وزارة التعليم العالي والبحث العلمي

جامعة العربي التبسي -تبسة-

كلية الحقوق والعلوم السياسية

قسم العلوم السياسية

الإستراتيجية الأمنية الإسرائيلية في مواجهة التهديدات السيبرانية

مذكرة مكملة لنيل شهادة الماستر في العلوم السياسية

- تخصص دراسات إستراتيجية -

إعداد الطالبتين:

- صنية قحايرية
- منية قحايرية

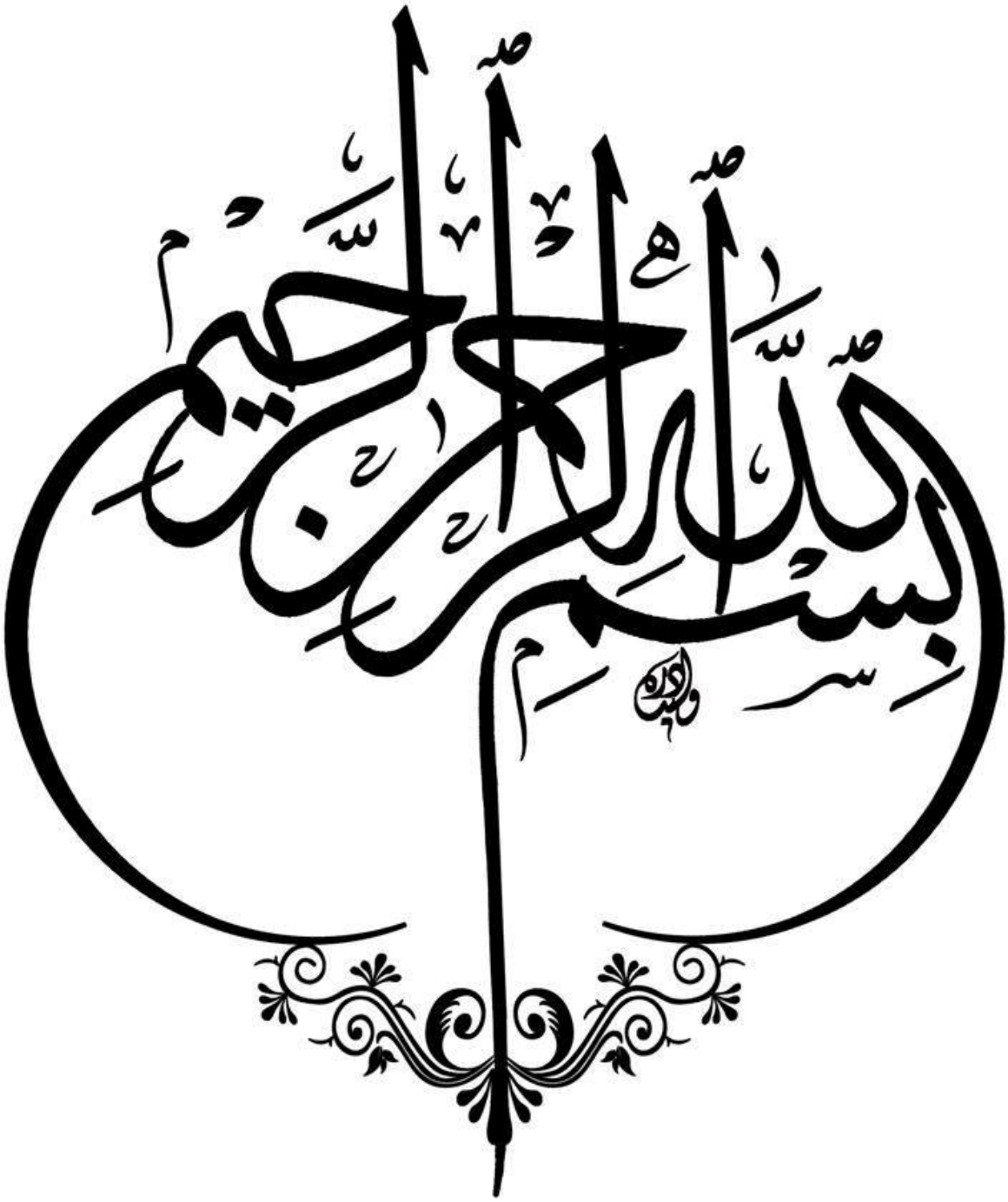
إشراف الأستاذ:

باديس بن حدة

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة
يوسف أزروال	أستاذ محاضر (ب)	رئيسا
باديس بن حدة	أستاذ مساعد (أ)	مشرفا ومقررا
أمين البار	أستاذ محاضر (ب)	عضوا مناقشا

السنة الجامعية 2018/2017


بسم الله الرحمن الرحيم

شكر وتقدير

"كن عالما...فإن لم تستطع فكن متعلما، فإن لم تستطع فأحب العلماء، فإن لم تستطع فلا تبغضهم "

الحمد لله الذي أنار لنا درب العلم والمعرفة وأعاننا على أداء هذا الواجب ووفقنا إلى انجاز هذه المذكرة التي لم تكن لترى النور لولا توفيق الله سبحانه وتعالى .

نتقدم بأسمى عبارات الشكر والتقدير لكل من ساعدنا على إبراز هذا الجهد.

نخص بالذكر الأستاذ باديس بن حدة رئيس قسم العلوم السياسية الذي تفضل بقبول الإشراف على هذه المذكرة وذلك بكثير من التشجيع والحرص على إتمام العمل واتقانه ومدى رحابة صدره وتحمله الإشراف على المذكرة حتى نهايتها، ولم يبخل علينا بنصائحه وتوجيهاته القيمة التي كانت عونا لنا في إتمام هذا العمل .

إلى من علمونا حروفا من ذهب وكلمات من نور وعبارات من أسمى وأحلى كلام في العلم،

إلى من صاغوا لنا علمهم حروفا ومن فكرهم منارة تنير لنا سيرة العلم والنجاح .

إلى من وقفوا على المنابر وأعطوا لنا من حصيلة فكرهم لينيروا دربنا .

نتقدم بالشكر إلى كل أساتذتنا في قسم العلوم السياسية لجامعة تبسة الذين نفتخر بهم لكوننا تكونا على أيديهم في سبيل تشجيع العلم والمعرفة فلهم منا جميعا جزيل الشكر والعرفان والتقدير.

نتوجه بجزيل الشكر والامتنان إلى كل من ساعدنا من قريب أو من بعيد على انجاز هذا العمل، وفي تذليل ما واجهناه من صعوبات .

صنية ومنية

ملخص الدراسة

تسعى هذه الدراسة إلى تسليط الضوء على التهديدات السيبرانية التي تتعرض لها إسرائيل من مصادر مختلفة، فرغم ما تتمتع به إسرائيل من مقومات تكنولوجية واستخباراتية متطورة ومعدات رقمية ومعلوماتية ذات قدرات عالية علاوة على الدعم الذي تتلقاه من كبريات دول العالم الصناعية والإلكترونية خاصة الولايات المتحدة الأمريكية، إلا أن ذلك لم يمنع من تعرض إسرائيل للهجمات والاختراقات الإلكترونية أثر ذلك على مختلف قطاعاتها وأبرز مؤسساتها نظرا لاعتمادها على منظومة إلكترونية في إدارة منشآتها الحيوية.

لذلك اتخذت إسرائيل اجراءاتها وعززت بذلك من إمكانياتها الإلكترونية والتقنية لمواجهة هذه التهديدات والتي تتصاعد وتيرتها من حين إلى آخر.

ويمكن الإشارة في إطار الاستعدادات التي تتخذها إسرائيل لحماية فضاءها السيبراني إلى اعتماد إستراتيجية دفاعية كإنشاء هيئات ووحدات وطنية لحماية المعلومات، التنسيق بين الجهات الحكومية وتشجيع وتطوير شركات إسرائيلية مختصة في الدفاع عن الفضاء الإلكتروني، والتعاون الدائم بين القطاع الحكومي والقطاع الأمني والقطاع الخاص إضافة إلى تعزيز دور المؤسسة العسكرية.

كما بادرت إسرائيل إلى بلورة وتفعيل إستراتيجية هجومية من خلال القدرة على الرد المباشر ضد كل من يهاجم الفضاء الإلكتروني الإسرائيلي.

Résumé de l'Etude

La présente étude vise à jeter la lumière sur les menaces cybernétiques dirigées contre Israël par les différentes sources en dépit des moyens utilisés par Israël tels que les supports technologiques et informatiques développés, ainsi que les matériels numériques de haute capacité et malgré le soutien qu'Israël reçoit de la part des grands pays industriels et électroniques notamment les Etat Unis d'Amérique, ce pays demeure exposé aux attaques et aux percées électroniques à la suite desquelles un grand dommage a affecté les différents secteurs et les plus importantes institutions en raison de leur dépendance totale du système électronique dans la gestion de leur entreprises vitales.

Cette situation a poussé Israël à prendre les mesures qui s'imposent et à renforcer ses capacités électroniques et techniques pour faire face à ces menaces qui se multiplient.

Il ya lieu de préciser que dans le cadre des préparatifs réalisés par Israël dans le but de protéger son espace cybernétique, des stratégies défensives sont élaborées telle que la création d'organes et d'unités nationales pour sauvegarder les informations, et assurer une coordination entre les organismes du gouvernement et encourager et développer des sociétés spécialisées dans la défense de l'espace électronique et mener une coopération permanente entre le secteur sécuritaire ainsi que le secteur privé, ceci en plus du renforcement du rôle des institutions militaires, Israël a également pris l'initiative de concevoir une stratégie offensive par le biais de la capacité à répondre directement contre toute attaque de son espace électronique.

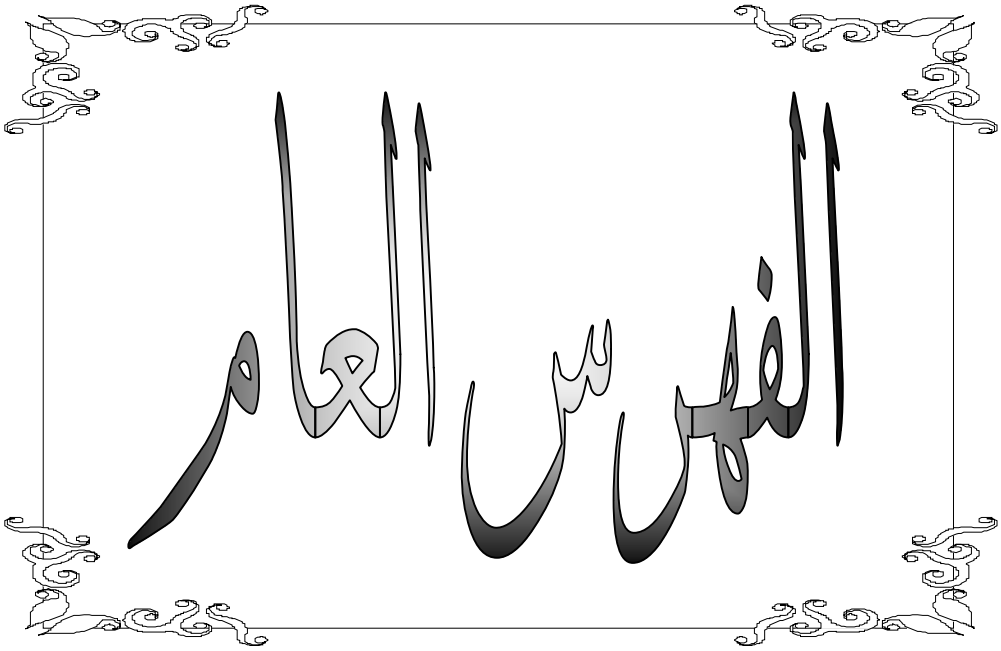
Summary of the Study

The present study aims to shed light on the cybernetic threats undergone by Israel from different sources, indeed in spite of the ability of Israel in the fields of modern technology, developed intelligence, numeric and data with high value and in spite of what it gets as support from the greatest industrial and electronic countries mainly USA, however, that does not save Israel from attacks and electronic breakthrough which affects the different sectors such as its institutions owing to its dependence on the electronic system in the management of vital enterprises.

For this reason, Israel has taken efficient measures and reinforced its capacities in the field of electronics and techniques so as to face those threats which are increasing from time to time.

It is worthwhile to mention that in the field of the preparation and readiness taken by Israel so as to protect its cybernetic space; several defensive strategies are adopted such as the creation of organs and national units to save information and to coordinate efforts of the different governmental organs and to encourage and develop Israeli companies which will specialize in defense of the electronic space and to set up a permanent cooperation among the governmental sector and the security one. This is in addition to reinforcing the role of the military institutions.

Israel has also taken an initiative aiming at crystallize and to update an offensive strategy through its capacity to respond immediately to any attack against the Israeli electronic space.


الفهرس العام

الفهرس العام

مقدمة

مقدمة

من بين التغيرات التي شهدها النظام الدولي بعد نهاية الحرب الباردة التحول على مستوى المفاهيم ويأتي في مقدمتها مفهوم الأمن الذي تغير مضمونه من الطابع العسكري التقليدي إلى الطابع الشامل المتعدد المضامين وقد إنعكس ذلك على التغير في طبيعة التهديدات الأمنية التي لم تعد تقتصر على تهديد دولة لدولة أخرى، بل أصبح العالم يتعرض لمخاطر وتهديدات جديدة لا حدود لها تتجاوز المسائل السيادية ولا يمكن التحكم فيها بسهولة أصبحت تمس كل قطاعات الأمن مثل: القطاعات الاقتصادية، الاجتماعية، السياسية والبيئية وحتى التكنولوجية، وأعيد بذلك النظر في الافتراضات الأساسية للأمن الأمر الذي يتطلب معالجة شاملة تتجاوز المقاربة التقليدية والتي تركز على قدرة الدولة في مواجهة أي خطر خارجي في بعده العسكري التقليدي.

كما لا يخفى علينا الثورة في مجال التنظير، حيث لعبت المقاربات النظرية دورا مهما في تفسير الأمن والتهديدات الأمنية وذلك بفضل الاختلاف والجدل في محاولة منهم اعطاء تفسير شامل لها.

وتعاطيا مع الاختلاف والتنوع في طبيعة التهديدات الأمنية تبرز لنا التهديدات السيبرانية لتأخذ بعدا إقليميا ودوليا، خاصة بعد اتجاه العديد من دول العالم إلى الاعتماد على التكنولوجيا الإلكترونية والرقمية في إدارة وتسيير منشآتها الحيوية ومؤسساتها بشكل جعلها تدخلها ضمن حساباتها الإستراتيجية وأمنها القومي، لكن بالرغم من المميزات التي تقدمها هذه الأخيرة إلا أن الدول أصبحت عرضة للعديد من الاختراقات والهجمات الإلكترونية والتي تهدد بذلك أمنها وقطاعاتها الحساسة، الأمر الذي جعل هذه الدول تعيد قراءة العديد من حساباتها وتحاول تكييف إستراتيجياتها وفقا للتغيرات الحاصلة حتى تستطيع الحفاظ على أمنها القومي أوالتقليل من حجم الخسائر المترتبة عن مثل هذه التهديدات المتفاقمة.

وتعتبر إسرائيل من الدول الرائدة في المجال التكنولوجي والإلكتروني فهي تعمد إلى أن تكون مصدرة لهذا العمل التقني، وبذلك منحت اهتماما كبيرا للصناعات التكنولوجية منذ خمسينيات القرن الماضي وأدخلتها ضمن عقيدتها الأمنية، وقد شهد العقد الأخير العديد من الخطوات الإسرائيلية لادراج الأمن السيبراني ضمن أولوياتها مستخدمة في ذلك تقدمها التكنولوجي والتقني واسهاماتها العالمية في صناعة البرمجيات ونظم الحماية السيبرانية وقد عملت على تكثيف الاهتمام بهذا المجال.

رغم ذلك تشكل التهديدات السيبرانية خطرا يهدد الأمن القومي الإسرائيلي باعتبارها من أكثر الدول عرضة لمثل هذه التهديدات سواء على المستوى الاقليمي أوحتى الدولي من أطراف مختلفة تتراوح بين دول

ومجموعات وحتى أفراد، على هذا الأساس كان لزاما على إسرائيل وضع إستراتيجيات وآليات لمواجهة ما يهدد أمنها السيبراني والسعي نحو الريادة العالمية.

أهمية الموضوع

تنبع أهمية هذا الموضوع من اعتبارات علمية وأخرى عملية يمكن تلخيصها في مايلي:

1- الأهمية العلمية

- يمثل هذا الموضوع أحد أبرز مواضيع الساعة فالتهديدات السيبرانية أصبحت تحتل صدارة اهتمامات الباحثين والمختصين، ويعد موضوع الأمن السيبراني وإستراتيجيات مواجهة التهديدات السيبرانية من المواضيع الهامة في العلوم السياسية.

- البحث في الأطر النظرية والأساليب والآليات التي تتخذها إسرائيل لحماية فضاءها السيبراني من جهة ومن جهة أخرى تأثير التهديدات السيبرانية على الأمن الإسرائيلي.

- بناء تراكم معرفي حول التهديدات السيبرانية ومصادرها المختلفة ومعرفة وتحليل إستراتيجيات مواجهتها.

2- الأهمية العملية

- الوقوف عند أهم الاختراقات التي تعرضت لها إسرائيل في مجال أمنها السيبراني.

- التقرب من معرفة الإستراتيجية الإسرائيلية الخاصة بمجابهة التهديدات السيبرانية المتعددة.

3-أسباب اختيار الموضوع

هناك العديد من الأسباب التي تبرر اختيار موضوع ما، وموضوع التهديدات السيبرانية من المواضيع الهامة التي أصبحت محل نقاش على مستويات عالمية، فلم يعد التهديد مقتصرا على الجانب العسكري فقط بل تعداه إلى قطاعات أخرى، لذلك فاختيار هذا الموضوع جاء نتيجة عدة عوامل مختلفة يتمثل أبرزها فيمايلي:

أ-الأسباب الذاتية

-ميول الباحث المعرفي إلى دراسة هذا الموضوع ولاسيما أنه من المواضيع المطروحة بقوة جلبت اهتمام الأوساط الرسمية وغير الرسمية.

- اهتمام الباحث بهذا النوع من الدراسات بحكم التخصص.

- محاولة اكتساب رصيد معرفي ونظري أكثر حول موضوع الأمن السيبراني ومهدداته، ومعرفة الآليات والوسائل التي اتخذتها إسرائيل لمواجهة هذه التهديدات.

– الرغبة في تقديم إضافة معرفية لباحثين آخرين حول موضوع التهديدات التي تؤثر على الأمن في مجال الفضاء السيبراني.

ب– الأسباب الموضوعية

– التعرف على أهم المضامين المفاهيمية المتعلقة بالأمن السيبراني والتهديدات السيبرانية ومصادرها المختلفة.

– تَعتبر إسرائيل نفسها محاطة بدول معادية لذلك يحاول الباحث فهم الأسباب والدوافع التي جعلت إسرائيل أكثر الدول التي تتعرض إلى هجمات إلكترونية مما جعلها تفرز تحديات و مخاطر مست أمنها السيبراني.

– البعد العام والإستراتيجي للموضوع بحيث أصبح محل اهتمام وانشغال الدول لاسيما الدول الكبرى في مجال الأمن السيبراني.

3–حدود الدراسة

أ–الحدود الموضوعية

تحاول هذه الدراسة القاء الضوء على التهديدات السيبرانية، حيث تبحث في أبعادها ومصادرها وتداعياتها على الأمن القومي الإسرائيلي ومن ثم التطرق إلى أبرز إستراتيجيات المواجهة.

ب–الحدود الزمانية

فيما يتعلق بالإستراتيجيات التي انتهجتها إسرائيل للدفاع عن أمنها السيبراني، بدأت منذ تسعينيات القرن الماضي من خلال القرارات والمبادرات التي اتخذتها الحكومة الإسرائيلية والتي تتعلق بوسائل الدفاع لصد الهجمات السيبرانية، وقد عرفت إسرائيل حملات واسعة من الهجمات الإلكترونية والاختراقات ضدها منذ سنة 2000م لكن هذه الهجمات بلغت ذروتها منذ الحرب على غزة في سنة 2009م إلى يومنا هذا.

ج–الحدود المكانية

ينحصر مجال الدراسة في إسرائيل باعتبار أنها تقع في منطقة الشرق الأوسط التي تشهد توتر وصراعا بين إسرائيل ودول وأطراف تعتبرها معادية لها، لذلك تواجه إسرائيل العديد من التهديدات السيبرانية على المستوى الداخلي والخارجي تهدد أمنها القومي.

4-إشكالية الدراسة

على ضوء ما تم تناوله من خلال التقديم يحاول الموضوع الإجابة عن سؤال مركزي ورئيسي والذي تمت صياغته كمايلي:

إلى أي مدى يمكن للإستراتيجية الأمنية الإسرائيلية النجاح في التصدي للتهديدات السيبرانية التي تواجهها في ظل المقاربة الإسرائيلية للحفاظ على أمنها القومي؟

ولتفكيك هذه الإشكالية وتبسيطها يمكن طرح الأسئلة الفرعية التالية:

السؤال الأول: ماهي أبرز المضامين الإيتمولوجية والنظرية المناسبة لدراسة الأمن السيبراني والتهديدات السيبرانية؟.

السؤال الثاني: ما هي أهم مقومات الفضاء السيبراني الإسرائيلي ؟.

السؤال الثالث:كيف تؤثر التهديدات السيبرانية على الأمن القومي الإسرائيلي؟.

السؤال الرابع: فيما تتمثل أهم الإستراتيجيات التي اعتمدتها إسرائيل في مجابهة التهديدات السيبرانية؟.

انطلاقا من الإشكالية المطروحة والتساؤلات الفرعية تم صياغة الفرضيات التالية:

أ-الفرضية المركزية

كلما زاد خطر وحِدة التهديدات السيبرانية على الأمن القومي الإسرائيلي كلما أدى ذلك إلى اتخاذ إستراتيجيات ناجحة لمواجهتها.

ب-الفرضيات الفرعية

الفرضية الأولى: إحاطة إسرائيل بدول وأطراف معادية لها أدى إلى اتساع دائرة التهديدات السيبرانية ضدها.

الفرضية الثانية: استفحال التهديدات السيبرانية وتعدد مصادرها يؤثر سلبا على الأمن القومي الإسرائيلي.

الفرضية الثالثة: كلما كان هناك تعاون وتنسيق على المستوى المحلي والدولي في مجال الأمن السيبراني كلما ساهم ذلك في التصدي لخطر التهديدات السيبرانية على إسرائيل.

الفرضية الرابعة: تزايد حِدة التهديدات السيبرانية وتصاعد وتيرتها يؤثر سلبا على فعالية ونجاح الإستراتيجية الأمنية الإسرائيلية المنتهجة.

5- الدراسات السابقة

انطلاقا من كون أن العودة إلى الأدبيات السابقة يهدف إلى الكشف عن الدراسات العلمية التي تتقاطع مع هذا الموضوع، فإنه يمكن رصد مجموعة من الدراسات في هذا المجال:

- **الدراسة الأولى:** قام بها المؤلف حسنين شفيق جاءت على شكل كتاب بعنوان:"الإعلام الجديد والجرائم الإلكترونية..التسريبات..التجسس..الإرهاب الإلكتروني"، عن دار فكر وفن، 2015م.

تطرق فيها الكاتب إلى الثورة المعلوماتية من زاوية الجانب السلبي والمتعلق بالجرائم المعلوماتية وتأثيرها على مكونات المجتمع.

كما تناول هذا الكتاب جرائم الإعلام الجديدة ممثلة في جرائم تسريب المعلومات عبر الانترنت وجرائم شبكات التواصل الاجتماعي، وغيرها من الجرائم الإلكترونية بأشكالها المختلفة .

وخلصت الدراسة إلى ضرورة تقنين قواعد جديدة لمكافحة الجرائم الإلكترونية مع الأخذ بعين الاعتبار الطبيعة الخاصة لهذه الجرائم.

- **الدراسة الثانية:** قام بها الكاتب فيصل محمد عبد الغفار جاءت على شكل كتاب بعنوان:"الحرب الإلكترونية" عن دار الجنادرية للنشر والتوزيع، 2016م.

اعتبر فيها الكاتب أن ظهور ثورة تكنولوجيا الإلكترونيات واستخدامها في الأغراض العسكرية يعد نقطة تحول كبيرة، سواء في فن الحرب أوفي إدارة الصراع المسلح ويضيف أن أسلحة القتال الحديثة ووسائله قد اتخذت مكان الصدارة في حسم أي صراع مسلح وخاصة أسلحة الهجوم الجوي الحديثة لاعتمادها على نظم السيطرة

والتوجيه الإلكتروني،كما تطرق الكاتب إلى مفهوم الحرب الإلكترونية وأهدافها ومراحل تطورها.

- **الدراسة الثالثة:** دراسة قام بها محمود محارب في مراجعة لكتاب "حرب الفضاء الإلكتروني: اتجاهات وتأثيرات على إسرائيل" للمؤلفين "شموئيل إيفن"و"دافيد لن سيمان"، صادرة عن المركز العربي للأبحاث ودراسة السياسات 2011م.

قدم المؤلفان في هذا الكتاب إطارا مفاهيميا للفضاء الإلكتروني والمجال الأمني، وسلطا الضوء على أهم العمليات الهجومية البارزة في الفضاء الإلكتروني.

وخلصت الدراسة إلى اعتبار الفضاء الإلكتروني مجال حيوي بالنسبة لأمن إسرائيل ولذلك يتوجب عليها اتخاذ كافة التدابير والإستراتيجيات لحماية فضاءها الإلكتروني والدفاع عنه.

– **الدراسة الرابعة:** قام بها الطالب وليد غسان سعيد جلعود جاءت في شكل مذكرة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية السياسية بعنوان:"دور الحرب الإلكترونية في الصراع العربي الإسرائيلي"، حيث طرح إشكالية:ماهو دور وتأثير الحرب الإلكترونية في الصراع العربي الإسرائيلي؟.

خلصت الدراسة إلى أن التطورات التقنية والإلكترونية الحديثة كالانترنت ووسائل التواصل والاتصال الحديثة وصفحات المواقع الاجتماعية، قد تحولت إلى أسلحة إلكترونية جندتها العديد من الدول لتخوض بها غمار حروبها الرقمية والمعلوماتية.

وكان للصراع العربي الإسرائيلي وقعه الخاص في ظل هذه التغيرات الرقمية والمعلوماتية، وذلك عبر منظومة إلكترونية تقنية تمتلكها إسرائيل وتجيد استخدامها في مقابل ضعف المنظومة الإلكترونية العربية، لكن هذه الأخيرة بدأت تشهد صحوة توعوية وتنموية نتيجة لتصاعد الحركات التوعية في العالم العربي.

– **الدراسة الخامسة:** قدم هذه الدراسة الباحث ربيع محمد يحي حول استعدادات ومحاور عمل إسرائيل في عصر الانترنت (2002م-2013م) بعنوان:"إسرائيل وخطوات الهيمنة على ساحة الفضاء الإلكتروني في الشرق الأوسط".

يوضح الباحث في هذه الدراسة مدى اهتمام إسرائيل بمجال التكنولوجيا المعلوماتية والإلكترونية وسعيها الدائم إلى الاحتفاظ بميزة التفوق النوعي على دول المنطقة، حيث شهد العقد الأخير العديد من الخطوات الإسرائيلية ليكون مجال الفضاء السيبراني ضمن أدوات الحرب المستقبلية مستخدمة في ذلك تقدمها التكنولوجي واسهاماتها العالمية في صناعة البرمجيات ونظم الحماية السيبرانية.

– **الدراسة السادسة:** قام بها المؤلف "Deborah Hossen Couriel" بعنوان " National Cyber Security Organization :Israel" أي المنظمة الوطنية للأمن السيبراني الإسرائيلي، تطرقت هذه الدراسة إلى المكانة التي توليها إسرائيل لقطاع تكنولوجيا المعلومات والاتصالات والدعم الذي تقدمه الحكومة لمراكز البحث العلمي وحجم الميزانية التي تخصصها لذلك، كما ركزت على حجم الاستثمارات الأجنبية في هذا القطاع وسلطت الضوء على نسبة مستخدمي الانترنت في المجتمع الإسرائيلي حيث ترى بأن هذه النسبة في تزايد مستمر.

6- صعوبات الدراسة

يمكن إجمال الصعوبات التي اعترضت الباحث في هذه الدراسة فيمايلي:

- اتسام إسرائيل بصعوبة الإفصاح عن المعلومات التي تخص أمنها السيبراني، أدى إلى نقص المادة العلمية فيما يخص الهجمات التي يتعرض لها فضائها الإلكتروني والتكتم عن حجم الخسائر التي تتكبدها جراء هذه الهجمات.

- كما أن حداثة الموضوع تجعلنا نجد صعوبة في إيجاد معلومات أكاديمية، يضاف إلى ذلك إحجام الكتاب العرب على دراسة هذا الموضوع جعلنا نستعين بترجمة العديد من المراجع الأجنبية باللغتين الإنجليزية والفرنسية.

- وجود عدد كبير من المواقع الإلكترونية لاتتمتع بالمصداقية، ويصعب تحديد المصادر التي أستيقت منها معلوماتها.

7- المناهج المعتمدة

نظرا لطبيعة الموضوع والجوانب التي يشتمل عليها وجب اعتماد المناهج التالية:

أ- المنهج الوصفي التحليلي

يستخدم هذا المنهج بصفة عامة في العلوم الاجتماعية والعلوم السياسية بصفة خاصة،حيث يتم من خلاله تحديد خصائص وأبعاد الظاهرة المدروسة ووصفها وصفا موضوعيا من خلال جمع الحقائق والبيانات وعلى استخدام أدوات وتقنيات البحث العلمي.

وقد تم الاعتماد عليه بشكل كبير في هذه الدراسة من خلال تحديد مفهوم الإستراتيجية ومفهوم الأمن السيبراني والتهديدات السيبرانية وغيرها.

ب-المنهج التاريخي

يركز المنهج التاريخي على دراسة أحداث وظواهر تمت في الماضي ومازالت تحدث في الحاضر، ليقوم بتحليل وتفسير بيانات ومعلومات ونتائج الدراسات الخاصة بهذه الأحداث والظواهر وذلك بتحديد التغيرات والتطورات التي تعرضت لها وتحديد العوامل والأسباب المسؤولة عن هذه الظواهر والتي منحتها صورتها الحالية، ويتم ذلك بدراسة نتائج البحوث السابقة أوالرجوع إلى بيانات ومعلومات سابقة عن هذه الأحداث، لذلك تم الاعتماد على المنهج التاريخي لدراسة نشأة وتطور العقيدة الأمنية الإسرائيلية ومراحل تطور قطاع أمن المعلومات الإسرائيلي.

ج- منهج دراسة الحالة

يقوم منهج دراسة الحالة بدراسة الظاهرة بشكل معمق وذلك بجمع بيانات ومعلومات شاملة ومفصلة عنها بهدف الوصول إلى فهم أعمق للظاهرة المدروسة أوما يماثلها من أحداث، وذلك بجمع المعلومات والبيانات عن الوضع الحالي والماضي لفهم أعمق وتفسير أفضل للأسباب وكشف الحقائق والمعلومات التفصيلية الدقيقة عن الظاهرة المدروسة، ولذلك تم الاعتماد عليه في هذه الدراسة من خلال استقصاء مجموعة من التفاصيل والبيانات حول التهديدات السيبرانية التي تتعرض لها إسرائيل ومدى تأثيرها على الأمن القومي الإسرائيلي والإستراتيجيات المتبعة لمواجهتها.

وتم الاستعانة **بالمقترب النسقي** من خلال معرفة مدى تأثير التهديدات السيبرانية على البيئة الداخلية لإسرائيل وكيفية تعامل الحكومة الإسرائيلية معها.

كما تم أيضا استخدام **المقترب الوظيفي** وذلك من خلال معرفة الدور الذي تقوم به إسرائيل للحفاظ على أمنها القومي على مستوى بيئتها الداخلية والخارجية.

8- هيكلة الدراسة

للإحاطة بمختلف جوانب الموضوع وللوصول إلى نتائج موضوعية للدراسة تم تقسيم البحث إلى ثلاث فصول يندرج تحت كل فصل مجموعة من المباحث والمطالب بالإضافة إلى مقدمة والخاتمة.

- **الفصل الأول:** يتضمن الإطار المفاهيمي والنظري للدراسة بحيث تم تخصيص المبحث الأول لمفهوم الإستراتيجية وسائلها وأهدافها بالإضافة إلى أهم المفاهيم المتداخلة معها، أما المبحث الثاني فقد تم التطرق فيه إلى مفهوم الأمن السيبراني، المفاهيم ذات الصلة، الأبعاد والعلاقة بين الأمن السيبراني والأمن القومي، وتم تخصيص المبحث الثالث لمفهوم التهديدات السيبرانية، مصادرها وأنواعها، أما المبحث الثالث فقد تم تخصيصه للإطار النظري للدراسة والذي تناول النظرية الواقعية، مدرسة كوبنهاغن و مدرسة باريس.

- **الفصل الثاني:** المعنون بالفضاء الإلكتروني في منظومة الأمن القومي الإسرائيلي(الأسس والمقومات) تم تقسيم هذا الفصل إلى ثلاث مباحث بحيث تناول المبحث الأول المقاربة الأمنية الإسرائيلية، المرتكزات والعوامل المؤثرة في تطور المقاربة الأمنية الإسرائيلية، أما المبحث الثاني تم تخصيصه لمراحل تطور قطاع أمن المعلومات الإسرائيلي و تناول المبحث الثالث أهم مقومات الفضاء الإلكتروني الإسرائيلي.

– **الفصل الثالث**: سيعالج هذا الفصل مهددات الأمن السيبراني الإسرائيلي وإستراتيجيات المواجهة بحيث تناول المبحث الأول نماذج عن أبرز الهجمات التي تتعرض لها إسرائيل وتأثيرها على الأمن القومي الإسرائيلي، أما المبحث الثاني فتم تخصيصه لأبعاد الاستعدادات الإسرائيلية في مجال الفضاء الإلكتروني وتناول المبحث الثالث الإستراتيجية الإسرائيلية الهجومية كآلية لمواجهة التهديدات السيبرانية.

9–تحديد المفاهيم

تتطلب الدراسة تحديد بعض المفاهيم وتوضيح معناها لمعالجة الموضوع بطريقة جيدة والتحكم فيه، لذلك سوف يتم تحديد المفاهيم التالية:

– **الأمن (Security)**: يعتبر مصطلح الأمن من المصطلحات السياسية الحديثة نسبيا التي لم يكتمل نمو مفاهيمها وتأكيد عناصره وإثبات قوانينه، فمازال يتغير ويضاف له تعريفات وعناصر ويتسع مفهومه أويضاف له لظهور حالات جديدة على الساحة الدولية، إضافة إلى أن الباحثين والأكاديميين مازالوا مختلفين فيما بينهم في كثير من أسس ومبادئ الأمن حتى في تعريفه ومفهومه.[1]

وتعني كلمة أمن بشكل عام كل التدابير التي يتبعها مجتمع معين أو مجموعة من المجتمعات لحماية البقاء من خلال تهيئة عوامل الاستقرار وتنمية وتطوير القدرات بما يحمي المصالح القائمة ويعزز المصالح التي يسعى لتحقيقها.

ويتمحور هذا المفهوم حول فكرة الدفاع عن البقاء ضد الأخطار الخارجية والسياسية والعسكرية والاقتصادية والبيئية وأيضا الداخلية، أوأية أخطار أخرى تهدد هذا البقاء وتمس المصالح القائمة أوتعوق تحسين شروطه والمصالح المترتبة في المستقبل.[2]

– **الفضاء الإلكتروني (Cyberspace)**: ظهر هذا المفهوم لأول مرة قي ثمانينيات القرن الماضي في إحدى روايات الخيال العلمي للكاتب الأمريكي الكندي"William Gibson" الذي ألف عدة روايات تضمنت

[1]– ليندة عكروم، "**تأثير التهديدات الجديدة على العلاقات بين دول شمال وجنوب المتوسط**"، (الأردن: دار إبن بطوطة للنشر والتوزيع، 2011)، ص 15.

[2]– رواء زكي الطويل، "**الأمن الدولي وإستراتيجيات التغيير والاصلاح**"، (الأردن: دار أسامة للنشر والتوزيع، 2012)، ص 194.

هذا المفهوم، ليتخذ مع الانترنت معنى الفضاء الجديد للاتصال حيث يُنشئ الأفراد عالما وهو ليس مكانا واقعيا كما أنه ليس فضاءا حقيقيا بل هومكان خيالي أووهمي يُنشأ من خلال النقر على لوحة مفاتيح الحاسوب.[1]

ويعرفه"فريدريك مايور" بأنه:"بيئة إنسانية وتكنولوجية جديدة للتعبير والمعلومات والتبادل، وهو يتكون أساسا من الأشخاص الذين ينتمون لكل الأقطار والثقافات واللغات والأعمار والمهن المرتبطة ببعضها البعض عن طريق البنية التحتية الاتصالية التي تسمح بتبادل المعلومات و نقلها بطريقة رقمية ".[2]

أصبح هذا المفهوم أشمل وأوسع من الانترنت ليضم كل الاتصالات والشبكات وقواعد البيانات، ويشير كذلك إلى مجموعة المعلومات المتوفرة إلكترونيا ويتم تبادلها وتشكيلها في مجموعات بناءا على استخدامها، ويتميز هذا الفضاء بالمعلومات المنتشرة بسرعة الضوء وإلغاء المسافات.

كما عرفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي على أنه:"فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية".[3]

كما تجدر الإشارة إلى أن مسألة تحديد مفهوم الفضاء الإلكتروني هي مسألة نسبية تتوقف على طبيعة إدراك وفهم كل دولة لأمنها القومي، ولذلك فهناك من يرى بأن هذا المفهوم يمثل الذراع الرابع للجيوش الحديثة.[4]

بفضل ثورة المعلومات ومع ظهور الانترنت ومواقع الويب أصبح الفضاء الإلكتروني أحد العناصر الرئيسية التي تؤثر في النظام الدولي بما يحمله من أدوات تكنولوجية تلعب دورا هاما في عملية التعبئة والحشد في العالم فضلا عن التأثير في القيم السياسية وأشكال القوة المختلفة سواء كانت صلبة أوناعمة.[5]

---

[1]– صافية قاسيمي، "**الفضاء السبراني والأغورا الإلكترونية –إشكالية خلق فضاء عمومي افتراضي حسب المنظور الهابرماسي**"، (جامعة: الجزائر 03، كلية الإعلام والاتصال، د س)، ص 07.

[2]– المكان نفسه.

[3]– إسماعيل قادير، "**إدارة الحروب النفسية في الفضاء الإلكتروني: الإستراتيجية الامريكية الجديدة في الشرق الاوسط**"، الندوة الدولية: عولمة الإعلام السياسي وتحديات الامن القومي للدول النامية، (جامعة: الجزائر 03، كلية العلوم السياسية والعلاقات الدولية، د س)، ص 04.

[4]– المكان نفسه.

[5]– ايهاب خليفة، "**القوة الالكترونية وأبعاد التحول في خصائصص القوة**"، مجلة أوراق، ع12، (2014)، ص 20.

الفصل الأول

الإطار المفاهيمي والنظري للدراسة

يتطلب أي بحث علمي وأكاديمي البدء في ضبط المفاهيم الأساسية لأن هذه العملية تسمح للباحث باستعاب المعنى الحقيقي للمفاهيم والمصطلحات المراد دراستها وتوضيحها بالشكل الذي يؤدي إلى فك الغموض والتعقيد، فكل مصطلح يحتاج إلى تقديم العديد من التعاريف لفهمه واستعابه ناهيك عن التطرق عن السياق التاريخي للموضوع محل الدراسة، إضافة إلى التطرق إلى المقاربات النظرية التي يتم تفسير أي موضوع من خلالها.

ويعتبر حقل العلاقات الدولية غني بالمفاهيم والمصطلحات الدالة على الظواهر، لذا سيتناول هذا الفصل الذي تم تقسيمه إلى أربعة مباحث مايلي :

- **الضبط المفاهيمي للإستراتيجية؛**
- **الضبط المفاهيمي للأمن السيبراني؛**
- **التهديدات السيبرانية: مقاربة مفاهيمية؛**
- **الإطار النظري للدراسة.**

المبحث الأول: الضبط المفاهيمي للإستراتيجية

تحظى الإستراتيجية كموضوع باهتمام متزايد وواسع النطاق من قبل المفكرين والمثقفين والأكاديميين، فضلا عن اهتمام النخب القيادية والمؤسسات الرسمية وغير الرسمية لما لها من تماس شديد وعلاقة وثيقة بالعديد من مجريات السياسة الدولية، فكلمة إستراتيجية تستخدم اليوم في مختلف ميادين الحياة وفي أنشطة وفعاليات عديدة حتى أصبح من الصعوبة بمكان تحديد ما المقصود بها على وجه الخصوص[1] أوالتحكم في المصطلح من قبل الباحثين، لذا وجب التوقف عند مفهوم الإستراتيجية وبدايات الدراسة العلمية لهذا المصطلح والتطرق إلى بعض المفاهيم ذات الصلة.

المطلب الأول: تعريف الإستراتيجية

الفرع الأول: التعريف اللغوي

الإستراتيجية (Strategy) مشتقة أصلا من الكلمة اليونانية (Strato) بمعنى جيش أوحشد، ومن مشتقات هذه الكلمة (Stratego) والتي تعني فن القيادة، ومن مشتقاتها أيضا (Stratagem) والتي تعني الخدعة الحربية التي تستخدم في مواجهة العدو.[2]

وانطلاقا من التحليل الكلاسيكي للمصطلحات نجد أن مفهوم أومصطلح الإستراتيجية يوجد في مختلف اللغات الأوروبية أواللغات الإغريقية اللاتينية.

ففي الألمانية نجد (Strategie)، وفي الروسية (Strategya) وفي الهنغارية (Strategi)، وعندما نقول (Stratos agein) فمصطلح الإستراتيجية ذاته مقسم إلى جزئين ويعني: "الجيش الذي ندفع به إلى الأمام" وبوصل طرفي المصطلح (Stratos) و(agein) نحصل على (Strategos) وهذا يعني الجنرال وفعل (Strategô) يعني قاد أوأمر.[3]

ويتضح من خلال ما تقدم ذكره في أصل كلمة إستراتيجية أنها قد ارتبطت بالجانب العسكري وبفن قيادة الجيوش وبفن الحرب وعلمها، لأن الإستراتيجية في تلك الفترة استحوذت على اهتمام القادة العسكريين.

1- عبد القادر محمد فهمي، "**المدخل في دراسة الإستراتيجية**"، (عمان: دار مجدلاوي للنشر والتوزيع، 2009)، ص 07.

2- **المرجع نفسه**، ص 17.

