بالسمعة..[158].

1-2- **البرامج الضارة Malware :** هو مصطلح يستخدم للتمثيل الجماعي للفيروس ، والديدان، وبرامج التجسس والبرامج الخبيثة الأخرى على شبكة الإنترنت. و في كلمات بسيطة،

---

[157] Brendan I. Koerner,"Inside the New Arms Race to Control Bandwidth on the Battlefield," **Wired Magazine.** 18 February 2014 ,Accessed 14 December 2015, http://www.wired.com/2014/02/spectrumwarfare

[158] جون باسيت، حرب الفضاء الالكتروني:التسلح وأساليب الدفاع الجديدة، **حروب المستقبلية بالقرن الواحدوالعشرين** ، مركز الامارات للدراسات والبحوث الاستراتيجية ،ط1 ،2014، ص 58.

يشار إلى أي برنامج يهدف إلى التسبب بضرر مباشر أو غير مباشر لنظام الحاسوب على أنه من البرمجيات الخبيثة [159].

3-1- **الحقيبة الكهروستاتيكية** : ففي المختبر القومي بولاية نيو ميكسيكو الاميركية، تمكن الباحثون من صنع جهاز على شكل حقيبة صغيرة تقوم بتوليد نبضات كهرومغناطيسية فائقة القدرة، يمكن بواسطتها تدمير الوحدات الالكترونية في أي إدارة أو مؤسسة مالية أو محطة إرسال ما يفقدها فعاليتها، كما ان هناك أبحاث لتطوير ميكروبات تتغذى على الالكترونات السليكونية وبذلك تدمر المعدات الالكترونية لدى العدو[160].

4-1- **الصاروخ الذكي** : ينطلق الصاروخ الذكي مثل صاروخ "توما هوك" من القاذفات – B52ومن الغواصات والمدرعات والمنصات الارضية ويبلغ طوله ٢٥،٦ متر، ويسير بسرعة 5،6 ماك ٨٠٠ كم"ساعة على ارتفاع ١٠ – ١٠٠ متر متجنباً وسائل الدفاع الجوي والمباني سابحاً في الفضاء بفضل حاسوب في رأس الصاروخ مسجل عليه الهدف الواجب تدميره والاهداف التي يجب تجنبها، يبلغ مداه ٦٤٠ – ٢٥٠٠ كلم يصيب هدفه بدقة عشرة امتار نسبة الخطأ لا تزيد عن عشرة أمتار فقط ، يتم توجيهه بواسطة الأقمار الصناعية (G. P. S) حيث يرسل الجهاز الالكتروني في رأس الصاروخ رسالة الى القمر الصناعي فيبث هذا القمر رسالة الى المحطة الأرضية بصور الاهداف المراد تفاديها وموقع الهدف المراد تدميره فتبثه المحطة الارضية للصاروخ فيظل يدور الى أن يجد هدفه النهائي فيطابق الصورة على الصورة التي في ذاكرته فإن تطابقا قام بالتدمير للهدف المراد تدميره .[161]

---

[159] أنواع مختلفة من البرامج الضارة وكيف تعمل - **مدونة الويب**
http://www.webbloog.com/2012/10/blog-post_2.html

[160] إسماعيل كاخيا ، **"** الحرب الإلكترونية **"**، في: **موقع مجلة الدفاع العربي** على شبكة الإنترنيت، 20 تشرين الثاني/ نوفمبر 2012. http://www.arabdefencejournal.com/article.php?categoryID=9&articleID=552

[161] اسماعيل كاخيا ، مرجع سبق ذكره .

5-1- **القنبلة الالكتروستاتيكية** : هي أحدث قنبلة في الترسانة الأميركية تعتمد فكرتها على إطلاق شعاع من الوحدات الضوئية عالية الطاقة في الذرات التي لها عدد ذري منخفض تجعلها تقذف شعاعا من الالكترونات ، وهي عبارة عن انبوبة نحاسية قابلة للتمدد ممتلئة بالمتفجرات الكيميائية خلفها مكثفات مولدة للمجال المغناطيسي ، عندما تشتعل الانبوبة فانها تلامس طرف الملف فتخلق دائرة مغناطيسية متحركة ينتج منها ذبذبة تيار كهربائي عالي الفولتية ينتج منه صاعقة ضوئية تبدو كضوء الفلوريسنت واجهزة التلفزيون والتي تعطلها عن العمل وتنبعث رائحة الاوزون المختلطة برائحة البلاستيك المحروق من الاعلفة الكهربائية حيث تنصهر الخطوط الكهربائية والتلفونية ، وتزداد شحنة البطاريات ودرجة حرارة الحواسيب ، ويتم تدمير معلوماتها المخزّنة [162].

6-1- **الطائرات الإلكترونية (دون طيار Drone)** : 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 وُتشكل 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 [163].

---

[162] المصدر نفسه .

[163] وليد غسان جلعود، مرجع سبق ذكره ، ص 105.

2- أهداف الحرب السايبيرية.

يشكّل السايبر الوسيلة الأمثل التي من خلالها تتنافس القوى الكبرى على تحقيق التفوق ، وارسال الرسائل العملية التي تثبت للآخر مدى قوتها وقدرتها على صعيد العسكر، وفي المنشآت والبنية التحتية المدنية . ولا تقتصر الحرب الإلكترونية ، على الفيروسات والبرامج المعادية ، فهي تشمل أيضا التشويش المادي المباشر، المتعلق بموجات البث السلكي اللاسلكي ، وشبكات الطاقة .[164]

وقد أشارت وكالة أسوشيتد برس إلى أن الهدف الجديد للقراصنة الإلكترونيين الروس – والصينيين هو قطاع النفط والطاقة الأميركية، وخصوصاً بولاية تكساس حيث كبرى شركات النفط العالمية ، وأكدت تعرض هذه المنشآت لأكثر من تسعمئة محاولة قرصنة خلال الفترة من 2011 إلى 2016 [165].

وهناك فيروسات مختصة **بالأعمال العسكرية** تتضمن (الهجوم والدفاع والتشويش والهاكنغ..) وتتعلق فقط بالشؤون العسكرية من أسلحة ورادارات وطائرات وصواريخ . وهناك فيروسات تستهدف **الاقتصاد والأموال** من مصارف وبنوك، أو **بنية تحتية ومنشآت** حيث تستهدف مكامن الثروات الطبيعية من نفط وغاز ومفاعلات نووية ، أو قطاعات حيوية مدنية مثل الكهرباء والماء.... حيث سيكون التأثير العسكري تدهور في أداء القادة والجنود والأسلحة ويتضح ذلك من الإجراءات الأمريكية في النزاعات في الشرق الأوسط ، أو كجزء من الضربة الجوية الإسرائيلية عام 2007 في سوريا [166].

---

[164] منى جبور ، مرجع سبق ذكره ، ص 69.

[165] زهير حمداني، **الاختراقات الروسية لواشنطن وظلال الحرب الباردة** ،2017/3/16.
2017/.../www.aljazeera.net/news/.../الاختراقات-الروسية-لواشنطن-وظلال-الحرب-الباردة

[166] David Makovsky. **'The Silent Strike: How Israel bombed a Syrian nuclear installation and kept it secret,' The New Yorker**, 17 September 2012, http://www.newyorker.com/magazine/2012/09/17/the-silent-strike.

وفي هذا السياق، ذكرت صحيفة The Daily Beast الأميركية، إن أي هجوم إسرائيلي على إيران سيكون مدعوماً بغارات إلكترونية ، من الفيروسات ، إضافة إلى عمليات التشويش فقد تمكنت إسرائيل من تطوير التكنولوجيا اللازمة ، لايقاف شبكة الهاتف الايرانية ، مع امكانية تعطيل نظام الإنذار لديها ، ومنعها من بثّ الرسائل اللازمة ، بعد هجمة إستباقية ، تشنها الطائرات مثلاً [167].

وما حدث لوزارة الدفاع الأميركية والبنتاغون من اختراق، وطاول أيضا مكتب السياسة الخارجية ومكتب الأمن الوطني Homeland Security خير دليل على ذلك ، وقد شكل الكود " TITAN RAIN " مجموع الهجوم الذي تعرضت له حواسيب الحكومة والجيش في عام 2003 ، والذي اتهم به مجموعة من الهاكرز الصينيين [168].

كما تم اختراق موقع وزارة الدفاع الفرنسية قبل عامين بغرض سرقة معلومات عن الاستطلاعات والمناورات والنظام الصاروخي الفرنسي ولا يقتصر الاختراق على المؤسسات العسكرية فقد تتعرض له المؤسسات النقدية وخصوصا البنوك المركزية والمؤسسات العملاقة[169].

3- الحرب الالكترونية في الميدان العسكري .

أصبحت مواطن النزاعات في الشرق الأوسط ، ميداناً مناسباً لتجربة الأسلحة الالكترونية من قبل الدول الضالعة في هذه الحروب ، وجولات من جولات استعراض القوة .

---

[167] Israel's Secret Iran Attack Plan: Electronic Warfare- **daily beast**, Nov 16, 2011 6:28 PM EST - http://www.thedailybeast.com/articles/2011/11/16/israel-s-secret-iran-attack-plan-electronic-warfare.html

[168] THOMAS RID, **cyber war will not took place** , .p85..

[169] قضايا .. الإرهاب الإسرائيلي الإلكتروني: العرب والتجسس الإسرائيلي الإلكتروني، **مجلة الوطن** ، 2015/04/18.على الرابط التالي: http://alwatan.com/details/57008

وتعتبر الساحة السورية حاليا أحد ميادين هذه الحروب ، فالضربة الأميركية الأخيرة على مطار الشعيرات في سوريا كانت جولة من جولات استعراض القوة بين الولايات المتحدة الأميركية وروسيا حيث تم استعراض لصواريخ توماهوك [170] فخر الصناعة الأميركية ، في حين أن عدم وصول عدد كبير من الصواريخ الأميركية هو نتيجة استخدام روسيا لموجات كهرومغناطيسية تسببت بحرف مسار الصواريخ ، أن "منظومة (Krasuha–4) [171] الروسية يمكنها إعطاء الصاروخ الموجه بالرادار أهدافا وهمية، فيقصفها لخداع العدو وايهامه بتحقيق هدفه "، فمن لديه مثل هذه المنظومة بإمكانه "إسقاط توماهوك كالذباب" [172].

وتستخدم العديد من البرامج والتطبيقات ، المصممة في الاساس لأهداف مدنية ، في المجال العسكري ، ويحضرهنا كمثال، برنامج "جوجل إيرث google earth " الذي يؤمن معلومات جغرافية ، ويعرض صورًا للكرة الأرضية ، وخرائط الدول ، بتفاصيل دقيقةً جداً ، ما يؤدي الى كشف أماكن المنشات النفطية والنووية والبنية التحتية والحكومية والعسكرية ، ويعطي معلومات شديدة الدقة حول موقعها ويعرضها بالتالي الى الاستهداف العسكري المباشر[173].

وتجدر الاشارة الى أن الجماعات التكفيرية المسلحة استفادت أيضا من قدرات الإنترنت للحصول على ميزة تكتيكية في أرض المعركة. حيث استغلت الجماعات التكفيرية المسلحة

---

[170] صاروخ "توماهوك يسير بنظام (TLAM/D) ويحتوي الصاروخ على 166 قنبلة عنقودية، وهو مخصص لضرب المنشآت الصناعية، ومحطات الكيروسين، ومراكز القيادة، ودشم الطائرات المبنية بجدران ضد المتفجرات، ومواقع الرادار، ومواقع الصواريخ أرض ـ جو، وغيرها.

[171] أن "منظومة (Krasuha-4) الروسية هو تعطيل نظام GPS ، وهذا كاف لإحداث العمى الجغرافي ، علما أنها قادرة على تعطيل باقي أنظمة توماهوك (INS, TERCOM, DSMAC)،كما انها عبارة عن موجات كهرومغناطيسية ، يمكنها إعطاء الصاروخ الموجه بالرادار أهدافا وهمية، فيقصفها وينحرف ويسقط قبل أن يصل إلى هدفه المنشود .

[172] محمد الطاهر ، خبير ألماني يكشف عما حصل للصواريخ الأمريكية المتجهة إلى "الشعيرات"، **موقع ارتي**، على الرابط الالكتروني: https://arabic.rt.com/middle_east/872546-صواريخ-توماهوك-حمص-الشعيرات-سقوط-خلل-سوريا-ترامب-الولايات-المتحدة تاريخ النشر:10.04.2017 | 06:29 GMT

[173] منى جبور ، مرجع سبق ذكره ، ص 75.

تطبيقات الإنترنت، مثل "خرائط جوجل" Google Maps لتحديد الأهداف بدقة وقصفها بالاسلحة البعيدة المدى[174].

إستنتاج الفصل الثاني

تشكل "حرب المعلومات" أهم أنواع القوة حاليا ، نظرا لأنها تذهب أبعد من مجرد مهاجمة أجهزة الحواسيب وشبكات الاتصالات، اذ يمكن أن تعيث فساداً و تتسبب في الدمار المادي في السياسة والاقتصاد والبنية التحتية المدنية ، ويمكن أن تلحق الضرر بالسكان المدنيين ، كما أنها تشكل خطرا على الأمن القومي للدول . ويمكن أن تتحول شبكة الإنترنت إلى سلاح يستخدم ضد أهداف خفية في الفضاء الإلكتروني كالترويج للعنف والاضطرابات والتحريض على الثورات وشن الحروب النفسية . فالجرائم المتصلة بالحواسيب، هي امتداد للهجمات الإرهابية، ولديها القدرة على جلب الآثار الجانبية الكارثية . بل إن الموجة الجديدة من التكنولوجيا المغّيرة لقواعد اللعبة تمكّنها من ذلك بوتيرة أسرع ، وتؤثر في قلب الموازين اذا ما تم استخدامها بطريقة ذكية .

[174] Anita R. Gohdes, "Pulling the Plug: Network Disruptions and Violence in Civil Conflict**," Journal of peace Research 52,** No.3,2015, p. 355.

خاتمة القسم الأول .

حرب قديمة مُتجدِّدة تشهدها الدول الكبرى على مستوى دوائر القرار والشركات الضخمة. تَتَداخل فيها الأهداف العسكريَّة بالأهداف الاقتصاديَّة، أو ما يُعرَف بالتجسُّس الصناعي. فضاء هذه الحرب هو الشبكات العنكبوتيَّة التي باتَت تُسيطر على العالم الافتراضي، وجنودها هم خُبراء في علم الكمبيوتر والإنترنت، أذكياء في قدرتهم على اختراق الحواجز الأمنيَّة للمعلومات السريَّة لدى الخصم أو المُنافس، وقرصنتها. حيث تغلغلت الحرب الإلكترونية بوسائطها الرقمية الجديدة فـي كـل المجتمعات حتى بات إستخدامها مرتبطاً بكل مجالات الحياة بشكل يومي . ومن خلال وسائطها الإلكترونية الرقمية التي لاتعرف سيادة وطنية للدول على حدودها ،اذ أن مجال عملها كبير بحجم العـالم الذي نعيش فيـه ، ما أدى الى قرع ناقوس الخطر لدى الدول ، وأفضى الى معادلة مفادها :" كلما ازداد اعتمـادنا على الإنترنت وتكنولوجيا الاتصالات كلما ظهرت إمكـانية حدوث اختراقات عالية الخطر" قد ترقي لتصنّف حرباً رقمية على مؤسسـات الدولة الرقمية ومؤسساتها ما يسبب الهلع العـام ودخول الدولة في حالة الفوضى.

وبدأت الدول الكبرى تتجه بقوة نحو بنـــاء ترسانـات الأسلحة الرقمية وتسعى أن تكون تلك الترسانات سرية وجاهزة لدعـم ومؤازرة أي حرب أو تحرك عسكـري مستقبلي . الا أنّ التطورات الكبيرة في مجال صناعة "الروبوتات"، والذكاء الاصطناعي، وغيرها... تؤدي إلى زيادة هائلة في القدرات العسكرية المتاحة للكيانات الصغيرة، حيث تمدها بقدرات اعتادت أن تكون حِكراً على القوى الكبرى، كما قد تتمكن الأسلحة الصغيرة والذكية والرخيصة التي يتم تطويرها، من إحداث تغييرات جذرية في طبيعة المعارك وطرق القتال.

القسم الثاني: الإستراتيجية الأمنية :"إسرائيل "– حزب الله ، في ظلً الحروب الإلكترونية .

يتصدر موضوع الأمن القومي قائمة الاهداف الاستراتيجية الرئيسة ل"إسرائيل"،حيث يتم تحديد الأوضاع والمتطلبات الخاصة بهذه المسألة على أنها تشكل مرادفا لوجودها، ويرتبط ذلك بالحفاظ على الأمن الاسرائيلي ازاء المخاطر والتهديدات الداخلية والخارجية ، من خلال العمل باتجاه تحليل المتغييرات الداخلية والخارجية ، التي تخضع لمعطيات الواقع الراهن على المستوى الداخلي والاقليمي وتحولات السياسة الدولية .

ف"اسرائيل" في مفهومها "للأمن القومي" إستندت الى مبادئ صهيونية منها " **نكون أو لا نكون**"، وعلى اعتبار أنها " في تهديد مستمر" من الدول العربية ، وأن قضية " الأمن" هي المفتاح الرئيس لجميع خطوطها السياسية ومنهج عمل الحكومات والقيادات الأمنية والعسكرية. فانطلقت في بناء نظرياتها "الأمنية" على العوامل الديمغرافية والاقتصادية والجيوسياسية . إن قواعد نظريات الأمن الإسرائيلي ، تعتبر في تطور دائم بناءً على إدراك القيادة العسكرية والأمنية الإسرائيلية ، بأنه من الصعب المحافظة على نظريات ثابتة ، لا سيما في ظل مفاهيم الأيدولوجية الصهيونية التي تتمحور حول التوسع والسيطرة . [175]

بلورت" إسرائيل" إستراتيجية متكاملة لمفهوم أمنها وسبل تحقيقه ، ووظفت لذلك كل مصادرها السياسية والاقتصادية والتعليمية والثقافية والتكنولوجية ، ويسجّل للقيادات الإسرائيلية أنها نجحت في صياغة روايتها التاريخية لجذور الصراع ومسبباته ، وإقناع الرأي العالم الاسرائيلي والأميركي والأوروبي براويتها لفترة زمنية طويلة (محرقة الهولوكست ومظلومية الشعب

[175] استراتيجية الأمن القومي الاسرائيلي، **عكا للشؤون الاسرائيلية**، حزيران 2016،على الرابط التالي:
http://akka.ps/2016/06/%D9%85%D8%AD%D8%AF%D8%AF%D8%A7%D

اليهودي) . لقد أصبحت اسرائيل ونتيجة لما شهدته المنطقة من تطورات سياسية بعد حرب تموز 2006، مطالبة بتأسيس نظرية أمن جديدة تقوم على قراءة دقيقة لما جرى في الحروب الماضية، واستخلاص العبر لتفادي أية انتكاسات جديدة .

وبما أن العنف والقوة والتفوق والريادة يسيطر على الذهنية الاسرائيلية ، فالجيش والعسكر سيطر على المجتمع بكل أطيافه ،حيث احتلّ الجيش مكانته و مسؤوليته في تأمين الوجود الإسرائيلى ومواجهة الأخطار ومصادر التهديد , وهو، الجيش ، يمتلك الأجهزة الخاصة بجمع المعلومات وتحليلها ورصد المستجدات والمعطيات وتحضير الخطط اللازمة بطريقة مهنية واحترافية تفوق غيره من المؤسسات فى الدولة الإسرائيلية , بل يكاد الجيش يكون عبر أجهزته وأقسامه المتخصصة فى التخطيط والمعلومات والتحليل المؤسسة الوحيدة التى تمتلك هذه القدرات والإمكانيات.

وفي ظل ثورة التكنولوجيا والمعلوماتية كان لا بد للدولة العبرية من مجاراة التطور الحاصل حيث دمجت "إسرائيل" بين تقدمها فى مجال الفضاء السيبرانى ، ووجود تهديد خطير يتمثل فى أعداء افتراضيين يحطيون بها ويهدّدون أمنها القومى . وخصوصا أن هذه القدرات الهجومية السيبرانية تمّكن "إسرائيل" من التّهرب من تحمل مسوؤليتها عن اعتداءات شنتّها أو قد تشنّها فى المستقبل ضد منشآت صناعية أو نفطية أو حواسيب دول تعتبرها معادية . فشرعت " إسرائيل" فى إحداث التغيرات المطلوبة لبناء قوتها ، وهناك ارتباط بين معالجة التهديد السيبرانى و حماية الأمن القومى للدولة حيث تركزت المعالجة فى : الأجهزة الامنية الجيش الاسرائيلى ، دوائر الاستخبارات ، الصناعة العسكرية والأمنية ، الشبكات الوطنية الحساسة المعرضة لهجمات سيبرانية ، والقطاع الخاص .

الفصل الأول

الفضاء الإلكتروني وعلاقته بالاستراتيجية الأمنية الإسرائيلية .

يستحوذ مفهوم الأمن على الذهنية الاسرائيلية ويحتل فيها المكانة الأكثر أهمية من أي قضية أخرى . ويحتل الجانب العسكري مكانة خاصة ومهيمنة في الأمن القومي ، وخصوصا الصراع العربي– الاسرائيلي. وتستلزم الطبيعة الدينية والوظيفية للدولة العبرية ، أن يكون الإطار العام للأمن القومي إطاراً أمنياً عسكرياً بالدرجة الأولى ، أما الإطار السياسي ؛ فهو عملية تكاملية لسد الثغرات المفتوحة في الإطار العسكري ، على أن صانعي القرار ورؤساء الوزراء هم جنرالات متقاعدون أو من أصول عسكرية من ذوي الخبرة والباع الطويل في الحروب والمعارك .

هي دولة غير مرغوب فيها إقليميا بسبب نشأتها السياسية والعسكرية ، ولأنها كيان استيطاني قام على أنقاض الدولة الفلسطينية ، لذلك فقد كان التفكير الأمني الاسرائيلي يركز على مفهوم "قلة مقابل كثرة" كما قال يسرائيل طال في كتابه الأمن القومي [176] ، وأنه يجب على" إسرائيل" مواجهة حقيقتها الجيوبوليتيكية، ووجودها محاطة بدول عربية في كل الاتجاهات ،مع اليقين بعدم تقبل هذه الشعوب لهذا الكيان الغريب والغاصب وعدم التسليم بشرعيته. فسعوا الى امتلاك القوة والتفوق العسكري لضمان بقائهم ووجودهم .

كما أنّ التحولات العميقة التي طرأت على تكنولوجيا الأسلحة العسكرية أو ما يطلق عليها "الثورة في الشؤون العسكرية"، أخذت تسبب تحدياً آخر للأمن الإسرائيلي، فمثل هذه الأسلحة

[176] يسرائيل طال ، **الأمن القومي،قلة مقابل كثرة** ، (بيطحون ليئومي:معطيم مول ربيم) ،(تل أبيب:دفير،1996) ، ص 15.

المتقدمة المزودة بتكنولوجيا رفيعة وأساليب حديثة جعلت الحديث عن الدفاع والأمن القومي الإسرائيلي ومهدداته موضوع جدل سياسي عام، يجري في سياق يسود فيه قلق كبير لدى الساسة الإسرائيليين من امتلاك جماعات متطرفة أو أفراد لمثل هذه التكنولوجيا المتطورة التي تهدد أمنها .

وبناء على ما تقدّم فقد تطور مفهوم الأمن القومى تجاه التهديدات الجديدة غير التقليدية ، واتسع مجال الأمن ليمتد من الجانب العسكرى لمجالات أخرى عديدة ، وحيث أن أجهزة الحكومة الإلكترونية فى العالم و"إسرائيل" من ضمنها فى فضاء مفتوح ، في ظل غياب الحدود الجغرافية ، ما أدى الى أن تكون أجهزتها عرضة للعديد من الاخطار تحت دوافع مختلفة ، ومن الممكن أن تتم مهاجمة أنظمة الحكومة الإلكترونية من داخلها أو من خارجها من طريق الهاكرز أو أجهزة الاستخبارات فى بلدان معادية عبر تنفيذ الهجمات الإلكترونية بهدف اختراق النظام الأمنى المعلوماتى للحكومة ، ولذلك بات يتم اختراق الأمن القومي عبر اختراق الأمن السيبراني .

تعتمد "إسرائيل" على قدرتها التكنولوجية وتقدّمها فى صناعة البرمجيات على خلق ديدان الحاسوب والفيروسات و البرامج الخبيثة ، التي تشن بها هجمات على دول تعتبرها معادية ، كما نجحت " إسرائيل " بفضل هذا التقدم في اقتحام أسواق عالمية وفى مقدمّها السوق الأمريكية ، إلى درجة وصلت إلى تحذير الخبراء الأمريكين من الغزو الإسرائيلى لسوق الاتصالات والتكنولوجيا فى أمريكا [177].

[177] Gil Baram ,"**The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case**" , Military and Strategic Affairs, Vol. 5, No. 1 , 2013 .

أما السبب وراء هذا النوع من السباق الى امتلاك المعرفة التكنولوجية نحو السعي لتحقيق التفوق (النووي سابقا حيث تعتمد الاستراتيجية النووية الاسرائيلية على الفكرة الأساسية بان الردع النووي يعزز أمن "إسرائيل" [178] ، وقد تجنبت **"**الردع النووي العلني **"** رغم الميزات الاستراتيجية التي يحققها فلجأت الى الضبابية حول امتلاكه واكتفت بالتلميح .[179]) وامتلاك المعرفة التكنولوجية السايبيرية حاليا يحقق الريادة والتفوق التي تسعى اليهما "إسرائيل" وهذا بالتحديد الموضوع الذي يرتكز عليه البحث في هذا الفصل .

المبحث الأول :النظرية الأمنية الإسرائيلية.

إن الدلالة العامة للأمن القومي تعني مجموعة الاحتياطات والتدابير ، النظرية والعملية الخاصة بحماية المجال الاقليمي لدولة ما ، على أن المجال الاقليمي هنا لا يعني الرقعة الجيوبوليتيكية من الأرض في ، بل يشمل الثروات الاقتصادية ، الأيدولوجية السياسية الخاصة بنظام الحكم في تلك الدولة والأهداف الوطنية الممثلة لخصوصيتها القومية والحضارية . " فالنظرية الأمنية ليست نظرية جامدة مقدسة بل هي رؤية واقعية متجددة ونظرة شاملة، تحدد الأخطار وتضع الحلول وتسعى لتوفير الإمكانيات اللازمة لهذه الحلول ".[180]

ولكي نفهم حقيقة الكيان العبري ، يجب أن نشير الى أن هذا الكيان بني على الكذب والأساطير ، وقد أشار الى ذلك اسحاق شامير حين قال:"من أجل اسرائيل يجوز الكذب"[181] وقد ذكر ذلك أيضا "موشيه شاريت" رئيس وزراء "إسرائيل" حينما قال :"لقد تعلمت أن دولة "إسرائيل " لا يمكن أن تهيمن في زمننا هذا من دون الخداع والمغامرة..."[182] فقادة الكيان

---

[178] أفنر كوهين، **اسرائيل والقنبلة ، القدس**:مؤسسة شوكن للنشر ،2000، ص 440.

[179] يوفل نئمان ،**"اسرائيل ومحدودية الردع النووي"**، نتيف ، 1-2(54-55)،1997، ص 167-170.

[180] محمد المصري ، النظرية الأمنية الاسرائيلية، **مجلة دنيا الوطن** ، على الرابط الالكتروني التالي:
https://www.alwatanvoice.com/arabic/news/2009/07/14/139596.hml

[181] Aviashi Margalit,"**THE VIOLENT LIFE OF YETZHAK SHAMIR**",NEW YORK Review of Books,May 1992,p. 23.

[182] المصدر نفسه.

الإسرائيلي مارسوا الخديعة بشتى الوسائل لهدف واحد هو اثبات مظلومية الشعب اليهودي وكسب استعطاف الشعوب الأوروبية والغربية ودعمها ، وإيجاد دافع قوي لليهود "ديني وقومي "من أجل المحافظة على هذا الكيان من قبل اليهود أنفسهم.

ما يدفعنا الى التساؤل التالي : لماذا الاصرار على إقامة هذا الكيان ؟

والسبب: أنّ"إسرائيل"_في حقيقتها_كيان استعمارى، استيطاني، احلالي، عنصري،عسكري، توسعي، عميل للقوى الاستعمارية الكبرى، تابع_اقتصاديا_لها،غريب_حضاريا_عن المنطقة العربية الاسلامية، وهي تسخّر، فوق ذلك، مقولات دينية توراتية وتلمودية وادعاءات تاريخية في خدمة أهدافها ومطامعها". [183] ويؤكد ذلك بن غوريون حينما قال: ان خلود اسرائيل يتميّز باثنتين: دولة "إسرائيل "والتوراة ."[184]والتي تستهدف إيجاد الوسائل العملية الداخلية لدى " إسرائيل" القادرة على تجسيد نظرية الأمن الإسرائيلي . وبناء على ما سبق فأنّ الحافز الأقوى للحركة الصهيونية هو تمكين الأمة اليهودية من تحقيق ذاتها من طريق تجميع اليهود في دولة خاصة بهم كما يقول وايزمن :" ان هدف الصهيونية بناء قومية تكون يهودية بقدر ماهي الأمة الفرنسية فرنسية وبقدر ما هي الأمة البريطانية بريطانية"[185].

وبما أنّ المشروع الصهيوني هو مشروع استيطاني ، فالهاجس الأمني يفرض على "إسرائيل" البقاء في حال دائمة من الصراعات ، وبالتالي ديمومة الاستعداد والتخطيط للحروب القادمة كما يؤكد شمعون بيريز فى كتابة "الشرق الأوسط الجديد" حول هذه المسألة : "إن موضوع الأمن لا يمكن اعتباره موضوعاً قابلاً للنقاش أمام أي رئيس حكومة إسرائيلية، إنه موضوع

---

183 عبد الفتاح ماضي ، مصدر سبق ذكره ، ص9.

184 المصدر نفسه ، ص9.

185 هيثم الكيلاني، دراسة في العسكرية الاسرائيلية، القاهرة: **معهدالبحوث والدراسات العربية** ،1969،ص113.نقلا عن كتاب حاييم وايزمن، **التجربة والخطأ** ، نيويورك 1949،،ص 244.

حياة أو موت بالنسبة الينا جميعاً، وعليه فإن النظر إلى الأمن الإسرائيلي يجب أن يتقدم سلم الأولويات قبل تنفس الهواء، فبقدر ما نضغط أمنياً على أعدائنا بقدر ما تتوافر فرص البقاء والوجود ".[186]

المطلب الأول: مرتكزات الأمن القومي الإسرائيلي.

ترتكز نظرية الأمن الاسرائيلي على جملة من العوامل المتداخلة المترابطة والتي تشمل مختلف مجالات النشاط والفعاليات الحيوية في "إسرائيل"، ومن هنا نظرية الأمن الإسرائيلي ظاهرة مركبة تتكون من القوة العسكرية والهجرة اليهودية الى "إسرائيل" فانّ توسيع عمليات الاستيطان وتخفيف الهجرة المعاكسة من " إسرائيل" الى الخارج وتقوية القاعدة الاقتصادية، وتأمين تحرك سياسي دبلوماسي خارجي يوظف لمصلحة تأمين متطلبات الأمن واستخدامها من أجل **التوسع وزيادة الأراضي والعمق الاستراتيجي لها** . وقد وضع ديفيد بن غوريون ، رئيس وزراء "إسرائيل" السابق، الفرضيات الأساسية لنظرية الأمن الإسرائيلية، والتي تعرضت للتغيير حسب ما تقتضيه الظروف الاقليمية والمتغييرات الطارئة . فمن مرحلة " العمق الاستراتيجي" و"الضربة المضادة الاستباقية" كما أشار شمعون بيريز، إلى "إستراتيجية الردع النووي" منذ العام 1975 ، وإلى "إستراتيجية الهجوم الاستباقي" المتبعة حالياً في الأراضي المحتلة وغيرها من الإستراتيجيات الأخرى.[187]

[186] محمد المصري ، النظرية الأمنية الاسرائيلية ، **دنيا الوطن** ،على الرابط الالكتروني التالي:
https://www.alwatanvoice.com/arabic/news/2009/07/14/139596.html
[187] محمد المصري ، النظرية الأمنية الاسرائيلية ، ص 5.

1- الإستراتيجية العسكرية الإسرائيلية .

إرتكزت الاستراتيجية العسكرية الاسرائيلية على ثوابت عدة ، أبرزها:

1-1- ضمان العمق الاستراتيجي :

وقد استندت هذه النظرية الى فكرة العمق الجغرافي ، المرتكز على الاحتفاظ بأكبر مساحة ممكنة من الاراضي المحيطة .[188]وقد أدركت اسرائيل مبكراً أن أحد أهم التحديات التي تواجهها تتمثل في محدودية العمق الجغرافي. عامل الجغرافيا السياسية، وكما تشير المعطيات فإنه يحتشد نحو 80 –90% من سكان "إسرائيل" في منطقة تمتد نحو 120 كلم على طول الشاطئ بين حيفا وأسدود، وهذا يشكل تهديداً أمنياً حقيقياً ل"إسرائيل" نتيجة العمق الإستراتيجي الضيق الذي يجتمع فيه غالبية السكان هناك، وما يشكله ذلك من خسائر بشرية فادحة في حال تعرضت "إسرائيل" لهجمات تطاول تلك المنطقة الجغرافية من "إسرائيل" .[189]

فالعمق الاستراتيجي شكّل أزمة وقلقاً كبيراً أرّق مضجع هذا الكيان منذ نشأته ، حيث سعى بكل الوسائل الى زيادة مساحة أراضيه من طريق غصب الأراضي من الدول العربية وقضمها، وكان بمثابة الهدف الأساسي والرئيس الذي تسعى اليه كل الحكومات التي تولّت الحكم ، والمحرّك الموجّه لصانعي القرار وكذلك لكل الحروب التي خاضتها ضد الدول العربية كما أن مبدأ الحفاظ على العمق الاستراتيجي مرتبط **بمبدأ الضربة الأولى** والحدود ذات القابلية للدفاع عنها **Defensible Borders**، وقد ساهم ذلك في بناء توجه لدى متخذي القرارات

---

[188] جوني منصور، فادي نحاس ، **المؤسسة العسكرية في اسرائيل (تاريخ، واقع ، استراتيجيات وتحولات)**، مدار المركز الفلسطيني للدراسات الاسرائيلية ، فلسطين ،2009 ، ص 255.

[189] محمد المصري ، مرجع سبق ذكره ، ص 16.

الاستراتيجية ، للبحث عن معنى التهديد الأمني في ظل عدم التوازن الكمي بين اليهود والعرب في الشرق الأوسط .[190]

2-1- الحرب الاستباقية "preemptive strike" ، والحروب الوقائية " preventive war"

أي نقل الحرب الى أرض العدو [191]، وذلك لايجاد عمق استراتيجي مصطنع [192]. وتشتمل على نظرية الهجوم المضاد والاستباقي "Anticipatory counter_attack" . وهي النظرية التي عمقّها ايفال الون في منتصف الستينات، وقد عرّفها بما يأتي :" انها مبادرة عملياتية إسرائيلية تتخّذ ضد التحشدات العدائية وتستهدف احتلال مواقع ذات شأن أمني حيوي عند العدو ، في وقت يقوم العدو بحشد قواته ، ولكن قبل قيامه عملياً بتنفيذ هجومه "[193]، وتهدف الى تحقيق النصر المباشر وتحاشي عوامل الضعف .

وهي صفة إتسمّت بها معظم الحروب التي شنّتها "اسرائيل" ضد الدول العربية ، والتي كانت تعتمد على عنصر المفاجأة والمباغتة . **وإن هدف الحروب الاستباقية أو الوقائية هو إثارة الذعر** .[194] حيث يتم تطبيق سياسة "**ننتظر لنرى**" على أمل ألا تحصل مشاكل ، وإثارة الذعر لخلق الانطباع بأن هناك خطرا مباشراً ، "فالحروب الوقائية ، وهي أساسا شكل من

---

[190] جوني منصور وفادي نحاس ، مصدر سبق ذكره ، ص 256.
[191] المصدر نفسه ، ص258.
[192] محمد المصري ، مرجع سبق ذكره ، ص 12.
[193]حسين اغا، أحمد الخالدي، قاسم جعفر،" **اسرائيل، العقيدة العسكرية وشؤون التسلح** "، سلسلة الدراسات الاستراتيجية ، المؤسسة العربية للدراسات والنشر، بيروت ،1982، ص 11.
[194] جون جي.ميرشيمر، مرجع سبق ذكره ، ص 78.

أشكال الدفاع عن النفس ، معترف بها على نطاق واسع بأنها مشروعة وعادلة في الوقت نفسه " .[195]

ولذلك كانت الدولة العبرية تسعى إلى شن المعارك و نقلها الى أراضي الدول العربية نظراً في اتساع مساحتها ولمعرفتها أن قيام المعارك على أراضيها يؤثر في الجبهة الداخلية التي تتسم بضعفها وانهيارها التدريجي . " فخسارة " إسرائيل" لمعركة حاسمة واحدة تؤدي إلى إنهيارها ، بينما يستطيع الطرف العربي استيعاب أكثر من هزيمة عسكرية من دون أن يشكل هذا خطراً على كيانه"[196]

3-1- مبدأ الحدود الآمنة :

وهي نظرية وُضعت أُسسها قبل 1967 لكنها تبلورت بعد حرب 1967، وقد شرحها (آبا إيبان) وزير الخارجية آنذاك ، أنها نظرية تقوم على حدود يمكن الدفاع عنها من دون اللجوء إلى حرب وقائية. ويُلاحَظ في هذه النظريـة غلبة المكان على الزمان بشكل تام، إذ يُنظَر للشعب العربي باعتبار أنه يجب القضاء عليه تماماً أو تهميشه، فنظرية الحدود الآمنة إعلان عن نهاية التاريخ العربي . [197]

لقد حددت الحركة الصهيونية فكرة الأمن بشكل جغرافي وأسقطت العنصر التاريخي ، وتصوّرت أنه من طريق الاستيلاء على قطعة ما من الأرض أو على هذا الجزء من العالم العربي أو ذاك ومن طريق التحالف مع الولايات المتحدة والقوة العسكرية ، فإنها تحل مشكلة

---

[195] Michael Walzer,**Just and Unjust Wars:A Moral Argument with Historical ILLustrations**,3rd ed.(NY:BASIC BOOKS,2000),p. 74-85.

[196] علاء طاهر، **حرب الفضاء ونظرية الأمن الاسرائيلي** ، الصلاح للدراسات الاستراتيجية ، ط1، باريس ، 1991، ص20.

[197] استراتيجية الأمن القومي الاسرائيلي ،**عكا للشؤون الدراسية** .

الأمن وتصل إلى الحدود الآمنة. [198] إنّ الحفاظ على الحدود الأمنة من الأولويات في "إسرائيل" نظراً إلى حساسيتها أمام **الخسائر المدنية والعسكرية** ، ما فرض عليها البحث عن السبل والوسائل التي تمكّنها من تحقيق هذة المرتكزات ومن أهمها :

أ- **تعزيز قوة الردع:** من خلال بناء قدرات عسكرية متفوقة بالقوة والامكانات ، بحيث تردع أعداء اسرائيل عن المبادرة لشن حرب ضدها .[199]

ب- **الانذار الاستراتيجي:** بحيث تمتلك قوة استخباراتية تعطي إنذاراً مبكراً عن نية العدو الإقدام على شن حرب (بمعنى التجسس والاستطلاع الدقيق لمعرفة خطط العدو مسبقاً والجهوزية التامة للتصدي له).

ت-**الحسم** : عندما يفشل الردع وتندلع الحرب ، يجب أن تكون "إسرائيل "على أهبة الاستعداد لنقل المعركة الى أرض العدو ، وحسم المعركة بأسرع ما يمكن .[200]

4-1- نظرية الردع .

الردع عمليةٌ مركبة جداً، وتنطوي بالدرجة الأولى على التهديد بتفعيل القوة في سبيل منع حدوث أمرٍ ما، أو قد يتم استخدامها كعقوبة بهدف منع العدو من القيام بإجراءٍ عنيف، وعملية الردع لها أكثر من نوع أو شكل ومنه؛ الردع المتبادل بين دولتين باستخدام خليط من الأساليب، وقد يكون بين دول إقليمية، أو ضد تنظيمات لا تعد دولة، ومن حيث حجم التوازن الردعي يمكن تقسيم الردع إلى قسمين: **ردع شامل ، وردع مصغر** ويقتصر على التوازن في جوانب محددة من الصراع .... لكن الردع أصلاً لا يشكّل أساس إدارة النزاعات وحلّها ،

---

[198] محمد المصري، مرجع سبق ذكره ، ص 15.

[199] المصدرنفسه ، ص9.

[200] ماهر الشريف،العقيدة الأمنية الاسرائيلية وحروب اسرائيل في العقد االخير ، **مؤسسة الدراسات الفلسطينية** ، بيروت 2015،ص2. على الرابط التالي :-www.palestine-studies.org/sites/default/files/uploads/images/alaqeeda.pdf

وإنما هو استراتيجيةٌ واحدةٌ ضمن عددٍ كبيرٍ من الإستراتيجيات التي تهدف إلى استقرار نظام العلاقات النزاعية ، وفي كثيرٍ من الحالات ينجح الردع لمدةٍ زمنيةٍ محدودة فقط ، كما أنه لا يحلّ محلّ التسويات السياسية، وإنما تكمن وظيفته في العمل على استقرار وتثبيت العلاقات العسكرية في حالات النزاع ، وتقديم الدعم لتسويةٍ سياسيةٍ في حال وصولها .[201]

إنّ النظرية الوقائية الاستباقية تؤلف ركناً أساسياً في نظرية الردع ، وهي بمثابة خط الدفاع العملياتي الثاني للمفهوم الإسرائيلي للحدود الآمنة ، ومقترن بفكر عسكري مرن يواكب التطورات العسكرية عند العدو والتجديدات والاكتشافات الحديثة في العالم والتكنولوجيا العسكرية ، كما يحتّم الإلتزام بترسيخ قاعدة اقتصادية ، وحليف خارجي قوي يمدّ " إسرائيل" بالخبرة والسلاح . [202]

" في العام 1995 التقى وزير الخارجية شمعون بيرس مع نظيره المصري عمرو موسى . " قال له : "يا شمعون نحن أصدقاء، فلماذا لا تسمح لي بان ألقي نظرة على المفاعل في ديمونا ؟، أقسم ألا أروي لأحد ". " يا عمرو، أأنت مجنون" أجبته. " لنفترض اني أتيت بك الى ديمونا ورأيت انه لا يوجد هناك أي شيء وتوقفت عن القلق ؟ **أنا افضل أن تواصل الشك . هذا هو ردعنا** " . [203]

وبالمحصّلة إن مفهوم الأمن القومي الإسرائيلي ينطلق من إنكار الزمان العربي والوجود العربي، والفلسطيني على وجه التحديد . وهذا يعني ضرورة فرض الوجود الصهيوني والشروط الصهيونية بكل الوسائل المتاحة ، أي أن ردع العرب وإضعافهم هو هدف أساسي للأمن

---

[201] يئير عفرون ، رؤى إسرائيلية استراتيجية حول حـرب لبنـان الثانيـة تموز/ يوليو 2006، **اعداد وحدة الدراسات الاسرائيلية**.

[202] حسين اغا، أحمد الخالدي، قاسم جعفر، مرجع سبق ذكره ، ص58.

[203] **يديعوت احرنوت** – يوآف كيرن - بيرس: "هكذا اقمت المفاعل في ديمونا" – 07\09\2017
http://www.raialyoum.com/?p=739251

القومي الإسرائيلي، وأن على الجيش الإسرائيلي أن يحتفظ بقدرته العسكرية النوعية والحفاظ على تفوّقه العسكري مقابل العرب ، فالحفاظ على تفوق" إسرائيل " العسكري همّ قومي متجذر في العقلية الصهيونية ومرتبط بأيدولوجية صهيونية إستيطانية . وأن عليها أن تحتفظ بعلاقاتها المتينة بالعالم الغربي الذي يدعمها ويموّلها ويضمن تفوقها العسكري الدائم ، فهناك ضرورة لوجود حليف عسكري دائم لها .

ولكن من أجل تكوين صورة مجملة للتفكير الصهيوني الإسرائيلي ، لا بد من شرح خصوصية قيام هذا الكيان ما يعطي فكرة واضحة للقارىء حول الخطر الوجودي الذي يسيطر على رؤسائه ومؤسسيه .

2- خصائص الكيان العبري .

إن فكرة إنشاء وطن قومي لليهود في فلسطين ليست محض صدفة ، إنما جاءت حصيلة جهود بذلها اليهود في جميع أنحاء العالم لكي يتجمعوا في وطن قومي لهم في فلسطين ، فكان أول مؤتمر لهم لتحقيق هذه الفكرة في بال بسويسرا 1897 ، وظل هذا الحلم يراود اليهود حتى تحقق عام 1948 في الرابع عشر من مايو بإعلان الدولة على الأراضي التي احتلت من فلسطين . حيث يقول بن غوريون "بالدم والنار سقطت اليهودية وبالدم والنار سوف تعود من جديد ".[204] إلا أن هذه الدولة تتميز بخصائص وسمات عدّة من خلالها نستطيع فهم الفكر الصهيوني ، وسبر أغوار الطريقة التي تدور في فلكها السياسة الخارجية لهذا الكيان وكيفية اتخاذ القرارات والسلطة.

---

[204] بسمة نامق ، تأثير مقومات قوة الدولة على سياستها الخارجية حالة دراسية (اسرائيل)، **مجلة المستنصرية للدراسات العربية** ، 2010 ص 122. على الرابط التالي :
www.iasj.net/iasj?func=search&query=au...formQuery=au...uiLanguage=ar

ومن أهم سمات نشأة الكيان العبري:

2-1- **الموقع الجيوبوليتكي الحساس للكيان العبري** . وقد جرت بعض الدراسات حول الضعف في مقومات وقدرة الدولة من الناحية الجيوبوليتيكية [205]، والذي يؤدي لزيادة الهاجس الأمني قوة بما يؤثر على سياسة الدولة الخارجية ، فيدفعها الى أنماط معينة من السلوك تركز على تقدم مطلب الأمن ومحاولة تلبيته بشتى الوسائل والسبل .[206] فهي مساحة مسطحة بشكل عام وضيقة، حيث ان مناطق واسعة من المراكز السكانية والأماكن الصناعية والقدرات العسكرية في متناول ايدي أعداء "إسرائيل". [207] حيث يحتشد حوالي 80_90% من سكان "إسرائيل" في منطقة تمتد نحو 120 كلم على طول الشاطىءبين حيفا وأسدود.[208]

2-2- "إسرائيل" دولة بلا حدود معترف بها دستورياً وعالمياً: حيث أنها لم تستكمل أهم شروط قيام الدول ، ألا وهي الحدود السياسية [209]، هذا فضلاً عن كونها دولة فريدة بموقعها المجاور ، فهي جيب محاصر من شعوب عربية تناصبها العداء السياسي والاثنوجرافي والثقافي والاجتماعي والاقتصادي والديني .[210]

2-3- "إسرائيل "هي الدولة الوحيدة (في عالمنا المعاصر)التي قامت على أساس هجرة أتباع الديانة اليهودية[211]، ولا تزال حتى اليوم وتطبيقا لقانون "العودة "و"الجنسية " مفتوحة أمام أي يهودي يرغب في الذهاب الى "إسرائيل "، وبل تمنح له الجنسية الإسرائيلية

---

[205] المقصود هنا بالواقع الطبيعي الجيوبوليتيكي للدولة هو واقع أرضها وموقعها الجغرافي وليس عقيدتها الجيوبوليتيكية.
[206] بسمة نامق الأوقاتي، المصدر نفسه ، من 106-141.
[207] الجزيرة نت ،2012/11/29.
[208] الجيش الاسرائيلي2000-2012 ، **مركز الزيتونة للدراسات والاستشارات** ، بيروت ، ص56.
[209] من أهم شروط قيام الدولة هي الأرض ، الشعب والسلطة. لا يوجد ارض لاسرائيل فقد قامت عن طريق اغتصاب الأرض الفلسطينية وتهجير شعبها.
[210] الجغرافية السياسية لاسرائيل ، **موقع غزة** على الرابط الالكتروني التالي :
site.iugaza.edu.ps/fjadba/files/2010/02/الجغرافيا-السياسية-لأسرائيل1.doc
[211] لا يوجد شعب ، بل خليط من قوميات مختلفة تمّ تجميعه باستخدام العامل الديني والأيدولوجي والقومي.

فوراً.[212] إذن فهي كيان استيطاني يقوم على تهجير يهود من كافة أنحاء العالم وتوطينهم في فلسطين بالعنف والتنكيل ، وقد نجم عن ذلك خليط من أقوام وجماعات لا يجمع بينهما سوى "الديانة اليهودية".[213]

2-4- أنشأ هذا الكيان نتيجة عدة عوامل وظروف ، منها دولية (الهولوكوست النازية ، وشعور أوروبا بالخوف من الشتات اليهودي وما لحقهم من ضيم) ، و صهيونية (الاستيطان وغصب الأراضي العربية لتأسيس " إسرائيل") ، ودينية توراتية خاصة (ووضع العقيدة الأيديولوجية اليهودية في خدمة العقيدة الأمنية .)

2-5- " إسرائيل" هي الدولة الوحيدة التي قبلت عضويتها في الأمم المتحدة بناء على القرارين (181، و194) [214]، فالقرار 181[215] هو الموجب الذي على أساسه قامت الجمعية العامة بإصدار القرار رقم 194 [216].

2-6- خاضت "إسرائيل" حروباً أكثر من أي دولة أخرى في العالم ، منذ إنشائها في العام 1948 وحتى اليوم، وغيرت حدودها الجغرافية ووسعتها وبدلتها عبر العقود الماضية بشكل وبوتيرة لم تضاهيها أي دولة أخرى في العصر الحديث .[217]

2-7- الخطر الوجودي الذي يسيطر على الذهنية الإسرائيلية ، انعكس بدوره على "إسرائيل" فهي دولة ليست كباقي الدول ، لا من حيث المكانة ولا من حيث الدور، وأدى ذلك

---

[212] عبد الفتاح ماضي ، مرجع سبق ذكره ، ص 25.

[213] المصدر نفسه ، ص19.

[214] أحمد حسن محمد أبو جعفر، **دراسة نقدية في قراري الجمعية العامة للأمم المتحدة 181 و194 المتعلقين بالقضية الفلسطينية** ،جامعة النجاح الوطنية نابلس، 2008، على الرابط التالي: https://scholar.najah.edu/.../دراسة-نقدية-في-قراري-الجمعية-العامة-للأمم-المتحدة-181-و194.

[215] صدر في العام 1947،حيث أدى الى قيام الكيان العبري على جزء كبير من الأراضي الفلسطينية ،وادى الى تشريد شعب بأكمله.

[216] صدر عام 1948 والذي ينص على حق الفلسطينيين في العودة الى ديارهم وحق التعويض لمن لا يريد العودة.

[217] محمود محارب ، عملية صنع قرارات الأمن القومي في اسرائيل وتأثير المؤسسة العسكرية فيها..،**المركز العربي للأبحاث ودراسة السياسة** ، على الرابط التالي:
www.arab48.com/بحث?searchText=الأمن%20القومي&SearchIn=...page=5

الى تسخير كل مقومات الدولة بما فيها الاقتصاد في خدمة جيش دولة قامت بحدّ السيف ، ويمثل التوسع البشري والجغرافي هدفاً نهائياً لها.[218]

2-8- أهمية العسكر والجيش في الواقع الإسرائيلي ، فتنامي دور المؤسسة العسكرية الأمنية هو ظاهرة «طبيعية» في سياق حالة "إسرائيل" الأمنية الناجمة عن توسيعاتها الدائمة ، وفي الماضي قيل مراراً : «**إسرائيل جيش له دولة، وليست دولة لها جيش**».[219]

2-9- يحتل الأمن القومي الإسرائيلي المكانة الأبرز في **الاعلام** ، وهو المؤثر الأكبر في معنويات المجتمع الإسرائيلي والمعيار الذي يمكن من خلاله بناء الرأي العام السياسي أو الحزبي . كما أن "إسرائيل" لا تجري العديد من التقويمات أو المراجعات في سياستها الأمنية ، فالتقريران الوحيدان اللذان أجرتهما المؤسسة الإسرائيلية هما تقرير "أغرانات " بعد حرب 1973 وتقرير" فينوغراد " بعد حرب تموز 2006.