3- صلاح نيوف، "**مدخل إلى الفكر الإستراتيجي**"، (الدنمارك: الأكاديمية العربية المفتوحة، د س ن)، ص 09.

الفرع الثاني: التعريف الإصطلاحي

يتفق معظم المفكرين والباحثين على أن الإستراتيجية هي مفهوم مثير للجدل في العلوم السياسية والفكر الإستراتيجي، ذلك أن هذا المصطلح ارتبط في البداية بالجانب العسكري وفنون القتال ونتيجة لتطور الدراسات والانفتاح على العلوم الأخرى أضحى هذا المفهوم واسع الانتشار، ومن بين ما قدم من قبل المفكرين والفلاسفة في تعريف الإستراتيجية نذكر ما يلي:

يقول المفكر الإستراتيجي الصيني "سان تزو" "Son Zi": "أن الأكثر تميزا من القادة بيننا هم هؤلاء الأكثر حكمة والأكثر استشرافا ورؤية".[1]

1- تعاريف المدرسة الغربية لمصطلح الإستراتيجية

- يعرف المفكر الألماني "كلاوزفيتش" "Clausewitz" الإستراتيجية بأنها: "فن استخدام الاشتباك كوسيلة للوصول إلى غايات الحرب، أوإلى الأهداف التي شنت الحرب من أجلها".[2]

والملاحظ أن هذا التعريف قد اعتبر الإستراتيجية وسيلة لتحقيق أهداف العمل الحربي وغاياته من خلال وضع الخطط وتوفير الإمكانات للوصول لهذه الأهداف.

- أما "ليدل هارت" فقد عرف الإستراتيجية بكونها: "فن توزيع واستخدام الوسائط العسكرية لتحقيق هدف السياسة".[3]

هنا "ليدل هارت" يرى بأن الإستراتيجية هي استخدام وتوظيف الوسيلة العسكرية لتحقيق الأهداف السياسية التي تشن الحرب من أجلها وعلى فن استغلال هذه الوسائل.

وما يؤخذ على تعريف كل من "كلاوزفيتش" و"ليدل هارت" أنهما ربطا الهدف السياسي بالهدف الإستراتيجي للنشاط العسكري الميداني (أي الحرب)، أن هناك حالات وإن كانت استثنائية لا يتحقق فيها الهدف السياسي بمعناه الإستراتيجي عندما تكون الحرب وسيلة لتحقيقه.[4]

[1]- **المرجع نفسه،** ص 06.

[2]- عبد القادر محمد فهمي، **مرجع سابق،** ص 13.

[3]- المكان نفسه.

[4]- **المرجع نفسه،** ص 14.

المدرسة الشرقية

– يرى "لينين" في تعريفه أن: "الإستراتيجية الصحيحة هي التي تتضمن تأخير العمليات إلى الوقت الذي يسمح فيه الانهيار المعنوي للخصم للضربة المميتة بأن تكون سهلة وممكنة".[1]

– أما "ماوت سيتونغ" فيعرف الإستراتيجية بـــأنها: "دراسة قوانين الوضع الكلي للحرب".[2]

والملاحظ أن هاذين التعريفين المقدمين لم يخرجا الإستراتيجية عن المجال العسكري والحرب، غير أن "لينين" ركز على الجانب النفسي للخصم من خلال إرباكه وانتظار الوقت المناسب للعمليات والتي تكون فيها الضربة مميتة التي تكون سهلة وممكنة.

بينما ربطها "ماوت سيتونغ" بالحرب ودراسة قوانينها.

المدرسة العربية

تعريف المدرسة المصرية: "هي أعلى مجال في فن الحرب وتدرس طبيعة وتخطيط وإعداد وإدارة الصراع المسلح، وهي أسلوب علمي نظري وعملي يبحث في مسائل إعداد القوات المسلحة للدولة واستخدامها في الحرب، معتمدا على أسس السياسة العسكرية كما أنها تشمل نشاط القيادة العسكرية العليا بهدف تحقيق المهام الإستراتيجية للصراع المسلح لهزيمة العدو".[3]

ويتضح أن تعريف المدرسة العربية للإستراتيجية لا يبتعد عن الإطار العسكري لخدمة أهداف السياسة ولعل ما يؤخذ على هذه التعريفات أنها اعتبرت الحرب الأداة الوحيدة لتحقيق الهدف الإستراتيجي للدولة.

ولعل ارتباط الإستراتيجية بالمجال العسكري لدى منظري الفكر الإستراتيجي في القرنين 18م و19م له ما يبرره فالحرب كانت تعني زوال الدول أوبقائها، كما أن الشؤون السياسية والعسكرية كانت بيد شخص واحد وهو الملك وتمركز القرار الإستراتيجي في يد القادة العسكريين.

غير أن الوقت الحالي عرف تعددا لمجالات الإستراتيجية و لم تعد مرتبطة بالنشاط العسكري للدولة، بل تعدت ذلك لتشمل الجانب السياسي والاقتصادي والاجتماعي والأمني وذلك بفضل التطورات التي مر بها النظام الدولي، حيث باتت متطلبات بناء الدولة الحديثة لا تستند على متانة قاعدتها العسكرية فقط بل على قوة بناء قاعدتها الاقتصادية والتكنولوجية والاجتماعية أيضا.

[1]- **المرجع نفسه**، ص 24.

[2]- المكان نفسه.

[3]- المكان نفسه.

بمعنى أن الدول أخذت ترسم إستراتيجياتها لا على أساس افتراضات الخيار العسكري حيث تقتضي ضرورة الحرب، وإنما في ضوء احتياجات ومتطلبات الواقع العملي وبمختلف معطياته السياسية والاقتصادية والاجتماعية والعسكرية وبشكل تؤلف فيه هذه الإستراتيجية كُلاً لا يتجزأ.[1]

وتتنوع الوسائل والأدوات بتنوع الأهداف والإستراتيجية في حد ذاتها، ذلك أن القدرة على تعبئة الموارد والإمكانيات اللازمة لتحقيق أهداف الإستراتيجية التي حددتها السياسة هوما يميز الإستراتيجية عن غيرها.

ويمكن تقسيم وسائل الإستراتيجية إلى مادية وتتمثل في الوسائل الجغرافية والاقتصادية والعسكرية وأخرى معنوية وتتضمن الثقافية والاجتماعية، وهنا يأتي دور صانع الإستراتيجية في التكييف والموازنة بين هذه الإمكانيات والأهداف المرجوة واحتواء ثغرات التفاوت الكمي والنوعي وانعكاسها على نسبة الإنجاز ومستواه.

وبالتالي وجب توفر مجموعة من الشروط لصياغة إستراتيجية شاملة وفعالة:

- وضوح الأهداف وتكاملها.
- واقعية الأهداف وتكاملها.
- الاختيار العقلاني بين الأهداف والوسائل.
- الاستمرارية: فأهداف الدولة لا نهاية لها لذا لابد أن تتصف عملية التخطيط بالاستمرارية.
- المرونة لمواجهة المواقف غير المحتملة أوغير المتوقعة في الظروف الاعتيادية مثل الحرب.
- الابتكار والاعتماد على الذات لأن الفكر الإستراتيجي يعتبر قمة الفكر الإبداعي.[2]

وكخلاصة فالحديث عن أي إستراتيجية يقودنا إلى أن:

- الإستراتيجية تعدت الجانب العسكري لتشمل مجالات أخرى.
- الإستراتيجية هي الموازنة بين الإمكانات المتاحة والأهداف المراد تحقيقها.

[1]- خليل حسين، وحسين عبيد، "**الإستراتيجيا**"، (بيروت: منشورات الحلبي الحقوقية، 2013)، ص 30.

[2]- علي محمد إبراهيم كردي، "**المفهوم العسكري للإستراتيجية والتطور التاريخي**"، تم تصفح الموقع يوم : 15 فيفري 2018. الرابط:

Renanaonline.com/users/alihordi/posts/352158

- الإستراتيجية هي علاقة بين الحاضر والماضي وتحديد المناهج والأدوات على ضوء رؤية مستقبلية للأهداف ونظرة فلسفية للتطور.[1]

الفرع الثالث: التعريف الإجرائي

ويمكن تعريف الإستراتيجية من الناحية الإجرائية على أنها القدرة على الموازنة بين الإمكانات المتاحة للدولة وبين الأهداف المراد تحقيقها على المدى البعيد وفقا لمبادئ وقواعد معينة وتتسم بالاستمرارية والمرونة.

المطلب الثاني: التطور التاريخي للإستراتيجية

يتفق المفكرون والباحثون الإستراتيجيون على أن الإستراتيجية مفهوم ليس حديث النشأة ويعود تأصيله التاريخي إلى قرون ماضية حيث مر بعدة مراحل، وهو ما ساهم في انتقال الإستراتيجية من الجانب العسكري وبفن الحرب وعلمها إلى مجالات أخرى، نتيجة التطورات التي شهدتها المجتمعات البشرية ويمكن إبراز هذه المراحل فيما يلي:

الفرع الأول: الفكر الإستراتيجي الآسيوي القديم – نموذج الفكر الصيني–

كان للكتابة مكانة رفيعة في الصين وقد كرس الكثير منها للأمور العسكرية حيث ظهر العديد من أعلام الفكر الإستراتيجي الصيني من أهمهم:

يعتبر الإستراتيجي الصيني "سان تزو" "Sun Tzu" في مؤلفه "فن الحرب" والذي يعتبر أقدم ما ألف في هذا المجال، حيث عرف الإستراتيجية على أنها: "يمكن مقارنة أي جيش بالماء فالماء يترك المرتفعات ويغزو الأماكن المنخفضة، وهكذا الجيش يتفادى القوة ويهاجم الضعف السيل ينتظم حسب تضاريس الأرض والانتصار يحرز بالتلاؤم مع وضعية العدو".[2]

ثم الجنرال "Caocao" في القرن السابع والثامن قبل الميلاد، إلى جانب "صان بن" "Sun Bin" أشهر أعماله "الإتفاقية العسكرية"، حيث يغلب الطابع العملي على رؤيته الإستراتيجية تحدث عن الدعم اللوجيستي وتأثير ذلك في زيادة فعالية إطالة الحملات العسكرية و"هي يانش" "Hi yanshi" أهم مؤلفاته الإستراتيجية:

---

[1]- عبد القادر محمد فهمي، "**المدخل إلى دراسة الإستراتيجية**"، (عمان: دار مجدلاوي للنشر والتوزيع، 2010)، ص 11.

[2]- نسيمة بوطويل، "**الإستراتيجية الأمنية الأمريكية في منطقة شمال شرق آسيا: دراسة لمرحلة ما بعد الحرب الباردة**"، رسالة مقدمة لنيل شهادة دكتوراه العلوم في العلوم السياسية، تخصص علاقات دولية، (جامعة: الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، 2010)، ص 22.

كتاب "معلم الفروسية" "Simo-Fa": نص مختصر ظهر في القرن الرابع أوالخامس قبل الميلاد يتحدث عن إدارة الجيوش، وضرورة أن تكون الحرب عادلة.

كتاب "الإستراتيجيات الثلاث" "Sen Lue": يحلل في سيطرة الحكومة والأبعاد السياسية للإستراتيجية.[1]

تعتبر مؤلفات هؤلاء المفكرين الإستراتيجيين الصينيين من ركائز الفكر الإستراتيجي الغربي رغم أن الغربيين تعاملوا دائما مع الفكر الصيني على أنه حكمة أكثر مما هو علم، ومع هذا ترجم كتاب "فن الحرب" لـــ"سان تزو" إلى كل اللغات الأوروبية إبتداء من الروسية سنة 1889 إلى الإنجليزية بداية القرن العشرين.[2]

الفرع الثاني: الفكر الإستراتيجي الغربي القديم

يمكن الحديث عن الإستراتيجية في الفكر الغربي القديم عند كل من اليونانيين والرومان على اعتبار أن المدرستين قد برعتا في الشؤون العسكرية في مجال الحرب والقتال والتخطيط وكذا التكتيك.

أولا: الفكر الإستراتيجي اليوناني

امتلك اليونانيون العديد من التحليلات التكتيكية والإستراتيجية في عصرهم القديم، فكان الإسبارطيون أول من كتب في الصراعات وإستراتيجية خوضها وكانوا أول من علموا هذه الأفكار من خلال معلمين عسكريين سموهم بالتكتيكيين.

يعتبر كل من "إني" و"أندرسونس" أقدم من كتب في الإستراتيجية خلال العهد اليوناني حيث اعتمدوا كثيرا على الممارسات العملية أكثر من التنظير، رغم وجود هذا الأخير في كتابات "إكسنوفون" حيث ظهر التفكير التنظيري في مؤلفه "تحليل الفروسية" فكان أول من نظر في التكتيك.[3]

ثانيا: الفكر الإستراتيجي الروماني

كان لدى الرومان فكرا عسكريا أصيلا وجديدا وصل إلى عمق الأشياء والأمور الإستراتيجية وذلك حسب النصوص الرومانية، ودلالة ذلك التفوق التكتيكي الروماني من خلال قرون متتالية مما أوحى بوجود

[1]- **المرجع نفسه**، ص 24.

[2]- المكان نفسه.

[3]- المكان نفسه.

بنية تنظيمية دقيقة للعقيدة العسكرية، فيؤكد على ذلك "بوليب" قائلا: "المرشحون للوظائف العامة كان عليهم المشاركة في عشر حملات عسكرية قبل اختيارهم من قبل المواطنين".[1]

أشهر مؤلفات الرومان في المجال الإستراتيجي جاء بها كل من "كاتوا"،"بوليب" و"فرونتينوس" في مؤلفه "تعليقات عسكرية عند هوميروس".

ثالثا: الفكر الإستراتيجي العربي الإسلامي

معظم الكتابات والمؤلفات التي سبقت ابن خلدون والتي تتعلق بالفكر الإستراتيجي فقدت بعد تعرض الدول العربية للغزو المتكرر على يد المغول، لذلك تعتبر مؤلفات ابن خلدون عن الحروب والطرق المستخدمة في المعارك من قبل مختلف الشعوب أول ما ظهر في التراث العربي في هذا المجال.

عرف القرن 13م حتى القرن 16م العديد من المؤلفات التي تقترب من التكتيك والإستراتيجية من بينها "تعليمات رسمية للنخبة العسكرية"، كتاب "الفن العسكري" كتبه محمد بن عبد الله، كتاب "الفن العسكري والفروسية" كتبه علي بن عبد الشامان بن هزيل.[2]

الكتاب والسنة لم يحددا شيئا في هذا الموضوع، لكن الكُتَّاب الغربيون يرون أن وجود رسالة والرغبة في نشرها يساعد على تحديد مهام الإستراتيجية والأهداف العامة للأمة.

رابعا: الفكر الإستراتيجي الأوروبي الحديث

يعتبر العصر الحديث أخصب ما أُلِّف وكُتب في مجال الإستراتيجية، حيث صدر العديد من المؤلفات التي دفعت بهذا المجال المعرفي وتطوره.

فالفكر الإستراتيجي العسكري بدأ الإعلان عن نفسه بشكل واضح في إسبانيا مع كتاب " libro de la guerra" (كتاب الحرب) حوالي سنة 1420م، وقد كتبه الماركيز "vellena" وكتاب "تحليل الانتصار العسكري" حوالي سنة 1459م وقد ألفه "Alfonso Hernandez".

في فرنسا نجد العديد من الكُتّاب مثل "Robert de Balsac" وكتابه "مبادئ الصراعات النبيلة" في سنة 1502م، وفي انجلترا في نفس الفترة الزمنية نجد كتاب "تحليل لفن الحرب" وضعه "Béraud Stuart" وفي ألمانيا كتاب "الحرب" لمؤلفه "phlippe von Seldeneck" نحو نهاية القرن الخامس عشر وفي إيطاليا نجد كتاب "Semedeus liber tertuis de re militaire" سنة 1438م لمؤلفه "Catone Secco"

---

[1]- **المرجع نفسه**، ص 25.

[2]- **المرجع نفسه**، ص 24.

"ميكيافلي" التكتيكي والإستراتيجي الذي ألّف الكتاب الأكثر شهرة في القرن السادس عشر ويحمل عنوان "فن الحرب" وفي الواقع هوكتابه الوحيد الذي نشر أثناء حياته، الكتابات العسكرية عند "ميكيافللي" هي بشكل أساسي كتابات سلبية أونقد للمؤسسات العسكرية التي كانت سائدة في عصره.[1]

والملاحظ هنا أن هذه الفترة كانت خصبة بالمؤلفات والكتابات حول الإستراتيجية وفن الحرب والتكتيك لأنها تأثرت بالحروب التي شهدتها تلك الفترة خاصة في القارة الأوروبية.

المطلب الثالث: الإستراتيجية وعلاقتها بالمفاهيم ذات الصلة

هناك العديد من المصطلحات التي تتداخل مع مفهوم الإستراتيجية، لذلك تقتضي الضرورة العلمية التمييز بين مفهوم الإستراتيجية وبين هذه المفاهيم وتحديد العلاقة بينهم ويمكن إبراز أهم هذه المفاهيم فيما يلي:

الفرع الأول: التكتيك

كغيره من المفاهيم عرف التكتيك محاولات عدة لتعريفه، فهويعرف على أنه: "مجمل العمليات التي تقوم بها الدولة للوصول إلى الهدف الإستراتيجي، وعندما تؤدي الحرب إلى معركة حقيقية فإن الاستعدادات التي تتخذ لإعداد مثل هذا العمل وتنفيذه يشكل ما يسمى تكتيكا".[2]

ويقول "HAMLEY": "إن مسرح الحرب هو مجال الإستراتيجية أما ساحة المعركة فمجال التكتيك".[3]

ولذلك يمكن القول أن التكتيك هوتنفيذ الهدف الذي تحدده الإستراتيجية، وأن التكتيك هوجزء من الإستراتيجية بينما الإستراتيجية هي خطة شاملة وعامة.

ويمكن تحديد أوجه الاختلاف بين التكتيك والإستراتيجية فيما يلي:

– على مستوى الأهداف: تكون أهداف الإستراتيجية ثابتة وغير قابلة للتجزئة أوالمساومة، بينما تكون أهداف التكتيك متنوعة.

---

[1]– صلاح نيوف، **مرجع سابق**، ص 42.

[2]– حنان لبدي، "**التحولات الدولية الراهنة وتأثيرها على الإستراتيجية الأمنية في منطقة الساحل الإفريقي**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية، (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، 2015)، ص 22.

[3]– **المرجع نفسه**، ص 17.

– على مستوى الحركات: قد تتضاعف الحركة في الإستراتيجية وقد تنعدم لثبوت الأهداف بينما في التكتيك تكون متعددة.[1]

الفرع الثاني: الاستشراف

العمل دون هدف لا معنى له والاستباق يولد العمل، هكذا إذا يمكن أن يقترن الاستشراف بالإستراتيجية ويمثل الاستشراف استباقا يستعد للفعل (PREACTIVE) ويستحدث الفعل (PROACTIVE) وينير العمل الحاضر على ضوء المستقبلات الممكنة والمأمولة.

فأن نتهيأ للتغيرات المتوقعة لا يمنع من أن نعمل على إحداث التغييرات المأمولة.[2]

الاستشراف من المفاهيم الحديثة ويعتبر أول ظهور له كمصطلح سنة 1953م من قبل "غاستون بيرجي" ليحل محل مفهوم علم المستقبل، فقد كان "غاستون بيرجي" "Gaston Berger" يقول: "إننا مع الاستشراف لابد أن ننظر نظرا بعيدا وفسيحا وعميقا وأن نفكر في الإنسان وأن نجازف"، ويضيف أن للاستشراف ثلاث خاصيات هي أن ننظر بطريقة مختلفة (أن نحضِر الأفكار المسبقة)، أن ننظر معا (التملك) وأن نستعمل مناهج صارمة.[3]

فالإستراتيجية تتحدث عن بعد النظر والتجديد والاستشراف يتحدث على تهيئة ظروف الفعل وعن استحداث الفعل، فكيف يمكن أن تتخيل فعل إستراتيجي دون أن يكون لنا بعد النظر وسعته وعمقه حسب "غاستون بيرجي" وبالتالي فالإستراتيجية تستدعي الاستشراف ولو لمجرد توضيح الخيارات التي تلزم المستقبل.

وخلاصة القول أن الغاية من الإستراتيجية هوتحقيق الأهداف التي تحددها السياسة باستخدام الوسائل والإمكانات التي تمكنها من تحقيقها فقد تكون هذه الإستراتيجية:

– **هجومية:** وهي قدرة الدولة على فرض إرادتها على دولة أخرى باستخدام الوسائل المتاحة لإيقاع التأثير وفرض الإرادة على الخصوم لتحقيق أهداف ذات طبيعة تكاد تكون عدائية، وذلك عبر سلوكيات متعددة منها امتلاك القدرات العسكرية والاقتصادية والتكنولوجية والثقافية المتفوقة.

---

[1]– عبد القادر محمد فهمي، **مرجع سابق**، ص 44.

[2]– ميشال غودي، وقيس الهمامي، "**الاستشراف الإستراتيجي والمشاكل والمناهج**"، مجلة ليبسور، العدد6، (2005)، ص 05.

[3]– **المرجع نفسه**، ص 06.

ويكون هدف الدولة إخضاع الخصوم بذلك تغلب على هذه الإستراتيجية سمة العدوان، وتنطوي على مزايا منها أنها تمتلك عنصر المبادئة وحرية اختيار وقت الحركة وأدائها ونقل الحركة إلى ساحة الخصوم فضلا عن أنها تكسب الدولة النفوذ والمكانة.[1]

– **دفاعية**: عند الحديث عن الإستراتيجية الدفاعية يتبادر إلى الأذهان تنظيم القوات المسلحة وأسلحتها وأساليب قتالها، ولكن الدفاع عن الدولة لا ينحصر في الشق العسكري والقتالي فقط فلمؤسسات الدولة كافة دور فيه إذ لكل منها دور أساسي في إعداد الوسائل وتحفيز المجتمع وتعبئة القوى الداخلية والخارجية لمساندة الجهد الدفاعي.[2]

فالإستراتيجية الدفاعية تتسم بشمولها جميع مؤسسات الدولة ومواردها لتتمكن من العمل ضمن آليات متكاملة تعتمد على مركزية القرار ولا مركزية التنفيذ.

كما تستدعي الإستراتيجية الدفاعية القوة في الوحدة الوطنية وهي ضرورة مطلقة في هذه الإستراتيجية.[3]

لذلك نجد أن لكل دولة إستراتيجية خاصة بها وقد تقوم دول أخرى بتطبيق الإستراتيجيتين معا، لذا فإن أية إستراتيجية فعالة يجب أن تبنى على الخبرة والاستفادة من دروس الماضي وأن تُصاغ وتوضع في إطار مناسب للمستقبل.[4]

[1]– سامر مؤيد، "**الإستراتيجية من منظور وظيفي إجرائي**"، تم تصفح الموقع يوم : 17 فيفري 2018. الرابط: Fcdrs.com/mag/issue-6-2.html

[2]– ميشال عون، "**دراسة موجزة عن الإستراتيجية**"، (الرابية، 2008)، ص ص 02–05.

[3]– المكان نفسه.

[4]– حنان لبدي، **مرجع سابق**، ص 15.

المبحث الثاني: الضبط المفاهيمي للأمن السيبراني

تثير المسألة الأمنية إنشغال الكثير من الباحثين والمختصين في حقل العلاقات الدولية بصفة عامة والدراسات الأمنية والإستراتيجية بصفة خاصة، فالدول لاتزال تبحث عن أنجع السبل التي تمكنها من الحفاظ على أمنها واستقرارها، ومع ظهور الثورة التكنولوجية الحديثة وفي ظل تنامي التهديدات الأمنية الجديدة أصبحت مسألة الأمن السيبراني تحظى باهتمام الدول كافة، بحيث عمدت بصفة مستمرة على تطوير ودعم بينتها المعلوماتية وكذا حمايتها لضمان أمنها وأمن أفرادها.

وقبل الخوض في مفهوم الأمن السيبراني وجب البحث في أصل كلمة سبرانية وفي معناها اللغوي والاصطلاحي.

المطلب الأول: مفهوم الأمن السيبراني

الفرع الأول: التعريف اللغوي لكلمة سيبرانية

كلمة سيبرانية مشتقة من الكلمة اليونانية (Kybernetes) التي وردت بداية في مؤلفات الخيال العلمي وكان يقصد بها قيادة ربان السفينة، وقد استخدمت هذه الكلمة سابقا من قبل الفيلسوف اليوناني "أفلاطون" أثناء محاوراته عن فن قيادة السفينة.[1]

وبالرجوع إلى قواميس اللغة يشير قاموس (المورد) إلى أن تعريف كلمة سيبرانية هوعلم الضبط، أي ضبط الأشياء والسيطرة عليها.[2]

ويعرف معجم "le petit la rousse" السيبرانية (Cyber) بأنها: "العلم الذي يدرس آليات الاتصال والتحكم في الآلات والكائنات الحية الأخرى".[3]

أما معجم "Oxford" الإنجليزي فيعرفها على أنها: "دراسة فاعلية العمل البشري بمقارنتها بفاعلية الآلات الحاسبة، وتتصل بسمات وخصائص الحواسيب وتكنولوجيا المعلومات والواقع الافتراضي".[4]

---

[1]– أحمد عيسى نعمة الفتلاوي، "**الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم المعاصر**"، (بحث مقبول للنشر في مجلة المحقق الحلي، جامعة الكوفة، كلية القانون، 2016)، ص 05.

[2]– منير البعلبكي ورمزي منير البعلبكي، "**المورد الحديث**"، (لبنان: دار العلوم للملايين)، ص 307.

[3]- "**la rousse dictionnaire de français**", p 104.

[4]- "**Oxford dictionaries language**", p 299.

أما الموسوعة العربية الإلكترونية فتعرف كلمة سيبرانية على أنها: "مجموعة من الدراسات النظرية للعمليات الناظمة لضبط الأجهزة الإلكترونية والميكانيكية بوجه عام والأجهزة البيولوجية على وجه الخصوص سواء أكانت آلية أم حيوية".[1]

إن معظم القواميس المتخصصة في المصطلحات العسكرية لم تُرجع كلمة (Cyber) إلى مصدرها بل عرفت في نطاق استخدامها الفعلي أي العسكري، كقاموس المصطلحات العسكرية الأمريكية إذ يعرفها بأنها: "أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أوالتعطيل لبرامج إلكترونية أخرى".[2]

فيما يعرفها قاموس مصطلحات الأمن المعلوماتي بأنها: "هجوم عبر الفضاء الإلكتروني يهدف إلى السيطرة على مواقع إلكترونية أوبنى محمية إلكترونيا لتعطيلها أوتدميرها أوالإضرار بها".[3]

أما في اللغة العربية وبالرجوع إلى المختصين فيها، فنجد أن هناك تحديا يواجهه هؤلاء المختصين في الوصول إلى مصطلح مقارب لمصطلح (Cyber) في اللغة الإنجليزية.

الفرع الثاني: التعريف الاصطلاحي لكلمة سيبرانية

كلمة سيبرانية في مفهومها الحديث استعملت لأول مرة من قبل عالم الرياضيات الأمريكي "نوربرت وينر" "Norbert wiener" وهوأستاذ الرياضيات في معهد ماساشوستس التقني (MIT) الذي أعطاها مفهومها الاصطلاحي الحديث وكان ذلك عام 1948م، من أجل وصف نظام التغذية الرجعية (Feed back) الذي وضعه والذي يعمل على الاستفادة من مخرجات الأنظمة في ضبط مدخلاتها وفي التحكم فيها واستقرار أدائها.

ورأى "وينر" أنه يمكن تطبيق هذا النظام على نطاق واسع في مختلف المجالات ليس العملية فقط بل الإنسانية أيضا، ووضع لذلك كتاب بعنوان "السيبرانية أوالتحكم والاتصال في الحيوان والآلة".[4]

وبالتالي فالمصدر الاصطلاحي الحديث لكلمة سيبرانية هوعلم القيادة أوالتحكم في الأحياء والآلات ودراسة آليات التواصل في كل منهما.

---

[1]– الموسوعة العربية، "**علم الحياة (الحيوان والنبات)، الاستقلالية**"، تم تصفح الموقع يوم : 03 فيفري 2018. الرابط: http://www.arab_ency.com/détails.php? Full=18nid=113

[2]– أحمد عيسى نعمة الفتلاوي، **مرجع سابق**، ص 05.

[3]– المكان نفسه.

[4]– سعد علي الحاج بكري، "**الأمن السيبراني ومعضلة حمايته**"، تم تصفح الموقع يوم : 03 فيفري 2018. الرابط: www.aleqt.com/2017/08/24/article.1241506.html

ويعرفها "لوب كوفينال" "L.covinal" في كتابه "السبرنتيك" بأن الفكر السيبراني يتميز بهدفه ومنهجه:

– الهدف: هوفعالية قيادة وتوجيه الفعل.

– المنهج: هوالاستبدال التماثلي الذي يسمح بصنع نماذج فيزيائية تمثل بعض الوظائف العقلية التي تبين بالتحليل أنها وظائف آلية يمكن مكننتها، إذ أنه يمكن صنع نماذج تمثل الغريزة والتعلم والتصرف حسب سلوك الوسط الخارجي والتخيل كما أن الفعل الرجعي هوأساس هذه النماذج في أكثر الوظائف العقلية.[1]

ويعرفها "أوديل دافيد" "O.David" بأنها: "التوضيح الكامل والجوهري للفكر الخاضع لهدف منها".[2]

ويعرفها "براي والتر" "B.Walter" بأنها: "علم الآلات العقلية".[3]

لقد لخص "نوربورت وينر" الحدود التي لا ينبغي أن يتعداها إيماننا بقدرات الآلة أوالخوف من طغيانها بقوله: "أعط ما للإنسان للإنسان، وما للعقل الإلكتروني للعقل الإلكتروني"، وهويعني بذلك أن الإنسان يظل له دوره العام والأساسي في عصر التقدم التكنولوجي، وأن أرقى أنواع الآلات يظل على الدوام أداة طيعة في يد صانعها وهي تتجه في نفس الطريق الذي يريدها الإنسان أن تسلكه سواء أكان خيرا أم شرا.

وكان ظهور علم السيبرنطيقا (Cybernetics) هذا العلم الجديد، هوبدوره واحدا من المعالم البارزة لعصرنا الحاضر حيث كانت أبحاث "وينر" هي الأساس الأول لاختراع العقول الإلكترونية.

فقد كانت فكرة هذا العالم هي تطبيق ما يحدث في الإنسان بوصفه جهازا حيا متكاملا على الآلات من أجل بلوغ مرحلة جديدة في تطورها مختلفة عن كل ما استخدمت فيه الآلات من قبل، وعلى هذا الأساس فقد درس "وينر" الوظائف الذي يقوم بها الجهاز العصبي للإنسان والتي يتمكن الإنسان بواسطتها من أن يصحح مسار أفعاله ويعيد توجيهها وفقا لما يواجهه، وأن يأمر نفسه ويطيعها ويختبر نتائج سلوكه ويعدلها.[4]

وحين أمكن تطبيق نتائج هذه الدراسات في صنع جيل جديد من الآلات كانت تلك الآلات من نوع لم يألفه الإنسان من قبل، فهي ليست تلك الآلات التي تحتاج إلى إشراف دائم للإنسان ولا تعمل إلا وفقا لأوامره ولا تسير إلا في خط واحد يرسمه لها مقدما، بل أنها كانت آلات تصحح مسارها بنفسها وتتبادل مع

---

[1]– ضياء وراد، **مترجما**، "**الكون الرقمي: الثورة العالمية في الإتصالات**"، (المملكة المتحدة: مؤسسة هنداوي سي آي سي للنشر،2017)، ص 21.

[2]– **المرجع نفسه**، ص 22.

[3]– المكان نفسه.

[4]– فؤاد زكريا، "**التفكير العلمي**"، الطبعة الثالثة، (الكويت: المجلس الوطني للثقافة والفنون، 1978)، ص 144.

نفسها الأوامر وتنفيذ الأوامر وتقوم بأعمال إنتاجية أعقد وأكمل بكثير مما كانت تقوم به الأجيال السابقة من الآلات سواء منها البخارية والكهربائية.

وهكذا كانت فكرة تلك الآلات تتضمن في داخلها عقلا حاسبا يراقب عملها ويعدله ويصححه ويعيد توجيه سيرها وفقا لما يجريه من حسابات.[1]

وقد نجحت هذه الآلات في إحداث تحول كبير في ميدان الإنتاج المادي فضلا على أنها توفر نسبة كبيرة من الأيدي العاملة، أي أنها كانت تحقيقا فعليا لحلم بشري هوحلم الآلة التي تقوم بكل أعمال الإنسان وتعفيه من مشقة العمل.

ويعد الإنجاز الأكبر الذي قامت عليه هذه الآلات الجديدة كان تطبيقها في ميدان العمل العقلي باختراع نوع جديد من الآلات هوالعقول الإلكترونية والذي يعد خطوة جديدة في طريق التقدم العلمي.[2]

الفرع الثالث: تعريف الأمن السيبراني

تعتبر مهمة تحديد المفاهيم أول تحد يواجهه المفكرون ويتعرض له الباحثون في جميع التخصصات وفي شتى الدراسات، وذلك لما تطرحه من إشكاليات تجعل من الصعوبة بمكان الإتفاق على تعريفات واضحة وشاملة وموحدة بين فرقاء المجتمع العلمي يمكن تعميمها على جميع الحقول المعرفية.[3]

ويعتبر مفهوم الأمن السيبراني من أكثر المفاهيم المثيرة للاهتمام والدراسة، حيث عرف تعددا في التعريفات المقدمة له والتي يمكن إبرازها فيما يلي:

- فقد عرفه "ريتشارد كمرر" "Richard A.Kemmerer" على أنه: "عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة".[4]

---

[1]- **المرجع نفسه**، ص 147.

[2]- **المرجع نفسه**، ص 153.

[3]- عنترة بن مرزوق، "**الأمن السيبراني كبعد جديد من السياسة الدفاعية الجزائرية**"، (محاضرات مقدمة لطلبة جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، د س)، ص 65.

[4]- محمد مختار ، "**Cyber Security: هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية؟**"، مجلة مفاهيم المستقبل، العدد 06، (يناير 2015)، ص 05.

– بينما يعرفه "إدوارد أمورسو" "Edward amoroso" على أنه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أوأجهزة الحاسوب أوالشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة".[1]

الملاحظ أن كل من "ريتشارد كمرر" و"إدوارد أمورسو" قد ركزا في هذين التعريفين على اعتبار أن الأمن السيبراني هووسيلة دفاعية ضد الهجمات وعمليات القرصنة على مختلف الحواسيب والشبكات.

وطبقا لتعريف الاتحاد الدولي للاتصالات (International Télécommunication Union) فإن الأمن السيبراني هو: "مجموعة الأدوات والسياسات ومفاهيم الأمن والضمانات الأمنية ومناهج إدارة المخاطر والإجراءات والتدريبات وآليات الضمانات والتكنولوجيا التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستخدمين".[2]

وتشمل البيئة السيبرانية أجهزة الحاسب الآلي والبرمجيات والتطبيقات الموجودة عليه والشبكات المتصلة من خلالها والعناصر البشرية والبنية التحتية وأنظمة الاتصالات فيما بينها، بالإضافة إلى جميع المعلومات سواء كانت محفوظة على الأجهزة أومنقولة فيما بينها، وفي ذلك يسعى الأمن السيبراني للحفاظ عليها وحمايتها من المخاطر والتهديدات السبرانية.

ويتبين من خلال هذا التعريف أن الأمن السيبراني يشمل جميع السياسات والوسائل والأدوات والمناهج لإدارة المخاطر وكذا حماية البيئة السيبرانية من المخاطر والتهديدات السيبرانية.

فالأمن السبراني يعني حماية المعلومات من خلال ثلاث محاور رئيسية: محور المعلومات الشخصية، محور المعلومات داخل الشركة ومحور المعلومات عبر الدول.

ومن ناحيته يعرفه قاموس "أكسفورد" على أنه: "الإجراءات والتدابير المتخذة للحماية من الاستخدام الإجرامي أوالاستخدام غير المصرح به للمعلومات الإلكترونية".[3]

[1]– المكان نفسه.

[2]– المكان نفسه.

[3]– المكان نفسه.

كما يمكن تعريف الأمن السيبراني على أنه: "الحد من خطر هجوم ضار للبرمجيات وأجهزة الكمبيوتر كذلك يشتمل على الأدوات المستخدمة للكشف عن عمليات الاقتحام ووقف الفيروسات ومنع المتطفلين من الوصول إليها". [1]

ويمكن تعريف الأمن السبراني انطلاقا من أهدافه بأنه: "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج ولا تتحول الأضرار إلى خسائر دائمة". [2]

الملاحظ من هذا التعريف أن حماية الموارد البشرية والمالية وكل ما يرتبط بتقنيات الاتصالات والمعلومات هي من أهداف الأمن السيبراني، والغرض من ذلك هوالحد من الخسائر والأضرار والحيلولة دون وصول هذه الأضرار إلى خسائر دائمة تعيق حركة الإنتاج وديمومته.

وكخلاصة فإن الحديث عن الأمن السيبراني يقود إلى أن:

– الأمن السيبراني هوتلك الوسائل والأدوات والسياسات الدفاعية لمواجهة مختلف التهديدات السيبرانية ومختلف عمليات القرصنة من أجل حماية البيئة السيبرانية.

– الأمن السيبراني يضمن إمكانات الحد من الخسائر والأضرار والحيلولة دون وصول هذه الأضرار إلى خسائر دائمة واحتوائها في أسرع وقت ممكن.

– الأمن السيبراني هوسلاح إستراتيجي بيد الحكومات والأفراد لاسيما أن الحرب السيبرانية أصبحت جزءا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول.

وتأتي أهمية الفضاء الإلكتروني كقضية تتعلق بالأمن القومي في ظل تزايد الاعتماد الدولي عليه فيما يتعلق بتسيير عمل البنية التحتية الكونية للمعلومات، ومن ناحية أخرى عكس حجم المخاطر المتزايدة أمام المنشآت المدنية والعسكرية مع تصاعد وتيرة الهجمات التي يقوم بها القراصنة أوتقف وراءها جهات أودول معادية أوحتى جماعات إرهابية، ليطرح بذلك أمن الفضاء الإلكتروني كقضية دولية وذلك مع أهميته على جميع الأصعدة الاقتصادية والسياسية والأمنية والاجتماعية.

[1] - Dan Craigen &Others, **"Defining Cybersecurity"**, (Technology innovation Management Review, Octobre 2014), p 14.

[2]– منى الأشقر جبور، "**الأمن السيبراني: التحديات ومستلزمات المواجهة**"، (جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، 2012)، ص 03.

وأدت علاقة الفضاء الإلكتروني بعمل عدد من المنشآت الحيوية سواء أكانت مدنية أوعسكرية في الوقت نفسه لإمكانية تعرضها لهجوم من خلاله، إما يستهدفه كوسيط وحامل للخدمات أوبشل 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 أوالحرب.[1]

ومن خلال هذه المعطيات يتضح أن قضية أمن الفضاء الإلكتروني أضحت قضية دولية تحظى بالمزيد من الاهتمام بشكل جعلها إحدى أولويات الأمن الوطني في العديد من الدول بل ارتباطها بالأمن الدولي ككل وهذا يتطلب وجود إستراتيجية خاصة يتكون أهم عناصرها في:

– إدراك درجة العلاقة بين أمن الفضاء الإلكتروني والأمن الوطني وبقضايا التنمية الاقتصادية والاجتماعية والاستقرار السياسي.

– أهمية وجود فهم للقضايا القانونية التي تتعلق بتكنولوجيا الإتصال والمعلومات وسوء استخدامها.

– أهمية وجود هيكل تنظيمي أومؤسسي يتولى مواجهة تلك المخاطر في وقت الطوارئ.

– فهم الإمكانيات والقدرات التقنية لتكنولوجيا الاتصال والمعلومات والاستخدام السيئ لها وفهم الأخطار المرتبطة به وكيفية الاستجابة لها تكنولوجيا.

– أهمية دور الأفراد في عملية الأمن بمعرفتهم بالإجراءات الأمنية التي يمكن أن تستخدم لتأمين مصادر تكنولوجيا الإتصال والمعلومات.

– أهمية وجود تعاون من جميع الفاعلين في مجتمع المعلومات العالمي لترسيخ ثقافة عالمية لأمن الفضاء الإلكتروني.[2]

المطلب الثاني: الأمن السيبراني وعلاقته بالمفاهيم ذات الصلة

مفهوم الأمن السيبراني يتشابك ويتداخل معه مفاهيم ومصطلحات أخرى الأمر الذي يخلق اللبس والتعقيد لذلك لابد من توضيح مواطن اللبس من خلال تقديم تعريفات لهذه المصطلحات وما يفرقها عن مصطلح الأمن السيبراني.

[1]– حنان علي سعادة، "**الأمن السيبراني والأمن المعلوماتي**"، تم تصفح الموقع يوم : 20 فيفري 2018. الرابط: http://ae.linkedin.com/sulse/D8A7D984D8A7

[2]– المكان نفسه.

الفرع الأول: الأمن المعلوماتي

يقصد بأمن المعلومات من زاوية أكاديمية العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية فيقصد به الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.

ومن زاوية قانونية فإن أمن المعلومات هومحل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أواستغلال نظمها في إرتكاب الجريمة، وهوهدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها.[1]

ويعتبر الأمن السيبراني مفهوم أوسع من أمن المعلومات حيث يتضمن تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أوالخارجية والتي يتم تخزينها في خوادم داخل أوخارج المنظمات من الاختراقات إضافة إلى ذلك فإن الأمن السيبراني يشمل بعض الأمور التي لا تندرج ضمن أمن المعلومات كحماية البنى التحتية والصواريخ الحربية وكاميرات المراقبة الرقمية[2]، كما أن الأمن السيبراني يهتم بأمن كل ما هوموجود على السايبر من غير أمن المعلومات بينما أمن المعلومات لا يهتم بذلك، إلى جانب ذلك فأمن المعلومات يهتم بأمن المعلومات الفيزيائية الورقية بينما لا يهتم الأمن السبيراني بذلك.[3]

الفرع الثاني: الأمن الإلكتروني

تعد الثورة الرقمية وعالم الانترنت في الوقت الحالي بيئة تنظم فيها الكثير من النشاطات الاقتصادية والإدارية والبحثية، كما تعد مجالا للتفاعل والتواصل والابتكار حيث لم يعد بالإمكان الاستغناء عن شبكات الانترنت ووسائل وتكنولوجيا الاتصال وحفظ البيانات والمعلوماتية في ظل الاتجاه نحوما يسمى بالإدارة والحكومة الإلكترونيتين والاقتصاد وكل هذه الأنواع من المعلومات والبيانات، حيث يتم تناقلها وحفظها في أغلب الأحيان عند شبكات الحواسيب، ومن هنا تأتي أهمية تأمين هذه الشبكات من مختلف التهديدات والمخاطر ولتجسيد ذلك ظهر ما يسمى بـــ"الأمن الإلكتروني" أوأمن المعلومات الإلكترونية، حيث بات يشكل جزءا أساسيا في أي سياسة أمنية وطنية وأصبحت الدول تنظر إليه كنظير منافس للأمن التقليدي ومُعَبر

---

[1]– فتيحة ليتيم، ونادية ليتيم، "**الأمن المعلوماتي للحوكمة الإلكترونية وإرهاب القرصنة**"، مجلة الفكر، العدد 12، (د ش، د س)، ص 239.