2-10- لا يوجد دستور في كل " إسرائيل" ، (وقد استعاضت عن ذلك بمجموعة من القوانين التي سنتها وتعالج كل الأذرع المختلفة للحكم والمؤسسات السياسية في الدولة وقام الكنيست الاسرائيلي بسنها بالتدريج) . وينص القانون الأساس للحكومة الذي سّنه الكنيست عام 1968، بأنّ الحكومة هي السلطة التنفيذية للدولة ، وتقوم بمسؤوليتها بعد حصولها على ثقة الكنيست ، ومسؤولة أمامه مسؤولية جماعية .[220]

2-11- طغيان المؤسسة العسكرية على المؤسسة السياسة ما انعكس بدوره على المناصب السياسية الأساسية لصنع القرار (معظمهم جنرالات ممن خدموا في الجيش،ولديهم تاريخ عريق في العسكر) و تعتبر حرب تموز 2006 من المفارقات التي لاقت انتقادات

---

[218] عبد الفتاح ماضي ، مرجع سبق ذكره ، ص 75.

[219] أسعد عبد الرحمان، . إضاءات حديثة على دور المؤسسة العسكرية الإسرائيلية في السياسة، **مجلة المستقبل** ،2008/10/31 almustaqbal.com/stories.aspx?StoryID=315560

[220] **كتاب القوانين540**،(سيفر هحوقيم540) ،1968، ص226.

لاذعة من قبل الراي العام الاسرائيلي ،حيث تولى فيها سياسيان لا ماضيًا عسكريًا أو أمنيًا لهما منصبي رئيس الحكومة ووزير الدفاع –إيهود أولمرت وعمير بيرتس.

13-2- يخصص أفراد المجتمع الإسرائيلي فترة زمنية من وقتهم في الأمن ، لا تضاهيها او تقترب منها أي دولة في العالم ، اذ يخدم كل يهودي إسرائيلي في الجيش خدمة الزامية لمدة عامين ونصف عندما يبلغ ثماني عشرة سنة . وبعد إنهائه الخدمة الالزامية يخدم في الجيش شهراً واحداً في كل عام حتى يبلغ سن الخامسة والاربعين .[221]

المطلب الثاني: النظرية الأمنية الإسرائيلية والمراحل التي مرت بها.

لقد مر مفهوم الأمن الإسرائيلي بأربع مراحل أساسية قبل حرب تموز 2006، مرحلة القاعدة الإستيطانية، ثم مرحلة تحويل القاعدة إلى دولة، ومرحلة التوسع، ومرحلة الهيمنة، ومن هنا ندرك أسباب هذا التغيير والحراك في المفهوم الأمني لما تقتضيه السياسة التوسعية التي تنتهجها "إسرائيل" ، فهو مفهوم متحرك يتبدل بتبدل الظروف السياسية والعسكرية المحيطة[222] غير أن هذه الحروب جميعها لم تحمل "إسرائيل " على إعادة صياغة نظريتها الأمنية كما بعد حرب تموز 2006، الا أنها شهدت بعض التحولات او المنعطفات ، لكنها لم تمثل خروجاً عن مرتكزاتها الأساسية ، مع أنها ظلت تحملها على تطوير ترسانتها العسكرية . ويمكن تقسيم هذة الفترة الى ثلاثة مراحل اساسية .

[221] محمود محارب ، مرجع سبق ذكره ، ص 2.
[222] محمد المصري ، مرجع سبق ذكره ، ص 11.

1- المرحلة الأولى: منذ نشأتها وحتى التسعينات.

خاضت " إسرائيل" حروباً عدة مع الدول العربية ، فكانت حرب 1948 بمثابة القاعدة الاستيطانية الأولى ، حيث قامت بالاستيلاء على الضفة الشرقية من فلسطين التي شكلّت النواة التي انطلق منها ما يسمى بالكيان الصهيوني ، وأخذت بالنمو والتوسع على حساب الدول العربية .

في العدوان الثلاثي على مصر تبنت "إسرائيل" استراتيجية هجومية تقوم على نقل المعركة الى" أراضي العدو" [223]، وقد انطلقت "إسرائيل" من منطلقين أساسيين في تحديد عقيدتها العسكرية : الأول غياب الحدود لانعدام **العمق الجغرافي** ، والثاني " **التفوق الكمي**" للعرب عليها[224]. ومن أهم العبر التي استخلصتها " إسرائيل" من حرب 1956، هي صحة مبدأ الهجوم الوقائي وصحة نقل الحرب الى أراضي العدو ، إضافة الى أهمية التفّوق الجوي لحسم المعركة .[225]

ولّدت نتائج حرب الأيام الستة عام 1967، شعوراً بالأمن لدى الإسرائيليين، وأدى احتلال الأراضي العربية (صحراء سيناء، صحراء النقب والجولان والضفة الغربية) ، والتي تقدر بأربعة أضعاف المساحة التي احتلتها" إسرائيل" في حرب 1948 ، إلى تقليل أهمية الهجوم المسبق وحيويته ولم يعد هذا المبدأ يشكل في الواقع عنصراً مركزياً في النظرية الأمنية الإسرائيلية ، نظرا الى زيادة العمق الجغرافي للكيان العبري . وفي هذه المرحلة قررت "إسرائيل" الإعتماد على وسائل تكنولوجيا مثل : الإعتماد على نظام استخباراتي متقدم يستطيع أن ينذر

---

[223] دافيد بوقاعي ، **"الخطر الكياني على اسرائيل:الرد الاستراتيجي"**، نتيف ،17(100)،2004، ص 10-17.
[224] جوني منصور وفادي نحاس ، مرجع سبق ذكره ، ص 263.
[225] نفس المصدر السابق ، ص 264.

بقيام حرب ، أو تطوير النظام الدفاعي الاقليمي ليكون قادراً على امتصاص الضربة الأولى في حال تأخر وصول الإنذار، وتزويد المستعمرات بكل الترتيبات الأمنية ووسائل المراقبة لتعزيز العمق الاستراتيجي للدفاع الاقليمي .[226]

وفي هذه المرحلة تبنى موشي ديان ويغال آلون إستراتيجية الردع التي تعد تطويراً للمعادلة الهجومية الإسرائيلية ، [227]والتي بدت واهية بعد حرب 1973، حيث فقدت "إسرائيل" ميزة البدء والمبادرة في الهجوم . فصاغ إسحق رابين البديل بما يأتي :" في حال عدم صمود قوة الردع سيتم النظر في قوة الحسم التي يتمتع بها الجيش الإسرائيلي" [228].

أثبتت حرب تشرين أول 1973 عدم ضمان تحقيق النصر الإسرائيلي في كل مجابهة عسكرية، كما هي الحال أيضاً في حرب لبنان تموز 2006. كما كشفت حرب 1973 أن العمق الاستراتيجي لم يكن حلاً لمشكلة الأمن الاسرائيلي ، وأثبت أنه لتوافر هذا العمق ثمناً باهظاً. ومهّدت الطريق أمام مبدأ الحدود الآمنة .[229] كما أثبتت أن الجيش الإسرائيلي يجد صعوبة في إدارة معارك دفاعية ، وذلك يعود أولاً وقبل كل شيء إلى عيب في النظرية التكتيكية الهجومية الإستراتيجية الأمنية ، يشمل أساليب القتال والتدريب والإستعداد في مجال الدفاع . وقد علق اللواء الاحتياط أبراهم إدان على هذه الظاهرة بقوله: "من السهل أن نرى اليوم أننا كنا أسرى بأيدي أنفسنا، عبيداً لنظرية ترعرعنا عليها، بأنه يجب أن نهاجم بأسرع ما يمكن وأن ننقل الحرب إلى أرض العدو"[230] . ما أدّى الى إعادة ذريعة الحرب الهجومية والوقائية كأساس للاستراتيجية الأمنية الاسرائيلية فكانت حرب لبنان **1982 أو سلامة الجليل**

---

[226] اهرون ياريف، **العمق الاستراتيجي ، وجهة نظر اسرائيلية في أمن اسرائيل في الثمانينات** ، 1980، ص27.
[227] جوني منصور وفادي نحاس، المصدر نفسه ، ص265.
[228] صلاح ابراهيم "استراتيجية الأمن القومي الاسرائيلي" **الفكر الاستراتيجي العربي**، العدد3، 31كانون الثاني 1990،ص35-
[229] محمد المصري ، ص 34.
[230] المصدر نفسه ، ص31.

هي الحرب التي قادها شارون . فقد أعلنت المفوضية العسكرية الإسرائيلية أن الهدف المباشر من عملية (سلامة الجليل) هو الانتقام لإطلاق النار على "مايا أرغون" السفير الإسرائيلي في لندن، أما الهدف العسكري فهو هدف دفاعي ضمني لوقف الهجمات الفدائية وتطهير مساحة 67 كيلومتراً من لبنان، ثم أظهرت أن الهدف الحقيقي هو فرض حكومة موالية ل"إسرائيل" في لبنان تحت حمايتها .[231]

وقد أرادت "إسرائيل" من خلال هذه الحرب أن تثبت أنّها قادرة على إنزال الهزيمة بالأسلحة التقليدية لدى خصومها، وأظهرت مدى فاعلية الإجراءات التي تم اتخاذها في أعقاب حرب 1973 على بنية الجيش الإسرائيلي وقوته ، وأظهرت مدى فاعلية التنظيم الحديث والتكنولوجيا التي تم إدخالها في نظام أوسع للقيادة والسيطرة والاتصال والإستطلاع .[232]

2- المرحلة الثانية من التسعينات حتى 2006.

في بداية التسعينات ، ومع المتغيّرات السياسية التي أصابت المجتمع الدولي من الحرب الباردة الى انهيار الاتحاد السوفياتي الى حرب الخليج ووصول الصواريخ العراقية (1991) الى المدن والمنشآت الاسرائيلية ومن ثم اندلاع الانتفاضة في فلسطين ، وانطلاق عمليات التفاوض(الأرض مقابل السلام) ، إضافة الى الحربين التي شنتهما "إسرائيل" في التسعينات "عملية الحاسبة" ضد حزب الله عام1993 لمدة 9 أيام ، والتي انتهت بمعاهدة شفهية بتجنيب المدنيين ولكنها لم تدم طويلاً ، حيث تلاها حرب نيسان " عناقيد الغضب " في نيسان 1996ومجزرة قانا " ، والتي انتهت بمعاهدة جرت على الاراضي السورية بضمانات دولية . إلا أنّ المفصل الحقيقي والتحول الجوهري في النظرية الأمنية الإسرائيلية هو

---

[231] المصدر نفسه ، ص 34.

[232] محمد المصري ، مرجع سبق ذكره ، ص34.

الانسحاب الإسرائيلي من لبنان في 2000م تحت ضغط ضربات المقاومة اللبنانية ، وهو ما شكّل سابقة في تاريخ الكيان الصهيوني . وبداية لسلسلة الانتصارات على صعيد حركات المقاومة .

وفي هذه المرحلة ، بدأ يتبلور مفهوم جديد يتلخص في : أن التهديد الأهم المحدق ب"إسرائيل" ليس غزو الجيوش وإنمًا في التنظيمات والمجموعات (الإرهابية) وهذا يشمل مواجهات محدودة بين " إسرائيل " وهذه التنظيمات وغيرها [233]. وهذا المفهوم أدى الى الإنسحاب الإسراثيلي من لبنان الذي شكّل كارثة حقيقية مدمرة في الوعي الإسرائيلي ، وكان من الطبيعي أن تنتقم " إسرائيل" لهذه الهزيمة وخصوصاً بعد انسحابها المذل من الأراضي اللبنانية ، فكانت حرب تموز 2006 .

وبالمحصلة فانّه ما قبل حرب تموز 2006 إعتمدت "إسرائيل" على عقيدة بن غوريون التي تركز على : " أهمية إقناع الدول العربية دوماً بالتسليم بالوجود الإسرائيلي". وأن تدفع "إسرائيل " العالم العربي إلى الاستنتاج : أنه لا سبيل عملياً لتدمير دولة " إسرائيل". كل ذلك يتم عبر "تحقيق إنتصارات متتالية تؤدي إلى تيئيس القيادات العربية "[234] . ولعل أبرزها: الحروب الاستباقية ، الردع ، نقل المعارك إلى أرض العدو، إنهاء الحروب العدوانية بالسرعة الممكنة والحسم السريع للمعارك .

وبالرغم من المراحل التي مرت بها النظرية الأمنية الاسرائيلية ، إلا أن "إسرائيل " لم تزل تواجه تحديات أمنية عدةّ بعيدة المدى هي:

---

[233] **وكالة أخبار الشرق الجديد - الكيان يعيد صياغة عقيدته الامنية** د. فايز رشيد
.www.neworientnews.com/archive1/news/fullnews.php?news_id

[234] فايز رشيد ، عقيدة آيزنكوت وتطوير الإستراتيجية العسكرية الإسرائيلية ، **مجلة القدس العربي**، \ 20 \ 08 \ 2015 ،

أ- صغر "إسرائيل" وقلة مواردها.

ب- إنعزالها من الناحية الجغرافية وضعف عمقها الاستراتيجي.

ت- حساسية الإسرائيليين للخسائر المدنية والعسكرية.

ث- رفض مجموعة من الدول العربية والاسلامية الاعتراف بشرعية" إسرائيل "ووجودها كدولة يهودية في المنطقة .[235]

3- حرب تموز 2006 حرب مفصلية.

يعتبر عدوان تموز 2006 تاريخاً مفصلياً في الصراع مع المقاومة ، فقد استمرت 33 يوماً واعتبرت أطول الحروب التي خاضتها " إسرائيل" منذ قيامها، وأكثرها تعقيداً وصعوبة وكلفةً من النواحي المادية والبشرية والمعنوية. والتي أثرت بشكل كبير في الوجدان الإسرائيلي وكان لها تداعياتها الأمنية والعسكرية والسياسية . كما شكّلت صدمة في الوعي الجمعي الإسرائيلي، لأنها ضربت "البقرة المقدسة" المتمثلة بالجيش الإسرائيلي، وحطمت مقولة "الجيش الذي لا يقهر" ، وعززت مقولة الأمين العام لحزب الله بأنها " أوهن من بيت العنكبوت " [236] وهو ما دفع صناع القرار الإسرائيلي للاستعاضة عن لجان التحقيق بجلسات الاستماع واستخلاص الدروس، عبر لقاءات سرية بعيداً من الإعلام، حتى لا تؤثّر في معنويات الجنود والضباط وقد استخلصت اللجنة الفشل الإسرائيلي على كافة المستويات الاستراتيجية، والعملياتية، والتكتيكية .[237]

---

[235] المصدر نفسه ، ص17.

[236] االصفة التي أطلقها الأمين العام لحزب الله على "اسرائيل" ،والتي أدت تحديدا للمواجهة التي حصلت في بنت جبيل أثناء حرب تموز 2006.

[237] Matt M. Matthews,**We Were Caught Unprepared: The 2006 Hezbollah-Israeli War**, OP 26,2008,p.61.on website: usacac.army.mil/cac2/cgsc/carl/download/csipubs/matthewsOP26.pdf.

وقد أدّت هذه الحرب إلى نسف عقيدة "**بن غوريون الأمنية القائمة على العمق الاستراتيجي** " والتفكير في صياغة وإعداد وتحديث عقيدة أمنية جديدة تواكب المستجدات العسكرية ، والتي تشكّل هماً رئيساً للقيادات الأمنية والسياسية في " إسرائيل" . حيث كشفت عن نقاط ضعف مهمّة وحساسة من أهمها : تعرّض الجبهة الداخلية المدنية الإسرائيلية، ولأول مرة في تاريخ الحروب العربية–الإسرائيلية، لقصف يومي ومكثف بالصواريخ، حيث لم تتمكن القوات المعتدية من إنهاء القتال بسرعة والحسم لمصلحتها ، فهو استمر 33 يوماً، استخلصت القيادات الأمنية والسياسية من خلالها أن العقيدة الأمنية، التي هي أساساً عقيدة هجومية ، تفتقر إلى مكوّن الدفاع ، الذي يشمل "الدفاع السلبي"، ويقوم على توعية المواطنين في أوقات الحرب واقتراب الصواريخ من أماكن وجودهم، وعلى تهيئة ملاجئ وغرف حصينة في المنازل؛ و"الدفاع الفعال"، الذي يقوم على تملك وسائل اعتراض الصواريخ والقذائف الصاروخية . كما كشفت المستوى الاستخباراتي المهم التي وصلت اليه المقاومة اللبنانية في مجال التنصت والاستخبارات والسايبر وهو ما صدم الجانب الإسرائيلي وقد تعرّض الجانب الإسرائيلي بعد حرب تموز الى كل أنواع الضغوطات التي بدأها الصحافيون ثم استكملت من قبل المؤسسات والرأي العام الإسرائيلي، للمحاسبة ولكشف الاخفاقات التي حدثت في خلال المعارك وتحديد المسؤول المباشر عنها ، ما أدى الى عقد لجنة "فينوغراد" .

4– لجنة فينوغراد.

سميّت اللجنة فينوغراد تيمنّا باسم القاضي الذي ترأسها ، وقد انتهى عمل اللجنة بتقريرين ، واحد سري لم ينشر حتى الآن ، والآخر علني تجاوز السبعمائة صفحة بحثت في خلالها أبرز الأسباب والأخطاء التي أفضت الى هذا الفشل، حيث ورد فصل خاص بعنوان **(أمن**

المعلومات في الحرب) للدلالة على أهمية **حرب المعلومات الالكترونية وأمنها** في المعادلة الجديدة وتداعياتها على الحروب المقبلة والتركيز عليها في العقيدة الأمنية الجديدة للدولة العبرية.

وقد خلصت لجنة فينوغراد الى الصعوبات التي واجهت " إسرائيل " في الحفاظ على سرية المعلومات من جهات عدّة، الأولى تلك المختصة بالجيش وكيفية سير المعارك **على الجبهات** وإخفاء سقوط الصواريخ على المستوطنات، والثانية تلك المتعلقة بالحكومة والمستوى السياسي الإسرائيلي حيث واجهت مشكلة تسريب المعلومات التي تتعلق باجتماعات الحكومة الاسرائيلية العادية والمصغرة ، وهو ما شكّل ضرراً كبيراً على الجانب الاسرائيلي .[238]

وأوصى التقرير في النهاية الى وجوب منع وسائل الاعلام من مصاحبة الجيش الى داخل المعركة وإعادة النظر في سياسة البث المباشر والتعامل مع موضوع أمن المعلومات برقابة شديدة. كما كشف التقرير نقاط الضعف الاسرائيلية الحساسة وهي ضعف الجبهة الداخلية "**العمق الاستراتيجي**" أمام الصواريخ وعدم فعالية " القبة الحديد" بالحماية فضلاً عن كلفتها الباهظة . ومن ناحية ثانية، وفرّت الحرب ضد حزب الله في لبنان الفرصة لإعادة الإعتبار إلى أهمية دور القوات البرية وضرورة إعادة تنظيمها وتأهيلها وتسليحها جيداً، وذلك بعد أن تبيّن في خلال الحرب أن هذه القوات كانت شبه مهملة وذلك من خلال الإخفاقات التي ظهرت جلية في مواجهات بنت جبيل ومارون الراس .

[238] تقرير لجنة فينوغراد، نقطة 188، ص468.نقلا عن ص 136(تأثير خطابات نصرالله على معركة تموز)

5- العقيدة الجديدية : "عقيدة أيزنكوت".

بخطوة غير مسبوقة في تاريخه، نشر الجيش الإسرائيلي على موقعه الإلكتروني، وثيقة إستراتيجية باللغة العبرية، بعنوان "إستراتيجية تْساهَل" [239]، وهي على امتداد 30 صفحة، في 5 فصول، و40 عنواناً فرعياً، تضمنت الوثيقة الخطوط العريضة لوظيفة الجيش الإسرائيلي، وحددّت مرجعيته الأمنية وأهدافه وطرائق تحقيقها، فتحدثت عن: الإطار الاستراتيجي للجيش، والبيئة التشغيلية والإستراتيجية، واستخدام القوة، ومبادئ القيادة والسيطرة، وتراكم القدرة. وحسب تقارير إسرائيلية عدة، هناك قسم سري للوثيقة ظل طيّ الكتمان لكونه يتعلق بمعلومات عسكرية حساسة.

إن المبدأ الأساسي لهذه الإستراتيجية هو **الدفاع ، فالهجوم من أجل الدفاع عن "الأمن الإسرائيلي" لا يُعتبر في أذهانهم هجوما بل هو عمل دفاعي** . وبالطبع فإن إستراتيجية الدفاع جاءت لتعبر عن تطور مفاهيم "الأمن الإسرائيلي" في ظل اختلاف الظروف.[240]

وقد ركزّت هذة العقيدة على **السايبر** في كل الميادين ، حيث باتت حروب السايبر تشكل جبهة قتالية جديدة لدى الجيش الإسرائيلي و أجهزته الأمنية، وتنفق عليها موازنات مالية هائلة، وتستقطب إلى صفوفها خيرة الكوادر التقنية من اليهود في "اسرائيل" وخارجها، بعد تعرضها لهجمات قرصنة من جهات معادية لها .[241] خصوصاً بعدما شهدت الساحة السياسية الإسرائيلية منذ بدايات 2015 جدلاً واسعاً حول مبررات إجراء تقليصات مالية في قطاعات

---

[239] الوثيقة منشورة على الرابط الإلكتروني: http://www.idf.il/SIP_STORAGE/FILES/9/16919.pdf

[240] فايز رشيد ،عقيدة آيزنكوت وتطوير الإستراتيجية العسكرية الإسرائيلية ، **مجلة القدس العربي**، \ 20 \ 08 \ 2015 .

[241] ترجمة عدنان أبو عامر، **استراتيجية الجيش الاسرائيلي** ، ا عداد الجيش الاسرائيلي، ترجمات الزيتونة 79 ، موقع يديعوت أحرونوت ، أيلول ، 2015،ص 18.

إجتماعية ومعيشية وإقتصادية لمصلحة المؤسسات العسكرية والجيش، الذي يشهد حال من " السمنة الزائدة " بدون مبرر، لاسيّما وأن هناك أزمة إقتصادية متفاقمة تشهدها الدولة .[242]

كما ركزّت على القوى المسلحة الغير دولانية [243]، مثل حزب الله وحماس بعدما انحصرت المعارك معها ، الا أن الخطر الحقيقي للكيان الصهيوني الأبرز هو حزب الله وخصوصاّ بعد الخبرة التي تراكمت من خلال الحرب السورية والإنجازات التي تحقّقت على أيدي مقاتليه .

وتنسب هذه العقيدة الى غادي أيزنكوت [244]، ومن الطبيعي أن تكون سيرة حياة أيزنكوت، وسلسلة المهام الميدانية والقيادية النوعية التي تولاها، قد تركت بصماتها على صياغة الوثيقة، وخصوصاً خدمته في مراكز إتخّاذ القرارات، ووظّف تجربته الغنية ومكانته في شبكة العلاقات بين القيادتين العسكرية والسياسية، بالحصول على إقرار العقيدة المسماة باسمه من قبل رئيس الحكومة ووزير الدفاع ، وبذلك أصبحت هذه الوثيقة عملياً خطة للدولة، لكون الجيش هو العمود الفقري للكيان الإسرائيلي .[245]

تعترف الوثيقة بأن خطة تغيير بنية الجيش تتكيف مع بعدين مهمين هما: **ضغوط الموازنة المالية، وتغيّر خريطة المخاطر المحدقة ب" إسرائيل"** . وفي جوانب استخدام القوة تحتوي

---

[242] المصدرنفسه ، ص 29.

[243] هو مصطلح جديد بدأ يستخدم للاشارة الى حركات المقاومة والفصائل من غير الدول (أمثال داعش وجبهة النصرة....).

[244] هو غادي آيزنكوت: 55 عاماً، رئيس أركان الجيش الإ سرائيلي منذ شباط/ فبراير،2015 شغل قائد المنطقة الشمالية، ثم قائد المنطقة الوسطى، ثم قائداً لشعبة العمليات في الجيش، وتدرج في المناصب العسكرية، حتى عين سكرتيراً عسكرياً لرئيس الحكومة، وينسب إليه صياغة "ا ستراتيجية الضاحية"، التي أضحت جزءاً من العقيدة القتالية للجيش الإ سرائيلي، وطبقها الجيش الإسرائيلي في حرب لبنان 2006 ، وغزة 2014 ، لأنه يعتقد أن على الجيش التصرف كحاملة طائرات، وليس كزورق حربي، يعمل بمنهجية ومهنية بعيداً عن العجلة، ويعرف عن آيزنكوت أنه غير منفعل، ومنضبط، وحذر ومحافظ، لكنه ليس خنوعاً، ويتمتع بحس دبلوماسي، وقدرة على المناورة، وتحا شي دخول حقول ألغام سيا سية، واكتساب الأعداء والخصوم داخل الجيش، ولا يتردد بتوجيه الانتقادات لصناع القرار.
من ترجمة عدنان أبو عامر، **استراتيجية الجيش الاسرائيلي** ،اعداد الجيش الاسرائيلي، ترجمات الزيتونة 79، موقع يديعوت أحرونوت ،أيلول ، 2015. ص 64.

[245] ابراهيم عبد الكريم، الاستراتيجية الجديدة للجيش الإسرائيلي: قراءة تحليلية ، **مركز الامارات للدراسات والبحوث الاستراتيجية**،2015/8/16، على الرابط التالي:
http://ecssr.ac.ae/ECSSR/print/ft.jsp?lang=ar&ftId=/FeatureTopic/Ibrahim_Abdel_Karim/FeaturTopic_1893.xml

إستراتيجية "تساهل"، ولأول مرة، على مبدأ الدفاع، إلى جانب المبادئ التقليدية؛ الردع، والإنذار، والحماية، والهجوم، والحرب الوقائية، والإنتصار والحسم.

ترسم الوثيقة خريطة التهديدات التي تواجه" إسرائيل" في بيئتها الجيوسياسية. وحسبما كتب أيزنكوت في مقدمتها: "**ترتكز النظرية التي تم تبنّيها على إدراك تراجع التهديدات التقليدية وغير التقليدية القادمة من الدائرة الأولى (دول الطوق)، مقابل ارتفاع التهديد شبه التقليدي الذي تمثله المنظمات الإرهابية وتهديدات السايبر وغير ذلك** ".[246]

تتأثر صيغة الوثيقة بوضوح بمعرفة أيزنكوت الواسعة والدقيقة بالجبهة الشمالية ، عندما تولى رئاسة قسم العمليات في رئاسة الأركان خلال حرب لبنان الثانية (2006)، وشغل بعدها منصب قائد المنطقة الشمالية لمدة ست سنوات. حيث صاغ أيزنكوت "عقيدة الضاحية الجنوبية"، معقل "حزب الله" في بيروت . وتشمل هذه العقيدة "تسوية المنطقة بالأرض"، عبر تفعيل الضغوط الهائلة على مراكز السلطة والسيطرة والمراكز المدنية، والتشديد على عقيدة "الصدمة والرعب"، ليس فقط في الجبهة الشمالية، وإنّما أيضاً في باقي الجبهات التي يخوض فيها الجيش الحرب ، بما يؤدي إلى تدمير كل المواقع أو التجمعات السكانية التي تطلق منها الصواريخ على" إسرائيل" .

تحّدد الوثيقة في فصل بناء القوة ؛ المبادئ الموجهة لبناء القوة – حماية الحدود في الأوقات العادية – والحماية من التهديد– والمناورة البرية– وإنزال قوات من سلاح المشاة من الجو – وإستخدام قوات خاصة في العمق – وبناء القدرات في مجال السايبر – وتطوير القدرات في مواجهة دول لا توجد معها حدود مشتركة .[247]

---

246 ابراهيم عبد الكريم ، مصدر سبق ذكره .

247 المصدر نفسه .

المبحث الثاني : الخطوات التي أنجزتها "إسرائيل" للسيطرة على الفضاء السيبراني.

تسعى " إسرائيل" دائماً إلى الاحتفاظ بميزة التفوق النوعي على دول المنطقة لضمان أمنها تحت ذريعة الخطر الوجودي ، وقد شهدت العقود الأخيرة العديد من الخطوات الإسرائيلية لإدخال مجال الفضاء السيبراني ضمن أدوات الحرب المستقبلية ، مستخدمة في ذلك تقدمها التكنولوجي وإسهاماتها العالمية في صناعة البرمجيات ونظم الحماية السيبرانية . ويلعب العامل التكنولوجي دوره الوظيفي البارز في الأمن الإسرائيلي ، فهو يشكل أحد أهم مرتكزات الأمن لديها ، حيث ترغب " إسرائيل" في أن تكون حاضنة لغالبية التكنولوجيات والإلكترونيات العسكرية في العالم، وتعمل لأن تكون مصدرًة لهذا العمل الّتقني ، لما لهذا الموضوع من أثر بالغ الأهمية ليس فقط في الدفاع عن أمنها بل ويشكل وسيلة ردع فعالة ضدالدول العربية والأعداء الذين يتربصون بها من جهة ، ومن جهة أخرى هو وسيلة لجني أرباح هائلة تنعكس بالتالي على إقتصادها " المحدودالموارد "، إضافة الى إقامة شبكة علاقات واسعة مع الدول الأخرى (في أوروبا والشرق الأقصى) بغية إشراكها في دعم أمن " إسرائيل" أو ضمان تابعيتها على الأقل . ويضع صانع القرار الإسرائيلي الأبعاد الأيديولوجية والعقدية والعداء المتبادل بين " إسرائيل" ودول المنطقة في الحسبان وخصوصاً أنها ما زالت تعيش هاجساً مزمناً يتعلق بوجودها وضمان استمرارها، وهي تغطي ذلك ، أو تعوّض عنه ، بالمبالغة بالتعويل على استخدام القوّة المفرطة ، والاتكاء على تفوّقها العسكري المطلق ، بالاعتماد على «الجيش الذي لا يقهر»، واحتكار التسلح النووي، وضمانة الولايات المتحدة لأمنها واستمرار تفوّقها في هذه المنطقة . وهذا ما عبّر عنه رئيس وزراء " إسرائيل" السابق بيريز

حينما قال: "أنّ المعلومة أقوى من المدفع " في ترجمة حقيقية لتحّول" إسرائيل" إلى كيانٍ برمجي والإعتماد على تكنولوجيا تتوارى فيه القوة العسكرية خلف التقدم الرقمي ، وتتوازى مع القوى الناعمة، ألا وهي قوة تكنولوجيا المعلومات. [248]

المطلب الأول: التقدم التكنولوجي في " إسرائيل " .

ثمّة من يقول أنّ من يمتلك المعرفة والتكنولوجيا الرقمية ، من شأنه أن يغير وجه العالم الذي نعرفه فهي تمنح ميزات نوعية وأولوية علمية لمن يجيد إستخدام هذه الأدوات التي قد تتسبب في تغيير موازين القوى في المستقبل. ونظراً الى أهمية هذا الموضوع عالمياً وحساسيته أو خصوصيته لدى الجانب الإسرائيلي ، فقد أولته الحكومة أهمية كبرى ، حيث تقدمت "إسرائيل" على العديد من الدول الرائدة عالمياً في هذا المجال ، من بينها الولايات المتحدة الأمريكية، من حيث قدرتها على الإستجابة لحالات الطوارئ السيبرانية طبقاً لتقارير دولية ، وبات الحديث عن إنشاء منظومة دفاعية رقمية على غرار منظومة صواريخ القبة الحديد الأمريكية المضادة للصواريخ على المحيط الهادئ .[249] سوف نتعرض في هذا الفصل الى المستوى التي وصلت اليه "إسرائيل " من خلال المعرفة التكنولوجية في كل الميادين.

1- الميدان الاقتصادي.

تتسّم تكنولوجيات المعلومات والفضاء الكتروني بأهمية إستراتيجية في" إسرائيل" على غرار اقتصادات الدول الأكثر تقدماً في العالم ، ويعتمد الإقتصاد الإسرائيلي إلى حد كبير على الهياكل الاساسيه للفضاء الكتروني. وتعدّ " إسرائيل " أحد قاده العالم في تطوير تكنولوجيا

[248] غسان وليد جلعود، مصدر سبق ذكره ، ص 130.
[249] ربيع محمد يحي، مرجع سبق ذكره ،ص 64.

المعلومات ، وفروعها ، التي تساهم بشكل مباشر وبشكل غير مباشر على النمو الاقتصادي ل "إسرائيل" ، فهي ذات أهميه خاصة. وهي قادره على المنافسة في السوق العالمية (وتصدير جزء كبير من المنتجات إلى الخارج) ، وهي ظاهرة بالغة الاهمية ، لأنّها تشكّل السبيل الوحيد لنمو " إسرائيل" بسرعة وذلك في طريق زيادة الصادرات . ويساهم إقتصاد الإنترنت مساهمة كبيرة في العمالة حيث أنه يستقطب أكاديميين من مختلف مجالات التكنولوجيا . ووفقا لدراسة استقصائية أجرتها الشركة الاستشارية الدولية العملاقة ، ماكينزي [250]، يمكن تقسيم اقتصاد الإنترنت في "إسرائيل" إلى حقلين، حيث يتضمّن الجزء الأكبر ميدان تكنولوجيا المعلومات والاتصالات التكنولوجيا ، ويشمل تطوير وإنتاج وبيع المعدات والبرمجيات والخدمات. أما الجزء الأصغر والمتزايد بسرعة فهو مجال التجارة الكترونيه التي تنطوي على بيع السلع والخدمات على الإنترنت.

فقد ساهم إقتصاد الإنترنت في "إسرائيل" في شكل مباشر في الناتج المحلي بنحو 50 مليار شيكل عام 2009 ؛ أي نحو 6.5 % من إجمالي الناتج المحلي، وهو ما يجعل " إسرائيل" واحدة من إقتصادات الإنترنت الرائدة في العالم. كما أظهر التقرير أن اقتصاد الإنترنت الإسرائيلي سيشهد نمواً بمعدل سنوي يصل إلى 9%؛ أي ضعف معدل النمو الاقتصادي، ومن المتوقع أن يساهم إقتصاد الإنترنت الإسرائيلي عام 2015 بنحو 85 مليار شيكل للدولة، وسوف يشكل نحو 8.5 % من إجمالي الناتج المحلي .[251]

[250] Noa Peleg, "Growing Big, Reaping Small," **Globes**, March 9, 2011.
[251] Shmuel Even and David Siman-Tov, **reference previous seen** ,p.75.

2- **البحث العلمي .**

ثمّة أسباب ومتغيرات كثيرة تقف وراء التطور التكنولوجي الذي وصلت اليه "إسرائيل " ، لعل من أهمها : الموارد البشرية التي اعتمدت على هجرات اليهود والأدمغة من الإتحاد السوفياتي بعد تفككه ، والميزانيات الضخمة والهائلة التي صرفها هذا الكيان في سبيل تحسين هذا القطاع ، إضافة الى السياسة العلمية التي يتبعها في دعمه لكل المشاريع العلمية والتكنولوجية بل لقد أدّى اعتبار تطوير هذا القطاع ضرورة قومية وأمنية أساسية الى جعله برنامجاً يدخل في صميم المناهج التربوية التي تواكب التلاميذ منذ الصغر [252].

ويلعب البحث العلمي دوراً وظيفياً في حماية "إسرائيل" و استمرارها ووجودها ، حيث إن كل مواطن – باستثناء اليهود المتطرفين والعرب– مطلوب منه بعد إكماله التعليم العالي إكمال دورة في الخدمة العسكرية ، وأن أفضل التلاميذ في علوم الحاسوب والرياضيات يتم إلحاقهم بوحدات النخبة الإلكترونية العسكرية منذ أن يبلغوا من العمر 14 عاماً.

لقد تمكّنت "إسرائيل" من الوصول إلى الجيل الرابع لأهم الصناعات الإلكترونية الحساسة وبالتحديد العسكرية منها . بالمقابل تعكس تقارير إستخبارية الصورة السوداوية للوضع العلمي التكنولوجي العربي . فهي ُتنفق سنوياً من موازناتها على البحث العلمي وفي أقل التقديرات أكثر ما ينفقه العرب مجتمعين . وهذا يدل على أن هناك فجوًة كبيرًة في التقدم الإلكتروني والتكنولوجي بين " إسرائيل" والدول المجاورة لها ، يصب في مصلحة " إسرائيل" من دون أدنى شك .[253]

---

[252] عدنان أبو عامر ، "البحث العلمي في إسرائيل وصنا عة القرا ر"، في: **موقع قناة الجزيرة** على شبكة الإنترنيت، 22 يوليو/ تموز 2012 م.على الرابط التالي :
http://www.aljazeera.net/analysis/pages/b8556851-0a25-4d54-b8ed-b85c3a3e35a4#2

[253] خليل حسين، " الصراع الإلكتروني العربي – الإسرائيلي "، في: **موقع مركز دراسات الخليج** (دار الخليج) على شبكة الإنترنيت، 23 كانون الثاني / يناير 2012 م.
http://www.alkhaleej.ae/portal/178a5781-4897-4350-b457-fd919d8fdfcc.aspx

3- الميدان العسكري.

يشكّل الفضاء الالكتروني مجالا حيويا للمجتمع ، وللعلاقة بين الحكومة والمواطنين ، وعلاقات " إسرائيل" مع العالم والأهم من ذلك ، له أهمية كبرى على الأمن القومي ل"إسرائيل" بالنظر الى التهديدات السسيبرانية المتطورة المهددّة لها في مجال تكنولوجيا المعلومات وإمكانية دمج الفضاء الالكتروني في ساحة المعركة الحديثة . ولقد قام الجيش الإسرائيلي بخطوة مهمة في الإعتراف في عام 2009 بالفضاء الالكتروني كفضاء إستراتيجي وعملياتي جديد وبعد ذلك أسس "**هيئة السايبر**" وهي هيئة الأركان للتنسيق والارشاد لأنشطة الفضاء .[254]

وفي شباط/فبراير 2013 ، أعلن الجيش الإسرائيلي أنه أصبح من بين أوائل الجيوش التي تؤسس غرفة حرب رقمية) Digital war room (لإدارة العمليات المتقدمة في مجال حرب الفضاء السيبراني ؛ بهدف تمكين الجيش من العمل بشكل سلس في الفضاء السيبراني وإعطاء صورة لحظية واضحة للتطورات المحيطة ، من خلال التعاون مع مشروع البنية الحكومية لعصر الإنترنت) TEHILA (، ومشروع) E-Government (للخدمات الحكومية الإلكترونية، والسلطة الوطنية لأمن المعلومات التابعة لجهاز الأمن العام (الشاباك). ويعتبر الجيش "غرفة الحرب الرقمية" مركز أعصاب الدولة في عمليات الحماية ، حيث سيكون بمقدوره القيام بعمليات إعتراض وتوجيه وتشغيل في الفضاء السيبراني بالتنسيق مع جميع وحدات الجيش. [255]

[254] Shmuel Even and David Siman-Tov , preface .

[255] ربيع محمد يحي، مرجع سبق ذكره ، ص 70.

4- البنية التحتية والمجتمع المدني .

تمّ إنشاء "هيئة السايبر الوطنية " وهي إضافية وتتفوق على أجهزة الدولة الناشطة مدنياً التي تعمل في هذا المجال ، مثل "السلطة الوطنية لحماية البيانات" ، للشاباك ومشروع " tehila"-تهيلا ".[256]

ولقد أنشئ مركز أمن المعلومات الحكومية الإسرائيليه ، تهيلا ، ومن بين وظائفه متابعة أحداث أمن المعلومات في جميع أنحاء العالم مع إيلاء إهتمام خاص لهجمات الشبكة التي تتعرض لها "إسرائيل "، وذلك للتنسيق بين الهيئات الحكومية من أجل حّل المشاكل الأمنيه وربط الهيئات الحكومية مع الهيئات الخارجية ، وإجراء البحوث في الميدان. ينشر مركز أمن المعلومات تحذيرات للمنظمات في مجال تكنولوجيا المعلومات التي لديها الاتصال بتهيلا أو المصادر الحكومية غير المصنفة . المشروع أيضاً يحافظ على الاتصال مع المصادر الدولية من أجل هزيمة الهجمات المحوسبة .[257]

لقد استطاعت " إسرائيل" إنشاء (فريق الاستجابة للطوارئ الحاسوبية) الذي يشكّل جزء من تهيلا ؛ ويترأسه حاملو الشهادات ، وهو مركز اتصال متاح يعمل للرد على هجمات الشبكة إدارة المخاطر ، إنشاء إجراءات أمان المعلومات ، التحكم بحركه المرور ، والتعامل مع تفشي الفيروسات ، ومنع البريد المزعج والتصيد ، ومكافحه الشبكة للقرصنة وسرقه الهوية ، والحفاظ على خصوصية المعلومات ، وزيادة الوعي عن الأمن . ويتقاسم الفريق أيضاً المعلومات مع مقدمي خدمات الإنترنت والشرطة وقوات الأمن مع تحديثه باستمرار." [258]

---

[256] TEHILA website, www.tehila.gov.il

[257] Israel Government Information Security website, www.cert.gov.il.

[258] Same reference.

ووفقاً لمكتب رئيس الوزراء : " إنّ الغرض الرئيسي من الهيئة هو توسيع القدرات الدفاعية للبلاد لأنظمة البنية التحتية الحيوية من الهجمات السيبرانية الارهابية، التي تنفّذ على حد سواء من قبل الدول الأجنبية والارهابيين .[259]

يشير غابي سيبوني في تقرير أجراه حول الثغرات والعيوب التي يعاني منها النظام الأمني للبنية التحتية ، الى أن السلطة تركز إهتمامها على الشركات المختارة في القطاعات الأساسية العسكرية والسياسية والدفاعية الأمنية تحديداً.. ، وتهمل باقي القطاعات الأخرى ، ولا تولّي إهتماماً كبيراً للمؤسسات والمنظمات المتصلة بالبنية التحتية كالغذاء و والدواء المستحضرات الصيدلانية....، على الرغم من مساهمتها الكبيرة في الانتاج ، والعمالة ، ونسيج الحياة . ونذكر على سبيل المثال المياه: (إن حماية إمدادات المياه والهياكل الاساسية لنوعية المياه في" إسرائيل" لا يؤثر فقط في العمليات في Mekorot "شركة المياه الوطنية الاسرائيليه "، بل على العشرات من موردي المياه الأخرى والجمعيات والشركات المائية وتحلية المياه ومرافق التوصيل والصرف الصحي من مرافق معالجة مياه الفضلات وهكذا دواليك. كما انّ عدداً كبيراً ممّن يقوم بتشغيل هذه المرافق أصحاب المشاريع الخاصة الذين لا يرون تفعيل أليات الحماية كأولوية عليا ، والوضع مماثل في الصناعات الأخرى) .[260]

بناء على ما تقدم ، **تشكل البنية التحتية في "إسرائيل " فرصة غاية في الأهمية (إذا أحسن استغلال عيوبها وثغرها) لمن يتربص بهذا الكيان ويسعى للقضاء عليه.**

[259] شموئيل ايفن ودايفيد بن سيمان ، مرجع سبق ذكره ، ص18،

[260] Gabi Siboni, "Protecting Critical Assets and Infrastructures from Cyber Attacks", **Military and Strategic Affairs 3**, no. 1 (2011): 96, at http://www.inss.org.il/ upload/(FILE)1308129638.pdf.

5-الميدان الأمني والاستخبارات.

تساهم تكنولوجيا المعلومات بشكل مباشر وغير مباشر في الدفاع عن أمن "اسرائيل" [261] ، لأنها تساهم في كسر العزلة عنها، وهي تعتبر من الدول الرائدة عالمياً في عالم الإتصالات وتكنولوجيا المعلومات ، إضافة الى مساهماتها التكنولوجية الفائقة المشهود لها

دولياً في الأمن السيبراني .[262] ففي العام 2014، تصدرت صادرات " إسرائيل" للمنتجات الأمنية الإلكترونية المصممة لحماية الشركات والمصارف والحكومات من "شبكه الإنترنت المظلمة" المتنامية للقراصنة والمحتالين والمتسكعين ، مبلغ 6 مليار دولار ، ويلتقط 8,000,000 نسمة حوالي 10% من السوق العالمية لأمن الفضاء الكتروني ، وتعتبر "إسرائيل " بالفعل واحدة من أكثر الأهداف العالمية للمال الاستثماري .[263]

غير أن الاستخبارات الأمنية الاسرائيلية لها مساهماتها ودورها الوظيفي الأساسي أيضا في حماية هذا الكيان من الخطر الوجودي الذي يحيط به ، مستفيدة بشكل كبير من كل تقنياتها التكنولوجية والمحوسبة في إطار جمع المعلومات وسرقتها ، لذلك تحتّل الأجهزة الأمنية في "إسرائيل" حيّزاً مهماً في مؤسساتها ، ويمكن تقسيم هذه الأجهزة إلى ثلاث أقسام؛ أولها داخلي ويسمى الشاباك Israel internal security ، وثانيها إستخباراتي عسكري ويسمى أمان Military Intelligence Division ، وآخرها خارجي ويسمى الموساد Israeli

[261] http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540rh/pdf/BILLS-112hr1540rh.pdf.

[262] **an interview by Steve Forbes of Forbes Magazine**, with George Gilder,a well known American expert on IT and the economy, February 16, 2011: on website: http://www.forbes.com/2011/02/11/gilder-nanotechnologyfiber optics-intelligent-investing-video.html.

[263] John Reed,Unit 8200: Israel's cyber spy agency, **Financial Times** [London (UK)] 11 July 2015: 16.

external security . [264] حيث تشكل هذه الأجهزة المنظومة الأمنية التي تدير شؤون هذا الكيان والتي تتولاها قطاعات مختلفة من الجيش الإسرائيلي .

5-1- الموساد.

تأسس"الموساد" في 13 ديسمبر من عام 1949، ليقوم بجمع المعلومات، والدراسات الاستخباراتية، وبتنفيذ العمليات السرية خارج حدود" إسرائيل". ويعمل "الموساد" بصفته مؤسسة رسمية بتوجيهات من قادة " إسرائيل"، وفقاً للمقتضيات الإستخباراتية والعملية المتغيّرة، مع مراعاة الكتمان والسرية في أداء عمله. وتقع على عاتق "الموساد" العديد من المهام التي تندرج ضمن مجالات متنوعة ، كالعلاقات السرية مع أطراف أخرى، وقضايا الأسرى والمفقودين ، والتقنيات والأبحاث، وعمليات الاغتيال . يعد "الموساد" أحد المؤسسات المدنية في "إسرائيل"، ولا يحظى منتسبو "الموساد" برتب عسكرية ؛ إلا أن جميع الموظفين في جهاز "الموساد" قد خدموا في الجيش الإسرائيلي، وأغلبهم من الضباط .[265]

5-2- جهاز الأمن العام "الشاباك" (الشين بيت) الإسرائيلي.

جهاز "الشاباك" هو جهاز الأمن الداخلي في "إسرائيل" ، يخضع مباشرة لرئيس الحكومة، يعدّ "الشاباك" من أصغر الأجهزة الاستخبارية، ويتكون من بضعة آلاف من العناصر، وعلى الرغم من ذلك إلا أنه يعتبر أكثر الأجهزة الأمنية حضوراً وتأثيراً على عملية صنع القرار السياسي والعسكري، ولا يمكن مقارنة تأثيره الطاغي بتأثير أي جهاز أمني آخر في " إسرائيل" .[266]

---

[264] وليد جلعود، **مرجع سبق ذكره** ، ص141.
[265] الأجهزة الأمنية الاسرائيلية،مركز المعلومات الوطني الفلسطيني- وفا، http://info.wafa.ps/atemplate.aspx?id=8024
[266] المصدر نفسه.

3-5- **الاستخبارات العسكرية الإسرائيلية "أمان".**

تعّد "أمان" هيئة عسكرية تقوم بتقديم خدمات وطنية إستخباراتية، وصلاحية وجودها الأساسية تتمثل في مساعدة الجيش الإسرائيلي في تنفيذ مهامه ، إلا أنه بفضل قدراته الكبيرة في مجال جمع المعلومات، فإنه يقوم بتنفيذ مهام وطنية خارج إطار الجيش، لمساعدة المستويين السياسي والأمني في "إسرائيل" للقيام بمهامهما.

يتلخص دور الإستخبارات العسكرية في عرض معلومات إستخباراتية على أصحاب القرار، سواء على المستوى السياسي أو العسكري، بغرض مساعدتهم للقيام بمهامهم المختلفة . ومن الناحية التنظيمية ، يتبع جهاز "أمان" مباشرة لرئيس الأركان، المؤتمر بأمر الحكومة، والتابع بدوره لوزير الدفاع . تعد هذه الوحدة أو الشعبة إحدى الأجهزة الأمنية المهّمة والسريّة في "إسرائيل" ، والتي تختص في القضايا المعلوماتية والّتقنية ومن أهم مهامها:

أ- تطوير المنظومات والوسائل التكنولوجية.

ب- تجهيز تقنيات مهنية لأجهزة الاستخبارات الأخرى بالجيش الإسرائيلي.

ج- دعم مجال الأمن المعلوماتي في الجيش الإسرائيلي.[267]

المطلب الثاني : الأجهزة الاستخباراتية وجمع المعلومات.

نظراً الى الهاجس الأمني الاستخباراتي الذي يسيطر على المناخ العام في "اسرائيل "، فإنّ السياسة الذي يتبعها هذا الكيان في العمليات الأمنية تختلف عن غيرها من الدول ، ولذلك فإن العمليات الأمنية ضد الخصوم في البيئة الإستراتيجية الإلكترونية تحتل أولوية الإهتمامات

[267] أمان .. رأس الحربة في أجهزة المخابرات الإسرائيلية ، 'group73historians.com/.../531ugn hgvhf -أعرف-عدوك---المخابرات-الاسرائيلي، أعرف عدوك – المخابرات الاسرائيليه منذ النشأه وحتي الان - **المجموعة 73 مؤرخين.**

وتدور في فلكها كل المؤسسات ويتم على أساسها صنع القرارات ، ولذلك نجد تعدديّة في الأجهزة الإستخباراتية الأمنية الإسرائيلية الاّ أنّ أهمها على الاطلاق هي "أمان".

ويمكن تصنيف الأنشطة الإستخباراتية في مجال الفضاء السيبراني ضمن ثلاث عناوين : أولها، جمع معلومات حول قدرات العدو ونياته ، سواء في أوقات الحرب أو الأوقات الأخرى؛ بهدف وضع تقديرات وبلورة إستراتيجيات ومن ثم اتخاذ القرارات المناسبة وبناء القوة العسكرية القتالية. وثانيها، التجسس الصناعي؛ بهدف سرقة معلومات حول التكنولوجيا والأعمال. وثالثها يستهدف جمع ثروات سيبرانية تخص العدو، مثل سرقة البرامج وقواعد البيانات أو الملكيات الفكرية .[268]

فبالنسبة إلى " إسرائيل" تحتّل " أمان " الموقع الأول والأهم بين أجهزة الأمن الإسرائيلية؛ للدور الكبير الذي تلعبه في بلورة القرار السياسي فيها، عبر ما يسمى " **مسألة التقدير القومي**" الذي يضع الرؤية المطلوبة للسياسات الإسرائيلية بناء على المعلومات التي تقدمها " أمان" .[269] وهو المسؤول عن مجالات عدّة أهمها:(التنصت) و(التقاط الصور الجوية)، و(البحث والمهام الخاصة).[270]

وهو يتفرع الى وحدات عدّة والتي تعدّ من وحدات النخبة نذكر منها:

1 –الوحدة8200. "هي ما يعادل وكالة الأمن القومي الامريكية وأكبر وحدة عسكرية في قوات الدفاع الاسرائيلي"[271]، وهي أشهر وحدات النخبة الخاصة التي شكّلها الجيش الإسرائيلي

---

[268] ربيع محمد يحي، مرجع سبق ذكره ، ص72

[269] الأجهزة الأمنية الاسرائيلية،**مركز المعلومات الوطني الفلسطيني- وفا،** http://info.wafa.ps/atemplate.aspx?id=8024

[270] أعرف عدوك – المخابرات الاسرائيليه منذ النشأه وحتي الان - **المجموعة 73 مؤرخين**.