[2]– فهد الدريبي، "**ما هو الأمن السيبراني**"، تم تصفح الموقع يوم : 21 فيفري 2018. الرابط:
Https://www.fadvisor.net/blog/2017/11/what is Cyber security/

[3]– المكان نفسه.

عن سيادتها وأمنها الوطني، لذلك أصبح صُنَّاع القرار في معظم دول العالم يصنفون مسائل أمن المعلومات الإلكترونية كأولوية في سياساتهم الدفاعية الوطنية.[1]

فالأمن الإلكتروني يعني الحماية الناجمة عن جميع التدابير الرامية إلى منع الأشخاص غير المصرح لهم من الحصول على معلومات ذات قيمة يمكن أن تستمد من اعتراضهم.[2]

بينما يعتبر الأمن السيبراني مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به على شبكات الكمبيوتر، وسوء الاستغلال واستعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان واستمرار عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات سواء الخاصة بالأفراد أوالجهات في الفضاء السيبراني.

والملاحظ من خلال التعرض إلى تعريف الأمن الإلكتروني والأمن السيبراني أن هناك تداخل وتقارب بين المصطلحين فكلاهما يرمي إلى نفس الأهداف وهي حماية أمن المعلومات وسلامتها من الهجمات والمخاطر، والسعي إلى تأمين وحماية خصوصية البيانات سواء تعلق الأمر بالأفراد أوالمؤسسات أوالدول.

المطلب الثالث: أبعاد الأمن السيبراني

يرتبط الأمن السيبراني بمجالات مختلفة سياسية وعسكرية واقتصادية وقانونية واجتماعية بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من أي تهديدات سيبرانية محتملة ويمكن توضيح ذلك من خلال ما يلي:

الفرع الأول: البعد العسكري

تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني بما يسمح بسهولة تبادل المعلومات وتدفقها وبسرعة إعطاء الأوامر العسكرية والقدرة على إصابة الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي اختراق خارجي قد يتسبب في شن هجمات إلكترونية مضادة على شبكات القوة المسلحة وأجهزة الاستخبارات ومن ثم تدمير قواعد البيانات العسكرية

[1]– د م، "**النظام القانوني للأمن الوطني الإلكتروني في ظل الثورة الرقمية**"، تم تصفح الموقع يوم : 22 فيفري 2018. الرابط:

www.univ-chlef.dz/fdsp/images/PDF/JE-DROIT-2017.PDF

[2]- "**Electronics security**", Web Site Visited in : 22 Februay 2018. Link: https://www.the freedictionary.com/electronics+security

وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها أوقطع أنظمة الاتصال بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر.

كما يمكن أن يتم شل أنظمة الدفاع الجوي أوالتوجيه الإلكتروني للخصم فضلا عن إمكانية فقدان السيطرة على وحدات القيادة والتوجيه بالإضافة إلى فقدان العدو قدرته على التحكم أوالاتصال بالأقمار الصناعية.[1]

الفرع الثاني: البعد الاقتصادي

يرتبط الأمن السيبراني ارتباطا وثيقا بالاقتصاد فالتلازم واضح بين إقتصاد المعرفة وتوسيع استخدام تقنيات المعلومات والاتصالات كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدمة على كل المستويات، كما تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لدول كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث في إدارة كلفة إنتاجها بأفضل الشروط.[2]

يضاف إلى ذلك دخول العالم عصر المال الإلكتروني ضمن بيئة تقنية متحركة بعد إطلاق الخدمات الإلكترونية، إذ تتزايد استثمارات المصارف والمؤسسات المالية في مجال المال الرقمي وتتنافس الشركات على إصدار تطبيقات تسمح بآليات دفع آمنة، وقد وضعت بعض الدول تشريعات خاصة بحماية أموالها وما يمكن أن يثيره هذا الأمر من صعوبات وما يتطلبه من تشريعات للحد من بعض الجرائم الاقتصادية والمالية الخطيرة والعابرة للحدود كتبييض الأموال والتهرب من الضريبة.

فالأمن السيبراني يضمن تقديم الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، كما يضمن الإقبال عليها بما يترجم عمليا بتطوير أسس اقتصاد سليم.[3]

الفرع الثالث: البعد السياسي

يتمثل البعد السياسي للأمن السيبراني بشكل أساسي في حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية التي تعني حقها وواجبها في السعي إلى تحقيق رفاه شعبها في وقت تؤثر موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان الفرد أن يتحول إلى لاعب أساسي في اللعبة السياسية كما أصبح

[1]– محمد مختار، **مرجع سابق**، ص 06.

[2]– منى الأشقر جبور، **مرجع سابق**، ص 30.

[3]– **المرجع نفسه**، ص 31.

بإمكانه الإطلاع على خلفيات ومبررات القرارات السياسية التي تتخذها حكومته عبر الكم الهائل من المعلومات التي يمكنه الوصول إليها.[1]

بالمقابل لا يتوانى العاملون في الشأن السياسي من الاستفادة مما تقدمه هذه التقنيات للوصول إلى أكبر شريحة ممكنة من الأفراد والترويج لسياساتهم في العالم، ومدى التأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات والمبادئ والمواقف التي تروج لها، فقد استخدم "أوباما" مثلا الشبكات الاجتماعية بشكل مكثف خلال حملته الانتخابية كما تركت التسريبات لآلاف الوثائق الدبلوماسية السرية عبر الويكيليكس أثرا سلبيا على العلاقات بين الدول.[2]

الفرع الرابع: البعد الإجتماعي

تساهم شبكات التواصل الاجتماعي بشكل خاص في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الاجتماعية بأشكالها المختلفة، كذلك تشكل مشاركة جميع شرائح المجتمع ومكوناته وسيلة لتطوير المجتمع مما يتيح الفرصة للإطلاع على الأفكار والمعلومات وبما تكونه من حاجة لدى المجتمع في الحفاظ على استقرار الفضاء الإلكتروني والمجتمع الذي يرتكز إليه، كما أن انفتاح مجتمع ما على المجتمعات الأخرى يؤسس لتبادل خبرات وأفكار وتكوين آفاق للتعاون والتكامل.

يضاف إلى ذلك ما يقدمه هذا الفضاء من إمكانات وقدرات للمجالات العلمية والثقافية والخدماتية حيث يسمح للوصول إلى مناطق بعيدة وإلى فئات محددة، هذا فضلا عن الدور الذي يمكن أن يؤديه في تبادل المعلومات في أوقات الأزمات والكوارث بحيث تتأمن المساعدات في أسرع وقت.[3]

والمساهمة في الحفاظ على القيم الجوهرية في المجتمع كالإنتماء والمعتقدات والعادات والتقاليد عبر إنشاء مجموعات تهتم بنشر الوعي حول هذه المسائل، وفي هذا السياق يأتي التشديد من قبل المنظمات والهيئات الدولية على نشر ثقافة الأمن في الفضاء الإلكتروني وضرورة التعاون من قبل فئات المجتمع بكل مكوناته على تحقيقه وضمانه لحمايته من التهديدات السيبرانية ذات التأثير السلبي على أخلاقيات المجتمع والتجنيد لقضايا تمس الأمن والسلم الدوليين.

---

[1]- **المرجع نفسه**، ص 29.

[2]- **المرجع نفسه**، ص 30.

[3]- **المرجع نفسه**، ص 31.

وعليه لابد من بناء مجتمع مسؤول ومدرك لمخاطر الفضاء الإلكتروني له القدرة على التعامل بحد أدنى من قواعد السلامة مع إدراك للعواقب القانونية التي يمكن أن تترتب على بعض التصرفات التي تمارس في الفضاء الإلكتروني.[1]

الفرع الخامس: البعد القانوني

تعد العلاقة بين القانون والتكنولوجيات علاقة تبادلية فالتطورات التكنولوجية المختلفة تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية منها ولكن بصورة عامة تفتقد الجريمة السيبرانية في الوقت الحالي للأطر القانونية الصارمة للتعامل معها، ولعل ذلك يعود لعوامل مثل طبيعة الجريمة الإلكترونية في حدا ذاتها وصعوبة تحديد هوية مرتكبي تلك الجرائم ومرونة التعريفات المرتبطة بتكنولوجيا المعلومات، إلى جانب ذلك فإن الجرائم السيبرانية غير مقيدة بحدود الدول، الأمر الذي يقتضي تفعيل التعاون الدولي المشترك لمكافحتها.[2]

المطلب الرابع: العلاقة بين الأمن السيبراني والأمن القومي

في عصر الثورة التقنية والمعلوماتية وجب الوقوف على حدود التفاعل الرقمي القائم بين أمن المعلومات الإلكترونية والأمن القومي للدول، فمع انصهار الحدود الجغرافية وتقلص المسافات بين أركان المعمورة بفعل الثورة الإلكترونية؛ أحدثت هذه التغييرات العديد من التأثيرات على الأمن القومي نتيجة البيئة التكنولوجية التي أتاحت للدول إمكانية الولوج في فضاء إلكتروني يحوي العديد من عناصرها ومعلوماتها القومية والأمنية والاقتصادية والسياسية والاجتماعية وغيرها من المقومات.[3]

لقد أصبحت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة الإلكترونية إلى أخطار إلكترونية وتهدد بتحول الفضاء الإلكتروني لوسيط ومصدرا لأدوات جديدة للصراع المتعدد الأطراف ودورها في تغذية التوترات الدولية، ومن جهة أخرى فرضت تلك التطورات إعادة التفكير في مفهوم الأمن القومي الذي يُعنى بحماية قيم المجتمع الأساسية وإبعاد مصادر التهديد عنها وغياب

[1]– محمد مختار، **مرجع سابق**، ص 07.

[2]– المكان نفسه.

[3]– وليد غسان سعيد جلعود، "**دور الحرب الإلكترونية في الصراع العربي الإسرائيلي**"، مذكرة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية السياسية، (جامعة: النجاح الوطنية، كلية الدراسات العليا، 2013)، ص 53.

الخوف من خطر تعرض هذه القيم للهجوم، وبذلك يتوافر أمن الفضاء الإلكتروني حال تحقيق إجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات.[1]

فالأمن بمفهومه العام يشير نظريا وعمليا إلى: "السلام والطمأنينة وديمومة مظاهر الحياة واستمرار مقوماتها وشروطها بعيدا عن عوامل التهديد ومصادر الخطر".[2]

وإن للأمن القومي مفهوم خاص يشير نظريا وعمليا إلى:

"القيم النظرية والسياسات والأهداف العملية المتعلقة بضمان وجود الدولة وسلامة أركانها وديمومة مقومات استمرارها وشروط استقرارها وتلبية احتياجاتها وتأمين مصالحها وتحقيق أهدافها، وحمايتها من الأخطار القائمة والمحتملة داخليا وخارجيا مع مراعاة المتغيرات الداخلية والإقليمية والدولية".[3]

لقد أصبح الأمن السيبراني والإلكتروني جزءا لا يتجزأ من الأمن القومي خاصة مع تنامي حجم التهديدات وعلاقة البعد الإلكتروني بعمل المنشآت الحيوية سواء كانت مدنية أوعسكرية.[4]

ويمكن الإشارة هنا إلى أن الأمن القومي لأي دولة له محاوره الرئيسية والمتمثلة في المحاور العسكرية السياسية، الجغرافية، الاجتماعية، الاقتصادية والأمنية وأخيرا التقنية، وهوالمحور الذي يهم الدول اليوم نظرا لاستنادها على منظومة تقنية وإلكترونية عالية الدقة وغزيرة التكنولوجيا تعتمد على صناعة المعلومات والبحث العلمي والمعلوماتي في جميع الجوانب، وبهذا يمكن الإشارة إلى أن الأمن القومي المعلوماتي هوعبارة عن: "مدى جاهزية الدول من الناحية التقنية والمعلوماتية لحماية مخزونها الإلكتروني من المعلومات وعدم الوصول إليها بأية طريقة تقنية أوتقليدية".[5]

لقد أدخلت ثورة المعلومات دول العالم في هاجس أمني قوي خاصة وأن هذه الدول قد قامت بوضع مدخراتها القومية على شكل معلومات رقمية عبر فضاء مذاب الخصوصية وضعيف الأمن لبعض دول العالم وفائق السرعة وزئبقي بشكل كبير، مما زاد من الفجوة المعلوماتية القومية بين الدول.

---

[1]– عادل عبد الصادق، "**الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي**"، (المركز العربي لأبحاث الفضاء الإلكتروني، 2017)، ص 02.

[2]– علي عباس مراد، "**الأمن والأمن القومي: مقاربات نظرية**"، (الجزائر: إبن النديم للنشر والتوزيع، 2017)، ص 12.

[3]– المكان نفسه.

[4]– عادل عبد الصادق، "**المجال الأعلى للأمن السيبراني خطوة في دعم إستراتيجية الأمن القومي**"، تم تصفح الموقع يوم : 23 فيفري 2018. الرابط:

www.accronline.com/article-detal.aspx?!d=20284.

[5]–وليد غسان سعيد جلعود، **مرجع سابق**، ص 53.

شَكَّل هذا التفاوت المعلوماتي القومي بين دول العالم هاجس الخوف من الطرف الآخر ومدى امتلاكه للأسلحة التكنولوجية والمعلوماتية المدمرة والتي لم تعد حكرا على القطاعات العسكرية للدول فحسب بل أصبحت سلاحا تتقن استخدامه غالبية مستخدمي الحواسيب ووسائل الاتصال الحديثة، في صورة زادت من تفاعل المعلومات الإلكترونية والأمن القومي بحيث رفعت من وتيرة الخوف الذي تعاني منه شعوب العالم المعاصر.[1]

غدت مُتلازمة أمن المعلومات الإلكترونية والأمن القومي ضرورة قومية وجب على جميع دول العالم احتضانها والعمل على إدراجها ضمن سياساتها العامة، فغالبية المحتوى المعلوماتي لهذه الدول متوفر على الشبكات العالمية لذلك أصبح لكل بعد أومحتوى أومجالا أمنيا قوميا لأي دولة في العالم وجها معلوماتيا ورقميا ينبغي الحفاظ عليه[2]، ومواجهة ما يهدد بقاءها.

[1]– **المرجع نفسه**، ص 54.

[2]– **المرجع نفسه**، ص 55.

المبحث الثالث: التهديدات السيبرانية: مقاربة مفاهيمية

أصبحت التهديدات السيبرانية أحد التحديات الرئيسية التي يتحتم على الدول مواجهتها خلال الفترة الحالية ومع تزايد الاعتماد على الانترنت خاصة في المجالات التي تتعلق بالأمن القومي مثل الشبكات العسكرية والبيانات المالية والمصرفية وتزايد الحديث عن أهمية مواجهة هذه التهديدات.[1]

وفي هذا الإطار سيتم التعرض إلى ماهية التهديدات السيبرانية التي يمكن أن تتعرض لها الدول وسيتم توضيح ذلك فيما يلي:

المطلب الأول: مفهوم التهديدات السيبرانية

يستوجب التطرق إلى موضوع التهديدات السيبرانية توظيف بعض المفاهيم الأساسية التي لابد من التدقيق في استعمالها ومعرفة فحواها ومن بين هذه المفاهيم مفهوم التهديد.

ومن أبرز التعريفات التي قدمت لهذا المصطلح نذكر ما يلي:

الفرع الأول: تعريف التهديد الأمني

اشتقت كلمة "تهديد" من الناحية اللغوية من لفظ "هدد" ويقصد به محاولة إلحاق الضرر والأذى بشيء معين قصد الإخلال بالأمن.[2]

ويشار إليه في اللغة الإنجليزية (Threat) واللغة الفرنسية (Menace) ويُعبر التهديد عن وجود نية لإيذاء أومعاقبة أوإلحاق ضرر من خلال عمل عدائي على شخص معين.[3]

ويرى "تيري ديبيل" أن التهديد: "عمل نشط وفعال تقوم به دولة معينة للتأثير في سلوك دولة أخرى ويشترط نجاحه توفر عدة عوامل أبرزها المصداقية والجدية والقدرات التي تتناسب مع التهديد، وهناك ثلاث سمات يتميز بها التهديد وهي: درجة الخطورة ومدى احتمالية وقوع التهديد وعنصر التوقيت".[4]

ويَعتبر الباحث التشيكي "جان إيشلر" أن التهديد يعبر عن إرادة إلحاق الضرر بفاعل (الفرد/جماعة/دولة) ويشترط فيه توفر العناصر التالية:

---

[1]– محمد مختار، **مرجع سابق**، ص 05.

[2]– عادل جارش، "**مقاربة معرفية حول التهديدات الأمنية الجديدة**"، مجلة العلوم السياسية والقانونية، (فيفري 2017)، تم تصفح الموقع يوم : 25 فيفري 2018. الرابط:

democraticac.de/?p=43831

[3]– المكان نفسه.

[4]– المكان نفسه.

- أن يسبب حالة من الهلع والخوف.

- توفر القدرة على الاستهداف: سواء استهداف الدولة مباشرة أومواطنيها أوالدول المجاورة للدولة، وهنا يكون للتهديد تأثير جيوسياسي.

- درجة الخطورة: أي طبيعة الخطورة (محتملة، فعلية، كامنة) فكلما كان التهديد خطيرا كلما تطلب ذلك رد فوري فعال من الطرف المهدد. [1]

ويمكن الإشارة إلى أن التغيرات التي شهدتها البيئة العالمية ساهمت في بروز فواعل جديدة غير الدولة تزامن ذلك مع التغير في طبيعة التهديدات الأمنية وخروجها من النمط التقليدي العسكري إلى نمط جديد كتعبير عن زيادة التعقيد والحركية والتطور المستمر الذي يمس الظاهرة الأمنية خاصة مع التطورات الحاصلة في المجال التكنولوجي والتقني والمعرفي.

ومن بين أبرز هذه التهديدات ما أصطلح عليه بالتهديدات السيبرانية التي أصبحت تشكل هاجسا أمنيا بالنسبة للدول تحركها في الكثير من الأحيان فواعل أمنية غير تقليدية تحاول تحقيق أهدافها المنشودة وتعبر عن مجرى جديد للبعد الأمني في العلاقات الدولية.

الفرع الثاني: تعريف التهديدات السيبرانية

عندما نواجه التهديدات السيبرانية فنحن هنا نجد أن هناك أوجه للتشابه إلى حرب بين الجيوش فطوال التاريخ قد اختلفت المعارك في النطاق والتعقيد والإستراتيجية والتكتيكات، ولكن الشيء المشترك لكل هذه المعارك هو العدو الذي يسعى إلى الاستفادة من البنية التحتية وقدرات لشن هجوم آخر وهونفس الشيء بالنسبة للتهديدات السيبرانية؛ هي قدرة العدو على الاستفادة من البنية التحتية لاستغلال نقاط الضعف للضحية، كما هوالحال مع الجيوش في المعركة وكل عدو يوظف مختلف التكتيكات والتقنيات والإجراءات.[2]

والشيء الوحيد الذي يجعلها أكثر صعوبة وتعقيدا هوفهم آثارها التي تكون في الغالب أقل وضوحا ومع ذلك فاستخداماتها والآثار المقصودة والأهداف هي في معظمها نفسها.

---

[1]- المكان نفسه.

[2] **- "What is Cyber Threat? how to Explain Cyber Threat your CEO, Blog featured Article. How-to-Guides?"**, Web Site Visited in : 25 Februay 2018، Link: https://www.threatconnect.com/blog/how-to-Explain-Whati-is-a Cyber-threat/

ويعرف قاموس "أوكسفورد" التهديدات السيبرانية على أنها: "إمكانية محاولة إلحاق الضرر عن قصد ونية سيئة أوتعطيل عمل شبكات الكمبيوتر أوالنظام".[1]

ومن الناحية الاصطلاحية يمكن تقديم تعريف أكثر شمولا يرتبط بنقطة ضمان المعلومات بأنها: "أي ظرف أوحدث ينطوي على إمكانية التأثير سلبا على العمليات التنظيمية (بما في ذلك المهمة أوالمهام أوالصورة أوالسمعة) أوالأصول التنظيمية أوالأفراد من خلال نظام معلومات عن طريق الدخول غير المصرح به أوالتدمير أوالكشف أوتعديل المعلومات والخدمات".[2]

ويرجع ظهور التهديدات السيبرانية منذ سنة 1975م عندما اخترع كل من "ستيف جوبز" و"ستيف وزيناك" أول حاسوب شخصي، ومع ظهور الحواسيب الشخصية جاءت مشكلات المتسللين الذين يريدون الوصول غير المصرح به إلى المعلومات الشخصية إما للربح أوللقيام بأعمال غير قانونية.

وبالتالي فالتهديدات السيبرانية هي: "أي فعل ضار الذي يحاول الوصول إلى شبكات الحاسوب بدون ترخيص أوإذن من أصحابها".[3]

وتهدف هذه التهديدات إلى الإضرار بسمعة شركة أوشخص، سرقة تصميمات المنتج وبراءات الاختراع والتأثير على السياسات الحكومية، كما تتسبب هذه التهديدات في تدمير البنى التحتية والاقتصاديات والتحكم في نظام الطاقة والشبكات وأنظمة التحكم الصناعية والبيانات الخاصة بالمدنيين.

وفي معظم الحالات يتم إستخدام العديد من هذه التهديدات لإستغلال نقاط الضعف في المؤسسات أوالشركات والوصول إلى الأصول فعلى سبيل المثال يمكن إستخدام البرمجيات الخبيثة لسرقة بطاقات الإئتمان والبيانات الشخصية، كما يمكن إستخدامها في حملات متعددة كما هوالحال في مجال التحايل.

وتتميز التهديدات السيبرانية بالسرعة وتحدث في وقت واحد وتتخذ أشكالا عديدة.[4]

---

[1] –**Op-cit**,Web Site Visited in : 25 Februay 2018. Link: https://www.threatconnect.com/blog/how-to-Explain-Whati-is-a Cyber-threat/

[2]- **"Cyber Threat Basics, Type of Threat intelligence and best practices"**,Web Site Visited in : 25 Februay 2018. Link: https://www.secure works.com/Blog/Cuber-threat basics.

[3]- **Op-cit**, Web Site Visited in : 25 Februay 2018. Link: https://www.secure works.com/Blog/Cuber-threat basics.

[4] - **"Cyber Threat"**,Web Site Visited in : 25 Februay 2018. Link: itlaw.Wikia.com/Cyber-threat

ويمكن أن يكون التهديد السيبراني غير مقصود، ويمكن أن يكون متعمدا أومستهدف أوغير مستهدف ويمكن أن يأتي من مصادر متنوعة بما في ذلك الدول التي تقوم بعمليات التجسس وحرب المعلومات والقرصنة وقد تنشأ من أفراد أومنظمات.

ويقصد بالتهديدات غير المقصودة هي الناجمة عن الموظفين غير المدربين، وفشل المعدات التي تُعطَل عن غير قصد كأنظمة الكمبيوتر أوالبيانات الفاسدة.

وتشمل التهديدات المتعمدة؛ الهجمات المستهدفة وغير المستهدفة، الهجوم المستهدف عندما يقوم فرد أومجموعة أفراد بمهاجمة نظام البنية التحتية ويكون هجوم غير مستهدف عندما يكون الهدف المقصود من الهجوم غير مؤكد، ومثال ذلك عندما يتم إطلاق فيروس أودودة أوبرامج ضارة على الانترنت دون أي هدف محدد.[1]

وانطلاقا مما سبق ذكره يمكن استخلاص النقاط التالية:

- أن التهديدات السيبرانية هي جهد محدد يهدف إلى إلحاق الضرر بسلامة أوسرية أوأمن نظام دون سلطة قانونية.
- قد تنشأ التهديدات السيبرانية خارجيا أوداخليا وقد تنشأ من أفراد أومنظمات.
- تهدف هذه التهديدات إلى الإضرار والتأثير على السياسات الحكومية وتدمير البنى التحتية للدول.
- التهديدات السيبرانية تتميز بالسرعة وتتخذ أشكالا عديدة.
- التهديدات السيبرانية تتطور باستمرار؛ فبإمكان فرد أومجموعة أفراد في أي مكان من العالم أن يحاول بشكل سري اختراق الأنظمة التي تحتوي على معلومات حيوية أوشن هجمات مدمرة على البنى التحتية الحيوية.

المطلب الثاني: مصادر التهديدات السيبرانية

هناك مجموعة متنوعة من مصادر التهديدات السيبرانية يمكن تلخيصها فيما يلي:

1- مشغلوا شبكة بوتنيت: وهي شبكة تسيطر عليها أنظمة التحكم عن بعد لتنسيق الهجمات ولتوزيع مخططات التَصيُّد الاحتيالي والرسائل غير المرغوب فيها والهجمات الخبيثة.

2- الشركات المنافسة: وهي التي تقوم باستهداف شركات أخرى حيث تسعى للحصول على معلومات حساسة لتحسين ميزاتها التنافسية في مجالات مختلفة.

[1] -**Op-cit**,Web Site Visited in : 25 Februay 2018. Link: itlaw.Wikia.com/Cyber-threat.

3- الجماعات الإجرامية: تسعى الجماعات الإجرامية إلى مهاجمة الأنظمة لتحقيق مكاسب نقدية، وعلى وجه التحديد تستخدم هذه الجماعات المنظمة الرسائل غير المرغوب فيها والتصيد الاحتيالي وبرامج التجسس، البرامج الضارة والاحتيال عبر الانترنت.[1]

4- الدول: تستخدم أجهزة الاستخبارات لجمع المعلومات والتجسس، كما أن العديد من الدول تعمل بقوة على تطوير عقيدة حرب المعلومات والبرامج والقدرات، حيث تمكن هذه القدرات الدول من إحداث أثر كبير وخطير من خلال تعطيل الإمدادات والاتصالات والهياكل الأساسية والاقتصادية التي تدعم القوة العسكرية.

5- قراصنة اقتحام الشبكات: وتهدف هذه المجموعات إلى الانتقام، مطاردة الآخرين، الربح النقدي، والحصول على المعلومات غير المصرح بها ويتطلب ذلك قدرا كبيرا من المهارة والمعرفة بالحواسيب ويمكن للقراصنة تحميل البرامج النصية للهجوم والبروتوكولات من الانترنت وإطلاقها ضد مواقع الضحايا، في حين أصبحت أدوات الهجوم أكثر تطورا وأصبحت أيضا أسهل للاستخدام.[2]

6- برامج التجسس/ البرامج الضارة: حيث يقوم الأفراد أوالمنظمات بتنفيذ الهجمات ضد المستخدمين من خلال إنتاج وتوزيع برامج التجسس والبرمجيات الخبيثة والعديد من الفيروسات المدمرة في الكمبيوتر بما في ذلك فيروس ميلسا، دودة نيمدا، كود الأحمر، دودة سلامر ودودة الناسف.

7- الجماعات الإرهابية: تسعى هذه الجماعات إلى تدمير البنى التحتية الحيوية أوتعطيلها أواستغلالها لتهديد الأمن القومي ويسبب خسائر جماعية وإضعاف اقتصاديات الدول، لكن رغم ذلك ترى وكالة المخابرات الأمريكية أن هذه الجماعات تشكل تهديدا سيبرانيا محدودا وستبقى تركز على الأساليب التقليدية للهجوم.

[1] - **Op-cit**,Web Site Visited in : 25 Februay 2018. Link: itlaw.Wikia.com/Cyber-threat.

[2] –**Op-cit**,Web Site Visited in : 25 Februay 2018. Link: itlaw.Wikia.com/Cyber-threat.

المطلب الثالث: أنواع التهديدات السيبرانية

إن الثغرات ونقاط التعرض في التكنولوجيا الرقمية تجتمع معا لتحقيق بيئة من عدم الأمن فتطور شبكة الانترنت واكبها التطور في أشكال وأساليب الجرائم في الفضاء السيبراني، إذ من الممكن للتكنولوجيا الجديدة تسهيل جميع أنواع التهديدات السيبرانية والتي يمكن الإشارة إليها وإبرازها فيما يلي:

1- الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها الذي ارتبط بتقنية المعلومات، فقد أُصطلح على تسميتها في البداية بإساءة إستخدام الكمبيوتر ثم احتيال الكمبيوتر، فالجريمة المعلوماتية ثم جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر ثم جرائم التقنية العالية إلى جرائم الهاكر، فجرائم الانترنت وأخيرا السايبر كرايم.

وتُعرف الجريمة الإلكترونية بأنها: "مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أوأجهزة إلكترونية أوشبكات الانترنت أوتبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أوالتحقيق فيها ومقاضاة فاعليها".[1]

وقد اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الإقتصادي والتنمية للجريمة المعلوماتية في إجتماع باريس سنة 1983م على أنها: "كل سلوك غير مشروع أوغير أخلاقي أوغير مصرح به، يتعلق بالمعالجة الآلية للبيانات أونقلها".[2]

ويمكن تعريف الجريمة الإلكترونية بأنها: "كل أشكال السلوك غير المشروع والمتعمد الذي يرتكب باستخدام الحاسب الآلي المرتبط بالانترنت والتي تمس به أوبمحتوياته أوبالعمليات التي تتم بواسطته بغرض إلحاق الضرر بالضحية أوالكسب المادي أوغير ذلك من الأغراض من طرف أفراد على دراية كاملة بتقنيات التكنولوجيا المعلوماتية وأسرارها".[3]

[1]- ياسمينة بونعارة، "**الجريمة الإلكترونية**"، (جامعة: الأمير عبد القادر للعلوم الإسلامية، د س ن)، ص 03.

[2]- **المرجع نفسه**، ص 04.

[3]- المكان نفسه.

2- البرمجيات الخبيثة

(MalWare) هي إختصار لــ (Malcious Software) وتعني برمجية خبيثة، البرمجيات الخبيثة هي برامج تهدف إلى إلحاق الضرر بالحاسوب أوتعطيله وجمع المعلومات والتجسس وعرقلة العمليات، وتتمكن بطريقة غير شرعية من عدوى نظام الحاسب بدون معرفة أوعلم المستخدم من أجل اختراق جهازه والتجسس عليه.[1]

ومن أنواع البرمجيات الخبيثة نذكر ما يلي:

أ- أحصنة طروادة: (Trojan Horses)

هي برامج تتضمن تعليمات خفية تهدف للتخريب وإلحاق الضرر بالنظام على الرغم من أنه في ظاهره يبدو كأنه يؤدي أعمالا عادية، فهي توحي للمستخدم بأنها تقوم بعمل معين في حين أنها في واقع الأمر تؤدي عملا آخر تخريبي في الغالب، فتقوم أحيانا بالتجسس ومتابعة كل ما يتم عمله من إجراءات وتسجيله من بيانات على الجهاز المصاب بها وتقوم أحيانا أخرى بإحداث أنواع أخرى من الأذى على الأجهزة المصابة مثل تشفير البيانات أومسحها أوغير ذلك، ولا تتمكن أحصنة طروادة من نسخ نفسها أوالالتصاق بالبرامج الأخرى ولكنها تؤدي عملا معينا تم تصميمها من أجله.[2]

ب- القنابل المنطقية (Logic Bombs) والقنابل الموقوتة (Time Bombs)

هي من أنواع أحصنة طروادة وتعمل القنابل المنطقية عند حدوث شرط منطقي محدد مثل بلوغ الموظفين عددا معينا أورفع اسم أحد الموظفين من كشف الرواتب، أوكتابة كلمة معينة أوعند تشغيل برنامج معين لعدد محدد من المرات، أما القنابل الموقوتة فتعمل وفقا لتوقيت معين مثل ساعة محددة أويوم محدد.[3]

1- جميل حسين طويلة، "**البرمجيات الخبيثة**"، (دليل عملي لإستخدام البرمجيات الخبيثة وبرمجيات التجسس وإجراءات الوقاية والحماية منها، د س)، ص 10.

2- فاتن سعيد بامفلح، "**حماية أمن المعلومات في شبكات المكتبات- دراسة حالة أم القرى**"،(جامعة: الملك عبد العزيز، د س ن)، ص 15.

3- المكان نفسه.

ج- الديدان (worms)

لا تحتاج الدودة إلى برنامج آخر تلتصق به للقيام بدورها كما هوالحال بالنسبة للفيروس الذي يلزمه حاضن (Host) لتنفيذ مهمته، ولكنها تعمل بمفردها حيث لديها القدرة على إعادة توليد نفسها والانتقال من ملف إلى آخر ومن جهاز إلى آخر متصل بالشبكة لتحقيق الانتشار.

ولا تعمل الديدن على تخريب الملفات وإتلافها كما هوالحال بالنسبة للفيروسات ولكنها تسبب زيادة عبئ على تحميل الشبكة حيث تقوم باستهلاك الذاكرة أوالمعالج أوالأقراص أوسائر موارد الحاسب وقد تؤدي بالتالي إلى توقف النظام.[1]

3- الاختراق:

يشار إليه في اللغة الإنجليزية (Hacking) ويسمى باللغة العربية عملية التجسس أوالقرصنة، حيث يقوم أحد الأشخاص غير المصرح لهم بالدخول إلى نظام التشغيل في جهاز الحاسوب بطريقة غير شرعية ولأغراض غير مسموح بها مثل التجسس أوالسرقة أوالتخريب، حيث يتاح للشخص المتجسس (الهاكر) أن ينتقل أويمسح أويضيف ملفات أوبرامج، كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أوالتصوير أوالتخزين[2]، وبالتالي يكون المستهدف عرضة لسرقة معلوماته وبياناته سواء أكان فردا أومنظمة أودول لإلحاق الضرر المادي في بناها التحتية أوتهديد أمنها.[3]

والمخترقون هم أشخاص يتمتعون بقدرة عالية على كتابة وتصميم البرامج وفهم عميق لكيفية عمل الحاسب الآلي مما يسهل عليهم اختراق أنظمتها وتغييرها، وهناك نوعين من المخترقين:

---

[1]- المكان نفسه.

[2]- شيماء جابر، "**الاختراق وطرق الحماية منه**"، تم تصفح الموقع يوم : 26 فيفري 2018. الرابط:
Https://download-internet-pDF-ebooks.com/4926.Free-book

[3]- أوس مجيد غالب العوادي، "**الأمن المعلوماتي السيبراني**"، (سلسلة إصدارات مركز البيان للدراسات والتخطيط، أوت 2016)، ص 19.

الأول: الهاكر (White Hat)

هم في العادة أشخاص فائقوا الذكاء يسيطرون بشكل كامل على الحاسب ويجعلون البرامج التي تقوم بأشياء أبعد بكثير مما صمت له أصلا، لذلك نجد أن بعض الشركات العالمية توظف أمثال هؤلاء الهاكر لتستفيد من قدراتهم سواء في الدعم الفني أوحتى لإيجاد الثغرات الأمنية في أنظمة هذه الشركات.[1]

الثاني: الكراكر (Black Hat)

هم من يُسخّرون ذكائهم بطريقة غير شرعية، وهم يهتمون بدراسة الحاسب والبرمجة ليتمكنوا من سرقة معلومات الآخرين الشخصية، ويغير أولئك المخربون أحيانا المعلومات المالية للشركات وتخريب أنظمة الأمان بالإضافة إلى أعمال تخريبية أخرى[2]، وفي أسوأ الأحيان يقوم بالقضاء على النظام المعلوماتي الإلكتروني بشكل كلي والكثير منهم يقوم بسرقة برامج وتوزيعها مجانا لهدف، فمنهم من يضع ملف "الباتش" بين ملفات هذا البرنامج وفي الغالب يكون عمله تخريبي.[3]

وفيما يتعلق بأنواع الاختراقات يمكن تقسيمها إلى ثلاث أنواع وهي كالآتي:

1- اختراق الخوادم والأجهزة الرئيسية للشركات والمؤسسات أوالجهات الحكومية وذلك عن طريق اختراق الجدار الناري للخوادم بعملية تدعى المحاكاة، والتي تعني انتحال شخصية للدخول إلى النظام إذ أن عنوان ال(IP) يحتوي على عناوين المرسل والمرسل إليه وهذه العناوين تشكل مادة أساسية وثغرة كبيرة للمحترفين.

2- اختراق الأجهزة الشخصية واستراق ما تحويه من معلومات وتعد هذه الطريقة شائعة جدا من قبل الهواة والمحترفين.

3- التعرض للبيانات أثناء انتقالها والتعرف على شفرتها في حال كونها مشفرة، وهذه الطريقة شائعة لدى المحترفين الذين يحاولون سرقة أرقام بطاقات الإئتمان البنكية وكشف الأرقام السرية لها.[4]

---

[1]- فاروق فؤاد حسن، " **مدخل إلى أمن المعلومات وتعريف الجرائم الإلكترونية وكيفية الحماية والإستخدام الأمثل للموارد المتوفرة للوصول إلى أقصى درجات الحماية في دوائر وزارة الداخلية العراقية**"، (وزارة الداخلية: المديرية العامة للإتصالات والمعلوماتية، قسم التدريب والتطوير، شعبة الدراسات والبحوث، د س)، ص 12.

[2]- المكان نفسه.

[3]- **المرجع نفسه**، ص 13.

[4]- أوس مجيد غالب العوادي، **مرجع سابق**، ص 20.

الهجمات الإلكترونية التي تتم عبر الانترنت أوالفضاء السيبراني تمتاز بسهولتها لأن تلك الهجمات تتم عن بعد وأن عملية الاختراق لا تتم إلا بوجود عاملين أساسيين؛ الأول هوالبرنامج المسيطر ويكون في جهاز المخترق والثاني يسمى الخادم ويكون في جهاز الضحية يقوم بتسهيل عملية الاختراق.

والجدير بالذكر أن طرق الإختراق تختلف وتتعدد وتتطور بتطور التقنيات، ولكن يبقى العنصر الأساسي هوضرورة وجود إتصال بين جهاز المخترق وجهاز الضحية.[1]

4- الفيروسات

تعد الفيروسات من أخطر مهددات الأمن السيبراني لذا فإن مؤشر وجود فيروس يمثل جريمة سيبرانية من جرائم الحاسب، فالفيروسات تهدف إلى السيطرة على الجهاز والإضرار بالنظام وسرقة المعلومات وتمكين المخترقين من الوصول إلى المعلومات بسهولة وإتلاف محتويات النظام كافة.

والفيروسات من وجهة نظر برمجية هي عبارة عن برنامج أوتطبيق يتم تصميمه بواسطة أحد المبرمجين لتحقيق هدف معين من الأهداف التي تمت الإشارة إليها آنفا، لذلك يتم برمجته ليكتسب القدرة على التدمير أوفتح الثغرات للوصول إلى المعلومات وسرقتها أوالسيطرة على أنظمة معينة، ومن الممكن للفيروس استنساخ نفسه عدة مرات أوإعادة إنشاء نفسه والانتشار أوربط نفسه ببرامج أخرى ومن أهم أنواع هذه الفيروسات:[2]

- **باب المصيدة:** هورمز يتم توزيعه حين يتم تركيب باب الحماية كي يعطي للمخترق الحرية في اختيار الوقت المناسب لعملية التخريب، حيث يسمح هذا الرمز بالنفاذ من خلال الشبكات في ظل وجود نظم حماية معينة.
- **فيروس العتاد:** يعمل هذا النوع من الفيروسات على توليد ملايين العمليات الحسابية وعمليات الإدخال والإخراج المتتالية التي تؤدي إلى إرتفاع كبير في درجة حرارة المعالج المركزي وإحراقه.
- **الباتشيات (Trojans):** عبارة عن برنامج صغير قد يكون مدمجا مع ملف آخر للتخفي، حينما يتم تنزيله وفتحه يصيب الـــRegistry ويفتح منافذ مما يجعل الجهاز الخاص بالمستخدم قابلا للاختراق بسهولة ويعد من أذكى البرامج.[3]

---

[1]- المكان نفسه.

[2]- **المرجع نفسه**، ص 24.

[3]- **المرجع نفسه**، ص 25.

5- الهجمات الطمسية

وتتمثل في استهداف صفحات الويب واستبدالها بصفحات أخرى، إذ يقوم المهاجم بخلق موقع شبكي مماثل للموقع الأصلي لاصطياد المشتركين واستدراجهم لمعرفة معلوماتهم أوبطاقات الإئتمان الخاصة بهم وغيرها.

6- الهجمات الخداعية

تتم من خلال استخدام بروتوكولات النقل والتحكم (TCP/IP) في اختراق أمن النظام أثناء عمل العميل والخادم، حيث يعمل البروتوكول أعلاه على تأمين وصلة ربط آمنة بين أي عميلين من خلال أرقام المنافذ ومحددات الهوية المنطقية، حيث يقوم المهاجم بتخمين أرقام المنافذ التي تخص تبادل البيانات وبالتالي يحل محل المستخدم القانوني ويخترق جميع الجدران الواقية للوصول إلى قواعد البيانات للضحية ويستغل المتسللون البروتوكولات في شل الشبكات وإعادة توجيه البيانات نحو مقصد زائف، تحميل الأنظمة فوق طاقاتها من خلال غمرها برسائل متعددة لمنع مرسل من إرسال بياناته.[1]

[1]- **المرجع نفسه**، ص 18.

المبحث الرابع: الإطار النظري للدراسة

شهد حقل العلاقات الدولية زخما فكريا ونظريا كبيرا عبر مراحل وفترات زمنية مختلفة من أجل تفسير الواقع الدولي بشكل مفهوم ومستصاغ، لذلك تعددت النظريات التي تحاول فهم وتفسير المتغيرات من جهة ومن جهة أخرى إبراز أهم ما تطرحه هذه النظريات.