[271] John Reed, Unit 8200: Israel's cyber spy agency**, Financial Times** [London (UK)] 11 July 2015: 16.

وتشكل احد أهم نقاط التسلل الإسرائيلي إلى عالم التكنولوجيا الرفيعة والمتطورة hight .tech[272]

تهتم وتتشغل الوحدة "8200 "بجمع المعلومات الإلكترونية واللاسلكية وانشأ مؤسسوها الكثير من الأقسام والوحدات الالكترونية الرديفة العاملة في مجال حماية المعلومات وشبكات الاتصال.

2- الوحدة 9900.

وتشمل الوحدة "9900 " " العوالم الجغرافية " و" الضوئية " القائمة في شعبة الاستخبارات التابعة للجيش الإسرائيلي " أمان" لذلك تضم أقسام متخصصة عدّة في مجال عملها وتعمل أيضا في مجال خلق حالة من " تراكم التكنولوجيا". وتتكون الوحدة "9900 " من وحدات عدة أو أقسام :

2-1- الوحدة الأولى وتتضمن " مركز المعلومات" المتخصص بدراسة وتحليل وسبر غور المعلومات وجمع المعلومات الميدانية.

2-2- الوحدة الثانية فهي قائمة ضمن قوام الوحدة الأم "9900 " فهي وحدة " الخرائط وتحليل المعلومات" والمتخصصة برسم الخرائط الخاصة بالعمليات التنفيذية وبقية احتياجات الجيش .

2-3- الوحدة الثالثة تعمل ضمن هذه المنظومة وتدعى وحدة" الأقمار الاصطناعية " المسؤولة عن أقمار التجسس الاصطناعية وتستخدم إمكانيات ووظائف هذه الأقمار وتسخرها

[272] تعرف على وحدة 9900 الالكترونية الإسرائيلية ، **وكالة معا**،2015/4/1.على الرابط التالي:
http://www.maannews.net/Content.aspx?ID=769797

في خدمة الأقسام والجهات التي تحتاج معلمات فورية تبدأ من لحظة إطلاق النار أو الصواريخ .[273]

3- متسفان.

يطلق عليها إسم "وحدة التحكم والسيطرة والإدارة " ، وهي مسؤولة عن تطوير القدرات التكنولوجية ذات الطابع الرقمي، وتعمل على تطبيقها في الجهد الحربي الواسع والمحدود للجيش. وحسب "معاريف"، فإن "متسفان" التي تتبع قيادة "الحوسبة" في الجيش، تلعب "دوراً مركزياً في تحديد وصياغة بنوك الأهداف التي يعدها الجيش لدى التخطيط لحروبه القادمة ضد الأعداء"، علاوة على أنه يتم توظيف تقنياتها وبرمجياتها في تحسين قدرة الجيش على ضرب أهدافه. كما تقوم الوحدة بتأهيل وحدات الجيش والاستخبارات الإسرائيلية المتعلقة بالجهد الإلكتروني، فيتردد عناصر أسلحة الجو والبحرية والمشاة والاستخبارات على مقر الوحدة لتلقي التأهيل. أما بالنسبة الى آلية توظيفها في الجهد الميداني الحربي فيتمثل بالتالي " تحديد شعبة الاستخبارات العسكرية (أمان) هدفاً ما يتوجب ضربه أو جمع استخبارات عنه، يتم وضع "متسفان" في صورة الأمر حتى توفر التقنية الرقمية التي تسهل على سلاح الطيران تنفيذ المهمة، لأن التقنيات التي توفرها الوحدة تساعد سلاح الطيران على اختيار حجم الصاروخ أوالقذيفة المناسبة لضرب الهدف".[274]

---

[273] المصدر نفسه.

[274] صالح النعامي،**"متسفان"**... ذراع الحرب الإلكترونية لإسرائيل ،**العربي الجديد**،على الرابط التالي:
https://www.alaraby.co.uk/medianews/2016/10/26/%D9%85-1.

4- الوحدة 504:

أو وحدة "العملاء والأسرى"، التابعة لشعبة الاستخبارات العسكرية "أمان"، وهي الوحدة السؤولة عن تجنيد العملاء . ولما كان "الموساد" مسؤولاً عن جمع المعلومات الاستخبارية عن جميع الأهداف التي تعني إسرائيل في العالم، فإن "وحدة 504" تعنى بجمع المعلومات الاستخبارية وتجنيد العملاء في المناطق العربية الحدودية المتاخمة لفلسطين المحتلة، مثل جنوب لبنان، والجولان السوري، والأردن، وسيناء المصرية، إلى جانب بعض المناطق في الضفة الغربية وقطاع غزة .[275]

[275] صالح النعامي، **العربي الجديد** : حرب عقول استخباريّة بين إسرائيل و"حزب الله" ، على الرابط التالي: https://www.alaraby.co.uk/politics/2015/1/4

إستنتاج الفصل الأول

سعت "إسرائيل" في شكل دائم إلى أن تكون في مقدمة الدول الرائدة تكنولوجياّ في الحماية السيبرانية في العالم . وكانت المسؤولية عن الدفاع عن شبكات الاتصال والحواسيب ملقاة على "الشاباك".ُ تعد الأجهزة الأمنية والإستخباراتية المعلوماتية الإسرائيلية السالفة الذكر البؤرة الأولى في تدفق المعلومات نحو " إسرائيل" من مختلف إرجاء العالم . فهي بمثابة العين التي ترى فيها "إسرائيل " ما يجري من حولها من تطوراتٍ وتغيراتٍ سياسية وإقتصادية وإجتماعية وّتقنية، والنواة الأولية والتأسيسية في الإعداد والتجهيز المسبق لدخول" إسرائيل" ساحة الحرب الإلكترونية القائمة في الفضاء الإلكتروني بشكلٍ عام، والصراع العربي الإسرائيلي على وجه التحديد، والذي أخذ منعطفاً جديدًا منذ تحوله إلى استخدام الأسلحة الرقمية والإلكترونية .

هناك ثلاثة إستخدامات أساسية لحرب السايبر. الأول استخدام دفاعي والآخران هجوميان. الدفاعي يختص في مجال أمن المعلومات – منع العدو من اختراق الحواسيب في "إسرائيل" في شكل عام، وحواسيب المؤسسات الحكومية في شكل خاص سواء كانت عسكرية أو أمنية أو مدنية. دفاع السايبر موجه لحماية الحواسيب والاتصالات بين الأجهزة الاستخبارية في الجيش والمواقع الاستراتيجية والحساسة: محطات الطاقة والمفاعلات النووية والمطارات والمستشفيات وخزانات المياه وحقول النفط والغاز والمؤسسات المالية وما أشبه. إن اختراق هذه الحواسيب قد يؤدي الى كوارث كبيرة وموت اشخاص كثيرين. في مجال الهجوم يرتبط السايبر عادة بالتجسس – من خلاله يتم الدخول في شكل سري الى حواسيب الأعداء وجمع المعلومات. الاستخدام الثاني الأكثر دقة وأكثر خطراً والذي لا يعرف الجمهور عنه هو الدخول

إلى الحواسيب وزرع فيروس فيها لاعطاء أوامر تلحق الضرر بها وبالأدوات التي تشغلها هذه الحواسيب. [276]

وتعتبر تكنولوجيا المعلومات والاتصالات في الجيش اليوم احدى اهم اذرع الجيش الاسرائيلي، حيث تم مؤخرا ربط كل الاذرع القتالية برا وجوا وبحرا بشبكة واحدة تمنح المقاتل او الجندي الاخير في الحلقات، الحصول على المعلومة الامنية والاستخباراتية والعملية في لحظة حصولها لكي يتخذ قراره الاصح عند الحاجة.

وفي مجال استثمار الحماية الأمنية من الناحية الاقتصادية تعمل "اسرائيل على توظيف الجغرافية السياسية ودمجها مع التكنولوجيا المتطورة في عالم السايبر، في محاولة لها لتحويل صحراء النقب أو "وادي السيليكون"، الى مركز لتوريد أحدث الأنظمة المعلوماتية والرقمية ووسائل حماية الأمن السيبراني للعالم . وهذا ما عبّر عنه نتنياهو بوضوح حينما قال : "ان السايبر سوف يؤدي الى تغيير طبيعة صحراء النقب ".

"Cyber, recently, is "changing the face of the Negev""[277].

[276] يوسي ميلمان- معاريف 2017/1/6،**عكا للشؤون الاسرائيلية،**

[277] John Reed, Unit 8200: Israel's cyber spy agency, **Financial Times** [London (UK)] 11 July 2015: 16.

الفصل الثاني : الإستراتيجية التي إعتمدها حزب الله .

برز "حزب الله " كلاعب أساسي في الصراع بين "إسرائيل "وحركات المقاومة ، وباعتراف الساسة في "إسرائيل" وتصريحاتهم المستمّرة بأن الخطر المركزي والأساسي الذي يهددهم هو حزب الله . وكان لحرب تموز 2006 أثرها البارز في تعزيز هذة النظرية وفي الإضاءة على مكامن الضعف في الكيان العبري وتسليط الضوء على القدرات الهائلة التي وصل اليها الحزب في ميدان الحروب الالكترونية وأمن المعلومات . ومن المعلوم أن كل من الطرفان أي " إسرائيل" والمقاومة في حزب الله يتربص بالآخر ويسعى جاهداً الى امتلاك كل الوسائل التي من شأنها أن تحقق له النصر الدامغ وذلك عبر امتلاك وسائل القوة العسكرية المناسبة في الميدان، ودمجها مع المعلومات الإستخباراتية الدقيقة لتحقيق إصابات مباشرة .

المبحث الأول: إستراتيجية "حزب الله" في مقارعة "إسرائيل".

إنّ مسألة مقارعة "إسرائيل " من الأسس الأساسية والثابتة في الميثاق المؤسس لعقيدة الحزب منذ نشأته عام 1982، حيث شكّلت محاربة " إسرائيل" ودحرها من الأراضي اللبنانية ، النواة التي قام عليها هذا التنظيم . ومن المعلوم للجميع أن البداية كانت بوسائل تقليدية وبدائية للغاية لكنها استفادت من ثلاث أمور أساسية : أولها منظمة التحرير الفلسطينية التي كان مقرّها لبنان (ورفدت المقاومة بالمقاتلين المتدربين على يديها) ، وثانيها الدعم المالي والمعنوي من الجمهورية الاسلامية في إيران بحكم العامل المذهبي (الشيعي) والديني (المسجد الأقصى كقبلة للمسلمين). كما استفادت من أيديولوجية سوريا العروبية في المطالبة باسترجاع فلسطين. وتطورت الى الشكل الذي أمست عليه ، وأدّت إلى دحر الاحتلال الإسرائيلي بطريقة مهينة لسمعته ، وكانت حرب تموز 2006، بمثابة الهزيمة المدوّية الشنعاء والتي أطاحت

سمعة "اسرائيل" ودفعتها الى إعادة تقويم حساباتها والوقوف مليا على كل الجوانب وملء الثغر استعدادا للحرب القادمة . ومن أهم أسباب تطوّرها أنها كانت أمام عدو ذكي ومتطور وهذا شكّل دافعاً مهماً في سعيها الدائم الى تطوير أسلحتها وتقنياتها وجمع المعلومات والمناورة بالطريقة التي تسمح لها باحراز النصر حتى نستطيع معرفة مدى قدرة وتطوّر الحزب في مجال الحروب الالكترونية ، لا بدّ أولا من التطرّق الى الاستراتيجية الأمنية التي يعتمدها الحزب في حروبه سعياً مناً إلى فهم طبيعته والعقيدة التي يتبنّاها .

المطلب الأول: الإستراتيجية الأمنية .

إنّ عملية البحث عن العناصر والمركبات التي تتألف منها المنظومة الأمنية والعسكرية لحزب الله هو أمر غاية في الصعوبة نظراً الى عدم وجود نصوص ، أو عدم توافر مدونات ووثائق مكتوبة ، فهو حزب لا يحظى بدعم كامل من قبل كل أطياف الشعب اللبناني بل يعتمد على جمهوره الخاص ، نظراً الى الإختلافات الطائفية التي تعمّ الوضع في لبنان "وإن كان قد أخذ بالتوسع فيما بعد " وهو يحظى أيضا بعناية خاصة من قبل إيران ، نظراً الى العامل الديني الذي تمُثله في قيادة المرجعية الشيعية ورعاية شؤونها . يعتمّد حزب الله على أسس وقواعد ثابتة في صياغة عقيدته القتالية ، خصوصاً أنه تنظيم خاص ولا يمتلك مقدرات الدول كما الحال في " إسرائيل" . فالحديث عن قدرات الحزب وتحصيناته ونسبة التقدم الحاصل عليه في التكنولوجيا والمعلوماتية القتالية التي حصل عليها هو من المحرمات والمحظورات لأنّ حزب الله يعتمد على السرية والكتمان والتعتيم المطبق والذي أثبت فاعلية في عدم إعطاء مجال ل"إسرائيل" لجمع المعلومات أو لتحديد بنك الأهداف . ونظراً لعدم توافر بيانات أو مدونات محسوسة وملموسة ، ولكننا سوف نستنتج بعض مكونات هذه

الاستراتيجية من خلال متابعة مجريات حرب تموز وتحليلها ، التي سوف نستشرف من خلالها سبب نجاحه والتكنولوجيا التي يمتلكها والأسس التي اعتمد عليها ألا وهي الغموض البنّاء والمفاجآت، الحرب النفسية بقيادة السيد نصرالله وحرب المعلومات وسير المعارك .

1- التعتيم والسرية والغموض البنّاء .

وهي إستراتيجية فاعلة ومؤثرة في إدارة الصراعات والحروب ، على أشكالها المختلفة الدبلوماسية والأمنية ، وقد تبنتّها العديد من الدول من ضمنهم الولايات المتحدة الاميركية و"إسرائيل" (وخصوصا في نهاية التسعينات خلال محادثات أوسلو) ، بقصد تضليل الخصم إخفاء حقيقة النيّات ، امتصاص الجهود، تحسين الصورة وتجميل العيوب الظاهرة في المواقف والسياسات، وإرباك الخصم وتشويش خياراته .[278]ويمكن رؤية آثارها و نتائجها في الكمّ الكبير من المفاجآت (في مجالات عدّة : المعارك البرية والبحرية والجوية إضافة الى المستوى المعلوماتي والأمني العالي التي اعترف بها قادة العدو) التي مني بها الجانب الإسرائيلي .

2- الحرب النفسية والاعلامية والقيادة الحكيمة .

برع حزب الله في قيادة الحرب النفسية عن طريق الأمين العام لحزب الله (أب الحرب النفسية)[279]، فإضافة الى قدرته الفاعلة والمؤثرة في إدارة سير المعارك والتلاعب بالآخر وإدارة الحرب النفسية والاعلامية ضد العدو بجدارة قلّ نظيرها ، وممارسة سياسة الردع بحسب ما تقتضيه المناسبة ،[280] وتعدّ خطاباته التي ألقاها في حرب تموز2006 بمثابة الحرب

---

278 يوسف نصرالله ، الحرب **النفسية قراءات في استراتيجيات حزب الله** ، دار الفارابي ، بيروت ، ط1، 2012، ص247.

279 وصف أطلقه الخبير الاسرائيلي في علم النفس السياسي الدكتور أودي ليبل على السيد حسن نصرالله ، وذلك في اطار مقاربة أوردتها صحيفة معاريف، الأول من شباط من العام 2007.

280 عقيدة بن غوريون (اذا قصفتم الضاحية سنقصف تل أبيب ومطار بن غوريون) ، خزانات الأمونيا في حيفا والقنبلة النووية التي يمتلكها حزب الله، واخيرا تهديده بان الحرب المقبلة سوف تكون مفتوحة أمام جميع حلفاء المقاومة من سلاح وتقنيات وقوات مسلحة ومفاعل ديمونا ...

النفسية والاعلامية التي مهدّت مسبقاً إلى تحقيق النصر وأدّت الى قلب المعادلة ، وكانت اللحظة التي أعلن فيها عن بدء مفاجأت حرب تموز ، وتحديداً بعد استهداف البارجة ساعر 5 القشة التي قصمت ظهر البعير وغيّرت مجريات الأمور باعتراف الباحث الاسرائيلي د. ليفيتان ،[281] بل وأصبحت خطاباته تدرّس في الجامعات الاسرائيلية أيضاً .

وكان لتأثير الكاريزما والمصداقية التي يمتلكها الأمين العام لحزب الله السيد حسن نصرالله دوراً بارزاً وأساسياً ومفصلياً في قيادة الحرب النفسية والاعلامية ، حيث نال ثقة الجمهور الإسرائيلي و كان محط انتظار المحللين السياسيين الاسرائيليين والجمهور من الطرفين ، بحسب استطلاع للرأي العام الذي أجراه الدكتور أودي ليفيل [282] ، حول الشخص الأكثر مصداقية بين المتحدثين السياسيين الاسرائيليين . " كما تمكن نصرالله من أن يكسب صفة الرجل الصادق ، الذي ثمّة تأثير كبير جداً لكلامه على حياة مئات الاف الاسرائيليين وعلى دولة "إسرائيل" كلها" [283] . والسبب أن نصرالله كان يوّفر للمشاهد ثلاثة أمور أساسية وهي صدق المعلومات واليقين وحالة الترقب والانتظار ، ممّا أجبر المحللين السياسيين والعسكريين في اسرائيل والاعلاميين والمتابعين للحرب على الاستماع والانصات له روحاً وجسداً لمتابعة وفهم الحرب [284]. وقد أقرّ بذلك شمعون بيريز في إعترافاته أمام لجنة " فينوغراد"حينما قال " أعتقد أنّه كان هناك سقوط نفسي كبيرجداً، والسبب هو أنّ حزب الله تألّق بخطيب لا يفتقر الى الكفاءة (السيد حسن نصر الله) [285].

---

[281] زهير اندراوس، خطابات نصر الله تُدرّس بالجامعات الإسرائيليّة ، **رأي اليوم** ، على الرابط التالي : HASAN NASRULLAH 03.07.17.jpg555 نقلا عن صحيفة معاريف(العبرية)

[282] عبد الحفيظ زهير جعوان، **تأثير خطابات حسن نصرالله على نتائج معركة تموز 2006**،جامعة بيرزيت، 2009،ص 134. على الرابط التالي:thesis.mandumah.com/Record/211438

[283] محمد بدير، نصرالله يتكلم ، **موقع صحيفة الأخبار الالكتروني** :http://www.al-akhbar.com/ar/node/40216

[284] عبد الحفيظ زهير جعوان، مرجع سبق ذكره ،ص 134.

[285] وكان شمعون بيريز قد أقرّبشهادته أمام لجنة فينوغراد بتفوق حزب الله في ميدان الحرب النفسية (أنظر تقرير فينوغراد). يوسف نصرالله،مرجع سبق ذكره ،ص263.

أما بالنسبة للاعلام لطالما كانت قناة المنار أداة البروباغندا الأولى في يد حزب الله وكان توسيع نطاق تغطية قناة المنار جزءاً مفتاحياً من دفاعاته ؛ فقد أصبح من الممكن لها حالياً البث إلى "إسرائيل "وغالبية العالم العربي.

3- سياسة القوة والردع .

لا يتوانى الحزب في أي مناسبة عن تهديد الجانب الاسرائيلي وتذكيره بمفاتيح القوة التي يمتلكها ، وتشكل خطابات السيد نصرالله أهم أدوات ممارسة هذا الترهيب والحرب النفسية والاعلامية ، وتلقى دوماً إنصاتاً ومتابعة من قبل المحلّلين السياسين حيث يتّم إرسال رسائل يتّم مناقشتها أمام شاشات التلفزيون وفي الجرائد ، كما يتم إعداد البحوث والدراسات حولها . وهي وسيلة فعالة لارساء معادلات دفاعية . وعقيدة حزب الله هي عقيدة تبادلية هدفها ضمان الردع . يطلقها نصرالله في مناسباته الحاشدة كالتي أطلقها في آب /2009 (اذا ضربتم بيروت فسوف نهاجم تل أبيب) ، وأخرى التي ألقاها في 2010/2/16، (اذا ضربتم الضاحية فسنضرب تل أبيب، واذا ضربتم مطار الشهيد رفيق الحريري في بيروت فسنضرب مطار بن غوريون في تل أبيب ، وإذا ضربتم موائننا فسنقصف موائنكم وإذا ضربتم مصافي النفط فسنقصف مصافي النفط عندكم) . ف"إسرائيل" تعرف حق المعرفة **أن الحرب مع حزب الله ليست نزهة.**

المطلب الثاني :القدرات التكنولوجية و الإلكترونية التي يمتلكها حزب الله .

تعتمد قيادة الحزب جانب الغموض البنّاء في التصريح عن إمكاناتها العسكرية والأمنية والإستخباراتية في مجال الإتصالات والمعلوماتية ، وذلك حرصاً منها على فعالية إرباك العدو كجزء من إستراتيجيتها العسكرية الثابتة لإحراز النصر الحاسم . ولكن من خلال متابعتنا

لمسيرة المقاومة سوف نرصد تباعاً العمليات الأمنية التي أجرتها مع مواكبة ومتابعة دقيقة لخطابات السيد نصرالله ، لمحاولة معرفة بعض القدرات التي تمتلكها وتسليط الضوء على التطور المعلوماتي التي وصلت اليه في مجال الحروب الالكترونية من خلال الأحداث والعمليات التالية :

1- عملية أنصارية .

هي عملية أمنية معقدة حملت اسم" قصيدة الصفصاف" ، نفذتّها وحدة الكوموندوس في سلاح البحرية الاسرائيلية "شييطت-13"[286] ، في الخامس من أيلول من العام 1997، بهدف اعتقال أحد كوادر المقاومة ، وأدّت الى مقتل عدد كبير من جنود العدو وقد بقيت أحداث هذة العملية من الأسرار الاستخباراتية التي أطبق عليها حزب الله ، الى أن كشف السيد حسن نصرالله في مؤتمر صحافي عقد في التاسع من اب من العام 2010، **عن سر اختراق المقاومة للبنية العسكرية الجوية الإسرائيلية ، حيث تمكن من التقاط بث طائرة ال(أم. كا).**[287] **و تمكن من التقاط بث صور طائرة الاستطلاع الإسرائيلية التي ترسلها إلى غرفة عمليات العدو.**[288]

ممّا يعني أنّ المقاومة منذ العام 1997 كانت قادرة على التقاط بثّ الطائرات الإسراثيلية رغم قدراتها المتواضعة كتنظيم سياسي في لبنان وكجزء من أدوات الحرب الإلكترونية .

---

[286]من الوحدات النخبوية في طليعة وحدات الكوماندوس البحري ، وتستحوذ على عناية الاسرائيلين وفخرهم .وتمتاز بالكفاءة والقدرة على المناورة والتسلل والأنسحاب ...

[287] يوسف نصرالله ، مرجع سبق ذكره ، ص216.

[288] السيد حسن نصرالله يكشف صوراً ووثائق تؤكد تورط اسرائيل باغتيال ...

www.alarab.com/Article/320186 قدم نصر الله عرضا استمر لأكثر من ساعتين ونصف وشمل مشاهد ولقطات فيديو عديدة لما قال عنه تصويرا من قبل طائرات استطلاع إسرائيلية للطرقات والمسارات التي كان يسلكها موكب الحريري وشخصيات لبنانية أخرى، بالإضافة إلى أماكن سكناهم وتواجدهم في أمكنة وأزمنة مختلفة ومن زوايا وجهات متنوعة.
أماكن تواجد الحريري وركزت اللقطات على تصوير قصور الحريري في قريطم واستراحته في منطقة فقرا الاصطيافية، بالإضافة إلى قصر الحكومة في بيروت ومقر سكن أفراد أسرة الحريري في صيدا، ومنطقة فندق سان جورج التي وقع فيها حادث اغتيال الحريري.

2- عملية اغتيال الشهيد الحريري.

أطلّ الأمين العام لحزب الله السيد نصرالله في مؤتمر صحافي لإلقاء الضوء حول إمكان تورط "إسرائيل" أو صلتها في عملية اغتيال الرئيس الحريري ، وتمّ عرض فيديوهات حول بعض العملاء وتورطهم في التجسس وجمع المعلومات لحساب " إسرائيل" . كما أشار نصرالله إلى قدرة العدو في مجال الإتصالات ، ومدى سيطرته الفنية الواسعة والتي تمكنّه من تحديد حركة ومكان أي شخص يريد استهدافه .

قدّم نصر الله عرضا استمر لأكثر من ساعتين ونصف وشمل مشاهد ولقطات فيديو عديدة لما قال عنه تصويراً من قبل طائرات إستطلاع إسرائيلية للطرقات والمسارات التي كان يسلكها موكب الحريري وشخصيات لبنانية أخرى، إلى أماكن سكنهم وتواجدهم في أمكنة وأزمنة مختلفة ومن زوايا وجهات متنوعة . وركزت اللقطات على تصوير قصور الحريري في قريطم واستراحته في منطقة فقرا الاصطيافية ، إضافة إلى قصر الحكومة في بيروت ومقر سكن أفراد أسرة الحريري في صيدا، ومنطقة فندق سان جورج التي وقع فيها حادث اغتيال الحريري.[289]

كما أوضح مارصدته الأجهزة التابعة للمقاومة للطائرة الإستخباراتية الإسرائيلية التي استمّرت من الصباح الباكر ، بالإضافة إلى ما رصدته في عملية اغتيال الشهيد الحاج علي ديب قبل عامين وللرصد في عملية اغتيال الشهيد محمود المجذوب .[290]

---

[289] محمد عبدالله ، النص الكامل للمؤتمر الصحافي للسيد نصرالله: قرائن ومعطيات..**موقع الخيام** قناة المنار 10\8\2010
http://khiyam.com/news/article.php?articleID=9730
http://www.rtv.gov.sy/index.php?p=13&id=63266

[290] السيد حسن نصرالله يكشف صوراً ووثائق تؤكد تورط اسرائيل باغتيال ...**موقع العرب**
www.alarab.com/Article/320186

وهذا يدّل على أنّ المقاومة تمارس عملها في الرصد وجمع المعلومات الإستخباراتية كما يفعل العدو ، وهي تتّربص بالعدو كما يتربص بها، و تسعى جاهدة لتحليل ما تجمعه لاستخدامها في مجال الصراع مع الكيان الصهيوني، وتكوين بنك للأهداف خاص بها وتحيطه بهالة من السريّة لضمان فعاليته .

3-**مرصاد-1.**

في نوفمبر (تشرين الثاني) 2004 ، أطلق حزب الله طائرة مرصاد -1،والتي حلقت حينها فوق العديد من المستعمرات الإسرائيلية وصولا إلى مستعمرة نهاريا الساحلية ثم عادت إلى قاعدتها بسلام. وكان تلفزيون المنار اذاع النبأ، وقال "ان الطائرة حلقت فوق مستوطنات الاحتلال وعادت الى قواعدها بسلام". اضاف ان "طائرة المرصاد حلقت فوق ثماني عشرة مستوطنة اضافة الى مدينتي عكا ونهاريا".[291] وقد وفرّت مرصاد-1لحزب الله قاعدة بيانات واسعة عن الشمال الفلسطيني،حيث المستعمرات والمستوطنات والمدن الاسرائيلية،ومعرفة أدق الاسرار الطبوغرافية ، والتي استفاد منها الحزب في حرب تموز 2006 لضرب البنى التحتية والمنشآت المدنية .[292] وقد أكدّ نصرالله أنها "من صنع مهندسي المقاومة الاسلامية ، وأنها طائرة استطلاع كاملة الأوصاف والطاقات والقدرات من أنواع التكنولوجيا المتوافرة التي يمكن شراؤها من المعارض".[293]

---

[291] **Saida City Net** - "مرصاد 1" تحلّق فوق عكا و18 مستوطنة /saidacity.net/news/2783

[292] يوسف نصرالله ، مرجع سبق ذكره ، ص 273.

[293] من خطاب الأمين العام لحزب الله خلال مراسم الاحتفال السنوي الذي أقامه الحزب بمناسبة يوم الشهيد في الحادي عشر من شهر تشرين الثاني/نوفمبر من العام 2004،في الضاحية الجنوبية لبيروت.

وتعدّ الطائرات بدون طيار من أهم الاسلحة الإلكترونية التي تعتمد على المعرفة المعلوماتية في مجال اللاسلكي وفي إطار عمل الردارات .إضافة الى أنها صنّعت من قبل وحدة الهندسة في المقاومة .

4-طائرة أيوب.

بعد 9 سنوات من عملية مرصاد -1، وفي سياق الرد الطبيعي على خرق العدو الصهيوني الدائم والمتكرر للأجواء اللبنانية كلما شاء وأراد ، أعلن السيد نصرالله عن الإنجاز النوعي والجديد للمقاومة الإسلامية في لبنان، عبر إرسال طائرة «أيوب»،التي اخترقت الأجواء الاسرائيلية ، وتعتبر "أيوب» أكثر الطائرات الاستطلاعية تطوراً لدى الحزب، وقد اتفق على تسميتها «أيوب» على اسم «الشهيد حسين أيوب» .

ومن مميزاتها قدرتها على القيام بتصوير آني، أي إرسال الصور مباشرة فور التقاطها إلى مركز التحكم ، كما أنها تستطيع تحميل المتفجرات ، ونقل عن الخبير الاستراتيجي أمين حطيط " ما يميز (أيوب) أنها قادرة على الطيران ما بين 1000 و1500 كم، كما أنها تفرض (العمى الراداري) أي تستطيع التملص من الرادارات، فقد تمكنت من خرق 7 منظومات من المراقبة الرادارية بسبب عاملين أساسيين: **طبيعة تركيبتها المعدنية التي تمتص الموجة ولا تعكسها**، وبسبب نجاح الجهة المشغلة في **عملية التمويه** من خلال استخدامها **لمسارب الطيران التي تستخدمها إسرائيل عادة** .[294]

وهذا يعني قدرة المقاومة في :

[294] الطائرة الاستطلاعية «أيوب» خرقت 7 منظومات من الرادارات وقد تحمل في المرة المقبلة متفجرات ، **جريدة الشرق الأوسط**، السبت 26 ذو القعدة 1433 هـ 13 اكتوبر 2012 العدد 12373.
...archive.aawsat.com/details.asp?section=4&article=699453

4-1-المجال التكنولوجي : وتعتبر الطائرات الالكترونية من دون طيار من أدوات الحرب الالكترونية[295].و تمتلك هذه الطائرات ُقدراتٍ عاليةٍ على التصوير والمراقبة، وحتى القصف بشتى أنواع القنابل. كما وُتشكل حلقات وصلٍ بين القاعدة المعلوماتية الموجودة على الأرض، وساحة العمليات الحربية الكامنة في المجال الجوي والافتراضي ، عبر مختبرٍ للتحليل المعلوماتي ، والذي يمكنّها من تحديد نيرانها بدقة .

4-2-**المجال الصناعي:** حيث أعلن السيد نصر الله أنها صناعة لبنانية محلية ، وهي باكورة الصناعة العسكري للحزب ، وقد صير الى تخليقها و ابتداعها والتوصل اليها بواسطة قدرات الحزب الفنية والتنفيذية .[296]

4-3-المجال الأمني المعلوماتي الاستخباري والرصد: لدى المقاومة تفاصيل دقيقة لمسارب الطيران التي تستخدمها "اسرائيل"، بمعنى أن الطائرة تسير في مسار مدروس طبقاً لقاعدة البيانات والمعلومات التي رصدها الحزب .

وقد ذكرت القناة العاشرة في "إسرائيل" أن "الطائرة أسقطت فوق ياعر ياتير ، إذ أنه بعد إسقاطها قامت وحدة الإنقاذ 669 في سلاح الجو الإسرائيلي بإغلاق المنطقة وجمع الحطام في طائرة يسعور ونقلها الى مقر قيادة أركان سلاح الجو". كما أفادت أن "سلاح الجو والرقابة العسكرية طلبوا تمويه صور الأجزاء التي عثر عليها من حطام الطائرة لأن الإستخبارات الإسرائيلية لا تريد أن يعرف حزب الله ، ما تعرفه " إسرائيل "عن الطائرة .

---

[295] وليد جلعود ، مرجع سبق ذكره ، ص105.

[296] يوسف نصرالله ، مرجع سبق ذكره ، ص 272.

وقد استلم الجيش الإسرائيلي أجزاء الطائرة من الشرطة الإسرائيلية وتم نقلها للجهات المختصة" .[297] وهذا يدّل على اهتمام الجانب الاسرائيلي بها والحرص على معرفة منشأها وقدراتها والثغرات التي يمكن من خلالها تفكيك الشيفرة أو التقاط البث.

5-طائرة مرصاد-2.

هي الجيل الثاني من مرصاد ، وتعدّ من الأسلحة الإستراتيجية التي تمتلكها تراسانات الحزب، وقد تمّ تطوير قدراتها على نحو تجاوزت فيها إمكاناتها المهام الاستطلاعية التجسسية خلف خطوط العدو الى القدرة على حمل كميات وازنة من المتفجرات . كما أنها تحمل صفة الذكاء (بمعنى امتلاك القدرة على إنتقاء الأهداف الحيوية والوصول اليها وتدميرها ، بما يتوافر منها من أجهزة معقدّة تمكنها من المراوغة والتفلت من الرقابة، والدفاعات الأرضية والمقاتلات الحربية .[298]

6-حرب تموز 2006.

ما يميّز حرب تموز 2006 ، أنّها الحرب التي كشفت النقاب عن قدرات حزب الله التي وصل اليها على صعيد تكنولوجيا المعلوماتية والإتصالات في الرصد والعمل الاستخباراتي والعسكري ، وهذا بدا واضحاً وجلياً في سير العمليات التكتيكية والمعارك في كل المجالات البرية والجوية والبحرية ، كما كشفت عن ضعف ووهن الدفاعات الجوية ل"إسرائيل" والقبة الحديدية التي لم تستطع تدمير منصات إطلاق الصواريخ في لبنان أو منع سقوطها على

---

[297] **موقع المقاومة الاسلامية في لبنان** :إسرائيل": طائرة أيوب التي أرسلها حزب الله هي الطائرة رقم 12، https://www.moqawama.org/essaydetails.php?eid=26482&cid.

[298] يوسف نصرالله ، ص 272.

الداخل الاسرائيلي . وأدّت هذه الحرب الى قتل 164 إسرائيليا، بينهم 119 جنديا.[299] وسوف نستعرض تباعا تأثير هذه الحرب في كل المجالات .

1-6- في المجال البحري .

حملت المفاجأة الأولى من حرب تموز 2006 وتحديداً تدمير ساعر-5 (درة السلاح البحري الاسرائيلي ، المصممة للافلات من الرادار ومن الأشعة ما دون الحمراء ، ويتألف طاقمها من 61عنصراً، مزودة بأسلحة متنوعة صواريخ أرض-أرض وأرض-جو ، كما تضم في مؤخرتها مهبطاً للمروحيات على نحو يجعلها قادرة على نقل مروحيتين) [300] بشائر التهديدات التي أطلقها نصر الله في مؤتمره الصحافي وصدقها . ولم تفصح المقاومة حتى الان عن أسرار الاطلاق ونوعه إلا أنّ الجانب الإسرائيلي أعلن أنه صاروخ أرض -بحر، طرازسي-802 [301]. وهذا انعكس على المجال البحري ، حيث سدّت المقاومة الطريق على البوارج الحربية للمشاركة في الحرب ، وأثبتت المقاومة بالمعادلة البحرية بأنّها قادرة على الحصار ومنع الملاحة في البحار مستقبلاً في حال وجود منظومة متكاملة ترتكز على 3 أساسيات:

أ - القدرة على الاستعلام، وتشمل استخدام الرادارات البحرية المتطورة والتنصت والمراقبة البصرية والرصد وتحليل الأهداف نوعيتها ومسافاتها.

---

[299] تموز 2006: تفاصيل جديدة عن معركة بنت جبيل وأهداف الحرب ،تاريخ النشر: 2015/05/06 - 14:2على الرابط التالي:https://www.arab48.com ، إسرائيليات ، دراسات وتقارير.

[300] عباس النابلسي ، **رعب اسرائيل: أسرار القدرة العسكرية لحزب الله** ، ط1، بيروت ، دار ايوان للطباعة والنشر والتوزيع ،2007، ص 157.

[301] حسب مزاعم "اسرائيل" ، أما مميزاته بأنه يوجه عبر الرادار،وهويلامس سرعة الصوت ،ويبلغ مداه 120كلم،ويزن 715كلغ،ويحمل رأسا متفجرة ويتضمن جهاز راداروأنظمة مضادة للتشوش ،ويعدّمن أفضل الصواريخ الاعتراضية . نقلا عن نشرة غ**لوبال سيكيوريتي** .

ب – القدرة العسكرية على الضرب من خلال الصواريخ البحرية القصيرة والبعيدة المدى والقوارب السريعة والقيام بعمليات تلغيم في المياه وإستخدام طائرات بدون طيار والاعتماد على ضفادع بشرية .

ج – القدرة على الاستمرارية في ضرب الأهداف البحرية .[302] وشكّل بروز قضية الثروة النفطية والغازية في المنطقة الاقتصادية الخالصة لكل من لبنان و" إسرائيل" ، عاملاً جديداً وتهديداً إستراتيجياً ل"إسرائيل "من قبل المقاومة ، تحديداً بعد إضافة المنصات النفطية التي تعدها "إسرائيل" إلى بنك الأهداف البحرية للمقاومة ، خصوصاً أنها لم تعلن حتى الآن عن المعادلة الجوية التي تقلق بال الإسرائيليين كثيراً .[303] سيّما بعدما نقله " رونين بيرغمان (معلّق الشؤون الأمنية في صحيفة "يديعوت احرونوت) ، عن مؤتمر الأمن الدولي المنعقد في ميونخ ، عن نجاح حزب الله في تهريب ثمانية من صواريخ "ياخونت" [304](والتي تفوق سرعة منظومة "باستيون" المزودة بصواريخ "ياخونت" المجنحة المضادة للسفن، ثلاث مرات سرعة الصوت، ويصل عددها في المجمع الصاروخي الواحد إلى 36 صاروخًا)، عبر البر من سوريا" .[305]

---

[302] علي دريج ، ماذا تخبئ المقاومة لإسرائيل من مفاجآت بحرية جديدة ، **صحيفة السفير**، العدد11946، الثلاثاء في 26تموز،2011، ص4.

[303] المصدر نفسه .

[304] وتستطيع صواريخ "ياخونت" ضرب أهداف على بعد 300 كيلومتر بسرعة 750 مترًا في الثانية، وعند الاقتراب من الهدف ينخفض ارتفاع تحليق الصاروخ إلى ما بين 15 مترًا و10 أمتار، وهي تستهدف سفنًا معادية، ومجموعات سفن على حد سواء، وذلك في ظروف المواجهة النارية والإلكترونية الشديدة، وهي مزودة بنظام تكنولوجي عالٍ يسمح لها بأن تكون محجوبة عن الرادارات. وصواريخ "ياخونت" تستطيع حمل رأس مدمر موجه بالرادار وزنه 200 كيلوغرام، كما يمكنها ملاحقة الهدف وتتبعه أوتوماتيكيًا وذاتيًا، وهو ما يعرف في المصطلحات العسكرية بـ"أطلق وانسَ".

[305] عباس الزين، الـ«ياخونت»... أدنى مفاجآت المقاومة!، **موقع المردة** ا/146316/elmarada.org/ html

2-6- في المجال البري والاستخباراتي :

شكلّت حرب تموز 2006 مفاجأة للكيان العبري لما وصلت إليه المقاومة في العمل الإستخباراتي والتجسس، بافادة مسؤولين مختصصين في هذا الشأن وباعتراف ساسة العدو وجنرالاته ، ففي معركة مارووون الراس دخل الجنود الى مقر للتنصت تابع لحزب الله. حيث وُجدت عند حزب الله معدات تتمتع بجودة عالية ، وتتفوّق كثيراً على المعدات التي امتلكتها وحدة التنصت الإسرائيلية . حزب الله كان يتنصت على الجيش الإسرائيلي 24 ساعة يومياً. على شبكة الهواتف في الوحدات على الحدود فحسب ، بل تنصّت على الوحدات الفاعلة ميدانياً. وكان أفراد حزب الله يمتلكون تفاصيل ومعلومات عن قادة الجيش، وأعدّوا ملفاً كاملاً عن غال هيرش (القائد السابق لفرقة الجليل) بعد تتبّعه» .[306] وهذا ما دفع قيادة الجيش الإسرائيلي في الكيان الصهيوني الى اتخاذ القرار بمنع الجنود والضبّاط من استخدام الهواتف الخلوية لاحقا ، خوفاً من تنصّت حزب الله على مكالماتهم ونقل عن مسؤولين كبار في أجهزة الاستخبارات العسكرية قولهم إن " حزب الله يتنصّت علينا تماماً مثلما نفعل نحن " .[307] وفي تقرير ترجمته صحيفة السفير تحت عنوان "الليلة التي سلّت فيها السكاكين" ، والذي يتناول تفاصيل دقيقة عن بعض المعارك البرية التي جرت إبّان حرب تموز بين المقاومة وقوات العدو الإسرائيلي ، والتي مفادها :

---

[306] حزب الله يستمع الينا"، **شبكة المعلومات السورية القومية الاجتماعية** ، على الرابط التالي:
http://www.ssnp.info/index.php?article=55676

[307] المصدر نفسه .

وجود أنفاق أو محميات طبيعية تحت الارض أقامها حزب الله في جنوب لبنان بعيداً من أي مكان سكن...القيادة والجمهور لم يدركا بشكل كامل معنى تواجد الجيش في قتال شديد مع عدو ذي خبرة وتدريب ومزود بوسائل متقدمة .[308]

كما أثبتت المعارك البرية في بنت جبيل ومارون الراس ، رغم التجهيزات الحديثة التي يمتلكها الجيش الإسرائيلي والمواكبة الجوية والبرية (إسناد جوي بالطائرات وإسناد بري عبر دبابات الميركافا والأليات العسكرية) قدرة المقاومة على التنسيق والتواصل والبسالة في الدفاع عن الأرض رغم إمكاناتها االمتواضعة .

أما بالنسبة الى العمليات البرية بدا واضحاً افتقار " إسرائيل" الى الدقة في الرصد وهذا انعكس على الأرض خلال سير المعارك (التفاجيء بالانفاق وبطبيعة الطرقات) .

ولمعالجة هذة الثغر تسعى قيادة الجيش في "إسرائيل " إلى إجراء مناورات و تدريبات خاصة يخضع لها الجيش ، لمعالجة الانفاق وتفجيرها وكيفية التعامل معها خلال الحروب.

وفي تقرير أعدته صحيفة الاخبار حول لقاء تمّ بين جوزيف سماحة والشهيد عماد مغنية ، تحدث فيه سماحة عن طبيعة المشاهدات التي راها وعن أنواع كاميرات حديثة ومتطورة ، مزروعة على طول الحدود تراقب العدو وترصد تحركاته ، إضافة الى القدرة على التنصت على شبكة الاتصالات الاسرائيلية وخرقها ، وامتلاك المقاومة لأنواع كبيرة من الأسلحة المتطورة التي أدهشته والتجهيزات الموجودة على طول الحدود ، هذا بالاذافة الى الأسرار التي لا يمكن البوح بها .[309]

---

[308] الرواية الاسرائيلية التفصيلية لهزيمة الجيش الاسرائيلى فى مارون الراس ، الجمعة, 29 يونيو 2007 .
http://www.estqlal.com/article.php?id=10208

[309] تموز 2006 – 2011 | لقاء جوزف وعماد، **الأخبار**،العدد 1459، الثلاثاء12تموز 2011.
http://www.al-akhbar.com/node/16471

وفي كتاب "بيت العنكبوت" لمراسلَي الشؤون العسكرية والعربية في صحيفة "هآرتس"، عاموس هارئيل وآفي يسكاروف ، الصادر عام 2008، يتحدّث الكاتبان عن وثائق عُثر عليها في مارون الراس، تضّم " قائمة موجات بث تكتيكية يستخدمها الجيش الإسرائيلي، وإلى جانبها نصوص لأحاديث على شبكة الإتصال الإسرائيلية العسكرية ، بعضها تابع لوحدات تدربت في الجولان وأخرى على شبكات الإتصال في الضفة الغربية . كذلك اكتُشفت وسائل رصد متطورة داخل أحد بيوت قرية ميس الجبل أيضاً. وإحدى نقاط التنصت كانت تتابع شبكة المروحيات التابعة لقيادة المنطقة الشمالية».

3-6- في المجال الجوي:

استطاعت المقاومة إسقاط مروحية من طراز "أباتشي" كانت تنقل جنوداً جرحى أصيبوا في معارك مارون الراس، فسقطت واحترقت بمن فيها، وادّعى العدو أن المروحية اصطدمت بالأسلاك الكهربائية .[310]

وهذا أدىّ الى تقييد سلاح الجو بعدما تمّ تحييد السلاح البحري . وأصبح الكيان يتوخى الحذر في إرسال المروحيات ولكنه فرض التعتيم الإعلامي والسرية والكتمان لخوفه من الرأي العام الإسرائيلي .

[310]الدرس الخامس: عملية الوعد الصادق
almaaref.org/books/contentsimages/books/...ashhor.../lesson5.htm

المبحث الثاني : حرب المعلومات الإلكترونية بين حزب الله و" إسرائيل" .

العالم اليوم هو عالم افتراضي وكل شيء محوْسب وموجود على الشبكة والرجوع الى الوراء مستحيل ، لذلك فانّ ميزان الرعب تغير من السلاح النووي الى سلاح تكنولوجيا المعلومات والاتصالات، و"إسرائيل" تمتلك الخبراء الافضل بالعالم في هذا المجال . وبما أن الاقوى هو من يملك القدرة التكنولوجية والمعلوماتية والبرامج المتطورة في الحاسوب والشبكة العنكبوتية والذي يستطيع أنّ يشل دولة اخرى أو منظمة أو مؤسسة من دون ترك بصمات . فإن هناك حرباً خفيةً تستعر بين الطرفين قوامها حرب المعلومات ، وقد عبّر عن ذلك غاد شمرون المسؤول السابق في الموساد الصهيوني ، حيث قال: "هناك حرب أدمغة بين حزب الله و" إسرائيل" وليس جديداً أن تتجسس "إسرائيل" على لبنان وليس هناك حاجة لوضع جاسوس على تقاطع طرق إنَّما عبر وسائل مختلفة..[311] وفيما يلي عرض لبعض الإجراءات التي يتم العمل عليها وتطويرها من قبل الطرفين .

المطلب الأول: التدابير التي اتخذتها " إسرائيل" في حماية المعلومات .

من المُسلّمات في "إسرائيل" أنّ إيران وحزب الله يتصدّران قائمة الأعداء ، وهذا ما عبّر عنه كثيرون منهم بوعاز غانور، المدير العّام ومؤسس مركز أبحاث السياسة ضدّ الإرهاب (ICT) في المركز المتعدد المجالات في هرتسليا، شمال تل أبيب، حيث قال: "إسرائيل" كانت وما

311 العدو يخسر مجدداً في حرب الادمغة .. و إسرائيل "تعترف" :
http://www.mounahada.org/modules.php?namepart=news_and_bayanat&number=1111

زالت العدو المركزيّ لحزب الله" [312] . وهذا ما أكدّ عليه هنري كيسنجر من أنّ إسرائيل تواجه خطرا مستقبلياً وليس آنياً .[313]

وبناءً على ذلك، لا تألو مراكز الأبحاث جُهدًا في محاولاتها لسبر غور منظمة حزب الله، ولا تبخل الحكومة الإسرائيليّة برصد الأموال لإجراء الأبحاث والدراسات وخوض الحملات المُكثفّة ضدّ حزب الله بهدف تضليل الرأي العام وسلبه جمهوره كجزء من الحرب النفسية والاعلامية وبما أنّ الإعلام الإسرائيلي هو إعلام مُتطوّع لمصلحة الأجندة الصهيونيّة، فإنّه يقوم تباعًا بنشر الدراسات والتحليلات لطمأنة الجمهور الإسرائيلي من ناحية ، ومن الجهة الأخرى ليؤكّد على أنّ "إسرائيل " كانت وما زالت وستبقى الرقم الصعب في منطقة الشرق الأوسط من الناحية العسكريّة، كمًّاً ونوعاً. ومن أهم هذه الدراسات : الدراسة التي أجراها شموئيل ايفن ودافيد بن سيمان ، الصادرة من معهد الأمن القومي (INSS) [314]، والتي عددوا خمسة من الإدارات التابعة للفضاء الإلكتروني وهي :

1- البنية التحتية الحكومية لعصر الإنترنت.

أقامت " إسرائيل" في سنة 1997 مشروع "بنية الحكومة التحتية لعصر الإنترنت" في داخل وزارة المالية الإسرائيلية. وحدد هدف هذا المشروع في حماية وتأمين استعمال الإنترنت في الوزارات والمؤسسات الحكومية. وأقيم داخل هذا المشروع "مركز حماية المعلومات لحكومة إسرائيل" وأنيطت به مهام متابعة تطور وسائل حماية المعلومات في العالم والتنسيق بين

[312] زهير اندراوس، حرب الأدمغة بين الشاباك وحزب الله: تحذير جديّ من وجود خلايا نائمة كبيرة وكثيرة في إسرائيل تنتظر الأوامر لتنفيذ العمليات الفدائيّة داخل عمق الدولة العبريّة .، في **مجلة رأي اليوم** ، على الرابط التالي:
http://www.raialyoum.com/?p=302271

[313] مؤتمر هرتسيليا السادس عشر 2016،حول الترتيبات القومية الجديدة لاسرائيل والتغييرات الاقليمية الحالية ، **ترجمة مركز قدس نت للدراسات والنشر والاعلام** ، ص 24.

[314] Shmuel Even and David Siman-Tov, ,p.75.

الوزارات والمؤسسات الحكومية من أجل إيجاد حلول لمشاكل حماية المعلومات وكذلك إجراء بحوث حول هذا الموضوع .

2- السلطة الرسمية لحماية المعلومات .

أنشأت في سنة 2002 "السلطة الرسمية لحماية المعلومات"، في داخل جهاز المخابرات العامة (الشاباك) . وأنيط بهذه السلطة مهام حماية البنى التحتية للحواسيب المهمة والحيوية في " إسرائيل" من مخاطر ما أطلق عليه "تهديدات إرهابية" و"عمليات تخريب" ونشاطات تجسسية .

3- هيئة السايبر في الجيش الإسرائيلي .

في سنة 1909، اعتبر غابي أشكنازي رئيس هيئة أركان الجيش الإسرائيلي الفضاء الالكتروني كمجال قتال من الناحيتين الاستراتيجية والعملياتية. وبناء على ذلك أقام الجيش الإسرائيلي "هيئة السايبر" في الوحدة 8200 في جهاز المخابرات العسكرية الإسرائيلية (أمان)، بغرض توجيه وتنسيق نشاطات الجيش الإسرائيلي في الفضاء الالكتروني. وأوضح عاموس يادلين، أن هيئة السايبر في الجيش الإسرائيلي تهدف إلى توفير دفاع جيد لشبكات الأنترنت العاملة في" إسرائيل" ، وكذلك القيام بهجمات في الفضاء الالكتروني على أهداف خارجية.

4- وحدة إدارة أنظمة المعلومات .

صادقت الحكومة الإسرائيلية في 27 أذار/ مارس على إقامة "وحدة إدارة المعلومات"، وهي تتبع مدير عام وزارة المالية الإسرائيلية ومسؤولة مسؤولية مباشرة على جميع أنظمة الاتصالات المحوسبة الحكومية، بما في ذلك مشروع "بنية الحكومة التحتية لعصر الإنترنت".

5- هيئة السايبر الوطنية.