وبناء على ذلك وجب التوقف عند أهم النظريات لفهم سلوك إسرائيل لمواجهة التهديدات السيبرانية ودوافع إستراتيجيتها وهوما يمكن إبرازه فيما يلي:

المطلب الأول: النظرية الواقعية

الواقعية هي الطريقة التي يتم وفقها النظر إلى العلاقات الدولية كعلاقات قوة ويتعين علينا الرجوع إلى اليونان القديمة والصين إذا أردنا تتبع جذورها النظرية، إذ أسس "ثيوسيدس" للواقعية ولعلاقات القوة التي تقوم عليها عبر تأريخه للحرب التي دارت رحاها بين أثينا وأسبرطا والتي عرفت بـــ **الحروب البلوبونيزية**، وقد قال في هذا الصدد أن: "إرساء معايير العدالة يعتمد على نوع القوة التي تسندها وفي الواقع فإن القوي يفعل ما تُمكنه قوته من فعله أما الضعيف فليس عليه سوى تقبل ما لا يستطيع رفضه"، وبدوره أسدى "سان تزو" الإستراتيجي الصيني الذي عاش في زمن "موتي" النصح للحاكم وكيفية صيانة بقائه واستعمال القوة لتعزيز مصالحه خلال زمن الحرب.[1]

إضافة إلى كتابات كل من "هوبز" "Hobbes" الذي صور العلاقات بين الدول على أنها علاقات تصارعية نتيجة للطبيعة البشرية الشريرة في كتابه (leviathan)، وفي كتابات "نيكولا ميكيافللي" "N.Mackiavel" من خلال كتابه الأمير (Le prince) أين اعتبر أن سلطة الأمير لابد أن تكون محكمة وخالية من الأخلاق نظرا لما تتميز به الطبيعة البشرية من تصرفات عدوانية تمس سلامة الأشخاص لذلك يتوجب عليه ضمان الأمن لكل الأفراد.[2]

---

[1]– عادل زقاع، **مترجما**، "**مفهوم الأمن في نظرية العلاقات الدولية**"، ، تم تصفح الموقع يوم : 17 فيفري 2018. الرابط:

Bohothe.blogspot.com/2010/03/blog-spot-26.html.

[2]– زكرياء بودن، "**أثر التهديدات الإرهابية في شمال مالي على الأمن الوطني الجزائري وإستراتيجيات مواجهتها 2010–2014**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية، تخصص علاقات دولية ودراسات إستراتيجية، (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2015)، ص 32.

ويعتبر "هانس مورغانتو" أب الواقعية التقليدية فهو يرى بأن الدولة هي الوحدة المرجعية للتحليل ولا يمكن اعتبار الأفراد جزءا منفصلا عن الدولة، فمن خلال السعي لتحقيق الأمن تعمل الدول على تعظيم قوتها العسكرية، كما يعتبر "كينث والتز" أب الواقعية الجديدة إلى جانب "جون ميرشايمر"، فــ "كينث والتز" يؤكد عكس "مورغانتو" بأن النظام الدولي ذوطبيعة فوضوية نظرا لغياب سلطة دولية ذات سيادة، فالفوضى هي السبب في قيام الحرب بين الوحدات المشكلة للنظام الدولي، في حين يرى "مورغانتو" أن النظام الدولي يصبح فوضوي نتيجة التنافس بين الوحدات المشكلة له.[1]

لدى معظم الواقعيين إجابة مباشرة عن مشكلة النظام العام (order) وهوالسلطة المركزية الفعالة، فالحكومات التي تدافع عن الحدود وتفرض تطبيق القوانين وتحمي المواطنين تجعل السياسة الداخلية أكثر سلمية مختلفة نوعيا عن السياسة الخارجية وتبقى الساحة الدولية نظاما من الفوضى السياسية والمساعدة الذاتية وساحة من العنف تبحث فيها الدول عن فرص لاستغلال بعضها بعضا.[2]

يمثل الواقعيون المنظور الأكثر دفاعا عن فكرة اعتبار الأمن من صميم اهتمام وصلاحيات الدولة وحدها أي أن مفهوم الأمن الوطني يرتبط مباشرة بالدولة، حيث يفسر الأمن على أنه أمن الدولة ضد الأخطار ذوالتهديدات الخارجية من خلال حماية حدودها الإقليمية وصيانة سيادتها الوطنية واستقرارها.[3]

من جهة أخرى عرف حقل الدراسات الأمنية جدالا واسعا بسبب ظهور مجموعة من المدارس الفكرية حسب تعبير "أولي ويفر" التي ارتبطت بشكل واسع بأماكن كـــ: باريس (أعمال "بيغو" المستوحاة من أعمال "بورديو") وكوبنهاغن (الأمننة) وتحديها للنقاش الأمني المهيمن في مراكز البحث الأمريكية المقتصر على النظريات الواقعية (الهجومية/الدفاعية) ومدرسة "أبريستويث" أوما يعرف بمدرسة "ويلز"، فالمقاربات الأوروبية الجديدة تشترك حسب "أولي ويفر" في الفرضيات التالية:

---

[1]– **المرجع نفسه**، ص 33.

[2]– ديما الخضرا، **مترجما**، "**<u>نظريات العلاقات الدولية: التخصص والتنوع</u>**"، (الدوحة: المركز العربي للأبحاث ودراسة السياسات، 2016)، ص 173.

[3]– جويدة حمزاوي، "**<u>التصور الأمني الأوروبي: نحو بنية أمنية شاملة وهوية إستراتيجية في المتوسط</u>**"، <u>مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، تخصص دراسات مغاربية ومتوسطية في التعاون والأمن</u>، (جامعة: الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2011)، ص 20.

- إعادة التفكير في مفهوم الأمن.[1]
- الاهتمام بمسألة إمكانية توسيع وتعميق قطاعات ومرجعيات الأمن.
- الأمن كممارسة.
- الانعكاس الذاتي للمحلل الأمني واعتماده على الممارسة/الفاعل الأمني خلال المعضلة المعيارية.[2]

واستجابة لهذه التحولات سيتم التطرق إلى كل من مدرسة كوبنهاغن وتوسيعها للقطاعات والمرجعيات الأمنية واستخدامها لمتغير الأمننة كأداة جديدة في التحليل الأمني، وكذلك مدرسة باريس التي تنظر للأمن كتقنية حكومية ومهنيوا الأمن كفواعل والاعتماد على التكنولوجيا المتطورة في إدارة المخاطر.

المطلب الثاني: مدرسة كوبنهاغن

على غرار النقاشات النظرية لفترة ما بعد الحرب الباردة والتي نادت بضرورة توسيع الأجندة الأمنية تجاوبت مدرسة كوبنهاغن مع هذه التغيرات الدولية خاصة بعد ظهور العديد من التهديدات الأمنية الجديدة التي تميزت باختلافها عن الطابع التقليدي للتهديد الذي كان سائدا أثناء الحرب الباردة، بالإضافة إلى انتفاء سيطرة البعد العسكري على مجال الدراسات الأمنية.[3]

ساهمت مدرسة كوبن هاغن في توسيع وتعميق مضامين الأمن من خلال أعمال "باري بوزان" في كتابة (People, States and fear) سنة 1983م، الذي سعى إلى توسيع مجال البحث في قطاعات أخرى غير العسكرية تتمثل في القطاع السياسي، القطاع الاقتصادي، القطاع المجتمعي والقطاع البيئي، بالإضافة إلى إسهامات المدرسة في مفهوم الأمن المجتمعي ونظرية الأمننة.

يرى "ميشال ويليامز" أن مدرسة كوبنهاغن تتبنى شكلا من أشكال البنائية الاجتماعية ولها جذور في النهج التقليدي الواقعي.[4]

---

[1]- أمينة مصطفى دلة، "**الدراسات الأمنية النقدية**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية، تخصص دراسات إستراتيجية، (جامعة: الجزائر3، كلية العلوم السياسية والإعلام، قسم العلوم السياسية والعلاقات الدولية، 2013)، ص 51.

[2]- **المرجع نفسه**، ص 52.

[3]- أمينة دير، "**أثر التهديدات البيئية على واقع الأمن الإنساني في إفريقيا: دراسة حالة دول القرن الإفريقي**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية، تخصص علاقات دولية وإستراتيجية، (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2014)، ص 18.

[4]- المكان نفسه.

تعد نظرية الأمننة (Securitization) من أهم الإسهامات النظرية للمدرسة حيث طورها "أولي ويفر" "Ole Waever"، ترى هذه النظرية أن الأمن لا يتم التعامل معه كشرط موضوعي لكن بوصفه نتيجة عملية اجتماعية محددة، وقد حدد "ويليامز" السياق الفكري لنظرية الأمننة فيقول بأنها: "تدمج بين أفكار الواقعية الكلاسيكية المتأثرة بأعمال "كارل شميت" وأفكار البنائية الأخلاقية".[1]

فحسب "أولي ويفر" الأمن يفهم كفاعل خطابي فهويعني اعتبار شيء ما كقضية أمنية يكسبها ذلك الإحساس بالأهمية والاستعجال الذي يضفي الشرعية لاستخدام الإجراءات الخاصة خارج العملية السياسية المعتادة للتعامل معه.

إذا فالأمننة كعملية يتم فيها تحويل المشاكل إلى قضايا أمنية من خلال إضفاء الطابع الأمني عليها، تفترض أن الأمن يمكن أن يفهم على أنه نتيجة لأعمال خطاب (Speech Act)، أي عملية الاستخدام المتكرر لإظهار حدث ما على أنه تهديد وجودي من خلال لغة خطابية موجهة للجمهور العام تقدم من خلالها هذه القضية على أنها تمس المادي والمعنوي وتتطلب إجراءات استثنائية مستعجلة لتشريع الأفعال خارج العملية السياسية المعتادة، ويرى "بوزان" أن فواعل الأمننة (Securiting Actors) الأكثر شيوعا قد تكون حكومات، قادة سياسيين، لوبيات، جماعات ضغط[2]، والحجة الرئيسية لنظرية الأمننة هوأن الأمن عبارة عن فعل كلام، حيث تصبح المشكلة الأمنية مهددة لوجود الدولة يستدعي ذلك اتخاذ تدابير إستثنائية لضمان بقاء الدولة، وذلك بتشريع الأفعال وانتقالها من مجال السياسة العامة إلى عالم السياسة الطارئة، وبالتالي يمكن التعامل مع المشكلة الأمنية بسرعة واتخاذ إجراءات إستعجالية اعتمادا على مجموعة من القواعد واللوائح لصنع السياسات لهذا الأمن.

وحسب "باري بوزان" يكون ذلك من خلال إتباع ثلاث خطوات هي:

- تحديد التهديدات الموجودة.
- إعلان حالة الطوارئ.
- التأثير على العلاقات بين الوحدات عن طريق كسر القواعد.[3]

---

[1]- المكان نفسه.

[2]- **المرجع نفسه،** ص 19.

[3]- Rita Taureck, **"Securitization Theory and Securitization Studies"**, (university of institutional repository, 2006), p 03.

المطلب الثالث: مدرسة باريس

مع بداية التسعينات من القرن العشرين كان البناء السياسي للأمن محل اهتمام عدد من باحثي تحليل الممارسات الشرطية (أجهزة الرقابة والضبط الاجتماعي)، يعتبر تشكيل الأمن الداخلي أكثر الموضوعات تناولا في الأجندة البحثية المستندة إلى منظورات علم الاجتماع السياسي والنظرية السياسية، قدم هؤلاء الباحثون أجندة ترتكز على مهني الأمن (Security Professional)؛ أي العاملين في الأمن مثل: الجنود، الخبراء والعقلانية الأمنية وتأثيرات التنظيم السياسي للتقنية والمعرفة الأمنية. [1]

تقوم مقاربة مدرسة باريس بتعديل المنظور السائد للأمن عبر ثلاثة طرق، أولا بدلا من تحليل الأمن كمفهوم حتمي تقترح مدرسة باريس معالجة الأمن باعتباره تقنية حكومية (Technique Government)، ثانيا بدلا من التحقيق في النوايا الكامنة وراء استخدام القوة تركز هذه المقاربة على تأثيرات ألعاب القوة (Power) (Games، ثالثا بدلا من التركيز على أفعال الكلام (Speech Acts) تؤكد على الممارسات والسياقات التي تسعى إلى تشجع أوتعميق إنتاج أشكال محددة من الحوكمة.[2]

على عكس المدارس السابقة يعود مصدر المنظور المقترح من قبل مدرسة باريس ليس إلى تغير الموضوع المرجع بقدر ما يعود إلى تغير طبيعة التهديد والطريقة الملائمة لمواجهته.

أدت الطبيعة الجديدة والمتغيرة للتهديدات إلى إظهار مدى ترابط واعتمادية العديد من المهن المختلفة التي قد تؤدي دورا فعالا في المهام الأمنية، قد تشمل هذه المهن: الاستخبارات، مكافحة التجسس وتكنولوجيا المعلومات ونظم مراقبة المسافات الطويلة، وكشف أنشطة حفظ النظام وإعادة إرسائه، كل هذه المهن كما يؤكد "ديديه بيجو" تتقاسم المنطق أوالخبرة والممارسة ذاتها كما تتلاقى في وظيفة واحدة تحت عنوان الأمن.[3]

الأمن في مدرسة باريس نمط من أنماط الحوكمة يختزل في ممارسة الشرطية عبر تقنيات المراقبة تعمل الشرطية عبر شبكات تجسد روابط بين مختلف المؤسسات الأمنية الوظيفية التي تتجاوز الحدود الوطنية، وفي عالم معولم أصبحت أنشطة الشرطة أكثر اتساعا، هذه الأنشطة تتم على مساحة تتجاوز الحدود الوطنية كما تتجاوز أيضا في طابعها بعض أنشطة الشرطة التقليدية وتصل إلى الأنشطة الخارجية.

---

[1]– سيد أحمد قوجيلي، "**تطور الدراسات الأمنية ومعضلة التطبيق في العالم العربي**"، (أبوظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2012)، ص 32.

[2]– المكان نفسه.

[3]– **المرجع نفسه**، ص 33.

تعتبر فكرة المراقبة أوالعين الإلكترونية حسب "دايفيد ليون" تجسيدا معاصرا لفكرة البانوبتية عند "فوكو" الفكرة الأساسية هنا أن السلطة يجب أن تكون منظورة وغير ملموسة، تتخذ هذه البانوبتية في مجتمعنا المعاصر أشكالا عديدة: استخبارات الإتصالات، الاستخبارات الإلكترونية، استخبارات الرادار واستخبارات الصور، كلها تعمل تحت علامة الاستخبارات التقنية التي تشكل نظاما جديدا للقوة في العلاقات الدولية.[1]

وبشكل عام يمكن تلخيص تصور الأمن في مدرسة باريس في سلسلة النقاط التالية:

- الأمن تقنية حكومية.
- تقوم على فاعلية ممارسات الشرطية التي تستخدم تقنيات المراقبة.
- احتكار المعرفة لتحديد طبيعة التهديد وشكل الحقيقة الأمنية.[2]

مختلف الأجهزة الإدارية المنتشرة عبر الحدود الوطنية تعمل وفقا لشبكات وهياكل مؤسساتية وقواعد معلوماتية تبادلية تستخدم فيها التكنولوجيا العالية الدقة لاحتواء التهديدات الأمنية والتي نذكر: منها الجريمة

[1]- **المرجع نفسه**، ص 34.

[2]- **المرجع نفسه**، ص 35.

خلاصة الفصل الأول

تقتضي الدراسة في الأساس الإحاطة بالجانب المفاهيمي والنظري للموضوع المراد دراسته من خلال ضبط المفاهيم الأساسية التي أثارت جدالا واسعا بسبب غموضها، ويرجع ذلك بصفة عامة لخضوعها للتحولات والتغيرات التي شهدتها الساحة الدولية، ويأتي في مقدمة هذه المفاهيم مفهوم الإستراتيجية بتعريفاتها التقليدية والتي تركز على المجال العسكري وبفن الحرب وعلمها ليتوسع هذا المفهوم إلى مجالات أخرى نتيجة تطور الوسائل المستخدمة في العلاقات بين الدول.

ويعتبر مفهوم الأمن السيبراني من أكثر المفاهيم المثيرة للاهتمام والذي يعبر عن الوسائل الدفاعية والسياسات التي تتبعها الدول من أجل الحد من خطر التهديدات السيبرانية.

أن التطورات الحاصلة في مجال المعلومات والتكنولوجيا ساهم في بروز تهديدات أصبحت تشكل هاجسا أمنيا أمام الدول تحتم عليها مواجهتها وإتباع إستراتيجيات للوقاية منها، أدى ذلك إلى تنوع مصادر هذه التهديدات وهي بدورها أخذت أشكالا مختلفة تهدف إلى إلحاق الضرر والتخريب والقضاء على النظام المعلوماتي الإلكتروني ككل.

من بين أهم المقاربات النظرية التي يمكن بها تفسير توجيه دولة ما لإستراتيجيتها لمواجهة التهديدات السيبرانية:

– ترى النظرية الواقعية أن على الدول حماية أمنها الوطني من أي تهديد باعتبار الدولة المرجعية الأساسية واعتبار الأمن من صميم اهتمامات وصلاحيات الدول.

– وابتعاداً عن المجال العسكري تجاوبت مدرسة كوبن هاغن مع التغيرات الدولية خاصة بعد ظهور العديد من التهديدات الأمنية الجديدة، حيث ساهمت في توسيع وتعميق مفهوم الأمن وتعتبر نظرية الأمننة من أبرز إسهامات مدرسة كوبن هاغن التي تتطلب إجراءات إستثنائية للتعامل مع المشكلة الأمنية.

– اعتبار الأمن تقنية حكومية واعتماد تقنيات المراقبة والتكنولوجيا المتطورة التي تقوم على فاعلية الممارسات الشرطية هي الأسس التي تقوم عليها مدرسة باريس لتحديد طبيعة التهديد وإدارة المخاطر.

الفصل الثاني

الفضاء الإلكتروني في منظومة الأمن الإسرائيلي (الأسس والمقومات)

ينصب الجهد الإسرائيلي منذ سنوات طويلة إلى السعي نحو تدعيم البنيان الداخلي للدولة من حيث المؤسسات السياسية وتطوير البنية العسكرية وما يتبع ذلك من تطوير للاقتصاد و تنمية مداخيله وايجاد مكان بين الأمم، فإسرائيل التي وُجدت بفضل المجتمع الدولي وجدت نفسها في محيط لاتنتمي ولا تقيم علاقات مع دوله كان ذلك محفزا لها للسعي نحو تطوير وتدعيم مقوماتها في شتى المجالات السياسية، الاقتصادية والاجتماعية وغيرها، لتأمين ضمانات ضرورية وقوية للحفاظ على أمنها وبقائها.

كما أنها تدرك أن نجاحها في توطيد علاقاتها مع الدول الكبرى والمجتمع الغربي من أجل ضمان التأييد السياسي والعسكري والتكنولوجي والمالي اللازم عند الحاجة كفيل بتحقيق تطلعاتها وحماية مصالحا الحيوية والمستقبلية، وكما بادرت إلى تكثيف جهودها الالكترونية والتقنية الداعية لتدعيم امنها القومي لانها ترى بأن مثل هذه الإجراءات ستعزز من وجودها الأمني وبلوغ الاهداف القومية التي تستطيع إسرائيل أن ترسمها لنفسها.

مما سبق تم تضمين الفصل الثاني بثلاث مباحث وهي كالأتي:

- **المقاربة الإسرائيلية للأمن؛**
- **مراحل تطور قطاع أمن المعلومات الإسرائيلي؛**
- **مقومات الفضاء الإلكتروني الإسرائيلي.**

المبحث الأول: المقاربة الإسرائيلية للأمن

يتصدر موضوع الأمن القومي قائمة الأهداف الإستراتيجية الرئيسية لإسرائيل حيث يتم تحليل الأوضاع والمتطلبات الخاصة بهذه المسألة على أنها تشكل مرادفا لوجودها.

ويرتبط ذلك بالحفاظ على الأمن الإسرائيلي إزاء المخاطر والتهديدات سواء الداخلية أوالخارجية لذلك بلورت إستراتيجية متكاملة لمفهوم أمنها وسبل تحقيقه ووظفت لذلك مقوماتها السياسية والاقتصادية والتعليمية والثقافية[1]، إلى جانب مصادرها التقنية والتكنولوجية لبلوغ الأهداف المرسومة وصياغة مقاربة أمنية تقوم على حماية الدولة من التهديدات التي يمكن أن تتعرض لها.[2]

المطلب الأول: مرتكزات المقاربة الأمنية الإسرائيلية

الفرع الأول: المرتكزات الأساسية المساهمة في تشكيل العقيدة الأمنية الإسرائيلية

الرؤية الأمنية الإسرائيلية تقوم على تأمين ضمانات قوية وضرورية لأمن إسرائيل فالعقيدة الأمنية الإسرائيلية تعكس قناعات ثابتة على أن الأمن ما هوإلا تعبير عن تلك الحالة التي تشكل قوة الدولة، وبعد البحث في الركائز التي ساهمت في تشكيل العقيدة الأمنية الإسرائيلية يتضح ما يلي:

- ✓ معضلة توازن القوى بمعطياتها الكمية والنوعية.
- ✓ العمق الإستراتيجي الأمني.

وتتم معضلة توازن القوى من خلال معالجة بعض القضايا ولعل ما يبدأ في مقدمتها تعبئة القوى البشرية من أجل ضمان قوة الاحتياط الإسرائيلي والموارد المالية والتكنولوجية، فالعامل التكنولوجي يعتبر من أهم العوامل ويكسبها تفوقا إستراتيجيا.[3]

---

[1]– أحمد عواد نويران الفاعوري، "**التحولات الإقليمية العربية وأثرها على نظرية الأمن الإسرائيلي (2006–2012)**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، (جامعة: الشرق الأوسط، كلية الآداب والعلوم، 2011)، ص 01.

[2]– **المرجع نفسه**، ص 09.

[3]– بشير النجاي، "**مستقبل تأثير الإستراتيجية الأمنية الإسرائيلية على الأمن العربي الراهن**"، تم تصفح الموقع يوم : 02 مارس 2018. الرابط:

www.ahewar.org/s.asp?aid=578455&r=0&u=&i=o&q=

أما بالنسبة لمعضلة العمق الإستراتيجي فهذه الإشكالية تبناها رئيس الوزراء الإسرائيلي السابق الذي يعتبر من المؤسسين الأوائل لإسرائيل "دافيد بن غوريون" منذ سنة 1948م عندما تبنى مفهوم نقل الحرب إلى أرض العدو وعمل على تطويرها بعد سنة 1967م، من خلال الحدود الأمنية والحدود القابلة للدفاع.[1]

وبالتالي يستند الأمن القومي الإسرائيلي على أربع ركائز أساسية هي:

أولا: إدراك التهديدات سواء الخارجية منها أوالداخلية.

ثانيا: رسم إستراتيجية لتنمية قوى الدولة والحاجة إلى الانطلاق المؤمن لها.

ثالثا: توفير القدرة على مواجهة التهديدات الخارجية والداخلية ببناء القوة المسلحة وقوة الشرطة القادرة على التصدي لهذه التهديدات.

رابعا: إعداد سيناريوهات واتخاذ إجراءات لمواجهة التهديدات التي تتناسب معها، وتتصاعد تدريجيا مع تصاعد التهديد سواء خارجيا أوداخليا.[2]

الفرع الثاني: المبادئ الأساسية لمفهوم الأمن القومي الإسرائيلي

تتمثل في مبدأين مركزيين هما:

– **المبدأ الأول:** جيش الشعب (التجنيد الإلزامي الصغير، وجيش الاحتياط الكبير).

– **المبدأ الثاني:** ويتمثل في الركائز الثلاث التالية: مثلث الأمن: الردع، الإنذار المبكر والحسم.

✓ **الردع:** إن قوة الجيش وتفوقه والقدرات السيبرانية (وسائل الاتصال الإلكترونية) المتطورة لديه، هي التي تمكنه من الرد على أعدائه.

✓ **الإنذار المبكر:** إن القدرات الاستخباراتية والتكنولوجية ستمكن إسرائيل من جمع المعلومات عن أعدائها، وفي الوقت ذاته ستمنعهم من الوصول إلى قاعدة بياناتها مما يشكل إنذارا فعالا بشأن نية أعدائها.

[1]– **المرجع نفسه،** تم تصفح الموقع يوم : 02 مارس 2018. الرابط:
www.ahewar.org/s.asp?aid=578455&r=0&u=&i=o&q=

[2]– محمد محمد ماضي، "**الأمن القومي الإسرائيلي وأثره على الأمن الفلسطيني (1948–2012)**"، بحث مقدم لإستكمال متطلبات الحصول على درجة الماجستير في القيادة والإدارة، (أكاديمية: الإدارة والسياسة للدراسات العليا، 2015)، ص 29.

✓ **الحسم:** تستخدم إسرائيل قوتها وقدراتها القتالية التي تمنحها قدرات التفوق في أي معركة من خلال اعتمادها على وسائل عنف، وأدوات تقنية متقدمة بهدف حسم المعركة.[1]

المطلب الثاني: العوامل المؤثرة في تطور المقاربة الأمنية الإسرائيلية

الفرع الأول: دور العولمة والثورة التكنولوجية

إن العولمة والثورات التكنولوجية في مجالات الاتصال والسايبر والفضاء والتغيرات الجيوسياسية الإقليمية والدولية وتغير طبيعة الحروب والمستجدات في المجتمع الإسرائيلي، كلها عوامل تستدعي إعادة درس العقيدة الأمنية وملائمتها لظروف الواقع الديناميكي للقرن الحادي والعشرين، وتكتسب ملائمة العقيدة الأمنية لأهداف الدولة ولبيئتها الإقليمية والإستراتيجية المتغيرة أهمية خاصة.[2]

يتنامى تأثير الوسيط السيبراني الذي يحتل مكانا مركزيا في كل مجالات النشاط المدني والأمني في العالم، ولقد أضحت إسرائيل كغيرها من الدول المتطورة شديدة الاعتماد على الحواسيب وعرضة لهجمات السايبر، وفي مجال الحرب السيبرانية يكتسب الدفاع عن المؤسسات الحيوية للدولة في مجالات الطاقة والمياه والحوسبة والاتصالات والنقل والاقتصاد وكذلك حماية البنى التحتية الحيوية أهمية قصوى، وعلى المستوى القومي مطلوب تصور منظومي شامل للدفاع عن الأنظمة المحوسبة والذي يمكن تسميته بالدفاع السيبراني.[3]

يسمح الفضاء السيبراني للعدو بإلحاق أضرار كبيرة من دون القيام بخطوات مادية عنيفة ومن دون ترك بصمات تكشف عن هوية الفاعل.

وتتحدى المستجدات الكثيرة في مجال تكنولوجيا الحرب السيبرانية النظريات الأمنية الحالية وتتطلب إعادة درس المفاهيم الأساسية، وإدخال التعديلات اللازمة على العقيدة الأمنية لتكون قادرة على مواجهة التهديدات الجديدة.

إن تطور تكنولوجيا الفضاء في العالم وتغير طابع الحروب واتساع مجال التهديدات ضد إسرائيل جعلت استخدام الفضاء الإلكتروني لأغراض أمنية أمرا حيويا لإسرائيل، وهذا ما يقتضي إدراج هذا البعد في عقيدتها الأمنية.[4]

---

[1]– **المرجع نفسه**، ص 30.

[2]– رندة حيدر، "**العقيدة الأمنية الإسرائيلية وحروب إسرائيل في العقد الأخير**"، إشراف وتحرير: أحمد خليفة، (بيروت: مؤسسة الدراسات الفلسطينية، د س)، ص 32.

[3]– **المرجع نفسه**، ص 37

[4]– المكان نفسه.

ويشكل استخدام الفضاء الإلكتروني بعدا إستراتيجيا جديدا لإسرائيل بالإضافة إلى الأبعاد التقليدية الثلاثة "برا، بحرا، جوا"، وفي السياق الأمني العسكري يبرز بعد الفضاء منذ الثورة التكنولوجية والتغير في طبيعة المواجهات بصفته مكونا رئيسيا من مكونات العقيدة الحديثة لاستخدام القوة العسكرية وبتكامله مع تكنولوجيات الحوسبة فإنه يخلق مجموعة متكاملة من أنظمة جمع البيانات الاستخباراتية والقيادة والتحكم والهجوم ويضاف عملياكعنصر قوة مع هذه العناصر الثلاثة ويعزز قوتها مجتمعة على مستوى إدارة الحرب إستراتيجيا وعمليا وتكتيكيا.[1]

الفرع الثاني: التغير في طبيعة التهديدات وتنوع مصادرها

أولت إسرائيل للقطاعات التكنولوجية والتقنية بشكل عام وتلك العسكرية والإلكترونية منها على وجه التحديد اهتماما كبيرا منذ مطلع الخمسينات من القرن الماضي، لأنها تعلم أنه لا يكفي أن تتمتع بنظام أمني داخلي يحفظ أمنها أوأن تعتمد على علاقاتها الخارجية ودورها الوظيفي والاستثماري في المنطقة في حفظ أمنها من الهجمات الخارجية فقط، بل أن بروز التهديدات الأمنية الجديدة والتي من بينها التهديدات السيبرانية ساهم في تطور المقاربة الأمنية الإسرائيلية لأنها أصبحت إحدى التحديات التي تمس كل قطاعات الدولة وكذا أفراد المجتمع، لذلك تسعى إسرائيل إلى تكييف عقيدتها الأمنية استجابة للتغيرات التي طرأت على طبيعة هذه التهديدات .

فللعامل التكنولوجي دوره الوظيفي البارز في الأمن الإسرائيلي فهو يشكل أحد أهم مرتكزاته، حيث ترغب إسرائيل في أن تكون حاضنة لغالبية التكنولوجيات والإلكترونيات العسكرية في العالم فهي تعمد لأن تكون مصدرة لهذا العمل التقني نظرا لتدفق رؤوس الأموال الكبيرة من الخارج إليها، وتوظيفها في إنتاج التكنولوجيات المتطورة كالأمن المعلوماتي والاتصالات والإلكترونيات وبرامج الحاسب والانترنت الهادفة للتجسس وجمع المعلومات.[2]

[1]– **المرجع نفسه**، ص 38.

[2]– **المرجع نفسه**، ص 129.

لقد ذكر "حاييم وايزمن"* أن: "العلم سلاح إسرائيل الجبار الذي يجب أن يستغل ببراعة ومهارة وبكل وسيلة متوفرة لنا، العلم هوسلاحنا وشريان قوتنا ومصدر دفاعنا".[1]

وقد أكد "عاموس بيرلموتر" وهو عضو سابق في مؤسسة الطاقة الذرية الإسرائيلية على العلاقة بين العلم ونظرية الأمن الإسرائيلية قائلا: "في إسرائيل كان العلم دائما مرتبطا بقوة مع الأمن، فمنذ سنة 1947م نُظمت فروع علمية ضمن أكفأ العلماء وورث الجيش هؤلاء العلماء الذين أصبحوا جزءا من العاملين في وزارة الدفاع وطوروا البحوث في المجالات العسكرية والنووية".[2]

بادرت إسرائيل منذ سنة 1959م إلى تكثيف جهودها الإلكترونية والتقنية والمعلوماتية الداعية لتدعيم أمنها القومي في منطقة تعج بالصراعات الرافضة لمثل هذا الوجود الإسرائيلي، اعتمدت بذلك على العامل البشري الموجود لديها في هذا المجال وبالتعاون مع الولايات المتحدة الأمريكية والدول الكبرى لنقل غالبية ما تمتلكه هذه الدول من تقنيات حديثة ومتطورة إلى داخل العمق الإسرائيلي.[3]

ركزت في أولى خطواتها التقنية على تعزيز تكنولوجيات الفضاء الخارجي لديها، والتي رأت أن سيطرتها على الفضاء الخارجي سيعزز من وجودها الأمني لتنتشر مراكز التصنيع التكنولوجي في قلب تل أبيب والتي عملت على تصميم جميع متطلبات العمل الذاتي والتكنولوجي للأمن القومي الإسرائيلي.

كما أنشأت الحكومة في سنة 1959م لجنة قومية تُعنى بشؤون الفضاء وأمنية المعلومات والتي تعني في مضمونها ومن زاوية أكاديمية العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها ومن زاوية تقنية فيعني الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.

---

*– **الدكتور حاييم وايزمن:** هومن أشهر الشخصيات الصهيونية بعد "تيودر هيرتزل" ولقد لعب الدور الأهم في استصدار وعد بلفور الشهير سنة 1917م، وكان رئيسا للمنظمة الصهيونية العالمية منذ سنة 1920م حتى سنة 1964م ثم أنتخب كأول رئيس لإسرائيل سنة 1949م.(أنظر: الحسيني الحسيني معدي، "**مذكرات حاييم وايزمان**"،(القاهرة: دار الخلود للنشر والتوزيع، 2015)، تم تصفح الموقع يوم : 11 أفريل 2018. الرابط: http://www.beirutme.com/?p=22834).

[1]– صفاء خليل كاظم، "**البرنامج النووي الإسرائيلي، الدوافع، الاتجاهات، المضامين والسيناريوهات المستقبلية**"، مجلة جامعة جيهان– أربيل العلمية، المجلد1، العدد 01، (حزيران 2017)، ص 57.

[2]– المكان نفسه.

[3]– وليد غسان سعيد جعلود، **مرجع سابق**، ص 66.

وفي سنة 1964م قامت إسرائيل بعقد اتفاقية مع الولايات المتحدة الأمريكية على تشييد محطة للأقمار الإصطناعية والتجسسية المعلوماتية لكي لا تترك فضاءها الخارجي مكشوفا.[1]

وكانت أولى ابتكاراتها الصناعية الفضائية في سنة 1967م كتجربة أمنية ومعلوماتية أولية لتتوالى الابتكارات الإسرائيلية والتي قادها نخبة من القيادات لتصل إلى أعلى المستويات من التطور الأمني التقني.

وفي سنة 1983م تأسست وكالة سالا (Sala) الفضائية الإسرائيلية على يد وزير البحث العلمي الإسرائيلي آنذاك "يوفال نئمان" "Yafal Neeman" والذي قام بالعديد من الخطوات التقنية لخلق جيل إسرائيلي معلوماتي قادر على ربط أمن إسرائيل بالكوكبة الرقمية.[2]

وبإسقاط طرح النظرية الواقعية يتبين أن الأمن يعتبر من صميم الاهتمامات وصلاحيات الدولة وحدها أي أن مفهوم الأمن القومي يرتبط مباشرة بالدولة، حيث يفسر على أنه أمن الدولة ضد الأخطار والتهديدات الخارجية من خلال حماية حدودها الإقليمية وصيانة سيادتها الوطنية واستقرارها، لذلك يرى اللواء الإسرائيلي "أبراهام تمير" أن: "أية قوة أمنية قومية تبنى في ضوء مجالين: مجال علاقات القوة الأمنية الشاملة ومجال علاقات القوى العسكرية؛ وفي مجال علاقات القوة الأمنية الشاملة يجب أن يؤخذ في الحسبان اعتبار كل عناصر الأمن القومي: السياسي والاقتصادي، الاجتماعي، العلمي التكنولوجي، الديمغرافي والعسكري".[3]

ويأتي هذا المفهوم قريبا مما ذهب إليه "دافيد بن غورين" أول من أسس لمفهوم الأمن القومي الإسرائيلي الذي يقول: "أنه لا يستطيع أن يرى أي شيء إلا من خلال نظارة الأمن، وإن الأمن مرتبط بكل فروع الحياة...والأمن يضم كل شيء وكل شيء مشتق منه ولن يقوم أمن إسرائيل على الجيش والسلاح فقط رغم أنه دون هذين لا يوجد أمن".[4]

يعتبر الأمن القومي لدى إسرائيل قضية وجود شامل يمس صميم الوجود المادي وأكد ذلك اللواء "يسرائيل طال" بقوله: "أن الفحوى الكامل لعبارة أمن في حالتنا يطابق مفهوم الوجود عموما...فإستراتيجيتنا لا تتقرر من نسب القوى وحدود القوة بل أيضا الأهداف القومية التي تستطيع إسرائيل أن ترسمها

---

[1]– **المرجع نفسه**، ص 67.

[2]– المكان نفسه.

[3]– محمد محمد ماضي، **مرجع سابق**، ص 09.

[4]– المكان نفسه.

لنفسها...فوق كل شيء من الحافز لدينا، فقوة الحافز تتناسب طرديا مع مدى حيوية المصلحة الفردية والقومية".[1]

كخلاصة يمكن القول أن العلاقة بين الأمن القومي والتكنولوجيا أصبحت متزايدة مع إمكانية تعرض المصالح الإستراتيجية ذات الطبيعة الإلكترونية إلى أخطار تهدد بتحول الفضاء الإلكتروني الإسرائيلي لوسيط ومصدر لأدوات جديدة للصراع المتعدد الأطراف على اعتبار أن إسرائيل في تهديد مستمر من الدول المحيطة بها، وأن قضية الأمن هي المفتاح الرئيس لجميع خطوطها ومنهج عمل الحكومات والقيادات الأمنية والعسكرية وأصبحت بذلك متلازمة أمن المعلومات الإلكتروني والأمن القومي ضرورة قومية وجب على إسرائيل احتضانها والعمل على إدراجها ضمن سياساتها العامة.

[1]– دينا محمد جبر، "**الإستراتيجية النووية الإسرائيلية (الثوابت والمتغيرات)**"، (جامعة: بغداد، كلية العلوم السياسية، د س)، ص 02.

المبحث الثاني: مراحل تطور قطاع أمن المعلومات الإسرائيلي

مما لاشك فيه أن الدول أصبحت تولي اهتماما كبيرا بأمنها المعلوماتي في ظل التطورات الحاصلة والتي عرفتها البيئة الدولية، أدى إلى انتشار استخدام شبكات المعلومات على نطاق واسع على اعتبار أنها تمثل الأساس لجل أنشطة المرور المعلوماتي الوطني والدولي.

وتعتبر إسرائيل من الدول الرائدة في مجال أمن المعلومات والذي مر بعدة مراحل يمكن إبرازها فيما يلي:

المطلب الأول: المرحلة الأولى (1981م-1990م)

يعد عقد الثمانينات نقطة البداية في تاريخ واقع وخصائص تقنيات أمن المعلومات الإسرائيلي والذي أسهمت شركات إنتاج البرمجيات المضادة للفيروسات، وشركات حماية البرمجيات التطبيقية وتشفير شبكات المعلومات في إرساء أسسه والارتقاء ببنيانه.

حيث قامت الشركات الإسرائيلية بإنتاج برمجيات متخصصة لمكافحة الفيروسات المنتشرة في البنية التحتية للمعلومات في إسرائيل لكي يتم توظيفها في عمليات مكافحة الفيروسات التي بدأ قراصنة المعلومات الإسرائيليون بإنتاجها، وحتى التي تهدد شبكات المعلومات من الخارج.[1]

وظهور الشركات التي تعنى بتوفير آلية تشفير لحماية حقوق المعرفة العلمية للبرمجيات التطبيقية الإسرائيلية ومجابهة عمليات تصديع النظم الأمنية المصاحبة لها.

الجدول التالي يبين أهم شركات الأمن المعلوماتي الإسرائيلي خلال المرحلة الأولى:[2]

القطاع	الشركات الإسرائيلية
تقنيات مكافحة الفيروسات	Carmel software Eng, BRM & Eliashim
تقنيات التشفير	RSA, NDS

لم توفر الحكومة الإسرائيلية خلال هذه الفترة أي نوع من الدعم لهذا القطاع بسبب غياب الأهداف الواضحة وتبني نفس السياسات السائدة في ميادين البحث والتطوير التقليدية.

[1]- د م، "**الخطوات العامة لسياسة المعلومات في إسرائيل**"، (د م ن، د س ن)، ص 101.

[2]- المكان نفسه.

المطلب الثاني: المرحلة الثانية (1990م-1996م)

تعد هذه الفترة ثمرة مباشرة لعمليتين سادتا إسرائيل في ظل التأثيرات المتزايدة التي صاحبت انتشار شبكات المعلومات داخل المؤسسات العملاقة وخارج حدودها، كانت إحدى هاتين العمليتين عند بداية حقبة حضانة التقنية في قطاع الجيش والثانية مع زيادة انتشار الانترنت وخدماتها المعلوماتية المختلفة.

لقد احتضنت وزارة الدفاع الإسرائيلي (IDF) و"الموساد" الإسرائيلي جل أنشطة هذه الفترة ووجهتها صوب تحقيق أهدافها التي شملت حاجات أمنها المعلوماتي الذي يتضمن ضمان أمن تناقل المعلومات داخل حدود هاتين المؤسستين والبيئة المجاورة لها، والحفاظ على سرية محتوى هذه المعلومات بشتى أشكالها.

ولم يقتصر دور المؤسستين العسكرية والمخابراتية على توفير بيئة ثرية بالأفكار والمتطلبات الآنية فحسب، ولكنه قد أسهم أيضا في توفير موارد بشرية وخبرات معلوماتية متقدمة من المجندين الذين مارسوا خدمة الاحتياط في صفوف الجيش الإسرائيلي ثم عادوا للعمل في القطاع المدني.[1]

المطلب الثالث: المرحلة الثالثة (الفترة من 1996م وما بعدها)

تميزت هذه الفترة بظهور لغات برمجية جديدة تم توظيفها لتعميق قدرات شبكة الانترنت وخدماتها المعلوماتية، لكن في المقابل أدى ذلك إلى ظهور تهديدات معلوماتية جديدة بعد أن ذللت الكثير من العقبات التي تعترض الجهات التي تقوم بإنتاج الفيروسات وتجاوز العقبات الأمنية التي تقيمها الجهات التي تنهض بأعباء إدارة نظم المعلومات الحكومية والمؤسساتية.

فبدأت شركات إسرائيلية جديدة تعمل بنشاط لسد الفجوة التقنية في سوق المعلومات الإسرائيلية والعالم الخارجي المحيط بها وكان في مقدمتها شركات مثل: Netguard, Vanguard, Eagleege, Security7, Abirnet, Finjan، بالإضافة إلى ظهور شركات بميدان التجارة الإلكترونية بدأت تطرح منتجات وبرمجيات معلوماتية توفر بيئة معلوماتية آمنة لتداول رؤوس الأموال الإسرائيلية من خلال منع عمليات القرصنة التي يمارسها قراصنة المعلومات.[2]

ومنذ بداية عقد التسعينات حصل تغير ملموس في ميدان قطاع رؤوس أموال المخاطرة " Venture Capital" بحيث برزت إلى السطح لجنة "يوزما" "Yozma" بوصفها مؤسسة حكومية لتمويل أنشطة هذا

[1]- المكان نفسه.

[2]- **المرجع نفسه**، ص 102.

الميدان، وقد أسهم هذا النشاط الجديد في زيادة حجم الاستثمارات بميدان صناعة أمن المعلومات بشكل ملموس.