أعلن رئيس الحكومة الإسرائيلية بنيامين نتنياهو في 18 أيار/ مايو 2011 عن إنشاء "هيئة السايبر الوطنية" في إسرائيل. وذكر نتنياهو أن الهدف الأساس لهذه الهيئة هو تعزيز قدرات " إسرائيل" الدفاعية عن أنظمة البنى التحتية الحيوية ، من "هجمات إرهابية" في الفضاء الإلكتروني ، التي قد تقوم بها دول أجنبية أو "منظمات إرهابية" . كل ما هو محوسب قد يتعرض للهجمات في الفضاء الالكتروني ، التي قد تشل أنظمة مرافق ومؤسسات حيوية للغاية التي تشغل الدولة مثل: الكهرباء والمياه والاتصالات والمواصلات .

وعلاوة على مهامها الدفاعية عن الفضاء الإلكتروني الإسرائيلي، فإن من مهام "هيئة السايبر الوطنية" تشجيع وتطوير شركات إسرائيلية متخصصة في الدفاع عن الفضاء الإلكتروني، بغرض الحصول على جزء من سوق الفضاء الإلكتروني الذي ينمو بسرعة كبيرة للغاية على الصعيد العالمي .

المطلب الثاني: التدابير الأمنية التي يتبعها حزب الله .

هناك حرب كونية تخوضها أجهزة الإتصالات الغربية بكل فروعها وتشعباتها ضد حزب الله ومنظومة الإتصالات التابعة له ، لأنه الحزب الوحيد الذي لا يملك **بصمة الكترونية** تتيح التجسس عليه .[315] وقد عبر الخبراء الصهاينة عن ذهولهم مما أسموه قدرة حزب الله الأمنية " وحدة مكافحة التجسس " ، التي نجحت في اكتشاف أجهزة التجسس الإسرائيلية المتطورة في مرتفعات صنين وجبل الباروك ، حيث لم تنفع جميع وسائل التمويه في إخفائها.

[315] رضوان الذيب، جنرال اميركي: استطعنا التنصت على كل الدول الا حزب الله ، **جريدة الديار**،2013/11/13. www.saidaonline.com/news.php?go=fullnews&newsid=58627

1- تفكيك أجهزة التجسس الإسرائيلية :

يمثل انتصاراً ميدانياً للحزب في مجال مكافحة التجسس ، ويدل على قوة الحزب وفاعليته في المسّ بمنظومات جمع المعلومات الإستخبارية الإسرائيلية وآخرها في الباروك . بالمقابل تبدو قدرة " إسرائيل" ضعيفة في جمع المعلومات عن حزب الله وتكتيكاته الأمنية ما صعّب عليها تحقيق إنجازات في الحرب الخفية التي تدور بين الطرفين، وفي ظل اعتماد الحزب سياسة الشك والغموض في جميع تحركاته ونشاطاته التكنولوجية .

2- شبكة الإتصالات :

توسعت شبكة الألياف الضوئية التي يمتلكها حزب الله 2006 وتضمنّت الضواحي الجنوبية لمدينة بيروت والمنطقة الساحلية الممتدة بين بيروت والجنوب ووادي البقاع وصولاً الى الهرمل ضمناً . كما أنّها متصلة بشبكة إتصالات عسكرية في سورية وتمّ ربطها مع العديد من محطات إستخبارات الإشارة السورية والإيرانية ، والتي من خلالها يتمّ تمرير المعلومات وبحسب مسؤولين عسكريين في حزب الله ، قسم استخبارات الاشارة هو أهم وأحدث مكونات الحزب التكنولوجية ، وتقنيوه هم أكثر من خضع للفحص والتدريب .[316]

3- اختراق الدفاع :

استطاع الحزب اختراق آلاف المواقع في "إسرائيل " من خلال الهاكرز جواد وكانت إولى الضربات في العام 2013 عبر إسقاط 20 موقعاً صهيونياً، بينما العملية الاخرى كانت في شباط من العام 2014 عبر إسقاط وإختراق 60 موقعاً . ومع بداية حرب تموز 2006 "

[316] المصدر السابق نفسه .

بدأت الضربات الأولى المتضمنة "هجمات فك الحزام وقطع الخدمة DDOS" والتي استهدفت موقع "الموساد" الإسرائيلي، وموقع مطار "بن غوريون" ، وموقع وزارة الدفاع الإسرائيلية وموقع وزارة النقل الصهيونية، بثوانٍ تمّ قطعها عن العالم وإيقافها ما دفع العدو لمحاولة استعادتها عبر تغيير بروتوكولات الخدمة IP دون ان يفلح، مع بداية حرب تموز 2006 .[317]

4- كاميرات المراقبة :

تبنت مجموعة "قادمون"، سقوط آلاف المواقع الإسرائيلية الحساسّة خصوصاً بعد ما أعلن عنه في الفترة الاخيرة عن فتح كاميرات المراقبة داخل الكيان، ومن ضمنها خرق لشركات الطيران ، حتى كاميرات المراقبة في مطار بن غوريون ونشر روابط للبث المباشر لتلك الكاميرات على صفحة "قادمون" على الفايسبوك ، قبل أن يسارع الفايسبوك الى إغلاق الصفحة .[318] أضف الى ذلك كاميرات مراقبة لحزب الله بالغة الدقّة تنتشر على طول الشريط الحدودي مع " إسرائيل" ، وتستطيع التقاط موجات بث طائرات التجسس واللاسلكي للجنود الإسرائيليين .[319]

---

[317] علي عواضة ، قادمون: العدو سَيُدَمَّرُ الكترونياً... لدينا يقينٌ في ذلك ، **البلد**، الإثنين 29 شباط , 2016 01:30
http://beirutpress.net/article/284332\

[318] المصدر نفسه .

[319] حرب الكترونية طاحنة بين حزب الله و اسرائيل : هل استطاع حزب الله من اختراق "الام كا " -http://defense
/arab.com/vb/threads/47617

إستنتاج الفصل الثاني .

هي حرب كرّ وفرّ بين الطرفين ، يسعى كل منهما الى استغلال الفرص والعيوب ونقاط الضعف والقوة ، والسعي الى امتلاك القوة والكفاءة المعلوماتية المتطّورة واستثمارها في الحرب الالكترونية ، ما يؤكد وجود صراع تكنولوجي حقيقي بين الجانبين. ويوحي المشهد التكنولوجي الإسرائيلي بأنه سلاحاً ذوحدين .

الأول، ويهدف إلى استمرارية التفوق التّقني والرقمي الإسرائيلي، بحيث تبقى "إسرائيل" مهيمنةً كقوةٍ عسكريةٍ في الشرق الأوسط ، حيث أجادت لغة العصر الحديثة واتبّعت سياسة "بن غوريون" الذي أكدّ أن التقدم العلمي مسألة وجودية لها تحتّم عليها إبقاء يدها العليا ، " **فالعلم سيعطينا ما حرمته منا الطبيعة** " [320].

والثاني، ويهدف في أن تكون "إسرائيل" مركز جذبٍ تكنولوجي ، ومصدّرة للتكنولوجيا العسكرية لكل بقاع العالم ، والذي يعود عليها بمردوداتٍ ماليةٍ وأمنيةٍ كثيرة

[320] عبدالله كمال ، الهولوكست المنسي.. حين حولت فرنسا الجزائر إلى حقل للتجارب النووية الإسرائيلية! 22 \ 08 \ 2017.https://www.sasapost.com/israels-nuclear-tests-in-algeria

خاتمة

ثمّة حروب خفيّة تديرها الأدمغة والعقول ، ميدانها شبكات الانترنت ، هدفها التجسس وسرقة المعلومات والبيانات ، ألقت بتداعياتها على سيادة الدول وأمنها وتهديد استقرارها ووجودها. فأمست المعلومة قوة تضاهي أحدث الأسلحة المتطورة مكانة في الحروب والأمن ، فأهمية المعلومات ليست ناجمة عن مجرد الحماية من هجمات واختراقات فردية فحسب ، فالأمر يتعدى ذلك ليصل إلى مفهوم أكثر شمولا واتساعا وهو الحرب الإلكترونية التي ألقت بأثارها السلبية على معظم الدول وإمكاناتها . ويمتاز الفضاء الإلكتروني بسرعته الديناميكية ، وتغيّراته المستّمرة ، وتشعبّاته الرقمية المتعددة ، وعناصره و خصائصه المتداخلة وهذا يؤدّي الى حدوث اختراقات وتجسس وقرصنة تطال نظم المعلومات بوتيرة تفوق سرعة البرق .

إنّ مجال الحرب الإلكترونية المتغّير يجعل من الصعوبة بمكان معرفة ما الذي يمكن أن يحدث في اليوم التالي من تطور، وأي خطر يمكنه أن يصيبك ، و أكثر ما يثير الذعر في " إسرائيل" هو أن تتعرض لهجمة إلكترونية تستهدف بشكل مباشر مرافقها الإستراتيجية المرتبطة بالفضاء الإلكتروني، مثل البنى التحتية (الكهرباء والمياه والمواصلات، والقطاع المصرفي)، وهيئات القيادة وشبكات التحكم العسكرية ، والأقمار الصناعية ، وكذلك مجمل التقنيات المتقدمة المرتبطة بهذا الفضاء.

وقد دخلت هذه الوسائل الصراع العربي الإسرائيلي، وأصبح يعرف بالصراع العربي الإسرائيلي الإلكتروني عبر الفضاء الإلكتروني ، والذي تُجيد " إسرائيل" معرفته بشكلٍ كبير كونها تهتم بالبحث العلمي والتّقني بشكلٍ واسع ، وتمتلك كوادر ماديةٍ وبشريةٍ متطورةٍ في هذا المجال،

تُساندها في هذا الشأن الولايات المتحّدة الأميركية والعديد من الدول الغربية .إلاّ أنّ التطورات التي تشهدها ساحة الفضاء السيبراني حولّت الجميع إلى ما يشبه البيت الزجاجي .

بالمقابل إستطاع حزب الله أنّ يشّكل التهديد الأول المركزي والأساسي ل"اسرائيل" وتمكّن من إحداث خرق إستخباراتي نوعي ودقيق لشبكاتها ، وشكّل قدوة وقوة تراكمية وتبادلية رفد بها كلِ من الأحزاب الفلسطينية وحركات التحرر في العالمين العربي والاسلامي . ويمتلك الحزب أحدث أجهزة التجسس الالكترونية التي تمكنّه من الحصول على كمٍ كبيرِ من المعلومات الدقيقة بالرغم من إمكاناته المتواضعة واستمرار الحصار المتزايد عليه ، ليشمل قطاعات ومؤسسات مدنيّة وتربويّة وصحيّة ..... فضلاً عن الضغوط الداخلية والدولية على عناصره وكوادره وقادته وأجهزته بل وعلى حساباته المالية ، مقابل دولة متقّدمة مثل " إسرائيل " تمتلك كل الوسائل المتاحة تكنولوجياّ وعسكرياً واقتصادياً بل وتحظى بدعم غربي ودولي واسع .

وتعاني " إسرائيل " حالياً من تصاعد التهديدات الإلكترونية عليها ، هجمات "الهاكرز" الذي تمّ مؤخراً من قبل مجموعة من الهاويين العرب " أنونيموس" ، بالإضافة الى الإختراقات التي ينفذّها حزب الله بين الفينة والأخرى والتي تعتمد" إسرائيل " فيها على السرية والتكتم الشديد **لذا يبدو من الصعب للغاية أن تقوم " إسرائيل " بتطبيق سياسة الردع ، التي تعتبر حجر الزاوية في إستراتيجيتها الأمنية ، ف " الدفاع الفعال " لا يعتمد فقط على التكنولوجيا المتطورة ، وإنما أيضا على شبكة محكمة ذات قواعد وإجراءات صارمة وعلى ثقافة تفّهم المخاطر وعلى انضباط شديد وعلى حماية المواقع وعلى رقابة بشرية قوية** . غير أنّ رئيس جهاز الإستخبارات العسكرية الإسرائيلية ، "عاموس يادلين "، قد أوضح خطط

وطموحات جهازه لتسخير التقدم التقني والإلكتروني في برامج عسكرية ، وأكدّ أنّ مجال الحرب الإلكترونية يتطابق تماماً مع العقيدة الدفاعية الإسرائيلية .. **وهو مجال لا يستطيع فيه الاعتماد على دعم خارجي أو تقنية ليست من صنع " إسرائيل" .**

بالمحصلّة لا توجد دولة محصّنة من الهجمات السيبرانية ، فكلّما تعاظمت درجة توظيف التقنيات المتقدّمة في تشغيل مرافق البنى التحتية والمؤسسات العسكرية والمدنية الحساسة كلما زادت فرص انكشافها أمام الهجمات الإلكترونية . وعلى هذا الأساس تشكّل الحروب الإلكترونية الرقمية وسيلة فاعلة في تحقيق توازن القوة بين حزب الله و"إسرائيل" ، بل فرصة مناسبة لحركات المقاومة عامّة في تسديد ضربات موجعة لها ، فمهما كانت القدرات التي تحظى بها أجهزة الإستخبارات الإسرائيلية ، إلا إنها يمكن أن تبقى عاجزة وقاصرة أمام تطّور الوعي الأمني لدى المقاومة ، والإجراءات الإستخبارية التي تتبعها . وإذا كانت نقطة التحّول في المعركة المقبلة بالنسبة ل "اسرائيل " متعلّقة بفعالية منظومات الإتصال والمعلومات ، وبسرعة نقل هذه المعلومات ، في الزمن الحقيقي ، إلى الإستخبارات التي تعمل على تحليل الصورة ، ثم إلى حاسوب الطائرة كي تقصف الهدف . فما هو الردّ المناسب و المفاجآت التي يخفيها حزب الله ؟ وهل سيتدخل حلفاؤه في الحرب المقبلة وتصبح المواجهة مفتوحة بين المحورين ؟

و هل ستستطيع " إسرائيل " الحفاظ على مكانتها التكنولوجية من الناحية الأمنية ؟ هذا ما ستكشفه الحرب المقبلة !

الفهرس

قائمة المصادر والمراجع

1- الكتب باللغة العربية .

• ابن خلدون: **المقدمة** ، دار مكتبة الهلال، بيروت ، 1983 .

• الأشقر جبور (منى) ، **السيبرانية هاجس العصر** ، المركز العربي للبحوث القانونية ، بيروت ،2016. https://carjj.org/node/4595 2016

• آغا (حسين) والخالدي (جعفر) و قاسم (أحمد) ،" **اسرائيل، العقيدة العسكرية وشؤون التسلح** "، سلسلة الدراسات الاستراتيجية ، المؤسسة العربية للدراسات والنشر ، بيروت،1982.

• إيفن (شموئيل) وسيمان طوف(دافيد) ، "**حرب في الفضاء السبراني: مفاهيم، واتجاهات، ودلالات لإسرائيل**"، معهد دراسات الأمن القومي، مذكرة رقم 109 ، تل أبيب 2011.

• بوقاعي، (دافيد) ، **الخطر الكياني على اسرائيل: الرد الاستراتيجي**"، نتيف،2004.

• توفلر (ألفن) ، **تحول السلطة** ، ترجمة لبنى الريدي ، الهيئة المصرية العامة للكتاب . 1995

• جلال (أحمد) ، **صراع القوى المدنية-العسكرية وأثره على السياسة الخارجية التركية،** المكتب العربي للمعارف للنشر والتوزيع والطباعة، القاهرة 2015 ، على الرابط الالكتروني التالي: https://books.google.com.lb/books?isbn=977276816X

• صبري مقلد (اسماعيل) ، **العلاقات السياسية الدولية: دراسة في الأصول والنظريات،** مطبوعات جامعة الكويت ،1984.

• طال (يسرائيل)، **الأمن القومي: قلة مقابل كثرة** ، (بيطحون ليئومي: معطيم مول ربيم)، تل أبيب، دفير 1996.

• طاهر (علاء) ، **حرب الفضاء ونظرية الأمن الاسرائيلي** ، الصلاح للدراسات الاستراتيجية ، ط1، باريس ، 1991.

• عبد الصادق (عادل) ، **أثر الإرهاب الإلكترونى على مبدأ استخدام القوة فى العلاقات الدولية** ، رسالة ماجيستير، جامعة القاهرة ، 2001-2007.

• عبد الصادق (عادل) ، **الإرهاب الإلكتروني: القوة في العلاقات الدولية : نمط جديد وتحديات مختلفة** ، مركز الأهرام للدراسات السياسية والاستراتيجية ، القاهرة، 2009.

• عباس (طارق) ، **مجتمع المعلومات الرقمي** ، ط 1 ، المركز الأصيل للطبع والنشر والتوزيع ، القاهرة ، 2004.

• العزي (غسان) ، **سياسة القوة مستقبل النظام الدولي والقوى العظمى** ، مركز الدراسات الاستراتيجية والبحوث والتوثيق، بيروت ، 2000.

• علوي (مصطفى) ، "**مفهوم الأمن في مرحلة مابعد الحرب الباردة**": قضايا الأمن في أسيا ، مركز الدراسات الأسيوية ، القاهرة ، 2004.

• كوهين (أفنر)، **اسرائيل والقنبلة** ، مؤسسة شوكن للنشر، القدس ، 2000.

• لونج، (أوستن) ، الحروب اللامتماثلة في القرن الواحد والعشرين الارهاب الدولي والتمرد وحرب الطائرات من دون طيار: **الحروب المستقبلية في القرن الواحد والعشرين**، مركز الامارات للدراسات والبحوث الاستراتيجية، على الرابط الالكتروني التالي:

ecssr.com/ECSSR/print/pb.jsp?lang=ar&publicationId=/Publicions/Books

• ماضي (عبد الفتاح) ، **الدين والسياسة في اسرائيل**، مكتبة مدبولي ، القاهرة ، ط1 ،1999.

• مازن (بلال) ، **الحرب غير المتوازية الإرهاب** ، مطبعة اليازجي ، ط 1، شباط 2002.

• النابلسي (عباس) ، **رعب اسرائيل:أسرار القدرة العسكرية لحزب الله** ، ط1 ، دار ايوان للطباعة والنشروالتوزيع ، بيروت ،2007.

• المجذوب (محمد) ، "**التنظيم الدولي: النظريّة العامّة والمنظمّات العالميّة والإقليميّة والمُتخصِّصة**"، ط8 ، منشورات الحلبي الحقوقيّة، بيروت، 2006.

• منصور (جوني) و نحاس (فادي) ، **المؤسسة العسكرية في اسرائيل (تاريخ ، واقع ، استراتيجيات وتحولات)**، مدار المركز الفلسطيني للدراسات الاسرائيلية ، فلسطين ،2009 .

• ميرشيمر (جون جي.) ، **لماذا يكذب القادة ؟ حقيقة الكذب في السياسة الدولية** ، مجلة عالم المعرفة، العدد443، ترجمة غانم النجار ، المجلس الوطني للثقافة والفنون، الكويت ،2016 .

• نئمان (يوفل) ،" **اسرائيل ومحدودية الردع النووي**"، نتيف، 1-2(54-55)،1997.

• ناي، (جوزف)، **القوة الناعمة وسيلة النجاح في السياسة الدولية**، ترجمة محمد البجيرمي، العبيكان ، 2007.

• نصرالله (يوسف) ، **الحرب النفسية قراءات في استراتيجيات حزب الله** ، ط1، دار الفارابي ، بيروت ، 2012.

• نعمة (كاظم هاشم) ، **العلاقات الدولية** ، جامعة بغداد ، كلية العلوم السياسية ، شركة اياد للطباعة ، بغداد ، 2007.

• وايزمن (حاييم) ، **التجربة والخطأ** ، نيويورك ، 1949.

• **كتاب القوانين 540**، (سيفر هحوقيم540) ،1968 .

• ياريف (اهرون) ، "**العمق الاستراتيجي: وجهة نظر اسرائيلية في أمن اسرائيل في الثمانينات**" ،1980 .

2- الكتب باللغة الأجنبية.

• Bartelson Jens, "**The Concept of Sovereignty Revisited**", The European Journal of International Law, vol17 ,no.2,2006.

• BELLEFONDS DE LINANT ET HOLLANDEA. , " **(Droit de l'informatique et de la télématique,** J. Delmas et cie, 2ème edition.

• CLAYTON MARK ," **from the man who discovered stuxnet,Dire wamings one year later** ", the Christian science monitor ,September 22.

• DUNN MYRIAM A. ," **The Internet and the Changing Face of International Relations and Security** ", Vol. 7, Issue number: 1, ProCon Ltd., Sofia, Bulgaria, 2001.011.

• GROSS Michael Joseph ,"**a declaration of cyber –war**", vanity fair, Apr. 2011.

• GUMAHAD ARSENIO T. , **Cyber Troops and Net War: The Profession of Arms in the Information Age**, Maxwell AFB, AL: Air University, Air War College, April 1996.

• HUYGUE Francois-Bernard , **"Cyberguerre et guerre de l'information, stratégies, règles et enjeux"**, under Daniel Ventre's supervision, 2010, introduction». Lavoisier.

• KARATZOGIANNI Athina, "**Cyber-Conflict and Global Politics'**",ed. Routledge and Taylor & Francis Group. , 11th September 2008.

• KNAPP KENNETH J. , **cyber security and global information assurance**, information science reference, 2009, Newyork.

• KUEHI DANIEL T. , " **From Cyberspace to Cyberpower: Defining the Problem,"** in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., Cyberpower and National Security (Washington, D.C.: National Defense UP, 2009) "joseph neye

• LEWIS JAMES.A , **cyberse security recommendations for the next administration testimony,**center for strategic and international studies , september2008 ,Washington DC, subcommittee on emerging threats ,cyber security, science and technology.

• LIBICKI MARTIN C. , **Conquest in Cyberspace:National Security and Information Warfare,** Cambridge University Press, 2007.

• LIND William S et al. **,“ The Changing Face of War: Into the Fourth Generation,”** Marine Corps Gazette (October 1989).

• MAIRE JEROME, **Stratégie hybride, le côté obscure de l’approche globale** ?,tribune n0 811,sur website: www.defnat.fr – 02 septembre 2016.

• MARGALIT AVIASHI,"**THE VIOLENT LIFE OF YETZHAK SHAMIR**", NEW YORK Review of Books ,May 1992.

• MATTEWS Matt M. **, We Were Caught Unprepared: The 2006 Hezbollah–Israeli War** ,OP 26,2008,p.61.on website: usacac.army.mil/cac2/cgsc/carl/download/csipubs/matthewsOP26.pdf.

• MODELSKI G.**, theory of foreign policy** ,Newyork:pall MALL,1962.

• PELEG Noa, “**Growing Big, Reaping Small**,” Globes, March 9, 2011. Michael Walzer,Just and Unjust Wars:A Moral Argument with Historical ILLustrations,3rded.(NY:BASIC BOOKS,2000).

• RID THOMAS , **cyber war will not took place**, Hurst&Company, London tome 2,2013.

• SIffre Jean-Paul , **LA GUERRE ELECTRONIQUE, MAÎTRE DES ONDES, MAÎTRE DU MONDE,** Éditions Lavauzelle , 2003.

• SMITH Ron et KNIGHT Scott , **L’APPLICATION DES SOLUTIONS DE LA GUERRE ÉLECTRONIQUE À LA SÉCURITÉ DES RÉSEAUX**, r evue militaire canadienne , Automne 2005 on website: www.journal.forces.gc.ca/vo6/no3/doc/electron-fra.pdf.

• WAXMAN Mathew c. ,"**Cyber-Attacks and the use of force**",the yale journal of International law,vol 36,2011.

• WAYNE H.FERRIS ,**the power capabilities of nations states**,(U.S.A laxington book,1973) .

• WILSON EMEST J. ,III, "**Hard Power, Soft Power, Smart Power**", Annals of the American Academy of Political and Social Science, Vol. 616, Public Diplomacy in a Changing World (Mar., 2008), Published

by: Sage Publications, Inc. in association with the American Academy of Political and Social Science, Article Stable URl. http://www.jstor.org/stable/25097997

3-الدراسات الجامعية باللغة العربية:

• عبد الحفيظ زهير جعوان، **تأثير خطابات حسن نصرالله على نتائج معركة تموز 2006**، رسالة ماجيستير ، جامعة بيرزيت ، 2009. على الرابط التالي: thesis.mandumah.com/Record/211438.

• أحمد حسن محمد أبو جعفر، **دراسة نقدية في قراري الجمعية العامة للأمم المتحدة 181 و194 المتعلقين بالقضية الفلسطينية** ، جامعة النجاح الوطنية نابلس، 2008، على الرابط التالي: https://scholar.najah.edu/.../دراسة-نقدية-في-قراري-الجمعية-العامة-للأمم-المتحدة-181-و194.

• سماح عبد الصبور، "**القوة الذكية في السياسة الخارجية: دراسة في أدوات السياسة الخارجية الإيرانية تجاه لبنان منذ 2005**"، رسالة مقدمة لنيل درجة الماجستير، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، 2013.

• وليد غسان جلعود ، **دور الحرب الالكترونية في الصراع العربي الاسرائيلي**، أطروحة في جامعة النجاح الوطنية ، فلسطين،2003،.على الرابط الالكتروني التالي: https://scholar.najah.edu/sites/default/files/وليد%20جلعود. pdf

4- مراكز الأبحاث .

• استراتيجية الأمن القومي الاسرائيلي، **عكا للشؤون الاسرائيلية** ، يونيو 2016، على الرابط التالي:

http://akka.ps/2016/06/%D9%85%D8%AD%D8%AF%D8%AF%D8%A7

• ماهر الشريف ، العقيدة الأمنية الاسرائيلية وحروب اسرائيل في العقد الأخير ، **مؤسسة الدراسات الفلسطينية** ، بيروت 2015. على الرابط التالي : www.palestine-studies.org/sites/default/files/uploads/images/alaqeeda.pdf

• شموئيل ايفن ودايفيد بن سيمان، حرب الفضاء الالكتروني، معهد دراسات الأمن القومي، ترجمة محمد شاهين ، **مركز قدس نت للدراسات والاعلام** .

• مؤتمر هرتسيليا السادس عشر 2016، حول الترتيبات القومية الجديدة لاسرائيل والتغييرات الاقليمية الحالية ، **ترجمة مركز قدس نت للدراسات والنشر والاعلام** .