لقد بدأت السلطات الأمنية المعلوماتية الإسرائيلية تعتقد يقينا بعدم إمكانية تجاوز عقبة الأمن المعلوماتي لكيانها وأن آلية الحفاظ عليه لن تكون أسهل من الحفاظ على أمنها ووجودها، لذا فقد تبنت سلسلة من الإجراءات الأمنية والاحترازية لنقل البيانات والمعلومات من موقع إلى آخر، مع إجراء تعديلات مستمرة على هذه الإجراءات لكي تتناسب مع متطلبات كل مرحلة.[1]

من أجل ذلك عمدت إلى توظيف نظم معلوماتية ذات خمسة مستويات للحماية لضمان مستوى أمني معلوماتي محكم ضد هجمات قراصنة المعلومات من الداخل والخارج وتتمثل هذه المستويات فيما يلي:

يعالج المستوى الأول الهجمات التي تمتاز بكونها عفوية و لم تنشأ عن تخطيط مسبق، أما المستوى الثاني فيعنى بأنشطة القرصنة الخاصة بحصول مستخدم محلي في الشبكة على امتيازات تفوق الممنوحة له بموجب المكانة التي يتبوؤها والتي تشمل قراءة أدلة أوملفات أوتعديل محتوياتها، ويشمل المستوى الثالث جميع الأنشطة التي تنشأ عن تهديد معلوماتي قادم من خارج حدود النظام المعلوماتي يحاول صاحبه ممارسة عملية الدخول إلى الملفات الموجودة في مضيفات النظام، أما المستويين الرابع والخامس فيشملان جميع أنشطة القرصنة التي تفقده مقومات الكفاية المعلوماتية وتجعله عرضة لعمليات واسعة النطاق مثل: القراءة، التعديل والتغيير، تنفيذ برمجيات تطبيقية، استغلال موارد معلوماتية على شبكات النظام، أي أن هذين المستويين يجعلان عملية القرصنة متاحة وسهلة لاختراق النظام من طرف قراصنة المعلومات والعبث فيها.[2]

كذلك بدأت تركز اهتماماتها على آليات التشفير كإحدى وسائل الحماية الأمنية للمعلومات، فأصدرت قوانين وسنت تشريعات صارمة تمنع استخدام أي نوع من أنواع التشفير دون إذن مسبق من السلطات العسكرية، بالمقابل دعت إلى اعتماد هذه الآليات عند نقاط تناقل البيانات والمعلومات غير المحظورة على المواطن الإسرائيلي (Undassified Information) بين المؤسسات الحكومية الحساسة لضمان عدم تسربها إلى جهات معادية.[3]

---

[1]– المكان نفسه.

[2]– **المرجع نفسه**، ص 103.

[3]– المكان نفسه.

وكخلاصة لما سبق يمكن القول أن المراحل التي مر بها قطاع أمن المعلومات الإسرائيلي ساهم في توفير بيئة معلوماتية ثرية لاستخدام المعلومات وتداولها، لكن في المقابل أدى ذلك إلى بروز العديد من التهديدات التي يتوجب على الحكومة الإسرائيلية مواجهتها، هذه التهديدات التي قد تنشأ عن سوء استخدام هذه المعلومات والبيانات سواء على المستوى الداخلي أوالخارجي.

المبحث الثالث: مقومات الفضاء الإلكتروني الإسرائيلي

إن مقومات قوة الدولة المتغيرة ومتجددة حسب ظروف الواقع الدولي وهذا التغير يختلف من فترة زمنية إلى أخرى، بحيث لم يعد بمقدور الدولة أن تثبت مكانتها كقوة إقليمية أودولية بالاعتماد فقط على المقومات التقليدية للقوة بل تجاوزت المعنى العسكري الشائع إلى مضمون أوسع ليشمل جوانب سياسية واقتصادية وفكرية واجتماعية وأخرى ثقافية وتقنية، لذلك أصبح من الضروري الاعتماد على مقومات القوة العصرية ويعتبر امتلاك الهيمنة في الفضاء الإلكتروني أوالسيبراني علامة أساسية من علامات تقدم الدول وتأثيرها في البيئة الدولية.

تصنف إسرائيل في مصاف الدول المتقدمة تكنولوجيا ورقميا لما تتوفر عليه من مستويات عالية في المجال الرقمي والإلكتروني، والذي يؤهلها لخوض الحروب الإلكترونية والمعلوماتية حيث يتكون الفضاء الإلكتروني الإسرائيلي من العديد من المقومات للحفاظ على أمنها من الهجمات المعلوماتية الإلكترونية الآخذة بالتوسع ضدها.[1]

لذلك سيتم التطرق في هذا المبحث إلى أهم المقومات التي تتوفر عليها إسرائيل في مجال أمنها المعلوماتي والتي يمكن إبرازها على النحو التالي:

المطلب الأول: برنامج الفضاء الإسرائيلي "الفضاء الخارجي"

يعد الغزو الإسرائيلي للفضاء الخارجي أول الخطوات التأسيسية الإسرائيلية للحرب الإلكترونية وأحد أهم المجالات الحرب المعلوماتية التي تشنها إسرائيل على العالمين العربي والإسلامي، فمنذ أوائل ستينيات القرن الماضي إنصب الاهتمام النخبوي الإسرائيلي على تغطية الفضاء الخارجي بكافة الوسائل التي تمكنه من رصد أي تحركات من أعدائها.[2]

تبعا لذلك طورت إسرائيل سنة 1963م ما يعرف باللجنة القومية لبحوث الفضاء والتي أنشأتها كخطوة أولى في هذا المجال، مع إشراك العلماء والمختصين الإسرائيليين في إعداد البحوث والمؤتمرات المتعلقة ببحوث الفضاء والتركيز على تطوير البنية الصناعية الفضائية الإسرائيلية كخطوة تبقى متجددة في إسرائيل والتي أثمرت بانضمامها إلى نادي الفضاء العالمي.[3]

---

[1]– وليد غسان سعيد جعلود، **مرجع سابق**، ص 133.

[2]– **المرجع نفسه**، ص 134.

[3]– المكان نفسه.

شاركت هذه الجهود الإسرائيلية في العديد من مراكز الأبحاث المتخصصة بالإنتاج الأمني والعسكري الفضائي، ففي منتصف الستينيات وبداية السبعينيات من القرن الماضي تم تأسيس محطات لإنتاج وبرمجة الأقمار الإصطناعية لغزو الفضاء الخارجي كهيئة تطوير الأسلحة الإسرائيلية (رافائيل) والتي تعتبر من أكبر الشركات الصناعية الخاصة بتصنيع الأسلحة الحربية والتكنولوجيا العسكرية فيها.[1]

لم تتوانى إسرائيل عن تدعيم برنامجها الفضائي والذي يضم أبعادا أمنية وعسكرية وتقنية ورقمية في محاولة منها لتزويد قوتها بالأقمار الإصطناعية والمعدات التجسسية وغيرها من وسائل جمع المعلومات ليستمر الحراك التكنولوجي الإسرائيلي المنادي بضرورة استحواذها على برامج لفضائها الخارجي ويؤهلها لخوض الحروب الإلكترونية المستقبلية عبر الأقمار الاصطناعية.[2]

وفي هذا السياق تتمثل قدرات إسرائيل في مجال الأقمار الصناعية "التجسسية" فيما يلي:

1. القمر (أفق1) (Ofeq1): تم إطلاق هذا القمر إلى الفضاء الخارجي بتاريخ 1988/09/19م حيث كان عبارة عن قمر تجريبي خصص لأغراض التجسس، ولكن ضمن الأطر المحدودة نظرا لكونه قمرا تجريبيا قليل الإمكانيات التقنية والتكنولوجية.

2. القمر (أفق2) (Ofeq2): يعتبر أكثر تطورا من القمر الذي سبقه لتتسع دائرته الوظيفية حيث زود بآلات تصوير عالية الدقة وذات أبعاد استكشافية مهمة، تم إطلاقه إلى الفضاء الخارجي بتاريخ 1990/04/03م[3].

3. القمر (تكسات1) (TKSAT1): في شهر مارس من سنة 1995م حاول مجموعة من الطلبة الإسرائيليين المتخصصين في مجال التقنيات الفضائية والمعلوماتية إطلاق هذا القمر الصناعي المخصص للأغراض العلمية في الفضاء الخارجي وذلك بالتعاون الروسي إلا أن تجربتهم باءت بالفشل.

4. القمر (أفق3): بدأ التقنيون الإسرائيليون بإجراء دراسات مكثفة على الأقمار الصناعية التي تم إطلاقها في السابق، وقد تكللت نتائج هذه الدراسات بالنجاح بتاريخ 1995/04/05م، حيث أطلق هذا القمر إلى الفضاء بجاهزية عالية جدا وزود بكاميرات رقمية متطورة ذات إمكانيات تصورية كبيرة تصل إلى مسافات

---

[1]– المكان نفسه.

[2]– **المرجع نفسه**، ص 136.

[3]– منذر سلامة أبوسويرح، "**الإستخبارات الإسرائيلية: البناء التنظيمي ووسائل التجسس**"، (د م ن، د د ن، 2016)، ص 63.

بعيدة وضمن أي ظرف، علاوة على الخصائص التكنولوجية الأخرى التي يتمتع بها هذا القمر الإسرائيلي الصنع.[1]

5. القمر (عاموس) (Amos): تم إطلاقه بتاريخ 1996/07/16مخصص لأغراض الاتصالات والتواصل وهوعبارة عن قمر ثلاثي المحاور يقوم بنقل المعلومات إلى القواعد الأرضية مع إمكانية استخدامه في إدارة أعمال القوات الإسرائيلية المتعلقة برصد المعلومات والاختراقات الإلكترونية الأخرى.[2]

6. القمر (أفق5): تم إطلاقه بتاريخ 2002/05/28م جمع هذا القمر الكثير من الخصائص التي تمتعت بها الأقمار الإسرائيلية السابقة ولكن بشكل أكثر تطورا، مما أدخله بقوة في مجالات التجسس والاستطلاع العسكري والمجالات الإلكترونية الأخرى.[3]

7. القمر (بولاريس) (Polaris): يضاهي هذا القمر تكنولوجيا الأقمار الصناعية الأمريكية وله قدرة عالية على تغطية مساحات واسعة ومخصص للاستخدام العسكري، وذلك عبر توجيه الحزم الإلكترونية المطلقة نحو أهدافها بشكل عالي الدقة.

8. القمر (أفق9): أطلق هذا القمر في سنة 2010م لتدعيم تجسسها على إيران مع العلم أن إسرائيل تمتلك منظومة أقمار صناعية تقدر بعشرة (10) أقمار تسبح في الفضاء الإيراني.

ولهذه الأقمار قدرة على إعاقة شبكات الإتصالات السلكية واللاسلكية للدول العربية والإسلامية وذلك عبر وسائل الاستطلاع التي تمكن إسرائيل من اختراق هذه الشبكات الاتصالية والتواصلية.[4]

وهوما يتوافق مع طرح مدرسة باريس التي ترى بأن التغير في طبيعة التهديدات أدى إلى إظهار مدى ترابط واعتمادية العديد من المهن المختلفة التي قد تؤدي دورا فعالا في المهام الأمنية، وقد تشمل هذه المهن الاستخبارات، مكافحة التجسس ونظم مراقبة المسافات الطويلة والقدرة على توفير المعلومات المفصلة التي تعتبر بمثابة مصدر تقني إستراتيجي للحقيقة الأمنية.

---

[1]– **المرجع نفسه**، ص 64.

[2]– المكان نفسه.

[3]– **المرجع نفسه**، ص 65.

[4]– **المرجع نفسه**، ص 66.

المطلب الثاني: الأجهزة المخابراتية والمعلوماتية الإسرائيلية

الفرع الأول: المؤسسة العسكرية الإسرائيلية

يتميز المجتمع الإسرائيلي بصبغة عسكرية شاملة فجميع فئاته لهم القدرة على حمل السلاح وأداء الخدمة الإلزامية، ولهذا السبب ينطبق على هذا المجتمع صفة "المجتمع المسلح" أو"الأمة المسلحة" أو"جيش له دولة" كما يصف الإسرائيليون أنفسهم.

لذلك تعتبر المؤسسة العسكرية أداة لتحقيق الأهداف السياسية والمصالح الإستراتيجية للدولة، كما تتغلغل في معظم أوجه الحياة السياسية بدءا بإقامة المستوطنات وتنظيم الهجرة إلى الأراضي الفلسطينية وتحقيق التكامل بين المهاجرين إليها، وتنظيم البرامج التعليمية لأفراد الجيش ومراقبة أجهزة الإعلام وتوجيهها وتطوير البحث العلمي إلى تحديد حجم الإنفاق العسكري والتأثير على مجال الصناعة وخاصة الصناعات الحربية والإلكترونية.[1]

ويعتبر التطور التكنولوجي والعلم من أهم مرتكزات المؤسسة العسكرية كون التفوق فيها يساعد في التغلب على مجالات كانت تدفع إسرائيل لزيادة الاهتمام بها بحيث تضع جميع الطاقات الصناعية في إسرائيل تحت تصرف وقيادة المؤسسة العسكرية، لذا فإن الصراع العربي الإسرائيلي أصبح في فترات عديدة صراعا علميا بفعل تطور الأسلحة المستخدمة من قبل كل طرف ضد الطرف الآخر كما أسهمت معطيات عديدة في دعم هذا التطور العلمي والتكنولوجي، الأمر الذي وفر لها وسائل التقدم وزاد في توسيع القاعدة العلمية والتكنولوجية بشقيها المدني والعسكري ومما زادا في إتساع الفجوة بينها وبين العرب.[2]

يعد الجيش الإسرائيلي من الجيوش العالمية المتطورة من الناحية التقنية ومن حيث نوعية العتاد العسكري، حيث تمتلك إسرائيل ترسانة عسكرية تقنية متطورة كونها تحتوي على أحدث الأسلحة الأمريكية هذا بالإضافة إلى الأسلحة التي تم تطويرها في المؤسسات الصناعية العسكرية، كما تتمتع بالقدرة على اعتراض الصواريخ الباليستية عن طريق شبكة صواريخ "آرو" المطورة محليا وأنظمة باتريوت.[3]

---

[1]– د م، "**تحليل للتطورات السياسية والأمنية**"، مجلة باحث للدراسات الفلسطينية والإستراتيجية، العدد 28، (نوفمبر 2016)، ص 02.

[2] – محمد حسين المومني، وسعد شاكر شلبي، "**المؤسسة العسكرية في النظام السياسي الإسرائيلي**"، (الأردن: دار الحامد للنشر والتوزيع، 2013)، ص 119.

[3]– رأفت خليل حمدونة، "**القدرة العسكرية الإسرائيلية 2017**"، (مركز الأسرى للدراسات والأبحاث الإسرائيلية، 2017)، ص 19.

– **قوة السايبر**: أنشأ الجيش الإسرائيلي قوة السايبر كسلاح عسكري يشبه في قوته سلاح الجو وسلاح البحرية وسلاح المشاة، ومن أجل الاستعداد لمواجهة هجمات "السايبر" الإلكترونية أقامت إسرائيل شبكة قومية للدفاع بواسطة السايبر وعينت رئيسا لها، وتعتبر هذه الشبكة إحدى قوى السايبر والحرب الإلكترونية الخمس الرائدة في العالم لها القدرة على اختراق العالم مع التكنولوجيات التي طوروها.[1]

لقد استحدث الجيش الإسرائيلي أهم المعايير في استخدام القدرات الدفاعية والهجومية في عالم السايبر والتي يمكن إبرازها على النحو التالي:

1. العالم الافتراضي في شبكة الانترنت هوجبهة قتالية تتضمن عمليات هجومية ودفاعية وجمع المعلومات.

2. نظرا لأهمية عالم السايبر قررت قيادة هيئة الأركان في الجيش الإسرائيلي إقامة قيادة خاصة بهذه الجبهة القتالية تكون تابعة لرئيس هيئة الأركان وتكون مسؤولة عن التخطيط وتنفيذ العمليات الهجومية والدفاعية عبر شبكة الانترنت.[2]

3. اقتناء كل ما تنتجه هيئات الصناعات العسكرية التكنولوجية في العالم من قدرات تقنية ذات بعد عسكري توفر حماية كاملة للمنشآت الحساسة من أي اختراقات أوهجمات قرصنة من خلال دائرة الدعم اللوجيستي.

4. تطوير القدرات العسكرية لوجود قاسم مشترك بين جميع الأذرع العسكرية في الجيش الإسرائيلي: البر، البحر والجو والسايبر والتي لها دور كبير في توحيد الردود والمبادرات العسكرية.

لا يمكن الحديث عن تطوير للقدرات العسكرية الممكنة في الجيش الإسرائيلي دون توفر إمكانات استخباراتية قوية تابعة للجيش: استخبارات قومية، استخبارات إستراتيجية، استخبارات عملياتية تعتمد على المعايير التالية:

– الاهتمام بجمع المعلومات عن كل ما يتصل بتشكيل مخاطر جدية على إسرائيل حتى ولو لم تكن بصورة مباشرة من جميع الجبهات القتالية الحالية والمرشحة في المستقبل.

– جمع المعلومات الاستخباراتية اللازمة حتى يستفيد منها الجيش الإسرائيلي في إعداد الأهداف على المدى القريب والبعيد، يمكن اللجوء إليه في فترة زمنية قصيرة.[3]

---

[1]– المكان نفسه.

[2]– عدنان عبد الرحمان أبوعامر، **مترجما**، "**إستراتيجية الجيش الإسرائيلي**"، إعداد: الجيش الإسرائيلي، العدد 79، (بيروت: مركز الزيتونة للدراسات والاستشارات، سبتمبر 2015)، ص 52.

[3]– **المرجع نفسه**، ص 53.

هذه المعلومات توفر على الاستخبارات الإسرائيلية القدرة على تتبع العدو في كل المواقع التي قد يلجأ إليها وضرورة مرور عملية جمع المعلومات في جميع القنوات القيادية.

تحتل وحدة السايبر في الجيش حيزا خاصا ومهما من خلال بناء جيش سايبر وتحويل هذا الذراع إلى إحدى أهم وسائل الدفاع والهجوم في الحروب الإسرائيلية المقبلة وفي العمليات السرية المختلفة.[1]

وبإسقاط طرح مدرسة باريس فإن استخدام تقنيات المراقبة المتطورة من طرف مهينوا الأمن وفقا لشبكات وهياكل مؤسساتية وقواعد معلوماتية تبادلية يؤدي إلى احتواء التهديدات الأمنية العابرة للحدود، حيث أصبحت أنشطة مهنيوا الأمن أكثر اتساعا تتم على مساحة تتجاوز الحدود الوطنية كما تتجاوز في طابعها بعض أنشطة الشرطة التقليدية وتصل إلى كل الأنشطة الخارجية.

الفرع الثاني: جهاز الأمن الداخلي الإسرائيلي المخابرات العامة (الشاباك)

"الشاباك" هو عبارة عن جهاز استخباراتي معلوماتي أمني يخضع مباشرة لرئاسة الحكومة الإسرائيلية أنشأ سنة 1949م ، مكلف بوقاية الأمن الداخلي للدولة وحماية معلوماتها الداخلية والقومية وكشف الأنشطة التجسسية.

يركز "الشاباك" في عمله بشكل كبير على المقاومة الفلسطينية وإجهاض مخططات المقاومة في ضرب العمق الداخلي لإسرائيل، حيث يعمل به آلاف من الوكلاء والعملاء السريين وغير السريين والموزعين على مختلف الأماكن والمناطق الفلسطينية والإسرائيلية.

يهتم هذا الجهاز بجمع المعلومات الاستخباراتية وتحليلها بشكل معلوماتي وأمني، ومن ثم تقديمها للجهات المختصة.[2]

ويعتبر أصغر الأجهزة الاستخباراتية الأمنية في إسرائيل، ومن مهامه جمع المعلومات حول الأشخاص المرشحين لمناصب ووظائف حساسة ومن اختصاصاته توفير الحماية الشخصية لكبار مسؤولي القطاع العام وتأمين البنية التحتية وحماية شركات الطيران الإسرائيلي والسفارات في الخارج.[3]

---

[1]– نضال محمد وتد، "**جنود السايبر**"، مجلة الراصد للشؤون الصهيونية، مركز غزة للدراسات والإستراتيجيات، (فيفري 2017)، ص 04.

[2]– وليد غسان سعيد جعلود، **مرجع سابق**، ص 142.

[3]– نصر الدين ديب سعد خلف، "**دور المؤسسة العسكرية الإسرائيلية في صناعة القرار السياسي الخارجي (السلطة الفلسطينية ولبنان نموذجا) 2000–2009**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، (جامعة: الأزهر، كلية الاقتصاد والعلوم الإدارية، 2012)، ص 111.

ومع أن جهاز "الشاباك" هومن أصغر الأجهزة الأمنية في إسرائيل إلا أنه من أكثرها تأثيرا وفاعلية على القرار السياسي داخل الدولة، حيث تهتم الحكومة الإسرائيلية بتوصيات هذا الجهاز ولا يمكن مقارنة تأثيره الطاغي بتأثير أي جهاز أمني آخر خاصة عندما يتعلق الأمر في منطقة اختصاصه.

ويوصف "الشاباك" بأنه هيئة أمنية قومية مستقلة بذاتها ويتشابه مع الجيش الإسرائيلي في كونه مسؤولا عن الحفاظ على أمن الدولة في مواجهة التهديدات السرية، إذ أن أساس أنشطته هي السرية وعلى هذا الأساس فإنه يعد هيئة استخباراتية قومية نظرا لامتلاكه قدرات في مجال جمع المعلومات والبحث والعمليات الاستخباراتية التي تساعد معظم أجهزة المخابرات الإسرائيلية الأخرى.[1]

وكخلاصة يمكن القول أنه بالرغم من أن هذا الجهاز يأخذ الطابع الأمني والعسكري بصورة كبيرة إلا أنه يعتبر النواة الأساسية في الأمن السيبراني والمعلوماتي الإسرائيلي كونه يزود القائمين على الحروب الرقمية بقدر عال من المعلومات التي تؤهلهم لتصويب أسلحتهم التكنولوجية نحو الأهداف المطلوبة، كما يقوم في بعض الأحيان بمساندة القطاعات الرقمية في تنفيذ هجماتها الإلكترونية.[2]

الفرع الثالث: شعبة الاستخبارات العسكرية الإسرائيلية "أمان" (Aman)

إن اسم هذا الجهاز عبارة عن اختصار للكلمتين العبريتين (أرغون موديعين) أي مكتب الاستعلام ويتبع هذا الجهاز وزارة الدفاع، ويعتبر رئيس "أمان" عضوا في رئاسة هيئة الأركان العامة برتبة عميد ويساعده أربعة أجهزة كما ينص بذلك التشكيل العسكري وهي:

1. جهاز الاستخبارات في الجيش.
2. جهاز الاستخبارات لسلاح الجو.
3. جهاز الاستخبارات البحرية.
4. جهاز مكافحة التجسس.

و"أمان" مسؤولة عن جمع المعلومات العسكرية والجغرافية والاقتصادية وعلى وجه الخصوص حول الدول العربية، ومسؤولة أيضا عن أمن القوات المسلحة والمناطق التي تحتلها إسرائيل وهناك مهمة أخرى ألقيت

[1]– منذر سلامة أبوسويرح، **مرجع سابق**، ص 41.

[2]– وليد غسان سعيد جلعود، **مرجع سابق**، ص 141.

على عاتق الاستخبارات العسكرية وكانت سرية جدا تتعلق بالعمليات العسكرية، كما كلف هذا الجهاز بمسؤولية الرقابة العسكرية على الصحف والإذاعة والرسائل.[1]

وتكمن المهام الأساسية لجهاز "أمان" في النواحي التالية:

1. توفير المعلومات الأمنية والاستخباراتية لقادة الدولة، والجيش وأجهزة الأمن الأخرى التي من شأنها تقدير قوة العدووالتعرف على نقاط ضعفه وقوته ومحاولة استكشاف أهدافه اتجاه إسرائيل.

2. تقديم التحذيرات والإنذارات للمستويين السياسي والعسكري في إسرائيل في حالة نشوب حروب وتنفيذ عمليات فدائية معادية.

3. إمداد الجهات الرسمية في الدولة بالمعلومات الاستخباراتية بصورة محدثة.

4. العمل بصورة دائمة على تحليل وتفحص المعلومات الاستخباراتية ورفعها لصناع القرار والاستفادة منها في اتخاذ القرار المناسب.

5. الحرص على إمداد الجيش بالمعلومات الأمنية اللازمة من أجل تقديم أفضل أداء لمختلف أسلحته ووحداته القتالية والعمل بصورة دائمة على تطوير القدرات التكنولوجية.[2]

وفي ضوء أنه جهاز فائق الأهمية مكون من عدة وحدات وأقسام تعمل في مجالات:

1. جمع المعلومات، بحثها وتحليلها.

2. المهام الخاصة.

3. التطوير التكنولوجي

يهتم هذا الجهاز بأدوات الحرب الإلكترونية بشكل كبير خاصة التجسسية منها وذلك بحكم بيئة عمله والتي تتعلق بجمع أكبر قدر ممكن من المعلومات عن قادة المقاومة وبعض عناصر السلطة الفلسطينية، واستطلاع الآراء من المجتمع الفلسطيني عبر استخدام الوسائل الإعلامية المختلفة وأساليب الهندسة الاجتماعية ومواقع التواصل الاجتماعي.

---

[1]– محمد إسماعيل محمد الجيش، "**الأوضاع الداخلية في إسرائيل وأثرها على حرب 1967**"، مذكرة مقدمة لنيل شهادة الماجستير في التاريخ الحديث المعاصر، (الجامعة: الإسلامية، كلية الآداب، قسم التاريخ والآثار، 2008)، ص 126.

[2]– شموئيل إيفين، وعاموس غرانيت، "**المخابرات الإسرائيلية...إلى أين؟**"، (بيروت: مركز باحث للدراسات، 2009)، ص 20.

تستخدم "أمان" العديد من أسلحة الحروب الإلكترونية في جمعها للمعلومات أهمها:

✓ **آلات التصوير**: قام منتسبوا هذه الشعبة بوضع كاميرات رقمية كبيرة على أبراج الاستقبال الإسرائيلية القريبة من المناطق الفلسطينية وذلك لرصد تحركات عناصر المقاومة الفلسطينية.

✓ **الطائرات دون طيار**: يعمل جهاز "أمان" وبالتعاون مع سلاح الجوالإسرائيلي على تسيير طائرات استطلاع دون طيار، وذلك لتتبع تحركات عناصر المقاومة الفلسطينية واللبنانية وغيرهم[1]، وتسهيل عمل ألوية وفيالق مشاة الجيش الإسرائيلي أثناء التوغل في العمليات الإسرائيلية البرية وتزويد قادة سلاح الطيران الإسرائيلي بأماكن تواجد الشخصيات الفلسطينية المراد استهدافها واغتيالها.[2]

يتحمل هذا جهاز مسؤولية التحذير من احتمال نشوب حرب ومن اندلاع الأعمال العدائية والإرهابية كما يتحمل مسؤولية التقدير الاستخباراتي القومي في المجالين العسكري والسياسي وتوفير معلومات استخباراتية عسكرية شاملة وتوزيعها، ومسؤولة أيضا عن أمن المعلومات الوقائي في الجيش.[3]

إن وصف هذه الجهاز بأنه تابع لهيئة الأركان العامة لا يعكس بدقة جوهر عمله وأن هذه الشعبة هي شعبة خاصة بسبب مسؤوليتها القيادية لمجموعة كبيرة من وحدات جمع المعلومات والأبحاث والعمليات والتكنولوجيات، وهي تشبه على هذا الصعيد الذراع كالذراع البحري أوالجوي بيد أن هذا الذراع لا يعمل في مجال المعلومات.

ورغم أن شعبة الاستخبارات هي شعبة عسكرية إلا أنها تعتبر مركز للخدمات الاستخباراتية القومية، تقوم بجمع المعلومات والعمليات الأخرى اللازمة كالأبحاث لمساعدة الجيش الإسرائيلي في تحقيق أهدافه وبفضل قدرتها الكبيرة في مجال جمع المعلومات فإنها تعلب أدوارا وطنية أيضا خارج الجيش من أجل مساعدة الكوادر السياسية والجهات الاستخباراتية الأخرى على أداء أدوارها.[4]

وبالتالي فشعبة "أمان" هي جهاز للاستخبارات العسكرية ومسؤولة أيضا عن الرقابة العسكرية والأمن المعلوماتي.[5]

---

[1]– وليد غسان سعيد جعلود، **مرجع سابق**، ص 145.

[2]– **المرجع نفسه**، ص 146.

[3]– بدر عقلي، "**الموساد، الشاباك، أمان وأسلحة الدمار الشامل الإسرائيلية**"، (عمان: دار الجليل للنشر والتوزيع، 2009)، ص 07.

[4]– المكان نفسه.

[5]- Eric Denece, et David Elkaîm, **"Les Service Secrets Israéliens: Aman, Mossad et Shin Beth"**, (Paris : Edition Tallandier, 2014), p 06.

الفرع الرابع: وحدات شبكة الاستخبارات العسكرية "أمان"

وتشتمل شعبة الاستخبارات العسكرية على عدة وحدات وتتمثل فيما يلي:

أولا: الوحدة 8200

الوحدة 8200 هي أكبر وحدة في قوات الدفاع الإسرائيلية تتألف من عدة آلاف من الجنود الإسرائيليين مماثلة في وظيفتها لوكالة الأمن القومي في الولايات المتحدة الأمريكية (NSA)، مسؤولة عن جمع المعلومات الاستخباراتية العسكرية من التلفزيون والإذاعة والصحف وشبكة الانترنت وترجمة مختلف المعلومات التي يتم جمعها من الاستخبارات الأساسية ومن قبل الوحدات الأخرى وفقا لتقارير وسائل الإعلام، تقدم الوحدة ما يزيد على نصف معلومات أجهزة الاستخبارات العامة.

وفي مجال الأمن السبيراني فالوحدة 8200 مسؤولة عن تكوين الخبراء السيبرانيين ذوي المهارات العالية وعمليات التشفير ومراقبة كل ما يتعلق بالجريمة السيبرانية، مخابرات الويب، والتهديدات السيبرانية ومجال الاتصالات، وقد زودت هذه الوحدة بوحدات إضافية تتناول الأمن السيبراني سواء أكانت العمليات هجومية أودفاعية.[1]

تأسست هذه الوحدة سنة 1952م في نفس السنة التي تأسست فيها وكالة الأمن القومي الإسرائيلي والتي امتدت مهامها من جمع المعلومات الاستخباراتية إلى إدارة شبكة من الشركات الأمنية في 40 دولة حول العالم إضافة إلى بيع تطبيقات التجسس إلى الحكومات، يتعلم فيها التجسس، الاختراق الشبكي، وصنع أسلحة الفضاء الإلكتروني ويتوزع متقاعدوها بين الشركات الأمنية حول العالم.[2]

تعتمد هذه الوحدة بالأساس على التكنولوجيا وهي التي ساهمت في تطور قطاع تكنولوجيا المعلومات والفضاء الإلكتروني في إسرائيل وحتى الولايات المتحدة الأمريكية استفادت من الخبرات الإسرائيلية في التجسس خصوصا على الشرق الأوسط.[3]

---

[1]- **"Cyber Security landscape and investment Israel, 2016"**, (Cyber DB research department, January 2017), p 04.

[2]– عبد الله علوان، "**تعرف على وحدة الاستخبارات الإسرائيلية 8200 ومهامها الخطيرة في العالم**"، تم تصفح الموقع يوم : 09 مارس 2018. الرابط:

https//www.youtube.com/Watch§VZRZRZNSEW04

[3]- Peter Rousseau, **"the history and impact of unit 8200 on Israel Hi-Tech Entrepreneurship"**, (Athesis presented to the Homors tutorial college, Ohio university, 2017), p 07.

من ضمن مهام الوحدة حماية بيانات إسرائيل الحساسة إلى جانب جمع وفك رموز وتحليل ملايين (إن لم تكن مليارات) أجزاء من المعلومات التي تعترضها وتلتقطها وتستهدفها في شبكتها الإلكترونية المعقدة.

تقوم هذه الوحدة أيضا بالتنصت على الاتصالات الإلكترونية، الاتصالات الصوتية والبيانية التي تجري من خلال شبكات الاتصالات.

بحيث يعتبر "يوسي ميلمان" المؤرخ الإخباري لأجهزة الاستخبارات في إسرائيل أن هذه الوحدة هي الأهم في حقل التجميع وهي الأكثر أهمية في مجال الاستخبارات تتعدى مهامها مهام "الموساد"، وهي طريقة تتعدى الاستخبارات العسكرية.[1]

لقد أصبحت هذه الوحدة مصدرا لا يستهان به للأبحاث وتطوير التقنيات في قوات الدفاع الإسرائيلية الموجهة نحوالتقنية والمجال المعلوماتي بشكل كبير.[2]

إن الدور الذي تقوم به الوحدة 8200 قد جعل إسرائيل ثاني أكبر دولة في مجال التنصت في العالم بعد الولايات المتحدة الأمريكية بحيث توازي نظيرتها في الولايات المتحدة الأمريكية "وكالة الأمن القومي الأمريكي"، وإن التقدم الكبير الذي حققته إسرائيل في مجال صناعة التقنيات المتقدمة قد وظف بشكل كبير في تطوير عمليات التنصت التي تقوم بها الوحدة وتوسيعها[3].

تقوم أيضا بالتنصت على الهواتف، الفاكسات، التسلل إلى الحواسيب واعتراض الوسائط الرقمية، وفك التشفير، وحروب السايبر للحصول على المعلومات وإلحاق الضرر بالحواسيب ومنظومات المعلومات حيث يحدث رد فعل متسلسل ويمس بالبنى التحتية الإستراتيجية وغيرها.[4]

وتمثل هيئة السايبر في وحدة 8200 الأنشطة الهجومية، بينما تمثل هيئة السايبر في "الشاباك" الأعمال والأنشطة الدفاعية الهادفة لتحصين ومنع هجمات السايبر المعادية.[5]

---

[1]– سعيد الحسينة، **مترجما**، "**جواسيس ليمتد: شركات وصناعات متطورة يديرها أسياد الاستخبارات الإسرائيلية**"، (بيروت: الدار العربية للعلوم، 2005)، ص 131.

[2]– **المرجع نفسه**، ص 132.

[3]– منذر سلامة أبوسويرح، **مرجع سابق**، ص 26.

[4]– **المرجع نفسه**، ص 27.

[5]– **المرجع نفسه**، ص 30.

ثانيا: شعبة المعلومات الضوئية الوحدة 9900

تختص شعبة المعلومات الضوئية المعروفة باسم الوحدة رقم 9900 بتحليل الصور ووضع الخرائط والاستخبارات القائمة على معلومات ضوئية متوقعة.

وتشمل الوحدة 9900 العوالم الجغرافية والضوئية القائمة في جهاز الاستخبارات التابع للجيش الإسرائيلي "أمان"، لذلك تضم عدة أقسام متخصصة في مجال عملها وتعمل أيضا في مجال خلق حالة من "تراكم التكنولوجيا".

وتختص أيضا بجمع المعلومات الضوئية من مصادر متنوعة مثل: الأقمار الصناعية، طائرات المراقبة، إضافة إلى المعلومات الظاهرة والمنشورة، ليقوم بعدها بنقل وتحويل رؤيته الاستخباراتية وتنبؤاته لمتخذي القرار في إسرائيل والقوات العاملة في الميدان.[1]

وحدة الاستخبارات الخاصة 9900 هي وحدة مخصصة لكل ما يتعلق بالجغرافيا، بما في ذلك رسم الخرائط وتفسير صور الأقمار الصناعية وبحوث الفضاء، وداخل هذه الوحدة يوجد وحدة صغيرة من الجنود الإسرائيليين ذوي المؤهلات العالية الذين لديهم القدرات البصرية والتحليل والتي يمكن بها الكشف عن أصغر التفاصيل وأدقها.[2]

وتتكون الوحدة 9900 من عدة وحدات وأقسام وهي كالآتي:

1- مركز المعلومات المتخصص: ويعنى بدراسة المعلومات وتحليلها وجمع المعلومات الميدانية لتشكيل صورة تنفيذية واعية ومدركة تشمل أعمال تحليل محاور المواصلات وجمع معطيات ميدانية، والخروج بفهم وإدراك جوهري لطبيعة التهديدات، فعلى سبيل المثال يدرك محللوا الوحدة كيفية تشخيص أنواع الوسائل القتالية من خلال الصور الجوية.

وتصل المعلومات التي تخضع للتحليل عبر مجسات فضائية ونقاط رقابة أرضية ومجسات جوية داخل الطائرات التي تعمل بنظم المعلومات الجغرافية (GIS)، فيما يتم استخلاص جزء كبير من المعلومات من خلال دراسة وتحليل معلومات غير سرية ومكشوفة.[3]

---

[1]- **المرجع نفسه**، ص 33.

[2] - **"Autism In the IDF: the Solidiers of Intelligence Unit 9900"**, Israel Katters Issue, Number 81, (June 2014).

[3]- منذر سلامة أبوسويرح، **مرجع سابق**، ص 33.

2- وحدة الأقمار الصناعية: مسؤولة عن أقمار التجسس الاصطناعية وتستخدم جميع إمكانيات هذه الأقمار ووظائفها لخدمة الأقسام والجهات التي تحتاج إلى معلومات فورية.

ويعد مشروع "نبني العوالم" أحد التطورات المركزية التي شهدتها الوحدة في الفترة الأخيرة ويقوم هذا المشروع على رؤية ربط عالم الخرائط وتحليل المعلومات وإنتاج نموذج يسمح باستخدام نظارات واقعية من طبقات مثل: "نظارة غوغل"، وذلك بهدف تزويد القوات الميدانية بمعلومات استخباراتية في الوقت الحقيقي على خلفية صورة من الواقع الميداني،[1] ما يسمح للقوة العسكرية على سبيل المثال برؤية ما يوجد داخل مبنى أوغيره ويتم تحديد الجنود بإشارة معينة والعدوبإشارة أخرى للتمييز بينهما، كما يمكن للجنود تلقى أكبر قدر ممكن من المعلومات المتعلقة بطبيعة المنطقة.

توفر الوحدة 9900 المعلومات على جميع المستويات للقيادة السياسية وكبار صانعي القرارات العسكرية وقادة الكتائب حيث يتم إرسال المعلومات فورا بعد تلقي الطلب، كما تساعد في العمليات المعقدة التي تقوم بها القوات الخاصة في جيش الدفاع الإسرائيلي والقوات الجوية.

كما تلقت هذه الوحدة نظم تجهيز المعلومات الجديدة التي تسمح لها بالاستفادة الكاملة من المعلومات الاستخباراتية التي يتم جمعها، فالوحدة يمكن أن تتلقى طلبات من مختلف قوات جيش الدفاع الإسرائيلي ودوائر الاستخبارات في أي وقت.[2]

ومن مهامها أيضا توجيه الأقمار الصناعية لتصوير المنشآت العسكرية في أي دولة وتزويد القادة العسكريين بمواقع الأهداف المطلوبة بدقة، ورصد تحركات الخلايا المسلحة ومراقبة ما يجري في الدول المجاورة والمنشآت النووية الإيرانية عبر بث مباشر من القمر الصناعي إلى شاشة عرض كبيرة في الوحدة، وتساعد في التواجد دائما في المكان المناسب وفي الوقت المناسب.

وكخلاصة يمكن القول أن تعدد أجهزة الاستخبارات الإسرائيلية بمختلف مسمياتها ومهامها يعكس حجم الاهتمام البالغ الذي توليه إسرائيل لأجهزة جمع المعلومات، حيث أن الاعتقاد السائد منذ نشأة الدولة أن لأجهزة جمع المعلومات دورا بارزا في إنشاء الدولة وكذلك معرفة نوايا البيئة الإستراتيجية بإسرائيل وحمايتها.

---

[1]- **المرجع نفسه**، ص 34.

[2]- **"9900: the Israel Satellite intelligence unit"**, Web Visited in : 09 March 2018, Link: https://i-hls.com/archives/22809.

ثالثا: وحدة جمع المعلومات من المصادر المفتوحة (حتساب)

يقوم عمل هذه الوحدة على متابعة المصادر العلنية للمعلومات مثل وسائل الإعلام المختلفة، وسائل التواصل الاجتماعي، المنتديات الحوارية وشبكة الانترنت بشكل عام، ومتابعة كل ما يتم نشره من صور على مواقع التواصل الاجتماعي واستنباط المعلومات الاستخباراتية منها.[1]

بناءا على ذلك فثورة التواصل الاجتماعي مكنت الاستخبارات الإسرائيلية من الحصول على معلومات ذات قيمة وفي زمن حقيقي ومن دون تجنيد إمكانيات كبيرة، ولا يقتصر مجال عمل هذه الوحدة على الفلسطينيين فقط بل على كل الدول التي للاستخبارات مصلحة في متابعة ما ينشر في مواقع التواصل الاجتماعي، ومن مهام هذه الوحدة أيضا رصد ومتابعة توجهات الرأي العام في كل دولة عربية لقياس مدى استعداد المجتمعات في هذه الدول لخوض ثورات أخرى ضد أنظمة الحكم، ويكتسب هذا الأمر أهمية قصوى بسبب تأثير مثل هذه الثورات على البيئة الإستراتيجية الإسرائيلية.[2]

الفرع الخامس: جهاز الأمن الخارجي الإسرائيلي الموساد (Mossad)

"الموساد" (mossad.gov.iL//Eng) هي هيئة الاستخبارات والعمليات الخاصة[3] تأسس سنة 1951م بقرار من "بن غورين" ليكون بمثابة ذراع استخباراتي ومعلوماتي وأمني خارجي داعما وجامعا لأجهزة الاستخبارات السرية المتعددة، ترتكز بيئة عمله بشكل خاص خارج حدود الدولة الإسرائيلية كما له دور في العمل الاستخباراتي داخل فلسطين حيث يتم توظيف هذه المعلومات الإستخباراتية الداخلية في معرفة بعض المعلومات عن المقاومة الفلسطينية كمصادر تمويلها وساحات عملها الخارجية، واتصالاتها مع حركات وأذرع المقاومة خارج فلسطين وغيرها من المعلومات التقنية والأمنية.[4]

---

[1]– منذر سلامة أبو سويرح، **مرجع سابق**، ص 19.

[2]– زهير أندراوس، "**شعبة الاستخبارات العسكرية "أمان"**"، تم تصفح الموقع يوم : 10 مارس 2018. الرابط: Https://www.raialyoum.com/index.php

[3]– إبراهيم فؤاد عباس، "**الموساد تحت المجهر**"، (القاهرة: دار المنار للطباعة والنشر، 2010)، ص 11.

[4]– وليد غسان سعيد جعلود، **مرجع سابق**، ص 146.

ويعتبر "الموساد" هيئة استخباراتية قومية ويختلف عن جهاز "أمان" في كونه هيئة مستقلة بذاتها ويختلف عن "الشاباك" في كون مهامه ليس بها مسؤوليات محددة فيما يتعلق بالأمن القومي، ولكن تتمثل مسؤوليته في كونه ذراع عمل سري خارج الدولة، ويمكن مقارنة "الموساد" كجهاز للاستخبارات بوكالة الاستخبارات البريطانية (M16) أووكالة الاستخبارات الأمريكية (CIA).[1]

ويضم "الموساد" قسما لمكافحة التجسس الإلكتروني والمعلوماتي والاختراق، كما يأخذ في حساباته العلمية والعملية آخر المستجدات الحاصلة في العالم والتي أهمها التقنية والرقمية منها، علاوة على اهتمامه بتعيين عناصر ذوي خبرة تنفيذية في صفوفه وعدم اقتصار عمله على النواحي المعلوماتية الأمنية فحسب بل يتعدى ذلك لتكون النشاطات الاقتصادية الإقليمية والدولية من اختصاصاته أيضا.[2]

لذلك يمكن سرد أهم آليات العمل التجسسية والمعلوماتية لجهاز "الموساد" بما يلي:

✓ جمع المعلومات الأمنية والاستخباراتية عن دول معينة، لاسيما المواقع العسكرية والمحطات الأمنية والتي تعتقد إسرائيل أنها تشكل خطرا عليها في المستقبل خاصة إذا استدعى الأمر دخول في مواجهة عسكرية معها، تزود إسرائيل عناصرها العاملة في هذا المجال بأحداث آلات التصوير والخرائط الإلكترونية ومحطات البث والإرسال والاستقبال وغيرها.[3]

✓ تدريب جواسيس "الموساد" على أحدث الأجهزة الإلكترونية، والتي تساعدهم على رصد غالبية تحركات عناصر المقاومة خارج فلسطين كمخابئهم السرية وأماكن تواجدهم.

✓ القيام بعمليات التخريب الاجتماعية والأخلاقية والثقافية، وذلك بهدف الاسقاطات وتجنيد الجواسيس لصالح إسرائيل لاسيما على صعيد نشر العديد من شبكات التجسس والاستقطاب عبر شبكات الانترنت ومواقع التواصل الاجتماعي ومحطات البث الخلوي، واستخدام أساليب الهندسة الاجتماعية الرامية إلى زعزعة استقرار الدول خاصة العربية والإسلامية.[4]

ولهذا الجهاز دور مهم في إدارة الحروب الإلكترونية عبر الفضاء الرقمي والمعلوماتي، كونه يعتمد وبشكل رئيسي على الحرب على العقول والميول القائمة على البيئة الإستراتيجية والتي تؤهله للتأقلم العملي في ظل أي بيئة قد يوضع بها، فهويهدف إلى تطوير القدرات الهجومية والدفاعية لعناصره والأجهزة التجسسية

[1]– إبراهيم فؤادعباس، **مرجع سابق**، ص 12.

[2]– وليد غسان سعيد جعلود، **مرجع سابق**، ص 147.

[3]– المكان نفسه.

[4]– **المرجع نفسه**، ص 148.

الأخرى العاملة لحساب إسرائيل على الشبكة العنكبوتية كموضع قتال جديد في عصر المعلومات وتوفير معلومات دقيقة وبكميات عالية لدعم قدرات الجيش الإسرائيلي وذلك بالتعاون مع وسائل الإعلام الإسرائيلية.[1]

وبذلك فإسرائيل استطاعت بناء مجتمع رقمي معلوماتي وهذا ما يؤهلها للمنافسة التقنية والمعلوماتية والرقمية على مستوى العالم، مما جعلها محطة للاستقطاب التقني والعلمي والمعرفي خاصة في الجوانب التكنولوجية العسكرية.

المطلب الثالث : الإعلام الإسرائيلي ومراكز البحث العلمي

الفرع الأول: الإعلام الإسرائيلي

تعد صياغة وتشكيل الرأي العام في المجتمعات من الأدوار الرئيسية التي تقوم بها وسائل الإعلام ويتضاعف ذلك مع التطورات النوعية المتزايدة التي نشهدها بشكل متسارع في مجالات تقنية الاتصالات والتي منحت وسائل الإعلام إمكانات وقدرات هائلة في التأثير على الآخرين وتغيير المفاهيم.[2]

ويُشكل الإعلام الركيزة الأساسية في الإستراتيجية الإسرائيلية منذ قيام الحركة الصهيونية على يد الصحافي الإسرائيلي "تيودور هيرتزل" والذي استطاع عقد المؤتمر الصهيوني الأول في سنة 1897م في مدينة "بال" بسويسرا، وكان من نتائج هذا المؤتمر إصدار مجلة أسبوعية حملت اسم "دي وولت".

ومثل "تيودور هيرتزل" ظَلَّ "ديفيد بن غورين" مؤمنا بأن للإعلام دورا ووظيفة، فأعلن بعد توليه منصبه عن تأسيس "هيئة رؤساء تحرير الصحف"[3] والتي اعتبرت إحدى أذرع "الموساد"، لذلك فقد ركز الإعلام الإسرائيلي منذ نشأته على مراكز الثقل السياسية العالمية في أوروبا، ثم توجه بعد ذلك نحوأمريكا الشمالية لأن إسرائيل ربطت نفسها منذ البداية بالدول الكبرى وبطموحاتها السياسية والاقتصادية، فقد حرصت على أن تحافظ على علاقة خاصة بالدول صاحبة القرار السياسي المؤثر وليس على المستوى السياسي فحسب ولكن على المستوى الإعلامي أيضا من خلال تأثيرها على الرأي العام في تلك الدول.[4]

---

[1]– المكان نفسه.

[2]– وسيم وني، "**الإعلام ودوره بالصراع مع الاحتلال الإسرائيلي**"، تم تصفح الموقع يوم : 10 مارس 2018. الرابط: www.pm-news.net/news.php?extend.6189.7

[3]– باسل يوسف النيرب، "**الإعلام الإسرائيلي....ذراع الجلاد**"، (الرياض: مكتبة الملك فهد الوطنية للنشر، 2010)، ص 11.

[4]– **المرجع نفسه**، ص 12.

فقد أدت التطورات التكنولوجية وما تلاها من تطور في وسائل الإعلام إلى تغيير في مفهوم قدرات الدولة الشاملة، حيث أصبحت المعلومات والثورة الإعلامية عناصر مؤثرة في تأمين استقرار الدولة ودعم نفوذها الإقليمي ويعتبر الإعلام بمفهومه العلمي الواسع من أهم وأخطر الأدوات في إدارة الأزمات والحروب، كما أنه أداة من الأدوات المهمة التي تستعين بها الدول في إنجاح مساعيها وتوضيح سياساتها الداخلية والخارجية وتوضيح وجهات نظرها حول القضايا المختلفة.[1]

وتعتبر وسائل الإعلام إحدى أهم وسائل توازن الأمن في إسرائيل نظرا لما تمتلكه من إمكانيات عالية وقدرات على المناورات الإعلامية وهامشا كبيرا من التضليل والتضخيم للصالح الإسرائيلي.

كما يتسم الإعلام الإسرائيلي بأنه دعاية منظمة ومخططة ذات أهداف إستراتيجية واضحة، وبكونه دعاية تركز على تكرار مجموعة من القضايا التي يتم الإلحاح عليها لترسيخها في الأذهان وتثبيتها حتى تصبح بمثابة حقائق يجب التسليم بها.[2]

كما يلعب دورا هاما في تعزيز وتدعيم الفضاء الإلكتروني الإسرائيلي فهوأحد أسلحة الحروب الإلكترونية وأهم الوسائل الناقلة والحاملة للأيديولوجية الإسرائيلية، بحيث يمتلك إمكانيات مادية ومعنوية وبشرية وتقنية ضخمة، ومساحات كبيرة للمناورات التكنولوجية والمعلوماتية الواسعة عبر الفضاء الرقمي وقدرة كبيرة على تعبئة الرأي العام الإسرائيلي وفقا لقاعدة تهويل الأحداث وتضخيمها.[3]

ولتعزيز عمل قطاعات الإعلام الإسرائيلي في الحرب الإلكترونية، قامت إسرائيل بإطلاق برامج ناطقة باللغة العربية تبث عبر وسائل الفضاء الإلكتروني عامة من أجل تلطيف ممارسات العنف لآلة الحرب الإسرائيلية وجذب الرأي العام العربي للتعاطف مع إسرائيل، حيث نجحت هذه الأخيرة في استخدام الاستقطاب الإلكتروني والإعلامي لعدد من النخب العربية وخلق سبل للقاءات بين العرب والإسرائيليين عبر الفضاء الإلكتروني لتتحول إلى امتدادات واقعية لعمل العديد من جمعيات السلام المنادية بالتطبيع والتعايش مع إسرائيل.[4]

---

[1]– سامية أبوالنصر، "**الإعلام والعمليات النفسية في ظل الحروب المعاصرة وإستراتيجية المواجهة**"، (القاهرة: دار النشر للجامعات، 2010)، ص 06.

[2]– محمد أبوسعدة، "**مؤسسات الإعلام الصهيوني: خريطة أولية**"، (المعهد المصري للدراسات السياسية والإستراتيجية، أكتوبر 2016)، ص 03.

[3]– منذر عنتباوي، "**أضواء على الإعلام الإسرائيلي**"، (بيروت: مركز الأبحاث، 1968)، ص 17.

[4]– **المرجع نفسه**، ص 152.

الفرع الثاني: مراكز البحث العلمي في إسرائيل

شكلت مراكز البحث العلمي في إسرائيل مرحلة بناء البنية المؤسسية للجوانب العلمية والبحثية، حيث أنشأت الحكومة الإسرائيلية مجلسا للأبحاث العلمية والصناعية؛ مهمته الأساسية ربط الطاقة العلمية بالجهد الحربي وشكل نموذجا أوليا للمعالجة الرسمية لقضايا العلم والتكنولوجيا وأصبح وثيق الصلة بمراكز صنع القرار لاسيما في المجالين الاقتصادي والأمني فضلا عن الجانب العسكري.

وهكذا ومن منطلق اعتبار البحث العلمي أولوية قومية كان لابد من تخطيط الدولة للسياسة التعليمية وتحديد التعليم العالي والبحث العلمي، بما يمكنه من تخصيص كل قطاع أوفرع بحاجته من الموارد البشرية والمالية.[1]

تهتم إسرائيل بمراكز البحث العلمي حيث تعتمد عليها وتعتبرها من الركائز الأساسية لرسم وبناء الإستراتيجيات في جميع المجالات، كما تمثل المعرفة والعلم ومناهج البحث العلمي مصدرا مهما لبناء اقتصادها وإنتاجها الفكري وتحقيق التميز والمنافسة في مجال العلوم والتكنولوجيا، من خلال دعم وتطوير البنية التحتية لتكنولوجيا المعلومات والاتصالات من حيث الكم والكيف والتي تربط إسرائيل بمختلف أنحاء العالم عن طريق أقمارها الصناعية التي تقوم بمسح شامل حول الكرة الأرضية إضافة إلى التوسع والمنافسة في البحوث العسكرية لزيادة قوتها العسكرية وبالتالي ضمان أمنها القومي.[2]

تتطلع إسرائيل لتكون دولة عظمى في مجال الابتكار والبحث العلمي وتسعى إلى إقامة مراكز البحث والاستثمار باستيعاب الأدمغة في مجال التكنولوجيا والتطبيقات وتطوير البرامج والاتصالات والبرمجة والانترنت من خلال الجهود التي وظفتها، وتقاسم الأدوار بين المؤسسات العسكرية والمدنية والأكاديمية التي ساهمت في تحويل إسرائيل إلى دولة تكنولوجيا[3]، لمواصلة الهيمنة على العالم وكيفية الاستفادة من الأدمغة وتبادل الخبرات ويكون ذلك بواسطة التثقيف التكنولوجي المبكر وتقليص الفوارق الاجتماعية والاقتصادية ودمج كافة شرائح المجتمع في مشاريع الإنتاج والابتكار التكنولوجي وتشجيع المعاهد الأكاديمية والجامعات ومنحها كامل الحرية

---

[1]– عدنان عبد الرحمان أبوعامر، "**مراكز البحث العلمي في إسرائيل، السياسات، الأهداف، التمويل**"، (بيروت: مركز نماء للبحوث والدراسات، 2013)، ص 19.

[2]– **المرجع نفسه**، ص 22.

[3]– محمد محسن وتد، "**إسرائيل تسعى للريادة التكنولوجية بحلول 2024**"، تم تصفح الموقع يوم : 12 مارس 2018. الرابط: https://www.aljazeera.net/news/SC

في إنتاج المعرفة وجذب الكفاءات العلمية، وضرورة الانفتاح على المجتمع الدولي والاستعانة بجميع القدرات من جميع أنحاء العالم.[1] للدفع بمسيرة تطور البحث العلمي وتحقيق أهدافها للريادة عالميا بالتكنولوجيا العالية.

المطلب الرابع: الوحدات التقنية والتكنولوجية

تنقسم الوحدات التقنية والتكنولوجية في الجيش الإسرائيلي إلى عدة أقسام، والتي يمكن التفصيل فيها على النحو التالي:

الفرع الأول: جناح تكنولوجيا المعلومات والاتصال

يعمل هذا الجناح على تحديد سياسة تكنولوجيا المعلومات والاتصالات، وتحمل المسؤولية لهيئة الأركان العامة في توفير الحلول التشغيلية والتكنولوجية لمتطلبات تكنولوجيا المعلومات والاتصالات في الجيش الإسرائيلي، يدير هذا الجناح كافة العمليات الإلكترونية وتدريب الجنود الإسرائيليين على كتابة برامج توجيهية بواسطة الحواسيب وتطوير أنظمة إلكترونية عبر برامج التطبيقات الحاسوبية.

كما يتولى مهمة تحديد مفهوم تشغيل تكنولوجيا المعلومات والاتصالات الفوق رقمية في جيش الدفاع الإسرائيلي، تحديد السياسات وإجراء البحوث وتطوير أمان الأنظمة المحوسبة كذلك تحديد قانون تكنولوجيا المعلومات والاتصالات ، وتطوير وتعزيز الموارد البشرية بقوى سلاح تكنولوجيا المعلومات، كذلك تحمل المسؤولية الشاملة في تنسيق مجال التردد الكهرومغناطيسي من أجل التعايش بين الأنظمة الإلكترونية العسكرية.[2]

الفرع الثاني: الجناح التكنولوجي واللوجستي للدعم والإمداد

يُعنى هذا الجناح بتوفير حلول لوجستية لجميع الوحدات العاملة في الجيش الإسرائيلي وفقا لاحتياجاتها ومهامها خاصة من الناحية التكنولوجية، حيث يشمل هذا الدعم عدة مجالات منها: البحث والتخطيط والتطوير والتحسين وصيانة الأجهزة الآلية والحوسبة وغيرها من قضايا الدعم اللوجستي الرقمي والمعلوماتي ويقدم هذا الجناح العديد من الخدمات التقنية للجيش، أهمها إعادة التأهيل والصيانة لوسائل القتال التقليدية

[1]– المكان نفسه.

[2]– إجلال عبد اللطيف حسن، "**تكوين وحدات جيش الدفاع الإسرائيلي**"، تم تصفح الموقع يوم : 12 مارس 2018. الرابط: www.alhasahisa.net

وغير التقليدية وتوفير الجاهزية التقنية الكاملة للجيش الإسرائيلي في حال وقوع الحروب وتقديم الأبحاث الاستخباراتية والمعلوماتية للجهات المختصة وضمان الكفاءة والدعم اللوجستي في جيش الدفاع الإسرائيلي.[1]

الفرع الثالث: الشركات والوسائل التقنية الإسرائيلية

أولا: الشركات الإسرائيلية في مجال صناعة البرمجيات وتكنولوجيا المعلومات

هناك العديد من الشركات الإسرائيلية التي برزت في هذا المجال، إضافة إلى الدعم الخارجي في تطوير أعمالها ومن أهم هذه الشركات نذكر ما يلي:

1- تشك بونيت سوفت دير تكنولوجيز ليمتد (Check point Software Technologies LTD)

عرفت بأنظمة حماية البيئة وتطبيقات أمن الشبكات، وقد سوقت للبرنامج (Fire wall-1) المصمم لحماية الشركات الكبيرة والصغيرة من محاولات الاقتحام غير المشروع لبياناتها توزع منتوجاتها في جميع أنحاء العالم ومركزها في (رامات-جان) مركز عملياتها الخارجي في ولاية كاليفورنيا ويدعم برنامج (Fire wall-1) أكثر من 120 تطبيقا وبروتوكولا سابقا للبرمجة منها الويندوز (Windows) واليونكس (Unix).[2]

2- شركة نوليدج سيستمز ليمتد (Amaddin Knowlidge System Ltd)

تخصصت في أنظمة الحماية الأمنية لشركات الكمبيوتر وتطوير تطبيقات البطاقات الذكية تأسست سنة 1985م، مسجلة في بورصة (ناساداك) من أبرز تطبيقاتها (HASP)، (Hard Lock) ومن أبرز عملائها شركات عملاقة مثل (IBM, AT&T) وغيرهما.

لها شبكة توزيع دولية تدار من ستة مكاتب رئيسية في كل من تل أبيب ونيويورك، شيكاغوولندن وطوكيوولها أكثر من 50 موزعا عالميا يعملون في 40 دولة.[3]

3- شركة أكسنت (Accentco)

متخصصة في تصميم وتطوير البرامج والتطبيقات متعددة اللغات الخاصة بعملية "النشر المكتبي" ومستعرضات شبكة الانترنت، تأسست سنة 1988م ومسجلة ضمن بورصة (ناساداك) تنتشر منتجاتها في

---

[1]- وليد غسان جعلود، **مرجع سابق**، ص 154.

[2]- أحمد بهاء شعبان، "**العلم والسيطرة: كيف استخدمت إسرائيل تقدمها العلمي والتكنولوجي لبسط هيمنتها على منطقتنا؟**"، (القاهرة: الهيئة العامة لشؤون المطابع الأميرية، 2015)، ص 130.

[3]- **المرجع نفسه**، ص 114.

أكثر من 30 دولة، مركزها القدس وتمتلك مكاتب في كاليفورنيا ولندن حيث يتم تسويق منتجاتها في العالم العربي من أهم منتجاتها مستعرض انترنت مع أكسنت لاستعراض وتطوير صفحات الانترنت ويعمل بأكثر من 30 لغة (بينها اللغة العربية) في بيئات (Windows).[1]

4- شركة كروماتيس للاتصالات

أنشأها رجلا الأعمال الإسرائيليان "أوروني بتروشكا" و"رافي جدعون" اعتمادا على تمويل من مستثمرين للأموال في الشركات حديثة النشأة العاملة في مجال التقنيات العالية، تعمل في مجال نظم الاتصالات عبر الألياف الضوئية وقد شهد نموا مذهلا بتوسعها في إنشاء نظم شبكات الاتصالات الضوئية ذات الاستخدامات العسكرية والصناعية، يبلغ عدد مستخدمي الشركة 160 شخصا والتي لم يمضي على تأسيسها سوى عامين فقط.[2]

والدافع الأساسي الكامن من خلف هذا التقييم العالي للشركة الإسرائيلية يعود إلى تمكنها من اكتشاف تقنية متقدمة يمكن أن تتعامل فيها الألياف الزجاجية الضوئية مع 720 مليون اتصال (هاتف صوتي، فاكس، انترنت، بريد إلكتروني...الخ) في نفس الوقت وستسمح هذه التقنية لـــ"لوسنت تكنولوجيز" أن تهيمن على قطاع واسع من صناعة نظم الاتصالات.[3]

5- شركة كيلا للأبحاث والإستراتيجية: (Kela Research & Strategy)

وهي من أهم الشركات الإسرائيلية الخاصة لتقديم الخدمات المخابراتية وجمع المعلومات وتحليلها أسسها "دفير راز" وهومن المختصين في الأبحاث والتحليل كان ضابطا للتحليل والأبحاث في المخابرات العسكرية الإسرائيلية بالإضافة إلى ضباط سابقين في الجيش الإسرائيلي ومختصين في التخطيط والمخابرات الإسرائيلية.[4]

إذا اعتمدنا مؤشرا آخر من أحدث مؤشرات النموالتقني والتقدم العلمي وهومؤشر استخدام شبكة الانترنت في التبادل التجاري الدولي لتقدير حجم التطور الإسرائيلي في هذا المجال لوجدنا أن إسرائيل كانت من أوائل الدول التي انتبهت إليه وشاركت في تطويره ومن الطبيعي أن تتزايد فرص الاستفادة من سوق

---

[1]- المكان نفسه.

[2]- **المرجع نفسه**، ص 115.

[3]- المكان نفسه.

[4]- تحسين الحلبي، "**الشركات الخاصة الإسرائيلية للخدمات الأمنية الدور والأخطار**"، (دمشق: مركز دمشق للأبحاث والدراسات، 2016)، ص 13.

التجارة الإلكترونية الضخمة، أي فرص التسويق الضخمة عن طريق شبكة الانترنت العالمية لمنتجات وسلع إسرائيلية.[1]

تمثل الإنجازات الإسرائيلية في مجال التكنولوجيات المتقدمة حالة نموذجية لآليات التفاعل بين العناصر الخارجية والداخلية وللكيفيات التي تتحقق عبرها الاستفادة من المساندات الخارجية، عن طريق كفاءة الاستخدام والجاهزية الذاتية الأمر الذي يقود إلى نتائج عملية إيجابية وملموسة.

ومما لاشك فيه أن هناك مساعدات ضخمة قدمت من طرف الولايات المتحدة الأمريكية والغرب والدول الصناعية الآسيوية المتطورة لإسرائيل نظرا إلى الاتفاق العام في المصالح والإستراتيجيات لكن هذه المساعدات استمرت في التدفق عليها حتى في حالات التناقض المؤقت بين الطرفين في الرؤى والتكتيكات، ويعود هذا الأمر إلى كفاءة الحشد الإسرائيلي للأنصار والحلفاء وقدرتها على التأثير في صنع القرار الغربي في الأوقات الحرجة، كما يتضح من التطورات التي مر بها "اتفاق التعاون العلمي والتكنولوجي بين الاتحاد الأوروبي وإسرائيل".[2]

حيث استطاعت إسرائيل بكفاءة تعبئة أنصارها في مختلف العواصم الأوروبية ومؤسسات الاتحاد والمؤسسات الصناعية الأوروبية التي تسهم في المشروعات العلمية المشتركة مع المختبرات والمؤسسات الإسرائيلية.

ومن جهة أخرى أنشأت بريطانيا صندوق مشتركا مع إسرائيل لدعم المشروعات المشتركة في مجال التكنولوجيا المتطورة، لأن بريطانيا تعتبر إسرائيل رائدة في مجال الاتصالات السلكية واللاسلكية وبرامج الكمبيوتر، كما تتمتع بقوة متنامية في التكنولوجيا الحيوية وبأعلى كثافة في الخبرة العلمية والتقنية.[3]

من جهة أخرى فقد تطورت العلاقات بين إسرائيل والولايات المتحدة الأمريكية تدريجيا حتى بلغت مستوى التحالف الإستراتيجي بمضامينه السياسية والاقتصادية والعسكرية والتكنولوجية، حيث تم إدراجها في جميع برامج المساعدات الرئيسية التي تقدمها واشنطن للدول الأجنبية مثل برامج التعاون الفني، ونتج عن توطيد العلاقات الأمريكية الإسرائيلية تطور في غاية الأهمية يتعلق بالمجال العلمي وإعداد الباحثين والخبراء وتزويدها بالمعارف العلمية الأساسية والتطبيقية والتقنية والإلكترونية، وفي سبعينيات القرن الماضي تم توقيع اتفاقية شاملة

---

[1]– أحمد بهاء الدين شعبان، **مرجع سابق**، ص 117.

[2]– **المرجع نفسه**، ص 121.

[3]– **المرجع نفسه**، ص 122.

لتبادل المعلومات وتطوير أساليب جمعها بين الولايات المتحدة الأمريكية وإسرائيل بموجب تلك الاتفاقيات أصبح بإمكان إسرائيل الحصول على المعلومات اللازمة لإنتاج أجهزة التجسس ونظم الحرب الإلكترونية وتحقيق التعاون في مجال البحوث العلمية.[1]

تؤمن إسرائيل أن الطريق الوحيد الذي يمكنها من موازنة ضعفها الكمي بمزايا نوعية هوتأكيد المزايا النوعية لشعبها ولبنيتها التحتية من مؤسساتها العلمية والتكنولوجية، حيث استطاعت أن تستفيد من تقدمها العلمي والتكنولوجي في عدة مجالات أهمها المجال العسكري والإلكتروني والمجال الاقتصادي بل وأيضا المجال السياسي.[2]

ثانيا: وسائل وأساليب الاتصال والتواصل الاجتماعي

شهد العقد الأخير من القرن الماضي حركة تقنية متسارعة وتطورا كبيرا في مجال وسائل الاتصال والمعلومات كما تعددت وسائل التواصل مع الآخرين مع التقدم التقني دون أي حواجز.

أخذت شبكة الانترنت تغزوكل مناحي الحياة وأتاحت تواصل الأفراد مع بعضهم البعض وتفاعلهم مع مختلف الأحداث والسياسات، إذ أحدثت التطورات التقنية الحديثة نقلة حقيقية في عالم الاتصال وربطت أجزاء العالم بفضائها الواسع ومهدت لكافة المجتمعات الطريق للتقارب وتبادل الآراء والأفكار ولقد ساهمت التطورات المتلاحقة في شبكة الانترنت في إيجاد شكل جديد من الإعلام تعددت تصنيفاته ومسمياته لدى المهتمين والمختصين والذي أطلق عليه الإعلام الجديد أوالإعلام البديل الذي يشمل مواقع التواصل الاجتماعي.[3]

تستغل إسرائيل وسائل التواصل الاجتماعي بشكل كبير، فهي من أسهل الأساليب والأدوات التقنية والإلكترونية استخداما وأقلها تكلفة وأكثرها وأضخمها رواجا وانتشارا في المجتمعات خاصة العربية.

تعتبر مواقع التواصل الاجتماعي مصدرا معلوماتيا هام للموساد الإسرائيلي فقد أنشأت الجهات الإسرائيلية عددا كبيرا من الصفحات على مواقع الفيس بوك الناطقة باللغة العربية لتكون من جهة مصدرا للمعلومات

---

[1]– إبراهيم عبد الكريم، "**الصناعات العسكرية الإسرائيلية: المحددات–البنية–الصادرات**"، (أبوظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2004)، ص 44.

[2]– أحمد بهاء الدين شعبان، **مرجع سابق**، ص 17.

[3]– شدان يعقوب خليل أبويعقوب، "**أثر مواقع التواصل الاجتماعي على الوعي السياسي بالقضية الفلسطينية لدى طلبة جامعة النجاح الوطنية**"، مذكرة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية السياسية، (جامعة: النجاح الوطنية، كلية الدراسات العليا، 2015)، ص 02.

عنها ووسيلة لإطلاع المجتمعات العربية على أنشطتها، ومن جهة أخرى يعتمد "الموساد" الإسرائيلي على آلاف الصفحات لكتابة تقارير يومية وأسبوعية وشهرية عن الأوضاع داخل الدول العربية معتمدين في ذلك على آراء وتوجهات الشباب العربي الذين يتم إضافتهم كأصدقاء على تلك الصفحات.[1]

تتعاون إسرائيل في هذا المجال مع شركة أورانج (Orange) لخدمات الاتصال والهاتف والتي تتمتع بنفوذ إلكتروني ومعلوماتي قوي داخل إسرائيل وخارجها، تتيح هذه الشركة لضباط الاختراق والإسقاط الإلكتروني والأمني الإسرائيلي انتحال صفات وشخصيات عربية.[2]

تمثل مواقع التواصل الاجتماعي إضافة نوعية وسبلا أكثر سرعة وانتشار للترويج للقضايا الإسرائيلية وتعبئة الرأي العام ونشر الوعي السياسي وتنميته والاستفادة من المعلومات من خلال رصد ومراقبة هذه المواقع خاصة بأعدائها، ومما لاشك فيه أن العديد من الجهات الإسرائيلية تهتم اهتماما كبيرا برصد ومتابعة ما يحدث في العالم خاصة العربي وبالتالي فإن إسرائيل رصدت وأدركت أهمية ذلك في تطوير أساليب التجسس الأكثر احترافية للاستفادة من الكم الهائل من المعلومات المتاحة.

ثالثا: المجتمع الإسرائيلي كجزء داعم للفضاء الإلكتروني الإسرائيلي

ازدهرت وتطورت الصناعات القائمة على التكنولوجيا والعلم والابتكار نتيجة لما تتوفر عليه إسرائيل من مستويات عالية في كل المجالات والتخصصات، مما انعكس على المجتمع الإسرائيلي ليصبح تجمعا علميا وتكنولوجيا يتميز بالعقلية والممارسة الحياتية العلمية، وساعد على ذلك توفر مناخ الحرية والاستقلال والتزام إسرائيل بتهيئة أجواء البحث العلمي والتطور التكنولوجي، للارتقاء بجودة الكتلة السكانية ككتلة متعلمة ذات معرفة وصديقة للعلم والتكنولوجيا.[3]

ويعتبر المجتمع الإسرائيلي الداعم الأساسي للأمن القومي للدولة، وركنا مهما في دعم الفضاء الإلكتروني الإسرائيلي خاصة أولئك الذين يمارسون الأعمال الإلكترونية الداعمة للتوجه التقني الإسرائيلي الداعي لأن تكون إسرائيل مصدرا للاستقطاب التكنولوجي العالمي، وتبين دراسة استقصائية أجرتها أكبر شركة اتصالات

---

[1]– نسرين فوزي اللواتي، "**الفيس بوك أداة إسرائيلية للتجسس والتجنيد والمراقبة**"، تم تصفح الموقع يوم : 13 مارس 2018. الرابط:

Aitmag-ahram.org.eg/News/2068.aspx

[2]– وليد غسان سعيد جعلود، **مرجع سابق**، ص 172.

[3]– أشرف صوافطة، "**أثر البحث العلمي على صناعة القرار السياسي، إسرائيل نموذجا**"، تم تصفح الموقع يوم : 14 مارس 2018. الرابط:

Democraticac.de/?p=25826

في إسرائيل "بيزك" عن حالة استخدام الانترنت في إسرائيل والتي تقدم لمحة عن الحياة الرقمية للإسرائيليين في سنة 2017م.

ويبين التقرير أن عدد مستخدمي الانترنت في إسرائيل بلغ في سنة 2017م حوالي 6.6 مليون مستخدم ويستمر متوسط عرض النطاق الثابت للانترنت في الارتفاع بما يتماشى مع زيادة استخدام الشبكة، حيث يبلغ متوسط حزمة التصفح 67 ميغابايت، يقوم المتصفح المتوسط بتحميل ملفات بمعدل حوالي 5.7 ميغابايت في اليوم بزيادة قدرها 36% خلال عام. [1]

ومن خلال هذه التقارير نستخلص أن المجتمع الإسرائيلي يتميز بقدرات تكنولوجية قادرة على مساندة إسرائيل في مواجهة التهديدات السيبرانية، علاوة على كونها بيئة مناسبة لتجنيد المدنيين الإسرائيليين للعمل في الجبهات الرقمية والإلكترونية الإسرائيلية.[2]

أصبحت وسائل الاتصال الإلكترونية أداة للتغيير تستخدمها كافة شعوب العالم في شتى مجالات الحياة الإنسانية بشكل قوي، كما أضحت وسيلة قوية تستخدمها الدول دون أن تحرك جيوشها أوتهدر أموالها، الأمر الذي جعل منها سلاحا للتهديد والردع والرد، فعبر شاشة الحاسوب تستطيع الدول أن تدمر البنية التحتية لأي عدويواجهها مستخدمة في ذلك منظومة معلوماتية وتقنية.[3]

وتصف "كريس لافان" الثورة المعلوماتية بقولها: "عند بلوغنا القرن العشرين ظهرت قوتان تعبران عن نموذج الاتصال الجماهيري: الأولى هي استخدام الكمبيوتر كوسيلة لمعالجة وتحليل ونشر المعلومات والثانية التطور المتسارع لوظيفة هذه التكنولوجيا لتطوير الاتصال، وقد كسرت نموذج الواحد إلى العديد الذي كان يميز نظم الاتصال التقليدية...."[4]

---

[1]– وليد غسان سعيد جعلود، **مرجع سابق**، ص 175.

[2]– **المرجع نفسه**، ص 176.

[3]– **المرجع نفسه**، ص 03.

[4]– عباس مصطفى صادق، "**الإعلام الجديد: المفاهيم والوسائل والتطبيقات**"، (الأردن: دار الشروق للنشر والتوزيع، 2008)، ص 23.

خلاصة الفصل الثاني

تعتبر إسرائيل أن توفير العمق الإستراتيجي لأمنها يشكل نظرية ثابتة وأن أمنها القومي يعتبر المحرك لكل إستراتيجياتها لخلق حدود آمنة يمكن الدفاع عنها على اعتبار أنها في تهديد مستمر من الدول المحيطة بها.

أن قواعد نظريات الأمن الإسرائيلي تعتبر في تطور دائم بناءا على إدراك القيادة العسكرية والأمنية الإسرائيلية بأنه من الصعب المحافظة على نظريات ثابتة في عصر العولمة وثورة التكنولوجية الرقمية والإلكترونية.

أن التطورات التي مر بها أمن المعلومات الإسرائيلي جعل منها دولة رائدة في هذا المجال وساهم في توفير بيئة معلوماتية ثرية لاستخدام المعلومات وتداولها.

تمتلك إسرائيل قدرات ومقومات كبيرة لدعم فضائها الإلكتروني، بالإضافة إلى تمتعها بفضاء تكنولوجي عالي الحصانة ومواكب لكل ما هوجديد في عالم التقنيات والإلكترونيات.

ومن أسباب التفوق الإسرائيلي في مجال أمن المعلومات والتكنولوجيات الإلكترونية المؤسسة العسكرية ودورها في تطوير الخبرات والمختصين في مجال الأمن السيبراني وهذا يعتبر من أهم العوامل المؤثرة في دفع وتطوير الحلول الأمنية والتطبيقات المتعلقة بأمن المعلومات في إسرائيل.

أن أجهزة الاستخبارات الإسرائيلية بمختلف مسمياتها "الموساد" أوشعبة "أمان" أو"الشاباك" لها دور فعال في المجال المعلوماتي الإلكتروني وفي حماية إسرائيل ومعرفة نوايا البيئة الإستراتيجية المحيطة بها.

تهتم إسرائيل بمراكز الدراسات المختصة بالفكر والبحث العلمي وهي من الدول الرائدة في هذا المجال ومما لاشك فيه أن هناك علاقة ترابطية بين مراكز البحث العلمي وتطور إسرائيل في مجال تكنولوجيا المعلومات والتقنيات الإلكترونية، كما يساهم الإعلام في تشكيل وصياغة الرأي العام ويتضاعف ذلك مع التطورات الحاصلة المواكبة للتقنيات الحديثة.

ترتكز إسرائيل في مجال الأمن السيبراني على العديد من الشركات الإسرائيلية والعالمية المختصة في تكنولوجيا المعلومات وأنظمة الحماية الأمنية للحواسيب وتطوير البرامج الإلكترونية.

أصبحت مواقع التواصل الاجتماعي بمثابة نافذة وأداة فعالة للحصول على المعلومات وخدمة مصالح إسرائيل الأمنية وساهم في ذلك وعي المجتمع الإسرائيلي بضرورة توظيف هذه المواقع لتحقيق الأهداف المرجوة.

الفصل الثالث

مهددات الأمن السيبراني الإسرائيلي وإستراتيجيات المواجهة

لقد ساهم بروز التهديدات التماثلية واللاتماثلية في التأثير على أمن الدول خاصة وأن هذه التهديدات تتجاوز قدرة الدول على مواجهتها بشكل منفرد.

ومن أحدث انواع هذه التهديدات التي أصبحت تتعرض لها الدول خاصة منها المتقدمة في المجال التكنولوجي والالكتروني، ما يطلق عليها التهديدات السيبرانية التي تتميز بالتنوع والتداخل والتعقيد وسرعة الإنتشار.

تدرك إسرائيل باعتبارها دولة محوسبة تعتمد على تقنيات تكنولوجية عالية في تسيير غالبية مؤسساتها وقطاعاتها الحيوية أن مثل هذه التهديدات سيشكل تحديا يؤثر سلبا على أمنها، الامر الذي يجعل القادة الإسرائيليون يحاولون تكييف سياساتهم الأمنية مع طبيعة هذه التهديدات واتخاذ تدابير وبلورة استراتيجيات في مجال الدفاع السيبراني، وكذلك اللجوء إلى أساليب هجومية للرد على كل ما يشكل خطرا على وجودها في هذا المجال.

وعليه سوف يتم توضيح ذلك من خلال هذا الفصل المتضمن ثلاث مباحث تتمثل فيمايلي :

- **التهديدات السيبرانية وتأثيرها على الأمن الإسرائيلي؛**
- **أبعاد الاستعدادات الإسرائيلية في مجال الفضاء الإلكتروني؛**
- **الإستراتيجية الإسرائيلية الهجومية كآلية لمواجهة التهديدات السيبرانية.**

المبحث الأول : التهديدات السيبرانية وتأثيرها على الأمن الإسرائيلي

يواجه المجتمع الدولي في العصر الحديث عددا كبيرا من التهديدات الأمنية التي تتسم بتغيرها وتطورها المستمر وصعوبة التنبؤ بها أوالسيطرة عليها، واتساع نطاق تأثيرها بحيث لا يقتصر على الإضرار بأمن الفواعل بعينها وإنما يمتد ليؤثر في الأمن العالمي بشكل عام.

ولعل أبرز هذه التهديدات الأمنية المعاصرة وأكثرها حداثة وأوسعها انتشارا هي التهديدات السيبرانية (Cyber Threats)، فلقد أصبحت هذه التهديدات من التعقيد بمكان وبات من الصعب حصرها أوتطوير إستراتيجيات محكمة لمواجهتها بشكل كامل خاصة مع تعدد أشكالها ومصادرها وتطورها المتسارع والمستمر.[1]

لذلك تصدرت مواجهة هذه التهديدات قمة أولويات السياسات الأمنية للدول من أجل وضع تدابير وقائية لضمان أمنها وتفادي الأضرار الناجمة عنها.

ولا يمكن استثناء إسرائيل من مصاف الدول التي تمتلك المقومات التكنولوجية والعلمية في مجال الفضاء الإلكتروني إلا أن هذا لا ينفي تعرضها إلى العديد من الهجمات والاختراقات الإلكترونية من الأطراف الفاعلة التي تتراوح بين الدول ومجموعات القراصنة والتي يمكن إبراز أهمها فيما يلي :

المطلب الأول : نماذج عن أبرز الهجمات السيبرانية على الفضاء الإلكتروني الإسرائيلي

تواجه إسرائيل سلسلة من الهجمات الإلكترونية المتزايدة من مصادر عدة ولم تقتصر على اختراق أنظمة الكومبيوتر العسكرية أوالبنكية فحسب، بل امتدت لتشمل قطاعات داخلية مرتبطة بكل المجالات والقطاعات الحيوية فيها.

إن تعطيل العديد من المواقع الإسرائيلية الرسمية ومواقع التواصل الاجتماعي يجعل إسرائيل بما تملكه من قدرات نووية وبما تتمتع به في مجال المعلوماتية والتكنولوجية في موقع ضعف مما يؤدي إلى التشكيك في قدراتها على الحفاظ على أمنها المعلوماتي.[2]

---

[1]– نوران شفيق، "**أشكال التهديدات الإلكترونية ومصادرها**"، تم تصفح الموقع يوم : 17 مارس 2018. الرابط: http://www.europarabct.com/

[2] –Matthew Cohen, and Charles Friesisch, **"Israel and Cyberspace - Unique Threat and response"**, (international Studies Perspectives, August 2016), p 01.

فقد ساهمت شبكة الاتصالات الدولية المتمثلة في الانترنت في التقريب بين المنخرطين خلال عمليات الاختراق عبر السرعة في تلقي المعلومة وتوجيه الضربات بشكل فعال للهدف، ومنه تشكيل جيش إلكتروني يهدد الأمن القومي الإسرائيلي.[1]

وإذا كانت الدول العربية قد عرفت حراكا اجتماعيا بفعل استغلال الشباب العربي لمواقع التواصل الاجتماعي والذي كان من نتائجه إسقاط أنظمة سلطوية واستبداديه فهو حراك تهيمن في أغلبه مطالب داخلية للشعوب العربية كالمطالبة بالديمقراطية والحرية واحترام حقوق الإنسان وغيرها.

فاستمرار سياسات إسرائيل تجاه القضية الفلسطينية وسياسات التطبيع معها من طرف العديد من الدول العربية ساهم في خلق حالة عدم الرضى على السياسات الخارجية للدول العربية إزاء هذه القضية والتي لا يستجيب لطموحات الشعوب،[2] ساهم في بروز هذه المجموعات التي قامت بالعديد من الاختراقات والهجمات على البنى التحتية والمواقع الحساسة لإسرائيل ومن بين هذه النماذج نذكر مايلي :

الفرع الأول : الهجمات الإلكترونية على المواقع الإسرائيلية " مجموعة الأنونيموس "

تعد مجموعة " الأنونيموس" من أكثر المجموعات المؤثرة في تاريخ القراصنة الحديث، إذ تستمر فعاليات المجموعة إلى يومنا هذا في نشاطاتها ولا توجد أي معلومة حول عددهم أومجموعاتهم الفرعية، ومن بين أشهر العمليات التي قامت بها هذه المجموعة دعمهم لموقع (وكيليكس).

وقد سببت هذه المجموعة العديد من المشكلات السياسية عبر العالم، إضافة إلى هجومهم على مواقع شركات عالمية عدة وتدخلهم في الانتخابات الإيرانية سنة 2009م والقيام بمهاجمة مواقع حكومية أسترالية من أجل المطالبة بالسماح للمستخدم بالتصفح من دون حجب لأي موقع، ومواقع حكومية للعديد من الدول وتسريب معلومات شخصية لشخصيات معروفة في كل من البحرين والمغرب ومصر والأردن كما كان الربيع العربي ميدان عمل مكثف لأعضائها، إذ قدموا دعما فوريا للثورات الشعبية في تونس ومصر عبر شن هجمات قوية ضد المواقع الحكومية للدولتين.[3]

---

[1]- مصطفى الديماني، "**الحرب الإلكترونية على إسرائيل: الأبعاد والدلالات**"، تم تصفح الموقع يوم : 17 مارس 2018. الرابط:

www.m.ahewar.org/s.asp?aid:381345§r=0

[2]- فيصل محمد عبد الغفار، "**الحرب الإلكترونية**"، (الأردن: الجنادرية للنشر والتوزيع، 2016)، ص158.

[3]- خالد وليد محمود، " **الهجمات عبر الانترنت: ساحة الصراع الإلكتروني الجديدة**"، (الدوحة: المركز العربي للأبحاث ودراسة السياسات، 2013)، ص 02.

أصبح العالم أمام قوى تتسلح بالتكنولوجيا الحاسوبية ويمكنها الاختراق وارتكاب أفعال تقنية مضرة بالآخرين عبر العالم الافتراضي، وثمة العديد من التطورات والتجاذبات والسجلات الميدانية والنظرية التي ألقت الضوء على هذا المجال الجديد نسبيا، لاسيما بعد الهجمات الإلكترونية التي شنتها مجموعة "الأنونيموس" أوما يطلق عليها باللغة العربية (المجهولون) في العالم وفي الشرق الأوسط وتحديدا في إسرائيل.[1]

نفذت هذه المجموعة سلسلة من الهجمات المنسقة ضد مواقع وصفحات تابعة للحكومة الإسرائيلية وشركات ومواقع حكومية بما في ذلك قوات الدفاع الإسرائيلية بحيث تعرضت بنية الانترنت التحتية في إسرائيل لهجمات عديدة.