• يئير عفرون ، رؤى إسرائيلية استراتيجية حول حرب لبنان الثانية تموز/ يوليو 2006، **اعداد وحدة الدراسات الاسرائيلية.**

• محمود محارب، عملية صنع قرارات الأمن القومي في اسرائيل وتأثير المؤسسة العسكرية فيها..، **المركز العربي للأبحاث ودراسة السياسة** ، على الرابط التالي: www.arab48.com

• هيثم الكيلاني، دراسة في العسكرية الاسرائيلية ، القاهرة : **معهد البحوث والدراسات العربية** ،1969.

• شريف اللبان، خبرة عربية منقوصة : أمن المعلومات في ظل تحديات البيئة الرقمية **المركز العربي للبحوث والدراسات** ، الأربعاء 04/مارس/2015 - 11:06 ، على الرابط التالي: http://www.acrseg.org/36712

• صباح عبد الصبور عبد الحي، استخدام القوة الإلكترونية فى التفاعلات الدولية جزء 2، **المعهد المصري للدراسات الاستراتيجية** ، نوفمبر 2016/5،على الرابط الالكتروني التالي: http://www.eipss-eg.org/2/0/1224

• يمني سليمان ، القوة الذكية . المفهوم والأبعاد: دراسة تأصيلية، **المعهد المصري للدراسات السياسية والاستراتيجية** ، يناير 2016/12.على الرابط التالي:

http://www.eipss-eg.org/A9/2/0/320

• ايهاب توفيق، القوة الإلكترونية وأبعاد التحول في خصائص القوة، **وحدة الدراسات المستقبلية**، الاسكندرية ،2014. على الرابط الالكتروني:

https://www.bibalex.org/Attachments/…/20140703112924517 94awrak12pdf.pdf

• الأجهزة الأمنية الاسرائيلية ، **مركز المعلومات الوطني الفلسطيني**- وفا، http://info.wafa.ps/atemplate.aspx?id=8024

• الحرب اللامتماثلة ونظرية الأمن الاسرائيلي، على الرابط الالكتروني:
http://alma3raka.net/spip.php?page=imprimir_articulo&id_article=106
&lang=a

• عباس بدران ، "الحرب الإلكترونية: الاشتباك في عالم المعلوما ت"، بيرو ت: **مركز دراسات الحكومة الإلكترونية،** 2010.على الرابط الالكتروني التالي:

http://www.slideshare.net/abadran/cyberwar-book-in-arabic

• ابراهيم عبد الكريم، الاستراتيجية الجديدة للجيش الإسرائيلي: قراءة تحليلية ، **مركز الامارات للدراسات والبحوث الاستراتيجية** ،2015/8/16، على الرابط التالي:
http://ecssr.ac.ae/ECSSR/print/ft.jsp?lang=ar&ftId=/FeatureTopic/Ibr
ahim_Abdel_Karim/FeatureTopic_1893.xml

• علي حسين باكير، "المجال الخامس.. الحروب الإلكترونية في القرن الـ21". **مركز الجزيرة للدراسات.،** 2011/01/12 على الرابط الالكتروني التالي:
studies.aljazeera.net/ar/issues/2010/20117212274346868.html

• تعرف على وحدة 9900 الالكترونية الإسرائيلية ، **وكالة معا**،2015/4/1.على الرابط التالي: http://www.maannews.net/Content.aspx?ID=769797

5- **المجلات والدوريات :**

• صالح النعامي،"متسفان"... ذراع الحرب الإلكترونية لإسرائيل ، **العربي الجديد**، على الرابط التالي: https://www.alaraby.co.uk/medianews/2016/10/26/%D9%85

• صالح النعامي، **العربي الجديد** : حرب عقول استخباريّة بين إسرائيل و"حزب الله" ، يوسي ميلمان –معاريف . 2017/1/6 ، على الرابط التالي:

https://www.alaraby.co.uk/politics/2015/1

• بحث – النظرية الجيوسياسية – الموسوعة الجزائرية للدراسات السياسية

https://www.politics-dz.com/threads/alnzri-algiusiasi.5981

• بسمة نامق، تأثير مقومات قوة الدولة على سياستها الخارجية حالة دراسية (اسرائيل)، **مجلة المستنصرية للدراسات العربية** ، 2010 .

• داليا قانصو، "لماذا خسر دونالد ترامب وادي السيليكون" ، **جريدة السفير** 2016/11/04م.

• وثائق تؤكد: الهواتف الذكية أصبحت «مراكز تجسس» تخدم أجهزة الأمن ... **جريدة القدس العربي** ، على الرابط التالي: www.alquds.co.uk/?p=374079

• تقرير: "مركز بيو للدراسات" نشرته **جريدة النهار** متوفر على الرابط: http://newspaper.annahar.com/article/116498

• ربيع محمد يحي، اسرائيل وخطوات السيطرة على ساحة الفضاء السيبراني في الشرق الأوسط ، دراسة حول محاور وعمل الدولة العبرية في عصر الانترنت (2002-2013)،

رؤى استراتيجية . على الرابط التالي :

strategicvisions.ecssr.com/ECSSR/ECSSR.../rua03_064.pdf

• الطائرة الاستطلاعية «أيوب» خرقت 7 منظومات من الرادارات وقد تحمل في المرة المقبلة متفجرات ، **جريدة الشرق الأوسط** ، السبت 26 ذو القعدة 1433 هـ 13 اكتوبر 2012 العدد 12373.

• جمال سند السويدي ، عسكريون: تكنولوجيا المعلومات عصب حروب المستقبل ، **مجلة الاتحاد** ، المؤتمر السنوي الثامن عشر ، مركزالامارات للدراسات والبحوث الاستراتيجية، على الرابط الالكتروني التالي:

http://www.alittihad.ae/details.php?id=35263&y=2013&article=ful

• صلاح ابراهيم "استراتيجية الأمن القومي الاسرائيلي" **الفكر الاستراتيجي العربي** ، العدد3 31كانون الثاني 1990.

• قضايا .. الإرهاب الإسرائيلي الإلكتروني: العرب والتجسس الإسرائيلي الإلكتروني، **مجلة الوطن** ، 2015/04/18.على الرابط التالي: http://alwatan.com/details/57008

• أسعد عبد الرحمان، دور المؤسسة العسكرية الاسرائيلية، **مجلة المستقبل** .

almustaqbal.com/stories.aspx?StoryID=31556Oct 31, 2008.

• زهير اندراوس، خطابات نصر الله تُدرّس بالجامعات الإسرائيليّة ، **رأي اليوم** ، على الرابط التالي : HASAN NASRULLAH 03.07.17.jpg555 نقلا عن صحيفة معاريف(العبرية).

• رضوان الذيب، جنرال اميركي: استطعنا التنصت على كل الدول الا حزب الله ، **جريدة الديار**،2013/11/13.

• فايز رشيد ، عقيدة آيزنكوت وتطوير الإستراتيجية العسكرية الإسرائيلية ، **مجلة القدس العربي**، \ 20 \ 08 \ 2015 .

• **وكالة أخبار الشرق الجديد** – الكيان يعيد صياغة عقيدته الامنية د. فايز رشيد

www.neworientnews.com/archive1/news/fullnews.php?news

• محمد المصري النظرية الأمنية الاسرائيلية، **مجلة دنيا الوطن** ، على الرابط الالكتروني التالي:https://www.alwatanvoice.com/arabic/news/2009/07/14/13959 6.hml

• سيف الهرمزي،تحليل هانس مورغانثو لمفهوم القوة وتطبيقها على وحدات النظا م الدولي ، **مجلة تكريت للعلوم السياسية** ، م1، عدد1، السنة158. على الرابط التالي:

cpos.tu.edu.iq/images/cpos/2016/journal/no_one/ pdf

• معمر عطوي ونزار عبود حول "الوحدة 61398» تتَّخِذ من شنغهاي مُنطلقًا لهجماتها"، **صحيفة الأخبار اللبنانيَّة** في 21/ 02/ 2013.

• سعاد محمود أبو ليلة، «دورة القوة: ديناميكيات الانتقال من "الصلبة" إلى "الناعمة" إلى "الافتراضية" »، **مجلة السياسة الدولية**، ملحق اتجاهات نظرية القوة :كيف يمكن فهم تحولات القوة في السياسة الدولية ؟ العدد 188، 2012/16.

• ابراهيم اسماعيل كاخيا ، الحرب الالكترونية ، **مجلة الدفاع العربي** ، قراءة استراتيجية في يوم الاربعاء ، 22 مارش ،على الرابط التالي:

arabdefencejournal.com/article.php?categoryID=9&articleID=552

• الأمن الوطني، **مجلة درع الوطن** ، اعداد هيئة التحرير ،على الرابط الالكتروني التالي:

http://www.nationshield.ae/home/details/files/WMLzSVWGPIU

• حلمي موسى ، "حرب السايبر" تُشغِل إسرائيل: البحث في تحويل "النقمة إلى نعمة"، **صحيفة السفير اللبنانيَّة** في 31/ 01/ 2014، تصفُّح بتاريخ 9/ 04/ 2014). على الموقع الإلكتروني التالي: http:/ / www.assafir.com/ Windows/

• نينا عقل و ندين البلعة خيرالله ، **مجلة الجيش** ، الأمن السيبراني ، العدد 350-351، 2014. على الرابط الالكتروني: https://www.lebarmy.gov.lb/ar/content

• **صحيفة يسرائيل هيوم العبريَّة**، في 1/ 01/ 2013.تَتْبَع هيئة السايبر الوطنيَّة تساهل

• علي دريج ، ماذا تخبئ المقاومة لإسرائيل من مفاجآت بحرية جديدة ، **صحيفة السفير**، العدد11946، الثلاثاء في 26تموز،2011 .

• تموز 2006 ـ 2011 | لقاء جوزف وعماد، **صحيفة الأخبار**، العدد 1459، الثلاثاء12تموز 2011. http://www.al-akhbar.com/node/16471

• زهير اندراوس، حرب الأدمغة بين الشاباك وحزب الله: تحذير جديّ من وجود خلايا نائمة كبيرة وكثيرة في إسرائيل تنتظر الأوامر لتنفيذ العمليات الفدائيّة داخل عمق الدولة العبريّة ، **في مجلة رأي اليوم**، على الرابط التالي:

http://www.raialyoum.com/?p=302271

• علي عواضة ، قادمون: العدو سَيُدَمَّرُ الكترونياً... لدينا يقينٌ في ذلك ، **صحيفة البلد،** الإثنين 29 شباط , 2016 01:30 http://beirutpress.net/article/284332

• **يديعوت احرنوت** – يوآف كيرن – بيرس: "هكذا اقمت المفاعل في ديمونا" – http://www.raialyoum.com/?p=739251 2017\09\07

• قضايا .. الإرهاب الإسرائيلي الإلكتروني: العرب والتجسس الإسرائيلي الإلكتروني، **مجلة الوطن** ، 2015/04/18.على الرابط التالي: http://alwatan.com/details/57008

6- مواقع الانترنت .

• أمان .. رأس الحربة في أجهزة المخابرات الإسرائيلية ، – group73historians.com/.../531ugn hgvhf' أعرف–عدوك––المخابرات– الاسرائيلي، أعرف عدوك – المخابرات الاسرائيليه منذ النشأه وحتي الان – المجموعة 73 مؤرخين.

• أمن الفضاء الالكتروني ، اعداد لجنة الفضاء الالكتروني ، الشركة العامة لخدمات الشبكة الدولية للمعلومات .على الرابط الالكتروني التالي : https://www.scis.gov.iq/upload/upfile/ar/security.doc

• ترجمة عدنان أبو عامر، استراتيجية الجيش الاسرائيلي ، ا عداد الجيش الاسرائيلي، ترجمات الزيتونة 79 ، موقع يديعوت أحرونوت ، أيلول ، 2015.

• صحيفة فلسطين حول الموضوع "الإمكانات الإسرائيليَّة في حرب السايبر"، في 21/ 11/ 2013.على مواقع الانترنت . موقع فلسطين أون لاين الإلكتروني التالي

http:/ / www.felesteen.ps/ prints/ news/ 104454 :

• الجغرافية السياسية لاسرائيل ، موقع غزة لأسرائيل1.doc ، على الرابط الالكتروني التالي : site.iugaza.edu.ps/fjadba/files/2010/02/الجغرافيا–السياسية–

• محمد الطاهر ، خبير ألماني يكشف عما حصل للصواريخ الأمريكية المتجهة إلى "الشعيرات"، موقع ارتي، على الرابط الالكتروني: 06:29 GMT

https://arabic.rt.com/middle_east/872546-صواريخ-توماهوك-حمص-الشعيرات-سقوط-خلل-سوريا-ترامب-الولايات-المتحدة تاريخ النشر: 10.04.2017 |

• تموز 2006: تفاصيل جديدة عن معركة بنت جبيل وأهداف الحرب ،تاريخ النشر: 2015/05/06 - 14:2، موقع المقاومة الاسلامية في لبنان :إسرائيل": طائرة أيوب التي أرسلها حزب الله هي الطائرة رقم 12، https://www.moqawama.org/essaydetails.php?eid=26482&cid

• عبد الجليل المرهون ، " عصر الردع الإلكتروني"، موقع قناة الجزيرة ، 26 تشرين الأول 2012، على الرابط الالكتروني التالي: http://www.aljazeera.net/analysis/pages/7bf0ab16-7011-4e73-b8ee b756385c8a78?GoogleStatID=1#1

• شيرين الضاني، " الأمن القومي ومشروعيته في الإسلا م "، في: شبكة الحوار المتمدن محور الإرها ب، الحرب والسلام ،20 تشرين الأول/ أكتوبر 2010 م ، ع: 3160.

http://www.ahewar.org/debat/show.art.asp?aid=232581

• خليل حسين ، مفهوم الأمن في القانون الدولي العام ، 2009/1/16.على الرابط الالكتروني : http://drkhalilhussein.blogspot.com/2009/01/blog post_16.htm-

• نيكولاس سبيكمان و نظرية الإطار: 1893-1943 المدرسة الأمريكية ...

https://bohoht.blogspot.com/2016/04/1893-1943.htm

• الفضاء الالكتروني واسلحة الدمار الشامل ، مؤتمر الحروب السيبرانية https://seconf.wordpress.com/2015/05/15/الفضـاء-الإلكتروني-وأسلحـة-ال/

• الفضاء الإلكتروني http://www.arabic-military.com/t117864-topic

• محمود فخر الدين، حدودالمجال الخامس ،مايو2015/150 ،على الرابط الالكتروني: https://seconf.wordpress.com/2015/05/15

• جمال سند السويدي ، عسكريون: تكنولوجيا المعلومات عصب حروب المستقبل http://www.alittihad.ae/details.php?id=35263&y=2013&article=ful

• الموقع الإلكتروني للجنة الدوليَّة للصليب الأحمر حول موضوع "What limits does the law of war impose on cyber attacks" في 28/ 06/ 2013 .

• الفضاء الالكتروني وأسلحة الدمار الشامل ، مؤتمر الحروب السيبرانية ، الانتشـار الشـامـل بين ... https://seconf.wordpress.com/2015/05/1http://www.dtic.mil/doctrine/dod_dictionary/data/n/646.htm

• زكريا حسين ،" الأمن القومي"، موقع إسلام أونلاين دوت نت. مفاهيم ومصطلحات،2004.

http://www.islamonline.net/arabic/mafaheem/index.shtml

• الأمن السيبراني، وزارة الاتصالات في جمهورية مصر العربية ،على الرابط الالكتروني:

www.mcit.gov.eg/Ar/TeleCommunications/Cyber_Security

• طارق المجذوب، السَّايْبِر ساحة "خَفِيَّة" لحربٍ "ناعِمَة" قادِمة! | الموقع الرسمي للجيش

https://www.lebarmy.gov.lb/ar/.../السَّايْبِر-ساحة-خَفِيَّة-لحربٍ-ناعِمَة-قاد

• محمد مدحت محمد، الحكومة الالكترونية ، المجموعة العربية للتدريب والنشر ،2016، على الرابط التالي:

https://books.google.com.lb/books?isbn=9796500185453

• موقع الهيئة المُنظِّمة للاتصالات في لبنان حول "لمحة عامة حول الأمن السيبراني"، على الموقع الإلكتروني التالي: http:/ / www.tra.gov.lb/ Cybersecurity-AR

• كيف سيكون شكل الحرب الإلكترونيَّة الحقيقيَّة؟"، 17/ 09/ 2013. على الموقع الإلكتروني الآتي: http:/ / www.slabnews.com/ article/ 38744

• روسيا تُنشئ وحدات للحرب "السيبرانيَّة" بحلول العام 2017"، اليوم السابع، 30/ 01/ 2014. http:/ / www.youm7.com/ News.asp?NewsID=1481858

http://www.internetlivestats.com/internet-users

• محمد فخر الدين، حدود المجال الخامس – ما هى الحروب السيبرانية ؟،على الرابط الالكتروني التالي: https://seconf.wordpress.com/2015/05/15

• defense-arab.com › ... › قسم القوات الجوية AIR FORCE › الـدفاع الجوي Air defence، 2015/11/8

• يحيى اليحياوي ، " حرب المعلومات "، موقع الكاتب يحيى اليحياوي على شبكة الإنترنيت، 13 كانون الأو ل ، 2010، على الموقع الالكتروني التالي: http://www.elyahyaoui.org/medias_war.htm

• الحرب الالكترونية و أخر تطوراتها على الساحة الدولية ,

http://muha-hacker.blogspot.com/2012/01/blog-post.html

https://www.facebook.com/realestateKhal/posts/597750626955720

• التجسس الإلكتروني.. تخصص إسرائيلي بامتياز، موقع الجزيرة الالكتروني.

www.aljazeera.net/.../التجسس-الإلكتروني-تخصص-إسرائيلي-بام.

• حادي عشر: تكنولوجيا الإتصال والإعلام حولت الحرب النفسية الى ناعمة

https://www.almaaref.org/books/...fe...alharb.../lesson11.htm

• مقابلة مع "أسانج": www.it-scoop.com/2011/05/facebook-spying-machine-assange-wikileaks

• منيرة الحوشاني، الفضائيات بين الايجابيات والسلبيات ، شبكة الألوكة الثقافية ،2012/5/23،على الرابط التالي: http://www.alukah.net/culture/0/412

• زهير حمداني، الاختراقات الروسية لواشنطن وظلال الحرب الباردة ،2017/3/16.

www.aljazeera.net/news/.../2017/.../الاختراقات-الروسية-لواشنطن-وظلال-الحرب-الباردة.

• الجزيرة نت ،2012/11/29.

• وثيقة"أيزنكوت" منشورة على الرابط الإلكتروني:

http://www.idf.il/SIP_STORAGE/FILES/9/16919.pdf

• عدنان أبو عامر ، "البحث العلمي في إسرائيل وصنا عة القرا ر"، في: موقع قناة الجزيرة على شبكة الإنترنيت، 22 يوليو/تموز 2012م.على الرابط التالي:

http://www.aljazeera.net/analysis/pages/b8556851-0a25-

• خليل حسين، " الصراع الإلكتروني العربي – الإسرائيلي "، في: موقع مركز دراسات الخليج (دار الخليج) على شبكة الإنترنيت، 23 كانون الثاني / يناير 2012 م.

http://www.alkhaleej.ae/portal/178a5781-4897-4350-b457-

fd919d8fdfcc.aspx

• محمد بدير، نصرالله يتكلم، موقع صحيفة الأخبار الالكتروني

http://www-akhbar.com/ar/node/40216.al:

• محمد عبدالله ، النص الكامل للمؤتمر الصحافي للسيد نصرالله: قرائن ومعطيات.. 2010\8\10 قناة المنار

http://khiyam.com/news/article.php?articleID=97303563

http://www.rtv.gov.sy/index.php?p=13&id=63266

• السيد حسن نصرالله يكشف صوراً ووثائق تؤكد تورط اسرائيل باغتيال ...

www.alarab.com/Article/320186

• "مرصاد 1" تحلّق فوق عكا و18 مستوطنة ، saidacity.net/news/2783

• عباس الزين، الـ«ياخونت»... أدنى مفاجآت المقاومة!، موقع المردة.

html /elmarada.org/146316/ا

• حزب الله يستمع الينا"، شبكة المعلومات السورية القومية الاجتماعية ، على الرابط التالي:

http://www.ssnp.info/index.php?article=55676

• الرواية الاسرائيلية التفصيلية لهزيمة الجيش الاسرائيلى فى مارون الراس ،الجمعة, 29 يونيو

http://www.estqlal.com/article.php?id=10208. 2007

• الدرس الخامس:عملية الوعد الصادق

hg,ualmaaref.org/books/contentsimages/books/...ashhor.../lesson5.

• العدو يخسر مجدداً في حرب الادمغة .. و إسرائيل "تعترف" :

http://www.mounahada.org/modules.php?namepart=news_and_bay

anat&number=1111

• حرب الكترونية طاحنة بين حزب الله و اسرائيل : هل استطاع حزب الله من اختراق "الام

كا " http://defense-arab.com/vb/threads/47617

7- الدراسات باللغة الأجنبية.

• **Departement of Defense**,"Defense Strategique Guidance",Washington ,D.C.,Jan.2012.

• **U S Joint Chlefs of Staff** ,"Gen.Dempsey s Remarks at Kansas State University s landon lecture series ,"General Martin E. Dempsey,octobre 1,2012(http://www.jcs.mil/speech.aspx?id=1731).

• Joseph S. Nye, Jr. “Cyber Power,” **Harvard Kennedy School (Cambridge**: Belfer Center, May 2010.

• William H. McNeill, The Pursuit of Power: Technology, Armed Force, and Society since A.D. 1000 Chicago: **University of Chicago** Press, 1982.

• Shmuel Even and David Siman-Tov, Cyber Warfare:Concepts and Strategic Trends,**INSS-Institute for National Security Studies** Memorandum No. 117, May 2012,p.75. on website: https://www.files.ethz.ch/isn/152953/INSS%20Memorandum_MAY2012_Nr117.pdf.

• Pierre Caron, LA GUERRE ELECTRONIQUE N’AURA PAS LIEU, assossiation ege. on the

websitebdc.aege.fr/public/La_guerre_electronique_n_aura_pas_lieu.pdf.

• Sabrine Saad, Asymmetric Cyber-warfare between Israel and Hezbollah, **Saint-Joseph University**, Beirut, Lebanon.

• Gil Baram ,"The Effect of Cyber war Technologies on Force Buildup: The Israeli Case" , **Military and Strategic Affairs**, Vol. 5, No. 1 , 2013.

• Gabi Siboni, "Protecting Critical Assets and Infrastructures from Cyber Attacks," **Military and Strategic Affairs 3**, no. 1 (2011): 96, at http://www.inss.org.il/ upload/(FILE)1308129638.pdf.

• Joseph s.Nye,"cyber power"**Harvard kennedy school**,belfer center for science and internationalaffaires ,May 2010 . on the website http://www.dtic.mil/doctrine/dod_dictionary/data/n/646.html

http:/belfercenter.ksg:Harvard.edu/files/cyber-power.pdf

• Marc Lynch et al., "Syria's Socially Mediated Civil War," Blogs and Bullets III (Washington DC, United States Institute of Peace, 2014).

8- المجلات باللغة الأجنبية:

• Anita R. Gohdes, “Pulling the Plug: Network Disruptions and Violence in Civil Conflict,” **Journal of Peace Research 52**, No. 3

• Joseph S. Nye, J, "Soft Power", **Foreign Policy**, No. 80, Twentieth Anniversary (Autumn, 1990), Published by: Washingtonpost.Newsweek Interactive, LLC, Article DOI: 10.2307/1148580, Article Stable URL: http://www.jstor.org/stable/1148580

• Israel’s Secret Iran Attack Plan: Electronic Warfare- **daily beast**, Nov 16, 2011 6:28 PM EST - http://www.thedailybeast.com/articles/2011/11/16/israel-s-secret-iran-attack-plan-electronic-warfare.html

• Iran Blocks American ‘Virtual Embassy,**the new York times**, December 7,2011. http://thelede.blogs.nytimes.com/2011/12/07/iran-blocks-american-virtual-embassy.

• Brendan I. Koerner,“Inside the New Arms Race to Control Bandwidth on the Battlefield,” **Wired Magazine**. 18 February 2014 ,Accessed 14 December 2015, http://www.wired.com/2014/02/spectrumwarfare.

• David Makovsky. 'The Silent Strike: How Israel bombed a Syrian nuclear installation and kept it secret,' **The New Yorker**, 17 September 2012. http://www.newyorker.com/magazine/2012/09/17/the-silent-strike

• an interview by Steve Forbes of **Forbes Magazin**e, with George Gilder,a well known American expert on IT and the economy, February 16, 2011: on website:

http://www.forbes.com/2011/02/11/gilder-nanotechnologyfiber optics-intelligent-investing-video.html

• John Reed,Unit 8200: Israel's cyber spy agency, **Financial Times** [London (UK)] 11 July 2015: 16

9- مواقع الانترنت :

• Silent war,vanity fair,july2013.

)http://www.vanityfair.com/culture/2013/07/new- cyberwar-victims-**american-business** .

• Dictionnaire.cordial-enligne.Fr/definition/cyberguerre

• Israel's Secret Iran Attack Plan: Electronic Warfare- Nov 16, 2011 6:28 PM EST - http://www.**thedailybeast**.com>

• Joint Doctrine for Electronic Warfare, Joint Publication 3-51, le 7 avril 2000. [TCO] www.iwar.org.uk/iwar/resources/ew/jp3-51.pdf

• U.S. launches 'virtual' embassy for Iran, us today, 12/6/2011.

• http://www.usatoday.com/news/washington/story/2011-12-06/us-embassy-iran/51673966/1

• Gen Patrick Brady, The Role of Media in War, 1990,on website: http://www.defencejournal.com/2000/aug/role-media-war.htm

• TEHILA website, www.tehila.gov.il

• Israel Government Information Security website, www.cert.gov.il-

خطابات

– خطاب الأمين العام لحزب الله عند الاحتفال باسترجاع الأسرى المحررين وسمير القنطار في 16 تموز 2008.

–خطاب الأمين العام لحزب الله خلال مراسم الاحتفال السنوي الذي أقامه الحزب بمناسبة يوم الشهيد في الحادي عشر من شهر تشرين الثاني/نوفمبر من العام 2004،في الضاحية الجنوبية لبيروت.