وقد أستخدم في هذه الهجمات نحو خمسة ملايين حاسوب على الأقل تبنت مجموعة القراصنة المجهولين "أنونيموس" الكثير من تلك الهجمات ردا على العدوان على غزة في سنة 2009م.[2]

ومع ذلك كان الهجوم الذي وقع في 07 أفريل 2013م من أكثر الهجمات قوة حيث رفعت مجموعة "الأنونيموس" شعارها "محو إسرائيل من الانترنت" ردا على سياساتها تجاه الفلسطينيين مما تسبب في خسائر مادية وغير مادية.

وأبرز المواقع الإسرائيلية المخترقة هي :

- الكنيست الإسرائيلي
- وزارة الاستخبارات
- رئاسة الوزراء، موقع وزارة الأمن، وزارة التربية، سوق الأوراق المالية
- 2000 حساب فيس بوك، 500 حساب تويتر
- 3000 حساب مصرفي بمختلف البنوك الإسرائيلية
- حساب لشخصيات سياسية مهمة أبرزها صفحة رئيس الوزراء السابق "سيلفان شالوم"[3]
- موقع الموساد
- شؤون المحاكم التابع لما يسمى وزارة العدل الإسرائيلية والمعنية بالبنى التحتية

---

[1]– **المرجع نفسه**، ص 02.

[2] - Tavish Vaidya, **" Survey and Analysis of Major Cyberattacks : 2001-2013 "**,(Georgetown University, July 2015), p 04.

[3] –Khalid Walid Mahmoud, **" Cyberattacks, The Electronic Battlefield "**, (Doha : Arab centre for Research and policy Studies, 2013), p 15.

وقد اتخذت مجموعة "الأنونيموس" يوم 07 أفريل من كل سنة موعدا للهجوم على المواقع الإسرائيلية بالتنسيق مع أعضائها في مختلف دول العالم كلبنان وسورية وفلسطين والأردن والسعودية والجزائر وتونس والمغرب كما انضمت مجموعات من إيران وأندونيسيا ومناطق في جنوب إفريقيا.

ففي سنة 2016م قامت هذه المجموعة باختراق موقع القناة الإسرائيلية، وتسببت في توقف الموقع لفترة من الزمن وتعرض موقع مرتبط بمنظمة التجارة والنمو العالمي لهجمة إلكترونية أدت إلى تعطلها عن العمل.

كما استخدمت أحصنة طروادة في هجوم إلكتروني استهدف شبكة أنفاق مدينة "الكرمل" ونقاط تحصيل رسوم استخدام الطريق في شهر سبتمبر من نفس السنة وهي شفرة يتم تحميلها على الحاسوب بدون علم المستخدم فتمكن القرصان أوالمخترق من التحكم في حاسوب الضحية أوالمستهدف.

لأن أغلب هذه الأنظمة (أنظمة الطرق) أوتوماتيكية وبالتحديد إجراءاتها الأمنية حيث يتم التحكم فيها عن بعد إما عن طريق الانترنت أوبوسائل أخرى ولذلك فهي تعتبر هدفا سهلا للهجمات الإلكترونية.[1]

أصبحت مجموعة "الأنونيموس" ذات صدى كبير في مجال الحرب الإلكترونية لها تأثير على الحكومات لذلك أدرجت في قائمة مجلة "تايم" للمجموعات الأكثر نفوذا في العالم.

الفرع الثاني: حزب الله والصراع الإلكتروني مع إسرائيل خلال حرب تموز 2006م

يعتبر حزب الله حركة مقاومة إسلامية تخوض حربا تحريرية ضد إسرائيل منذ نشأته، وقد أبتكر وسائل عدة لمقاومة المشاريع الصهيو-أمريكية في المنطقة،حيث تمكن حزب الله من الجمع بين العمل المقاوم واستغلال الأدوات التقنية الحديثة ووسائل الاتصال التي خدمت قضيته ومساعيه وسارت بالتزامن مع خطواته نحوتحقيق الإنجازات المتلاحقة.[2]

[1]- د م،"**الحرب الإلكترونية تؤرق إسرائيل- تقارير وحوارات**"، تم تصفح الموقع يوم : 18 مارس 2018. الرابط: www.aljazeera.net/reports and interviews/.

[2]- رفقة نبيل مطلق شقور، "**أثر حزب الله في تطوير فكر المقاومة وأساليبها في المنطقة العربية**"، مذكرة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية السياسية، (جامعة: النجاح الوطنية، كلية الدراسات العليا، 2009)، ص 03.

تولي إسرائيل اهتماما كبيرا به كونه أكثر الحركات العربية والإسلامية المقاومة لها تنظيما وتكتيكا علاوة على التقاءه الفكري مع إيران والتي تعد أكبر الجهات الممولة لحزب الله في مختلف النواحي العسكرية، المالية، التكنولوجية والمعلوماتية .بمعنى أن الصراع الإسرائيلي مع حزب الله يقوم على اختبار الإمكانيات التقنية والمعلوماتية والعسكرية والتكنولوجية والإلكترونية أيضا.[1]

حول دور الانترنت في هذه الحروب يلاحظ أن حزب الله قد أطلق موقعا منذ سنة 1996م (Hizbollah.org) حيث طرح المحتوى الرقمي للموقع باللغتين العربية والإنجليزية وذلك من أجل أن يضمن وصول خطابه لأكبر عدد من مستخدمي الشبكة وبعد فترة أضيفت إلى هذا الموقع ثلاثة مواقع جديدة للحزب وهي :

- ❖ موقع المقاومة الإسلامية (https://www.moqawama.org).
- ❖ موقع تلفزيون المنار (https://www.manar tv.com.Ib).
- ❖ موقع زعيم الحزب : السيد حسن نصر الله (http://www.nasrollah.net).[2]

تمكنت الطواقم الفنية والإلكترونية التابعة لحزب الله سنة 2006م من التشويش على الأنظمة المضادة لإطلاق الصواريخ على متن البارجة الإسرائيلية حانيت (Hanit) المحاذية لشواطئ بيروت ومن ثم إصابتها بصاروخ أدى إلى تعطيل وظائفها.

وفي نفس السنة قام حزب الله .بمهاجمة طائرة إسرائيلية بصواريخ من نوع سام 16 وسام 18 والتي تمتاز باستعصائها على التشويش الإلكتروني وصعوبة رصدها بأدوات التتبع البصرية، مما أعطى لحركة حزب الله نوعا من التميز الإلكتروني تَمَثل بإمكانية إفلات صواريخها المطلقة صوب إسرائيل من التتبع الرقمي والتكنولوجي.[3]

وباستخدام التعتيم على معلوماته وبنك أهدافه وبطريقة إلكترونية ورقمية تمكن حزب الله من الولوج إلى مجتمع المعلومات الإسرائيلي باستخدام العديد من الوسائل الإلكترونية واختراق الترددات الاتصالية الإسرائيلية المشفرة، كما لعبت قناة المنار دورا في شن حرب معلوماتية ونفسية ضد الرأي العام في إسرائيل[4]

---

[1]– وليد غسان سعيد جلعود، **مرجع سابق**، ص 221.

[2]– رفقة نبيل مطلق شقور، **مرجع سابق**، ص 89.

[3]– وليد غسان سعيد جلعود، **مرجع سابق**، ص 221.

[4]– **المرجع نفسه**، ص 222.

واختراق موجات البث الخلوي للأجهزة المحمولة الإسرائيلية وتوجيه رسائل تهديد إلى عناصر الجيش الإسرائيلي لبث الرعب والخوف في نفوسهم.[1]

كما جند حزب الله خاصية غوغل (Google Earth) التي يقدمها محرك البحث العالمي (غوغل) في تحديد أهدافه بدقة وتوجيه صواريخه إلى أهداف محددة داخل إسرائيل علما بأن إسرائيل قد استخدمت نفس البرنامج في ضرب المواقع التابعة لحزب الله أثناء حربها على الجنوب اللبناني.[2]

الفرع الثالث : المواجهة الإلكترونية بين إيران وإسرائيل

إن التطور السريع في قدرة الحرب الإلكترونية لإيران وحلفاؤها هي التي اضطرت إسرائيل ودولا غربية أخرى إلى العمل وبشكل حاسم وممنهج لتحسين التفوق النوعي العملياتي في المجال الإلكتروني من أجل محاولة التصدي لمثل هذه العمليات.

إن سعي إسرائيل وقيامها بإنتاج القبة الفولاذية الرقمية هوتأكيد على إصرارها في بناء نظام فعال من أجل التصدي لهذه الهجمات وخاصة الموجهة من قبل إيران، وهوما تم التصريح به من قبل رئيس الأركان العامة السابق للجيش الإسرائيلي يقول :"ينبغي على الكيان الإسرائيلي أن يكون في مستوى القوى الكبرى في الفضاء الإلكتروني ولا ينبغي أن ننتظر في هذا المجال".[3]

أطلقت إيران من خلال مشروعها الفضائي قمرا لديه قدرة على استخدامات مزدوجة كالتجسس والاختراق وجمع المعلومات والتشويش والاستطلاع الفضائي والمسح، ليتيح لها مراقبة المنشآت العسكرية في المنطقة وكذلك يفتح المجال لإيران في المستقبل لإطلاق أقمار صناعية أكثر تطورا في هذا المجال.[4]

[1]– رفقة نبيل مطلق شقور، **مرجع سابق،** ص 88.

[2]– وليد غسان سعيد جلعود، **مرجع سابق،** ص 223.

*– غوغل أرث: هوبرنامج خرائطي وجغرافي معلوماتي أنشأ سنة 2004م، يرسم هذا البرنامج خريطة الأرض عن طريق تركيب الصور التي يتم الحصول عليها من الأقمار الصناعية والتصوير الجوي ونظم المعلومات الجغرافية الثلاثية الأبعاد.

[3]– نبيل العتوم، "**الجيش الإلكتروني الإيراني**"، (الأردن: دار عمار للنشر والتوزيع، 2015)، ص 17.

[4]– **المرجع نفسه،** ص 31.

قامت إيران في سياق هجماتها على إسرائيل إلى حظر استخدام محرك البحث العالمي (غوغل) وبعض المواقع الاجتماعية والمواقع الإخبارية الأجنبية وتبنيها لخطط إلكترونية تعرف إيرانيا باسم "الانترنت النظيف" في إشارة إلى استبدال إيران منظومة الانترنت العالمية بأخرى إيرانية.[1]

لقد برزت القدرات الإلكترونية الإيرانية منذ نشأة المؤسسات التعاونية الوطنية "هاكتيفيست" في العقد الأول من القرن الحادي والعشرين والتي كانت تهاجم بشكل منهجي شبكات المنظمات الأجنبية والحكومات المعادية للجمهورية الإسلامية والتي على رأسها إسرائيل، ويواصل العديد من الأعضاء السابقين في هذه الجماعات أنشطتهم اليوم لحساب النظام تحت مظلة الجيش السيبراني الإيراني.[2]

وتستخدم إيران الفضاء الإلكتروني لتطوير ونشر أدوات غير متماثلة ضد الولايات المتحدة الأمريكية والمنافسين الإقليميين وعلى رأسهم إسرائيل ودول الخليج، فالهجمات السيبرانية تسمح لإيران بالهجوم على خصومها بشكل مستمر على الصعيد العالمي لتحقيق تأثيرات إستراتيجية بطرق لا يمكن أن تكون متاحة في المجال المادي كما يقول خبير الانترنت "مايكل آيزنشتات".[3]

كما عكفت في السنوات الأخيرة على بناء جيش إلكتروني يتبنى فكرة (الجهاد الإلكتروني)، بحيث ينقسم هذا الجيش إلى عدة أقسام منها ما هومتخصص في الدفاع وصد أي هجوم إلكتروني ومنها ما هومتخصص بالمتابعة والرصد ووقف محاولات التسلل لشبكة الحواسيب الإيرانية، ومنها ما هومتخصص لاكتشاف الفيروسات الإلكترونية ووقف محاولات الوصول إلى أجهزتها الحاسوبية.

كما سجلت أجهزة الاستخبارات الإيرانية اختراقات واسعة للحواسيب الإسرائيلية شملت شخصيات بارزة من العسكريين والسياسيين من بين 1800 حاسوب إسرائيلي واستطاعت سحب المعلومات المخزنة فيها بما في ذلك الوثائق والصور ومراسلات البريد الإلكتروني، إضافة إلى اختراق حواسيب أخرى تابعة لخبراء وإعلاميين إسرائيليين وعلماء في مجال الفيزياء والطاقة النووية ومسؤولين في الجامعات والمعاهد البحثية الإسرائيلية وخبراء في الشؤون الإيرانية على مختلف مستوياتهم سنة 2016م.[4]

---

[1]- وليد غسان سعيد جعلود، **مرجع سابق**، ص 225.

[2]- عادل رفيق، **مترجما**، "**الجيوبوليتكس السيبراني والاستقرار في الشرق الأوسط**"، المعهد المصري_للدراسات، (يناير 2018)، ص 04.

[3]- **المرجع نفسه**، ص 09.

[4]- يحي دبوق، "**إيران تخترق الحواسيب الاسرائيلية: ضباط وخبراء وعلماء نوويون**"، تم تصفح الموقع يوم : 19 مارس 2018. الرابط:

al-akhbar.com

الفرع الرابع: الاختراقات الإلكترونية لحركة المقاومة الإسلامية "حماس" ضد إسرائيل

تعتبر حركة "حماس" إحدى الفصائل الأساسية في العمل النضالي الفلسطيني والإسلامي والتي تمتلك أهدافا وأيديولوجية خاصة بها تسعى لتحقيقها، سعت هذه الحركة إلى كسب التأييد الجماهيري في الداخل الفلسطيني من خلال استخدام العديد من الوسائل لتعزيز الثقة بين الطرفين.[1]

فحركة المقاومة الإسلامية "حماس" هي امتداد لحركة الإخوان المسلمين وجناح من أجنحتهم الممتدة في المنطقة العربية والإسلامية لدعم ساحة المقاومة والجهاد ولتصبح فصيلا فعالا في المقاومة الفلسطينية فقد انطلقت هذه الحركة سنة 1967م، ورفضت كل مشاريع التسوية السلمية مع إسرائيل التي تزامنت مع الانتفاضة الأولى لتضع ميثاقها في أوت 1988م.[2]

تعددت أشكال المقاومة في تصريحات حركة "حماس" وهذا ارتبط بممارسات إسرائيل وسياساتها التي تتبعها وبوجودها على الأراضي الفلسطينية، فإلى جانب المقاومة في شكلها المسلح تتبع هذه الحركة أساليب حديثة وعلى كافة المستويات للحصول على الحد الأدنى من الحقوق الفلسطينية وتعزز ذلك بفضل انتشار التكنولوجيا الحديثة والذي أصبح تحديا يواجه إسرائيل يحتم عليها حماية الخصوصية الفردية والأنظمة العامة التي أصبحت معرضة للاختراق.

فقد تمكنت هذه الحركة من تهكير مواقع إسرائيلية معروفة عن بعضها أنه سيادي كمواقع وزارة الدفاع و"الشاباك" بالاعتماد على خبرات عناصرها ومؤيديها وكان ذلك في سنة 2014م.[3]

كما تمكنت "كتائب القسام" مع بداية سنة 2017م من السيطرة على هواتف لجنود وضباط إسرائيليين في هيئات الأركان الميدانية وهيئة الأركان العامة، واستقت معلومات حساسة وتجسست على مناورات وعمليات عسكرية عبر وسائل التواصل الاجتماعي من خلال فتح حسابات مزيفة على الفيس بوك.

---

[1]- معتز سمير الدبس، "**التطورات الداخلية وأثرها على حركة المقاومة الإسلامية (حماس) 2000-2009**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، (جامعة: الأزهر، كلية الاقتصاد والعلوم الإدارية، قسم العلوم السياسية، 2010)، ص 24.

[2]- **المرجع نفسه**، ص 02.

[3]- ميرفت عوف، "**الحرب الإلكترونية تتأجج بين إسرائيل والمقاومة الفلسطينية فمن الأقوى؟!**"، تم تصفح الموقع يوم : 19 مارس 2018. الرابط: http :www.sasapost.com/electronic-warfare.resistance.israel

واستخدمت أيضا تطبيقات خاصة للسيطرة على هواتف العسكريين واستغلال كاميرات هواتفهم النقالة لتقوم بالتنصت على محاداثاتهم، وهوما يشكل تهديدا حقيقيا على أمن إسرائيل كما أنه يكشف عن قدرة حركة "حماس" على التجسس على مواقع التواصل الاجتماعي حيث استخدمت فيها لغة عبرية عالية المستوى للإيقاع بالجنود والضباط، ويدل ذلك على اهتمام هذه الحركة بجمع المعلومات عن تحركات الجيش الإسرائيلي وعن نوعية الأسلحة التي يستخدمها والسعي إلى استهداف بشكل مباشر مرافقها الإستراتيجية المرتبطة بالفضاء الإلكتروني مثل البنى التحتية (الكهرباء والمياه والمواصلات والقطاع المصرفي وهيئات القيادة وشبكات التحكم العسكرية ومجمل التقنيات المتقدمة المرتبطة بهذا الفضاء).[1]

الفرع الخامس : الهجمات السيبرانية للجيش السوري الإلكتروني ضد إسرائيل

الجيوش الإلكترونية مجموعة مدربة تعمل وفق أجندة خاصة هدفها اختراق العدو والترويج لوجهة نظر معينة عبر مختلف شبكات الإنترنت وتشويه سمعة المناوئين إلى جانب ترويج الإشاعات والأكاذيب، وقد بدأت الدول في إنشاء وحدات إلكترونية داخل أجهزتها العسكرية والأمنية لحماية أمنها القومي.

ويمكن القول أن الجيوش الإلكترونية هي مجموعة من الأشخاص وقراصنة الإنترنت (الهاكرز) تعمل لصالح أجهزة المخابرات والأمن وهي في الغالب تسعى لاختراق المواقع الإلكترونية الخاصة بالشخصيات والمؤسسات والدول، تستخدم مواقع التواصل الاجتماعي وغيرها من المواقع الإلكترونية للدفاع عن وجهة النظر الرسمية.[2]

انتشر المصطلح بشكل كبير سنة 2011م عقب الكشف عن "الجيش الإلكتروني السوري" الذي نجح في اختراق مواقع أوروبية وأمريكية وعربية، لتوجيه رسائل داعمة لنظام بشار الأسد بعد اندلاع الثورة السورية في نفس السنة.

يعتمد الجيش الإلكتروني في تحقيق أهدافه على طاقم فني مدرب ووسائل تقنية حديثة ومتطورة عند عملية الاختراق، حيث يتم في الغالب إرسال فيروسات تعمل على السيطرة على المواقع المستهدفة بطريقة

[1]– د م، "**هكذا اخترقت حماس جيش الاحتلال الإسرائيلي**"، تم تصفح الموقع يوم : 19 مارس 2018. الرابط: www.aljazira.net/encylopedia/military/15/01/2017

[2]– د م، "**ماذا تعرف عن الجيوش الإلكترونية**"، تم تصفح الموقع يوم : 19 مارس 2018. الرابط: http://www.aljazeera.net/encyclopedia/conceptsandterminology/2017/7/5/

لايمكن معها الكشف بسهولة عن مرتكبي عملية الاختراق وهوما يؤكد أن الجيوش الإلكترونية مرتبطة بمؤسسات الدولة الأمنية.[1]

تعرضت إسرائيل لاختراق نجح فيه الجيش السوري الإلكتروني، وقد نُفذ هذا الاختراق بتاريخ 28 جوان 2014م حسب تقرير لموقع (hackred.com) على المدونة الدولية للجيش الإسرائيلي وتعطيلها مع نشره بيانا باسمه جاء فيه: "ترتكب حكومة إسرائيل جرائم حرب يومية إزاء الفلسطينيين وهي من أكبر المنتهكين لحقوق الإنسان، إضافة للوضع الفلسطيني إنها رسالة تنبيه لإسرائيل من العمليات (القصف) التي تنفذها على مواقع عسكرية سورية".[2]

مع العلم أن مدونة الجيش الإسرائيلي تعمل تحت وحدة الناطق العسكري وعبرها ينشر الجيش الإسرائيلي أخباره وتوضيح سياسته للمجتمع الدولي.

الفرع السادس: أبرز نماذج القرصنة الإلكترونية للشباب العربي الإسلامي على المواقع الإسرائيلية

هناك العديد من النماذج الإلكترونية للشباب العربي والإسلامي التي وظفت خبرتها التقنية والمعلوماتية نحو إسرائيل لتضرب العمق الرقمي والتكنولوجي لها.

ومن بين هذه النماذج نموذج الشاب السعودي المعروف بـــ (أوإكس عمر) (Ox Omer) الذي حقق شهرة عالمية بعدما تمكن من كشف بيانات بطاقات الائتمان الخاصة بآلاف الإسرائيليين ما تسبب في هلع داخل الكيان الإسرائيلي بعدما اعترفت البنوك الإسرائيلية بحدوث اختراق لبيانات 400 ألف عميل.[3]

– اختراق موقع بورصة تل أبيب للأوراق المالية وموقع شركة العال (Elal) واصابتها بالشلل التام، حيث استهدفت الهجمات الإلكترونية قنوات الاتصال الخدماتية لهذه المواقع وخلقت بيئة افتراضية توحي بأن هناك مئات الآلاف من طلبات الدخول لينهار الموقع تحت وطأة الضغط مما أدى لإغلاق هذا الموقع بشكل تام.

---

[1]– المكان نفسه.

[2]– د م، "**الجيش الإلكتروني يخترق المدونة الدولية للجيش الإسرائيلي**"، تم تصفح الموقع يوم : 19 مارس 2018. الرابط:

http://www.almayadeen.net/news/604561

[3]– د م ، "**أخطر الهاكرز العرب على المستوى العالمي**"، تم تصفح الموقع يوم : 19 مارس 2018. الرابط:
https://www.ta3allamdz.com/2015/09/blog-post.html

- نجح السعودي (Ox Omer) في الوصول إلى أرقام مئات الآلاف من البطاقات الائتمانية الإسرائيلية ودعا الجميع عبر الانترنت إلى الشراء الإلكتروني على حساب إسرائيل معلنا الحرب الإلكترونية عليها ومهددا بالقضاء عليها رقميا وذلك انتقاما لسياستها بحق الشعب الفلسطيني.[1]

كما يعد الهاكر "سيلنت هل" (Dr.Silnt Hill) من أقوى الهاكرز في مصر ينتمي لفريق (Team Haker Egypt) حيث قام في سنة 2009م باختراق أكثر من 100 موقع بيع وشراء إسرائيلي وهذا ما أثر اقتصاديا على إسرائيل، كما نجح الهاكر السعودي (Sniper Hex) في اختراق العديد من المواقع الإسرائيلية مثل وزارة التعليم الإسرائيلية ووزارة السياحة وموقع حزب "الليكود" وتدمير أكبر موقع بحث إسرائيلي "Guide" والعديد من المواقع الأخرى.

- أعادت مجموعة إلكترونية تطلق على نفسها جماعة الكابوس (nightmare group) اختراق موقع البورصة الإسرائيلية وشركة العال للطيران، وعددا من المواقع الإلكترونية الأخرى.

- كما قامت مجموعة من المتضامنين العرب والأجانب مع القضية الفلسطينية بتوجيه ضربة إلكترونية كبيرة لإسرائيل، حيث نجحت في اختراق موقع ثاني أكبر شركة للمواصلات والنقل الداخلي في إسرائيل وهي شركة دان (Dan) واختراق خوادم مواقع أخرى.[2]

- قامت مجموعة من الهاكرز السعوديين باختراق 15000 بطاقة ائتمان من أصل 411 ألف، وقد أكد البنك المركزي أن الهاكرز اخترقوا سيرفرات ثلاث شركات بطاقات ائتمان وهي "أزرايل كارد" ولومي كارد" و"كال" وأنه في حالة استخدام هذه البطاقات من قبل الهاكرز فإن البنوك ستعوض الضحايا.[3]

- تمكن قرصان إلكتروني موريتاني من اختراق أكثر من 15 ألف حساب إلكتروني إسرائيلي على مواقع التواصل الاجتماعي (فيس بوك)، وتمكن من اختراق خوادم مواقع إلكترونية إسرائيلية أخرى.

[1]- د م، "**ملفات ساخنة: حرب التحكم الآلي سلاح الحرب الخامس**"، (الأردن: دار الجليل للنشر والتوزيع، 2013)، ص 190.

[2]- وليد غسان سعيد جعلود، **مرجع سابق**، ص ص 232-233.

[3]- د م، "**البنك الإسرائيلي يؤكد اختراق 15000 بطاقة إئتمان من قبل هاكر سعودي**"، تم تصفح الموقع يوم : 19 مارس 2018. الرابط:

http://www.alyaum.com/article/3039850

- كما تمكن الهاكر الجزائري حمزة بن دلاج الذي يعد أحد أخطر الهاكرز في العالم العربي، بحيث تمكن من اختراق العديد من المواقع وشركات إسرائيلية ومن أبرز المواقع التي سيطر عليها موقع الحكومة الإسرائيلية حيث قام بكشف أسرار الجيش الإسرائيلي للمقاومة الفلسطينية ونشر بيانات هامة لأفراده.[1]

المطلب الثاني : تأثير الهجمات السيبرانية على الأمن الإسرائيلي

أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، حيث تشمل هذه البنية الطاقة والاتصالات والنقل والخدمات الحكومية والتجارة الإلكترونية والمصارف والمؤسسات المالية ولقد جعل الفضاء الإلكتروني تلك المصالح مرتبطة ببعضها البعض في بيئة واحدة، والتي تعرف بالبنية التحتية القومية للمعلومات ومن ثم فإن أي هجوم على تلك المصالح يمثل سببا ومدعاة لحدوث عدم توازن إستراتيجي مما يكشف نمطا جديدا من أنماط التهديد للأمن القومي.[2]

لذلك أصبحت المخاطر والتهديدات السيبرانية تؤثر على كافة المجالات في إسرائيل نظرا لاعتمادها على الأنظمة الإلكترونية في كافة منشآتها الحيوية، ومن هنا وجب إبراز هذه التأثيرات التي مست الأمن الإسرائيلي خاصة في قطاعاتها الاقتصادية والاجتماعية والنفسية والسياسية والإعلامية أيضا.

الفرع الأول : التأثيرات الاقتصادية

منذ أن قامت إسرائيل بحوسبة قطاعاتها المختلفة وربطت اقتصادها بالتطورات التقنية والرقمية واتصاله مباشرة بالشبكات الإلكترونية ووسائل الاتصالات الحديثة كالحواسيب والانترنت والأجهزة الذكية وغيرها أصبحت الحياة الاقتصادية والاجتماعية الإسرائيلية مرتبطة بشبكات الاتصال بشكل وثيق[3]، كمواقع البورصة وبطاقات الائتمان وبيانات الأفراد والبنوك الأمر الذي جعلها هدفا لعمليات القرصنة الإلكترونية.

تعتبر المواقع الإلكترونية الاقتصادية الإسرائيلية أكثر القطاعات استهدافا للهجمات الإلكترونية خاصة من الهاكرز العربي والإسلامي، فمثلا تعرضت كبريات المواقع الاقتصادية في إسرائيل للاختراق الإلكتروني في العديد من المرات كمواقع البورصة الإسرائيلية وضرب خوادم حساسة لإثنين من أهم وأكبر بنوكها وهما بنك

---

[1]- د م، "**السفارة الأمريكية مطالبة بتوضيح مصير الهاركر PX1**"، السلام، 22 أوت، 2015، العدد 1323، الجزائر.

[2]- عادل عبد الصادق، "**الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي**"، تم تصفح الموقع يوم : 21 مارس 2018. الرابط:

http://accronline.com/article_detail.aspx?id=28395

[3]- وليد غسان سعيد جلعود، **مرجع سابق**، ص 235.

مسيد (Bank Msid)[1] وبنك أوتسيرها حيال (Bank Otser Hahial)، مما يعني أن القطاع الاقتصادي معرض للهجمات الإلكترونية الأمر الذي قد يكبد إسرائيل تكلفة عالية من الناحية المالية والاقتصادية والأمنية في عالم الاتصالات وتكنولوجيا المعلومات، فالبرغم من أن هذه الهجمات لم تدمر خوادم ومواقع البنوك والبورصة الإسرائيلية بشكل كامل إلا أنها شلت حركتها لعدة ساعات وهوما يكلفها على الصعيد الاجتماعي والاقتصادي الكثير.[2]

وعلى الرغم من محاولات إسرائيل التكتم عن خسائرها إلا أن شن مجموعة "الأنونيموس" لأكبر عملية قرصنة معلوماتية ضدها والتي استهدفت أكثر من 100 ألف موقع و30 ألف حساب مصرفي إسرائيلي كبد إسرائيل خسائر وصلت إلى 3 مليارات دولار.

فمنذ بداية الهجوم على المواقع الحكومية الإسرائيلية الإلكترونية بدأت مؤشرات البورصة الإسرائيلية بالانخفاض وتضخم الخسائر المالية جراء حجب الخدمة على مواقعه الحكومية والمصالح العامة.[3]

مما يعني أن إسرائيل بالرغم من توفقها الإلكتروني والتقني واعتمادها الكبير على التكنولوجيا الرقمية، إلا أن ذلك لم يمنع من تعرضها لهذه الهجمات والتي أضرت باقتصادها رغم أنها تحاول إخفاء تداعيات الهجمات السيبرانية على اقتصادها وعدم الإدلاء بحجم هذه الخسائر والتقليل من الإنجازات التي حققتها مجموعات قراصنة الانترنت.

الفرع الثاني : الانعكاسات الأمنية والسياسية

يعتبر الأمن بالنسبة لإسرائيل محور وجودها وبذلك فهي ترى بأن الحروب الإلكترونية الموجهة ضدها بمثابة حرب عليها وأن المساس بسيادة الفضاء السيبراني هوجزء من المساس بأمنها.

وتشكل هذه الحرب تحديا أمنيا جديدا لإسرائيل، فنجاح مثل هذه الهجمات يعني الطعن بنظريتها الأمنية وبالتالي التشكيك بالقادة السياسيين والأمنيين الإسرائيليين الذين أعلنوا أن إسرائيل تمتلك قدرة دفاعية في كافة المجالات وأنه من الصعوبة المساس بها.

---

[1]– المكان نفسه.

[2]– **المرجع نفسه**، ص 236.

[3]– د م، "**إسرائيل تتعرض لهجوم إلكتروني واسع ومئات المواقع بدأت تتساقط**"، تم تصفح الموقع يوم : 21 مارس 2018. الرابط: https://video.alwatanvoice.com

ويقول "عاموس يادلين" وهوضابط استخباراتي ورئيس جهاز الاستخبارات العسكرية الإسرائيلية "أمان" بين سنتي 2006 و2010م أن إسرائيل تواجه خطرا أمنيا ومعلوماتيا يكمن في احتمالية اختراق مواقع وحواسيب الدولة الحساسة، لكن في المقابل يؤكد أن هيئة السايبر[1] في الجيش الإسرائيلي تمتلك القدرات اللازمة لردع أي هجوم سيبراني إضافة إلى قدرة الهيئة على تنفيذ هجمات سيبرانية على أهداف معادية لها.

سياسيا وضعت هذه الهجمات السيبرانية القادة الإسرائيليين في موضع صعب أدى إلى التشكيك في القدرات الإسرائيلية، وأن هؤلاء القادة غير قادرين على حماية المواطن الإسرائيلي وبالتالي التقصير في توظيف التقنية الحديثة في منظومة الدفاع الإسرائيلي.[2]

أدى ذلك إلى تبادل الاتهامات بين الساسة والقادة الإسرائيليين وقد وجهت في ذلك العديد من التساؤلات والإنتقادات لوزير الدفاع الإسرائيلي "إيهود باراك" (Ehud Bark) عن مدى قدرة المنظومة الإسرائيلية الإلكترونية في حماية إسرائيل، الأمر الذي دفعه لتوجيه ميزانيات معتبرة مع تجنيد أشخاص قادرين على قيادة وإدارة الحرب الإلكترونية.

ظهر الارتباك السياسي الإسرائيلي جراء هذه الهجمات السيبرانية على وسائل الإعلام الإسرائيلية التي انشغلت بالحديث عن الحروب الإلكترونية، وعبر هذه الوسائل حاولت الحكومة الإسرائيلية التخفيف من حدة التأثيرات والعمل على نفي الحقائق، إلا أن التأثيرات التي تخلفها هذه الهجمات تتميز بسرعة الإنتشار في الفضاء الإلكتروني.[3]

الفرع الثالث : المؤثرات النفسية للهجمات الإلكترونية على إسرائيل

تتصاعد المخاوف داخل المجتمع الإسرائيلي من خطر الهجمات السيبرانية على إسرائيل، وهذا يؤكد نجاح هذه الاختراقات التي مست كبريات المواقع الإلكترونية الحساسة فيها خاصة الاقتصادية والأمنية منها، لأن بعض الحسابات البنكية المهددة بالاختراق تقدر بمبالغ كبيرة، الأمر الذي دفع البنوك والشركات إلى توقيف هذه البطاقات مما أدى إلى إشاعة حالة من الذعر الاجتماعي والنفسي بين جموع الإسرائيليين وهذا ما يوحي إلى نجاح هذه الهجمات في إدارة المعركة النفسية الموجهة ضد إسرائيل، فالحرب النفسية هي إحدى أهم

[1]– وليد غسان سعيد جعلود، **مرجع سابق**، ص 240.

[2]– المكان نفسه.

[3]– **المرجع نفسه**، ص 242.

أهداف الحروب الإلكترونية والتي لها تأثيراتها الخاصة بنقل الصراع من الواقع إلى العالم الإفتراضي[1]، وترجمته بشكل فعلي لتحقيق الأهداف وتحويلها إلى إنجازات اقتصادية وأمنية وعسكرية تستخدم ضد إسرائيل وقادرة على حسم المعارك لصالحها.

مست هذه الهجمات الجانب المادي للمجتمع الإسرائيلي لتأثيراتها وانعكاساتها الاجتماعية والاقتصادية على المواطن الإسرائيلي خاصة وأنه مجتمع ذو ميول رأسمالية، مما أدى إلى خلق حالة من الخوف بين الإسرائيليين.

من جهة أخرى فإن قلق صناع القرار في إسرائيل جراء هذه الهجمات السيبرانية لا يكمن فقط في الآثار المادية والاقتصادية بل الخوف من أن تكون مثل هذه الهجمات مرتبطة بدول تعتبرها إسرائيل معادية لها وذات مصلحة حقيقية في إلحاق الضرر بأمنها القومي.[2]

ومما لاشك فيه أن لإسرائيل تجارب في مجال الحروب النفسية الإلكترونية، فهي دائمة البحث عن مصطلحات للدعاية وبث المعلومات والأفكار عبر وسائلها الإلكترونية والمعلوماتية والإعلامية لتدعيم مواقفها، فمثلا تستخدم إسرائيل ما يعرف بالدعاية السوداء (Black Propaganda)، والتي تهدف من خلالها إلى نشر أكبر قدر ممكن من المعلومات المضللة وإرباك أعدائها، ورغم ذلك تمكنت العديد من الجهات من إبطال مفعول الهجمات النفسية التي تشنها إسرائيل وأن باستطاعتها إلحاق الضرر بها من كافة النواحي، وفرض أجندتها النفسية والإلكترونية عليها وإرباك الصف المدني والعسكري بحرب نفسية أستخدمت فيها الأسلحة الرقمية والتكنولوجية والمعلوماتية.[3]

وبإسقاط طرح مدرسة كوبنهاغن التي ترى بأنه عندما تصبح المشكلة الأمنية مهددة لوجود الدولة يستدعي ذلك اتخاذ تدابير استثنائية لضمان بقاء الدولة، وتوسيع وتعميق مضامين الأمن ليشمل قطاعات أخرى تتمثل في القطاع السياسي والاقتصادي والمجتمعي والقطاع البيئي.

ونخلص إلى أن هذه التهديدات لا تمس القطاع العسكري فقط بل تمتد تأثيراتها إلى قطاعات أخرى، وهي بطبيعة الحال مترابطة فيما بينها ومتكاملة وأن الإخلال بقطاع معين يؤدي إلى الإخلال بالقطاعات الأخرى.

---

[1]- **المرجع نفسه**، ص 237.

[2]- **المرجع نفسه**، ص 238.

[3]- **المرجع نفسه**، ص 239.

لقد عرفت الإستراتيجية تغيرا على عدة مستويات، فلم تعد مرتبطة بالنشاط العسكري للدولة وفن الحرب بل تعدت ذلك لتشمل الجانب السياسي والاقتصادي والاجتماعي والأمني وحتى الثقافي وذلك بفضل التطورات التي مر بها النظام الدولي ويأخذ هذا التحول مظهر أساسي وهوالتغير في طبيعة التهديدات.

وتتضمن الإستراتيجية الإسرائيلية مجموعة متعددة من المنطلقات التي تميزها عن غيرها من السياسات الأمنية الأخرى، فهي تعبر عن تصور شامل للقواعد الضرورية الواجب الرجوع إليها واعتمادها في تحديد المسار الرئيسي الواجب إتباعه.

مما لاشك فيه أن الهجمات السيبرانية التي يتعرض لها الفضاء الإلكتروني الإسرائيلي دفعت بها إلى اتخاذ العديد من الإجراءات الفنية والتقنية والدفاعية والهجومية ذات الطابع الإلكتروني لحماية نظامها المعلوماتي ضد خطر هذه التهديدات والتخفيف من حدة تأثيراتها على مجالاتها الحيوية.

وعليه سيتم التطرق إلى الإستراتيجية الإسرائيلية في مواجهة هذه التهديدات والتي يمكن التفصيل فيها على النحوالتالي :

المبحث الثاني : أبعاد الاستعدادات الإسرائيلية في مجال الفضاء الإلكتروني

إن التهديد السيبراني هونتيجة الدور الأساسي الذي تلعبه أنظمة الكومبيوتر في البنى التحتية للدول، فقد أسهم تطور وانتشار الشبكات الإلكترونية المرافق للتطور الإقتصادي والتكنولوجي المتسارع في فضاء جديد واسع للتعامل عن بُعد وهوما يسمى بالفضاء الإلكتروني، في الإهتمام بالجانب الأمني للحقل السيبراني حيث طرح كثيرون السؤال التالي : "من هوالمسؤول عن أمن هذا القطاع ؟".[1]

تمتلك إسرائيل إمكانيات تكنولوجية هامة وتعتمد مؤسساتها وكافة القطاعات الرئيسية فيها على تكنولوجيا المعلومات والاتصالات حيث يمثل أي اعتداء عليها تهديدا على أمنها القومي، وتقوم الإستراتيجية الإلكترونية الدفاعية لإسرائيل على أساس التطوير في إمكانياتها الإلكترونية إلى الحد الذي يجعل من هذه الإمكانيات قوى رادعة لأعدائها.[2]

إن الدفاع عن الشبكات المحوسبة وحماية المعلومات ليسا موضوعين مستجدين في إسرائيل، فقد كانت من بين الدول الأولى التي أدركت أهمية حماية شبكاتها المحوسبة الحيوية فمنذ سنة 1996م أخذت الحكومة الإسرائيلية قرارات تتعلق بوسائل الدفاع المطلوبة لصد الهجمات السيبرانية، وفي سنة 1997م أطلقت موقعا يسمى "تهيلا" الإلكتروني (البنية التحتية الحكومية لعصر الانترنت) (www.tehila.gov.il) الذي من مهامه حماية وربط وزارات الحكومة بالانترنت وتوفير خدمات تصفح مضمونة للمواقع الإلكترونية التابعة للوزارات، ليتم في سنة 1998م إقرار "قانون الإجراءات التنظيمية لضمان أمن الهيئات العامة" الذي يحدد ماهية المنظومات والشبكات المحوسبة الحيوية وينظم إجراءات الدفاع عنها.[3]

لقد شرعت إسرائيل في إحداث تغييرات لبناء قوتها في المجال السيبراني من خلال الربط بين معالجة التهديدات السيبرانية وحماية أمنها القومي وتركزت هذه الإجراءات في الأبعاد التالية :

---

[1]– جيل برعام، "**تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في إسرائيل**"، (مؤسسة الدراسات الفلسطينية ، د س ن)، ص 06.

[2]– نوران شفيق، " **تأثير التهديدات الالكترونية على العلاقات الدولية دراسة في أبعاد الأمن الالكتروني**"، (القاهرة: المكتب العربي للمعارف، 2016)، ص 88.

[3]– **المرجع نفسه**، ص 89.

المطلب الأول : البعد العسكري والاستخباراتي

الفرع الأول : البعد العسكري

تستخدم العديد من الدول القدرات التي يتيحها الفضاء الإلكتروني لاعتبارات الأمن والقوة العسكرية بشكل جعلها تضعه ضمن حساباتها الإستراتيجية وأمنها القومي، وظهر بعد جديد في الصراعات الدولية هو"صراع الفضاء الإلكتروني" حيث يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر وأن يتسبب في شل البنية المعلوماتية والإلكترونية الخاصة به وهوما يسبب خسائر عسكرية واقتصادية فادحة، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية مع بعضها البعض أوتضليل معلوماتها أوسرقة معلومات سرية عنها أومن خلال التلاعب بالبيانات الاقتصادية والمالية وتزييفها أومسحها من أجهزة الحواسيب.[1]

عندما بدأت إسرائيل الاهتمام بنظم أمن المعلومات كان تركيزها الأول على البنية التحتية العسكرية وأعطت الأولوية في ذلك للجيش وسخرت لذلك جميع موارد الدولة.

- ✓ في سنة 2003م أسست هيئة الأركان العامة في الجيش الإسرائيلي شعبة تحمل اسم (شعبة المعالجة عن بعد) (Teleprocessing) بهدف توفير استجابة فورية لحالات التعرض لهجمات سيبرانية معادية من أجل الربط بين نظم الحواسيب العسكرية بالجيش الإسرائيلي وعمل شبكات معلومات مشتركة لجميع هيئات الطوارئ فيها، وفي سنة 2013م تم الإعلان عن برنامج مستقبلي يحمل اسم "كود المستقبل" عبارة عن مسيرة تغيير وتنسيق تهدف إلى تحسين مدى جاهزية الجيش الإسرائيلي للعمل في مجال الفضاء السيبراني وخاصة في ظل المتغيرات في المنطقة.[2]
- ✓ اعتبر رئيس هيئة الأركان العامة السابق "جابي أشكنازي" في سنة 2009م الفضاء السيبراني كمجال حرب إستراتيجي تقني، لذلك تم تأسيس "إدارة الفضاء السيبراني" بالجيش كهيئة أركان للتنسيق وتوجيه العمليات السيبرانية وتأسست هذه الإدارة ضمن الوحدة 8200 التابعة لشعبة الاستخبارات العسكرية (IDF

---

[1]– إيهاب خليفة، "**التطبيقات الأمنية لـــقوة الفضاء الإلكتروني**"، تم تصفح الموقع يوم : 22 مارس 2018. الرابط: https://futureuae.com/ar/Mainpage/Item/851/cyber-power

[2]– ربيع محمد يحي، "**إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط: دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الانترنت (2002–2013)**"، رؤى إستراتيجية، (يونيو 2013)، ص 70.

Cyber Warfare Unit 8200)، ويشارك فيها مندوبين من شعبة الاستخبارات العسكرية وشعبة المعالجة عن بعد.[1]

- ✓ يعتبر جيش الدفاع الإسرائيلي أحد قادة قوات الانترنت في العالم ، بحيث يتم تجنيد المنخرطين فيه على كيفية الاختراق والدفاع وتطوير الأدوات والنظم واكتساب الخبرة التشغيلية[2]، وفي أعقاب الخدمة العسكرية الإلزامية يستمر الجنود في متابعة الدراسة سواء في الجامعات أوالمؤسسات التكنولوجية الإسرائيلية وفي كثير من الأحيان يتم تجنيدهم من إحدى الشركات التكنولوجية أوالشركات المتعددة الجنسيات في إسرائيل مثل (غوغل) و(سامسونغ) جميعها مراكز للبحث والتطوير.[3]

هيئة السايبر في الجيش الإسرائيلي

أنشأ الجيش الإسرائيلي "هيئة السايبر" في الوحدة 8200 التابعة لجهاز المخابرات العسكرية "أمان" بغرض توجيه وتنسيق الجيش الإسرائيلي في الفضاء السيبراني، وتوفير دفاع جيد لشركات الانترنت العاملة في إسرائيل ضد الاختراقات وكذلك القيام بهجمات في الفضاء الإلكتروني على أهداف خارجية.[4]

ودفاعا عن أنظمة حواسيب الجيش الإسرائيلي طور سلاح الإتصالات الإلكترونية (هيتكشوف) برنامجا اشتمل على الحلقات التدريبية لتعزيز المهارات في مجال الدفاع السايبيري.[5]

- ✓ وفي سنة 2013م 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 فعال في الفضاء السيبراني وإعطاءه صورة آنية وواضحة للتطورات المحيطة من خلال التعاون مع مشروع البنية الحكومية لعصر الانترنت (Tehila) ومشروع (E-Government) للخدمات الحكومية الإلكترونية والسلطة الوطنية لأمن المعلومات التابعة لجهاز الأمن العام "الشاباك" ، ويعتبر الجيش "غرفة الحرب

---

[1]– المكان نفسه.

[2] - "**paysage de Cyber Security et Investissements, Israël 2016**", Rapport sur l'industrie de la cyber sécurité, (Département de la recherche cyber D13, Janvier 2017), p 04.

[3] – "**paysage de Cyber Security et Investissements, Israël 2016**", **Op-cit**, p 05.

[4]– محمود محارب، "**إسرائيل والحرب الإلكترونية**"، معهد الدوحة: المركز العربي للأبحاث ودراسة السياسات، (أوت 2011)، ص 05.

[5]– جيل برعام، **مرجع سابق**، ص 14.

الرقمية" عصب الدولة في عمليات الحماية بحيث سيكون بمقدورها القيام بعمليات اعتراض وتوجيه وتشغيل في الفضاء السيبراني مع جميع وحدات الجيش.[1]

- ✓ في سنة 2009م أطلقت إسرائيل برنامجا جديدا بمنزلة "قبة حديدية رقمية" تابع لمكتب إسرائيل للحرب الافتراضية في عهد "بنيامين نتانياهو"، هذا المشروع يقوم على تدعيم قدرات إسرائيل التكنولوجية من أجل التعامل مع الهجمات الإلكترونية وتضم الطلاب الذين تتراوح أعمارهم ما بين 16 و18 سنة، حيث توكل إليهم مهمة اعتراض الهجمات الإلكترونية التي تشن على إسرائيل.[2]

اهتمت قوات الدفاع الإسرائيلية (IDF) بقضايا الأمن السيبراني والتهديدات السيبرانية لعقود من الزمن فقد وضعت في سنة 2015م وتزامنا مع نشر رئيس الأركان الإسرائيلي "جادي إيزنكوت" إستراتيجية جيش الدفاع الإسرائيلي ملخص عن النهج الشامل للجيش هذه وثيقة أُعتبر فيها الفضاء السيبراني مجال عسكري، وقد حدد بذلك أولويات المتابعة في بناء القدرات الدفاعية والجرائم السيبرانية على المستويات الإستراتيجية والعملية والتكتيكية وكذلك الوعي بالفضاء الإلكتروني.

أما على المستوى التنظيمي فقد تمثل في الشروع في عملية إنشاء بنية لقيادة الانترنت داخل جيش الدفاع، كما تشير وثيقة إستراتيجية الجيش إلى أن الدفاع السيبراني في حالات الحروب والطوارئ أمر ضروري لضمان استمرار عمل المؤسسات الوطنية في أوقات التوتر.[3]

الجيش الإسرائيلي يتعامل مع الأمن السيبراني كجزء لا يتجزأ من إستراتجيته العسكرية، بحيث تم تأسيس دورة تدريبية في سنة 2012م بالإضافة إلى العديد من البرامج التدريبية العسكرية في مجال الإنترنت والأمان الإلكتروني، وتقع المخابرات السيبرانية في إسرائيل ضمن اختصاص القطاعات العسكرية والدفاعية.[4]

- ✓ **التأهب للطوارئ وإدارة الأزمات**

إن الاستعداد لحالات الطوارئ في إسرائيل وإدارة الأزمات المدنية بما في ذلك الجوانب المتعلقة بالتأهب على استخدام الانترنت تتم تحت سيطرة وزارة الأمن العام ووزارة الدفاع وقيادة الجبهة الداخلية، كما أجرت

---

[1]– ربيع محمد يحي ، **مرجع سابق**، ص 70.

[2]– محمود محارب، **مرجع سابق**، ص 29.

[3] –Deborah Housen Couriel, "**National Cyber Organisation :Israël**", (Nato Cooperative Cyber defence : Centre Of Exellence, Tallinn, Estonia, 2017), p 09.

[4] –Deborah Housen Couriel, **Op-cit**, p 09.

الهيئة الوطنية لإدارة الطوارئ تدريبات بالتعاون مع جيش الدفاع الإسرائيلي والتي تشمل عناصر تتعامل مع الهجمات السيبرانية التي تستهدف البنى التحتية مثل شبكات الكهرباء الوطنية.[1]

الفرع الثاني : البعد الاستخباراتي

هناك ثلاثة أنواع من الأنشطة الاستخباراتية في مجال الفضاء السيبراني وتتمثل في :

✓ جمع المعلومات حول قدرات العدو سواء في أوقات الحرب أو السلم بهدف وضع تقديرات وبلورة إستراتيجيات ومن ثم اتخاذ القرارات المناسبة وبناء القوة العسكرية القتالية.

✓ التجسس الصناعي بهدف سرقة معلومات حول التكنولوجيا والأعمال.

✓ تستهدف سرقة البرامج وقواعد البيانات أو الملكيات الفكرية.[2]

ويشار إلى أن إسرائيل تمتلك في منطقة النقب الغربي واحدة من قواعد التنصت الكبرى التابعة للوحدة 8200 بالاستخبارات العسكرية الإسرائيلية، وتقوم هذه القاعدة بالتنصت على المحادثات الهاتفية والتسلل إلى عناوين البريد الإلكتروني للحكومات والمنظمات الدولية والشركات الأجنبية وكذلك الأفراد.[3]

✓ يتولى أيضا جهاز (C41) مسؤولية الاتصال وتنظيم القدرات الإسرائيلية وتنسيقها في الدفاع عن المجال الافتراضي، بالإضافة إلى تعيين ضابط ذورتبة عالية من جهاز الاستخبارات الإسرائيلي في مركز الشيفرة والأمن المعلوماتي المعروف باسم المختصر بالعبرية (ماتزوب)، ولديه المسؤولية لجمع المعلومات حول قدرات خصوم إسرائيل في مجال القرصنة الإلكترونية.[4]

ويقوم (ماتزوب) بشيفرة الاتصالات المنقولة من شبكات (الشين-بيت) و"الموساد" والجيش الإسرائيلي ولدى الجهاز نفسه فرق عمل تقوم بفحص الشيفرة وجدران الدفاع الافتراضي الإسرائيلي.

✓ في سنة 2002م أقيمت السلطة الرسمية لحماية المعلومات في جهاز الأمن العام "الشاباك"، وهي مسؤولة عن التوجيه المهني للهيئات ذات الصلة بنطاق مسؤوليتها في مجال حماية شبكات الحاسوب الحيوية من

---

[1] –**Op-cit**, p 14.

[2] –Deborah Housen Couriel, **Op-cit**, p 72.

[3] – جوني منصور، وفادي نحاس، "**المؤسسة العسكرية في إسرائيل: تاريخ، واقع، إستراتيجيات وتحولات**"، (فلسطين: المركز الفلسطيني للدراسات الإسرائيلية، 2009) ص 245.

[4] – محمود محارب، **مرجع سابق**، ص 28.

التهديدات الإرهابية والتخريب في مجال حماية المعلومات السرية وتهديدات التجسس والكشف[1]، كما تتولى السلطة الرسمية لحماية المعلومات مهمة مراقبة بعض المؤسسات بغرض حماية المعلومات فيها.

ترى إسرائيل أن مجال الفضاء السيبراني يكشفها أمام مخاطر أساسية وبارزة ومن بينها مخاطر تعرض البنية الحيوية والمؤسسات الأمنية لاعتداءات تتعلق بأدائها لوظائفها بالإضافة إلى إمكانية الإضرار بإقتصادها، وعلى خلاف الكثير من الدول ترى أنها تقف أمام أعداء لديهم دوافع واضحة ومعلنة للإعتداء عليها في جميع المجالات الممكنة وأن هؤلاء الأعداء يسعون إلى تحقيق قدرات سيبرانية هجومية بالإضافة إلى احتمال دخول المنظمات الإرهابية إلى مجال العمليات الهجومية التي تستهدف إسرائيل.

لذلك تعمل على بلورة إستراتيجية قومية لحماية فضائها السيبراني من شأنها أن تؤدي إلى تحقيق الأهداف الإستراتيجية بالموازنة مع إمكانياتها ومواردها، وتستخدم هذه الإستراتيجية كسبيل للعمل المشترك الذي تقوم به الكيانات المختلفة أولنشاط كل كيان يتعرض للاعتداء وتحديد مسؤولياته.[2]

أصبح التجسس الإلكتروني أحد أخطر أنواع التجسس فقد طغى بإمكانياته المتطورة ودقة نتائجه على أساليب التجسس المعهودة في السابق.

هنا أدركت إسرائيل أهمية هذا النوع من التجسس وقد خصصت إمكانياتها في هذا المجال على بعض الدول العربية والإسلامية بالإضافة إلى حلفائها كالأمريكيين والغرب، وبذلك امتد ذراع التجسس الإلكتروني الإسرائيلي إلى أقصى حد ممكن يخدم مصالحها.

واعتمدت بشكل كبير على الأقمار الصناعية للتجسس على الدول العربية، فقد ارتفعت نسبة الاعتماد تلك من 150% إلى 200% بهدف مراقبة ما يجري في المنطقة للحصول على المعلومات، فهي تسيطر على فضاء جميع الدول العربية بواسطة 6 أقمار صناعية مهمتها تصوير كل ما يحدث في الدول العربية وغير العربية، وتعرف الوحدة المسؤولة عن إدارة الأقمار الصناعية لأغراض التجسس في الجيش الإسرائيلي بمجموعة أقمار (عاموس).[3]

1- **المرجع نفسه**، ص 29.

2- ربيع محمد يحي، **مرجع سابق**، ص 72.

3- إلهام محمد علي، "**التجسس الإلكتروني: سلاح إسرائيل الذهبي لمراقبة العرب**"، تم تصفح الموقع يوم : 24 مارس 2018. الرابط:

https://www.noonpost.org/content/13821

المطلب الثاني: البعد الإعلامي والأكاديمي

الفرع الأول: البعد الإعلامي

تؤدي وسائل الإعلام الإسرائيلية دورا مهما للغاية في رفع مستوى وعي المواطنين بمخاطر التهديدات السيبرانية وتبحث عن سبل مبتكرة لإشراك المجتمع في الإستراتيجية الإسرائيلية الجديدة في هذا المجال والعمل على رفع مستوى وعي الرأي العام الإسرائيلي بمدى أهمية حماية المعلومات بصورة تفوق أي ميزانية كان من الممكن رصدها لتحقيق هذا الغرض.[1]

استخدمت الحكومة الإسرائيلية سنة 2002م مواقع الانترنت الحكومية كوسائل إعلام عبر الشبكة الإلكترونية لشرح السياسة الإسرائيلية، وتم ربطها بمواقع وزارة الخارجية ورئاسة الحكومة ومكتب رئيس الحكومة ووزارة الدفاع لتحديد مضامين المعلومات التي يتم نشرها، وأهم هذه المواقع ديوان رئيس الحكومة ووزارة الخارجية كذلك الجيش الإسرائيلي بالإضافة إلى المواقع الإسرائيلية بالعربية وأهمها صحيفة (يديعوت أحرنوت) ووزارة الخارجية.[2]

فقد أظهرت قضية الهاكر السعودي (OX.Omer) على سبيل المثال الدور الذي تؤديه وسائل الإعلام في هذا الصدد، ففي سنة 2012م أصدرت وسائل الإعلام والصحف الإسرائيلية عشرات التقارير حول قيام هذا الهاكر بسرقة بيانات بطاقات الائتمان الإسرائيلية، وفي نفس الوقت شنت حملة مضادة مستعينة بمجموعة من قراصنة الإنترنت أوالهاكرز الإسرائيليين من خلال القيام بعمليات سرقة مضادة تستهدف بيانات مئات الآلاف من السعوديين وبعض الدول العربية.

ووجه بذلك الإعلام الإسرائيلي الرأي العام نحومخاطر هذا المجال الجديد بالصورة التي تدل على اختلاف القضية أواستغلالها إعلاميا على الوجه الأمثل.[3]

تعتبر الرقابة العسكرية حلقة مهمة في سلسلة تعامل الإعلام الإسرائيلي مع التهديدات السيبرانية، فرغم التطور الكبير الذي شهدته وسائل الإعلام الإسرائيلية إلا أن الجانب الأمني مازال متحكما في انطلاقتها.

---

[1]– ربيع محمد يحي ، **مرجع سابق**، ص 71.

[2]– د م، "**الإعلام الإسرائيلي: بنية، أدوات، أساليب عمل**"، مركز المعلومات الوطني الفلسطيني، تم تصفح الموقع يوم : 24 مارس 2018. الرابط:

http://info.wafa.ps/atemplate.aspx?id=8788

[3]– ربيع محمد يحي ، **مرجع سابق**، ص 72.

تركز وسائل الإعلام الإسرائيلية على زيادة الوعي العام بقضايا الأمن الإلكتروني على أنها أحد أهم طرق ووسائل الدفاع الإلكتروني، وتعمل بعض برامج التوعية على تدريب المواطنين على حماية أنفسهم وتدريب الشركات الصغيرة على حماية قواعد المعلومات والأنظمة الإلكترونية الخاصة بها من الجرائم السيبرانية.

فمهاجمة أجهزة المواطنين أوالشركات قد تتطور فيما بعد إلى هجمات تهدد الأمن القومي إذا ما كان الهدف من ورائها سرقة المعلومات أوالقيام بهجمات الحرمان من الخدمة.[1]

وهوما يتوافق مع طروحات مدرسة كوبنهاغن التي ترى بأن الأمن يفهم على أنه نتيجة لأعمال خطاب أي عملية الاستخدام المتكرر لإظهار حدث ما أوقضية على أنها تهديد وجودي، من خلال لغة خطابية موجهة للجمهور العام وتقدم من خلالها هذه القضية على أنها تمس المادي والمعنوي وتتطلب إجراءات استثنائية مستعجلة لتشريع الأفعال خارج العملية السياسية المعتادة.

وبالتالي قد تكون فواعل الأمننة وسائل الإعلام يتم من خلالها تفعيل الخطاب عندما تصبح المشكلة الأمنية مهددة لوجود الدولة وأمنها على كافة القطاعات والمجالات وبنيتها التحتية، بالاعتماد على مجموعة من القواعد واللوائح وتصبح بذلك القضية مؤمنة عندما يتقبلها الجمهور.

الفرع الثاني : البعد الأكاديمي

أدت الثورة التكنولوجية والمعرفية والتغيرات وأيضا التحديات الاجتماعية والسياسية وتعدد الاهتمامات إلى التأكيد على دور الجامعة في تحديد مخرجات تتلاؤم وطبيعة هذا العصر، وتوسيع آفاق المجتمع المعرفية والثقافية وإجراء البحوث العلمية مع المساهمة في عملية التنشئة والنهوض بالمجتمعات إلى أفضل المستويات التقنية والتكنولوجية والاقتصادية وغيرها.

لقد نجحت المؤسسات الأكاديمية في إسرائيل في أن تضع نفسها كإحدى المؤسسات الهامة على المستوى الداخلي وعلى المستوى العالمي سواء في إنتاجها المعرفي والبحثي أوفي دورها المميز في بناء الدولة، ويظهر هذا التمازج بداية من الإنتاج المعرفي في كل حقوله الطبيعية والتكنولوجية والتقنية وسياسات إقامة فروع للجامعات في مناطق مختلفة من إسرائيل.[2]

---

[1]– نوران شفيق، **مرجع سابق**، ص 85.

[2]– أحمد أوأرتيمة، "**المؤسسات الأكاديمية: حول جامعات إسرائيل والمشروع الصهيوني**"، تم تصفح الموقع يوم : 24 مارس 2018. الرابط:

https://arabi21.com/story/903760

ومن خلال ذلك يمكن القول بأنه كان للمؤسسات الأكاديمية في إسرائيل دور في تدعيم إستراتيجيتها الدفاعية في مجال الفضاء الإلكتروني، ويتجسد ذلك من خلال إنشاء "المجلس القومي للأبحاث والتنمية" وهومؤسسة حكومية تخضع لمسؤولية وزارة التعليم والتكنولوجيا بهدف تقديم الاستشارات إلى الحكومة الإسرائيلية في موضوعات التخطيط والتنسيق والموازنة الخاصة بالأبحاث والتنمية وكان ذلك سنة 2004م، حيث تم تأسيس المجلس بناء على قانون المجالس القومية للأبحاث الذي صدر سنة 2002م بمبادرة من وزير العلوم آنذاك "ميخائيل إيتان" وقد تم تعيين اللواء احتياط البروفيسور "يتسحاق بن يسرائيل"* رئيسا للمجلس ومنح صلاحيات استثنائية.[1]

وفي سنة 2012م أعلنت جامعة (بن غورين) أنه سيتم اعتبارا من سنة 2013م إدراج مجال الفضاء السيبراني ضمن مقررات المرحلة النهائية والماجستير بقسم هندسة نظم المعلومات في إطار مبادرة بالتعاون مع وزارة الدفاع والإدارة الوطنية للفضاء السيبراني، وتتركز الأبحاث التي ستدخل ضمن المقررات على أساليب كشف الاعتداءات السيبرانية والحماية ضد الفيروسات والبرمجيات الخبيثة وحماية الشبكات ونظم التشغيل[2]، وتوفير برامج التدريب التعليمية والمهنية لزيادة الوعي وتعزيز دورات الأمن السيبراني في التعليم العالي لتكوين المهنيين سواء في القطاع العام أو الخاص لزيادة الوعي العام بالتهديدات السيبرانية.

وتعني هذه الخطوة أن المؤسسة الأكاديمية الإسرائيلية تؤهل للمرة الأولى هاكرز أكاديميين (Acedemie Hakers) يتم تدريسهم كيفية مهاجمة النظم التكنولوجية للدول المعادية والدفاع عن الدولة ضد الهجمات السيبرانية.

في سنة 2013م قام رئيس الحكومة الإسرائيلية بإدراج برنامج تدريبي وطني في مجال الحرب السيبرانية في كلية (عسقلان الأكاديمية) (Askelon Academie Collegue) واصفا إياه بالقبة الحديدية الرقمية*

[1]– ربيع محمد يحي، **مرجع سابق**، ص 71.

* البروفيسور يتسحاق بن يسرائيل هو من أبرز الشخصيات على صعيد تنظيم مجال الفضاء السيبراني في إسرائيل، تولى رئاسة فرع بحوث العمليات بسلاح الجو وتولى مناصب في شعبة العمليات، وكذا استخبارات سلاح الجو وشعبة التطوير كما تولى رئاسة وكالة الفضاء الإسرائيلية منذ سنة 2005م، وهو رئيس للمجلس القومي للأبحاث والتطوير منذ سنة 2010م، وفي شهر ماي سنة 2011م عين رئيسا لإدارة الفضاء الإلكتروني، مع العلم أنه كان شريكا في التخطيط لعملية (أوبرا) لتدمير المفاعل النووي العراقي. (أنظر: ربيع محمد يحي، **مرجع سابق**، ص 81.).

[2]– **المرجع نفسه**، ص 73.

ومشيرا إلى أن البرنامج يأتي على خلفية تعرض النظم الحيوية في إسرائيل لهجمات سيبرانية تأتي من إيران وجهات أخرى.[1]

✓ **مركز أبحاث الفضاء الحاسوبي (جامعة بن غورين)**

أطلقت جامعة (بن غورين) في بئر سبع مع هيئة السايبر الوطني مبادرة لإنشاء مركز أمن الفضاء السيبراني الحرم الجامعي، يشمل هذا المركز مختبر محاكاة الهجوم السيبراني ومختبر تحليل البرامج الضارة وأيضا مختبر أمن السايبر المخصص للأبحاث السرية في مجال الأمن السيبراني.

✓ **مركز البحث "بلافنتيك "**

أنشأ هذا المركز في جامعة تل أبيب كمبادرة مشتركة مع هيئة السايبر، يتكون هذا المركز من باحثين في جامعة تل أبيب يعمل فيه أكثر من 50 مختص في ميدان التدريس والباحثين في السايبر يحوي على ما يزيد عن 200 قسم من الإدارات المختلفة بما في ذلك علوم الحياة، علوم الحاسوب الآلي، القانون، الهندسة والعلوم الاجتماعية والإدارة والعلوم الإنسانية.[2]

✓ **معهد التكنولوجيا الصناعية "فراهوفر" الألمانية بالاشتراك مع مراكز الأبحاث الإسرائيلية التخنيون**

في جوان 2015م أعلن معهد التكنولوجيا الصناعية "فراهوفر" الألماني إنشاء مركز للبحوث السيبرانية بالتعاون مع معهد التخنيون الإسرائيلي، والذي يركز على البحوث الحاسوبية أيضا تطوير التطبيقات العملية مثل البرمجيات ونظم وخدمات القطاع الخاص.[3]

تمتلك إسرائيل أيضا برامج تدريب تشبه معسكرات الدفاع ولكن على الانترنت وهي جزء من مسعى إسرائيل لتصبح الدولة الرائدة عالميا في مجال الأمن السيبراني عن طريق تدريب وتعليم صغار السن من الأطفال والشباب على مهارات الاختراق وإدراجها ضمن مناهج التعليم في المدارس والمعاهد.

---

[1]– المكان نفسه.

[2] - Daniel Shkedi, **" The Cybersecurity Sector in Israel ",** (Embassy of India, Tel Aviv, commercial wing, 2015), p 05.

[*] نظام القبة الحديدية الأمني هو وسيلة دفاعية ضد صواريخ قريبة المدى وقذائف الهاون يقوم بتفجيرها في الجو قبل سقوطها.(أنظر: م د، "**ماهي القبة الحديدية**"، تم تصفح الموقع يوم : 30 مارس 2018م. الرابط : archive.cnn.com).

[3] – Daniel Shkedi, **Op-cit**, p 08.

لذلك قامت بإنشاء مركز وطني لتعليم الانترنت بهدف زيادة المواهب في مجال الاختراق وإعداد الأطفال للعمل في وكالات الدفاع السيبرانية وصناعة التكنولوجيا الفائقة.[1]

المطلب الثالث : البعد الاقتصادي وتفعيل التعاون المحلي والدولي في مجال الأمن السيبراني

الفرع الأول : البعد الاقتصادي

تعتبر إسرائيل من الدول المتقدمة في العالم في مجال تطوير التقنيات المعلوماتية والتكنولوجية، وقد حاولت تدعيم إستراتيجياتها الدفاعية في مجال الأمن السيبراني عن طريق الاستثمار بالشركات لتعزيز الصناعات الدقيقة وتطوير منظومة حماية المعلومات، وجذب المستثمرين الأجانب لإنشاء المزيد من الشركات لصناعة وابتكار أنظمة المعلومات وتسويقا للعالم بما يساهم في تعزيز وتدعيم الاقتصاد الإسرائيلي.

فالقادة الإسرائيليون غالبا ما يعتبرون أنه بالإضافة إلى الثورة الزراعية والصناعية يمكن الحديث عن الثورة في مجال الانترنت، لذلك يرى البروفيسور "أفياتار ماتانيا" مدير مكتب السايبر الوطني الإسرائيلي بأن الثورة الحاسوبية هي الثالثة بعد الزراعية والصناعية، فإقتصادها يعتمد بشكل كبير على المعلومات ومن الواضح أن إسرائيل ترى هذه النقطة كقضية إستراتيجية ومسألة اقتصادية بحتة.[2]

إلى جانب احتياجات الدول والشركات للأمن السيبراني تسعى إسرائيل إلى أن تصبح رائدة عالميا في السايبر، ففي خطاب لرئيس الوزراء الإسرائيلي للأمم المتحدة في سنة 2016م أكد بأن أوجه التعاون الاقتصادي تسمح أيضا بتفعيل البعد الدبلوماسي وأن التعاون الاقتصادي يسمح بإجراء اتصالات حقيقية بين الدول عن طريق إنشاء مصالح مشتركة والمساهمة في أمن الفضاء الإلكتروني العالمي.

حيث اتخذت إسرائيل العديد من المبادرات لتعزيز قطاع الأمن السيبراني خاصة من خلال الاقتصاد الإسرائيلي، ففي سنة 2015م بلغ معدل النمو الاقتصادي نحو2.5% والتقديرات في سنة 2016م كانت حوالي 3% وفي سنة 2017م حوالي 3.3 %.[3]

وحسب تقرير أبحاث رأس المال الاستثماري في إسرائيل يتم جزئيا صناعة التكنولوجيات الجديدة المخصصة للأمن السيبراني والتي تمثل أكثر من ثلث إجمالي الناتج المحلي الإسرائيلي بنحو 20% في هذه الشركات

---

[1]– مؤنس حواس، "**ماذا يتعلم الأطفال في إسرائيل**"، تم تصفح الموقع يوم : 24 مارس 2018. الرابط:
https://www.youtube.com/watch?v=yxt9TDBbhbI

[2] –Olivier Danino, " **L'economie de la Cybersecurité en Israél** ", (Chaire de cybersécurité, Saint-cyr, Sogeti, Thales, 2017), p 01.

[3] - Olivier Danino, **Op-cit**, p 02.

كما يوجد فيها ما يقارب عن 430 من شركات الأمن السيبراني هذه الشركات النشطة في السوق الإسرائيلية المحلية أثبتت نفسها أيضا على الصعيد العالمي، فقد بلغت صادرات أمن الفضاء الحاسوبي الإسرائيلي في سنة 2013م حوالي 3 بليون شيكل أي 5% من السوق العالمية.

أيضا ركزت إستراتيجية القادة الإسرائيليين على استقطاب رأس المال العالمي في مجال الأمن السيبراني، وقد كان فعالا بين 2013م و2015م من خلال الاستحواذ على 11% إلى 20% من الاستثمارات العالمية، هذه الأرقام والنسب وضعت إسرائيل في المركز الثاني بعد الولايات المتحدة الأمريكية.[1]

الانفتاح على العالم الخارجي يهدف إلى تزويد صناعة الأمن السيبراني في الأسواق الإسرائيلية وأيضا في بناء شراكات والتي يمكن من خلالها تمكين الإسرائيليين من تحسين معرفتهم واكتساب خبرات جديدة.

أطلقت إسرائيل مشاريع جديدة في معظم القارات منها "ستيفانيني" في البرازيل ورافائيل، التعاون بين إسرائيل ونيجيريا لمحاربة الجريمة السيبرانية، في صناعة الطيران استثمرت 40 مليون دولار في آسيا، مع زيادة التعاون مع الولايات المتحدة الأمريكية في الصناعات والاستخبارات وأيضا عززت التعاون مع سنغافورة من خلال العلاقات التجارية والأمن السيبراني، وكذلك عقد اتفاقيات مع ألمانيا في التكنولوجيا والأمن السيبراني.[2]

الفرع الثاني : تفعيل التعاون المحلي والدولي في مجال الأمن السيبراني

1- على المستوى المحلي

تقوم هيئة السايبر الوطنية بتعزيز قدرات إسرائيل الدفاعية خاصة فيما يخص أنظمة البنية التحتية الحيوية من الهجمات الإلكترونية من الدول المعادية أوالمنظمات وحتى الأفراد وذلك بالتنسيق والتعاون بين الهيئات الحكومية ووزارة الدفاع والأوساط الأكاديمية والهيئات الصناعية والأعمال التجارية والهيئات الأخرى ذات الصلة بمجال الانترنت.[3]

أنشأت الحكومة الإسرائيلية وحدة (منمار) مديرية منظومة المعلومات الحكومية في سنة 2011م وهي هيئة بين وزارية وتنسيقية مهمتها تركيز على مجال الاتصالات الإلكترونية في إسرائيل ، ويفترض بهذه الهيئة التي تخضع لمسؤولية المدير العام في وزارة المالية أن تقوم بتوجيه وحدات الاتصال الإلكتروني في وزارات الحكومة.[4]

[1] - Olivier Danino, **Op-cit**, p 03.

[2] - **Op-cit**, p 05.

[3] –"**Cyber Wellness Profile Isreal**", (ITU Statistics, Decembre 2013), p 03.

[4]–محمود محارب، **مرجع سابق**، ص 28.

ولتحصين شبكات الإنترنت في إسرائيل ضد القرصنة وحماية القطاع الخاص في هذا المجال استحدثت الحكومة في سنة 2011م جهاز يسمى "الفريق القومي المخصص للمجال الافتراضي" يتكون من 80 شخص يقومون بمهمات دفاعية، والقيام بتخصيص موارد لتحسين البحث الجامعي المتعلق بالدفاع عن المجال الافتراضي ورفع عدد الطلاب المهتمين بهذا الموضوع.[1]

كما خصص معهد الأمن القومي الإسرائيلي برنامجا تدريبيا حول الأمن السيبراني أوأمن المعلومات، وقد أصدر المعهد في سنة 2012م تقريرا مفصلا عن الحرب السيبرانية، أدرجت فيه توصيات الإدارة الإسرائيلية بالعمل على تطوير القدرات الهجومية والدفاعية وإجراء تدريبات وطنية ودولية كذلك رفع حالة التأهب القصوى مع إدراج الأمن المعلوماتي في إستراتيجيات الدفاع الإسرائيلية.[2]

– إشراك القطاع الخاص والتعاون بين الأوساط الأكاديمية وقطاع الأعمال التجارية

إسرائيل من رواد التعاون الأمني بين أصحاب المصلحة المتعددين؛ بين الحكومة والمؤسسات الأكاديمية والقطاع الخاص فالتعاون في مجال الأمن السيبراني هوامتداد طبيعي للنموذج الحالي في مجالات أخرى.

يعتبر مشروع مبادرة الإبتكار "Cyber Spark" في بئر سبع في سنة 2014م كمشروع مشترك بين هيئة السايبر وجامعة (بن غورين) والشركات الأجنبية مثل "Lockeed Martin " و" Deutsche Telecom" و"Elbit" والجيش الإسرائيلي لجذب الاستثمارت الأجنبية المتخصصة في الأمن السيبراني.

بالإضافة إلى مبادرة "Cyber Spark" تم إنشاء حوالي 20 مركز للأبحاث والتطوير في مجال الأمن السيبراني في إسرائيل من طرف الشركات متعددة الجنسيات من أجل تطوير حلول أمنية للسوق العالمية.

ومن أمثلة هذه الشركات : Paypal، Vm Ware، General Electric، Cisco، Ciscom وتقوم الشركات أيضا بإنشاء مراكز للانترنت في إسرائيل في الوقت الحالي.[3]

كما طورت إسرائيل العديد من الشركات الناشئة في صناعة التكنولوجيا وصناعة الأعمال والخبراء وعمدت على تشجيع القطاع الخاص وتفعليه عن طريق توفير التمويل وجذب الاستثمارات الخارجية لتأمين الدفاع في فضائها الإلكتروني بالتعاون مع الشركات متعددة الجنسيات باستثمار إجمالي يقدر بـــ 581 مليون

[1]– **المرجع نفسه**، ص 29.

[2]– المكان نفسه.

[3] - Heno Ouwendijk, "**Cybersecrity and Hemeland Secrity in Israel** ", (Rijks-dienst voor ondernement, Nederland, 2015), p 02.

دولار، وتحصل الشركات الإسرائيلية على نسبة 15% من الاستثمارات في قطاع الأمن السيبراني وهذه الأرقام تعتبر مرتفعة جدا لدولة يبلغ عدد سكانها 8 ملايين نسمة فقط.

وذلك بالاعتماد على العلاقات التجارية مع كل الأوساط الأكاديمية والحكومة ودعم الشركات الناشئة مثل شركات الكهرباء لإسرائيلية، فهي مشروع مشترك أنشأ سنة 2013م مع رواد الأعمال الشباب "Cyber Gym" للتدريب وتقديم الاستشارات في مجال الدفاع السيبراني.[1]

2- على المستوى الدولي

تنشط علاقات التعاون المشترك في مجال الفضاء السيبراني بين إسرائيل في علاقاتها الخارجية حيث تقوم هيئة السايبر بتنسيق التدريبات الوطنية والدولية وكذلك التعاون مع الهيئات الموازية في الخارج، ويعمل المكتب على تطوير العلاقات الخارجية في المجال السيبراني مع الدول التي لها علاقات جيدة معها لأغراض مختلفة مثل تبادل المعلومات والبحث والتطوير المتبادل.

إسرائيل هي عضو في مبادرة (ITU-Impact) ولديها إمكانيات للوصول إلى خدمات الأمن السيبراني كما ينسق مكتب السايبر في إسرائيل التدريبات الوطنية والدولية.

في إطار الشراكة الإستراتيجية بين الولايات المتحدة الأمريكية وإسرائيل في مجال الأمن السيبراني تعمل كل منهما معا ضمن 15 دولة للحد من خطر الهجمات السيبرانية على شبكات الكومبيوتر من خلال التعاون، ففي سنة 2008م وقعت إسرائيل والولايات المتحدة الأمريكية على اتفاقية لزيادة التعاون في العلوم والتكنولوجيا في محاولة لمواجهة مجموعة واسعة من التهديدات العالمية والتي من ضمنها التهديدات السيبرانية.[2]

ولتدعيم بنية تحتية دفاعية مشتركة وتعزيز بحوث القطاع الخاص وتطوير التكنولوجيا بشكل مشترك وقعت إسرائيل والولايات المتحدة الأمريكية في 2016/06/22م اتفاقية تهدف إلى زيادة التعاون الثنائي في مجال الدفاع السيبراني، وإنشاء شراكات في القطاع الخاص وتمويل البحوث بين وزارة الأمن الداخلي الأمريكية ونظيرتها الإسرائيلية (الجهاز القومي للأمن الإلكتروني)، وتستخدم الشركات في إسرائيل في مجال الأمن السيبراني نسبة 20% من التقنيات المتطورة مما يجعل هذه الشركات رائدة في هذا القطاع.[3]

---

[1] –Heno Ouwendijk, **Op-cit**, p 03.

[2] –"**The U.S. Israël Stratégie Partmership**",Web Sit Visited in : 24 March 2018. Link : http://www.mepc.org/future-us-israel-strategic-partnership.

[3] –Hadas Klein, "**Global Cyber. Biweekly Report**", (The institute for National Security Studies, July 2016), p 01.

كما شاركت إسرائيل كعضو في فريق الخبراء الحكوميين التابع للأمم المتحدة التي أصدرت تقريرا عن التطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي وذلك سنة 2015م.

في 2016/09/01م انضمت إسرائيل رسميا إلى اتفاقية "مجلس أوروبا" لسنة 2001م بشأن الجرائم الإلكترونية، إضافة إلى عقد علاقات ثنائية لتعزيز الأمن السيبراني مع عدد من الدول والمنظمات الدولية بما في ذلك المعاهدات الثنائية.[1]

المطلب الرابع : تخصيص الميزانيات لتعزيز الحماية في مجال الأمن السيبراني

أدركت إسرائيل أن اهتمامها بالعلوم والمعرفة قد أصبح مكونا رئيسيا لعقيدتها نحوالتفوق وإقامة الدولة، ويتحقق ذلك من خلال وضع إستراتيجية منظمة ومحددة الأهداف للبحث العلمي في شتى مجالات المعرفة.

وانطلاقا من الفرضية القائلة بأن تقييم الميزانيات يسمح بتقدير حجم الأهمية المعطاة للموضوع من قبل صانعي القرار في إسرائيل بادر المجلس القومي للبحث والتطوير (مولموف) في سنة 2007م إلى تمويل دراسة حول مؤشرات العلوم والتكنولوجيا والابتكار في إسرائيل بالتعاون مع مكتب الإحصاء المركزي وكان الهدف الأساسي من المبادرة دراسة الميزانيات المخصصة للعلوم والتكنولوجيا فيها، فأظهرت الدراسة أنه من خلال العقد الأخير أنفقت إسرائيل حوالي 30 مليار شيكل جديد* في السنة وهو ما يعادل 8.1 مليار دولار أمريكي على أعمال البحث والتطوير المدني كما بينت أن نسبة الناتج المحلي المستثمرة في البحث والتطوير هي الأعلى فيها مقارنة مع الدول الأخرى[2]، نسبة 4.3 % في سنة 2009م في المقابل 1.8 % كمعدل وسطي في دول منظمة التعاون الاقتصادي والتنمية، وأكثرية التمويل في إسرائيل نحو79% مصدره قطاع الأعمال حيث تساهم الحكومة مباشرة بنحو5 مليار شيكل جديد أي ما يعادل 1.4 مليار دولار لتمويل البحث والتطوير لأغراض مدنية بالإضافة إلى الميزانيات المخصصة للبحث والتطوير الأمنيين.[3]

---

[1] – Hadas Klein, **Op-cit**, p 02.

*– الشيكل الجديد: هو عملة إسرائيل الرسمية بدأ التداول به لأول مرة في: 1985/09/04 كجزء من خطة الاستقرار الاقتصادي لعام 1985، وقد بدأ العمل به رسميا في 1986/01/01، (أنظر: الرابط http://www.wikiwand.com/ar/).

[2] – جيل برعام، **مرجع سابق**، ص 11.

[3] – المكان نفسه.

وتبين هذه الأرقام مدى اهتمام الحكومة وقطاع الأعمال في إسرائيل بمراكز البحث العلمي لذلك يتم استثمار مبالغ كبيرة من الأموال في أعمال البحث والتطوير في المجال التكنولوجي، ويمكن إضافة الميزانيات المخصصة لهذه الأبحاث في ميادين تطبيقية ونظرية في المجال السيبراني.

إن أحد أهم بنود الإنفاق في مشروع الميزانية العامة للدولة للسنتين 2011 و2012م هوبند " الأمن والنظام العام" ويشمل هذا البند مخصصات أجهزة المؤسسة العسكرية والأمنية المتعددة التي تشمل مهامها معالجة المجال السيبراني.[1]

وبلغ مجموع مخصصات الأمن الإجمالية 61.8 مليار شيكل جديد ما يعادل 16.8 مليار دولار في سنة 2011م، في مقابل 63.4 شيكل جديد سنة 2012م ما يعادل 17.2 مليار دولار أمريكي.

تستحوذ وزارة الدفاع على القسم الأكبر من مخصصات هذا البند بقيمة 50.5 مليار شيكل جديد في سنة 2012م وعلى ما نسبته 18% من مجموع نفقات الميزانية العامة للدولة.[2]

ومن بين أهم أسباب التفوق الإسرائيلي في هذا المجال سعي الحكومة إلى تطوير الخبرات وتكوين المختصين، ويعتبر هذا الأمر من أهم العوامل المؤثرة في دفع وتطوير الحلول الأمنية والتطبيقات المتعلقة بأمن المعلومات في إسرائيل.[3]

ولا يقتصر الامتداد الإسرائيلي في مجال تقنية المعلومات على الأمن السيبراني بالرغم من أنه أهم المجالات وأكثرها انتشارا بل تتفوق كذلك الصناعة المعلوماتية الإسرائيلية في الكثير من المجالات الأخرى مثل التشفير، التراسل الفوري كبرنامج "ICQ" من شركة "Mirabilis" وبرنامج "Gooey" من شركة "Hypernix".[4]

تسعى إسرائيل من أجل تدعيم إستراتيجيتها إلى استقطاب الكفاءات والمتخصصين في الأمن السيبراني وهي من أكثر الدول الداعية لذلك بنسبة 89.2% متقدمة بذلك على ايرلندا في المركز الثاني ثم بريطانيا في المركز الثالث والولايات المتحدة الأمريكية في المركز الرابع.

[1]– **المرجع نفسه**، ص ص 11–12.

[2]– المكان نفسه.

[3]– عبد الفتاح محمد عبد الفتاح الفولي، "**تحديات إنشاء الحكومات الإلكترونية : دراسة في أمن المعلومات من وجهة نظر الأمن القومي العربي**"، (القاهرة: دار الخبرة للبحوث والتدريب، د س ن)، ص 21.

[4]– **المرجع نفسه**، ص 22.

ويمكن القول أن الوسائل الدفاعية في مجال الفضاء الإلكتروني تختلف باختلاف تلك التهديدات وطبيعة الأضرار التي قد تحدثها، لذلك وجب توفير ضمانات كافية لتحقيق الأمن السيبراني بما لا يضر الأمن القومي وأمن نظم المعلوماتية.

المبحث الثالث : الإستراتيجية الإسرائيلية الهجومية كآلية لمواجهة التهديدات السيبرانية

يظهر التحدي الحقيقي أمام قدرات الدول وتطوير مهاراتها في التصدي للهجمات الإلكترونية مقابل التطور الكبير الذي يتمتع به المهاجمون، لذلك فإن مستوى الخطورة يزداد مع كل تطور تكنولوجي.

إن توظيف التكنولوجيا الحديثة لإلحاق الضرر بالآخرين أعاد للأذهان ضرورة التفكير في كيفية تجنب الأضرار الناجمة عنها والبحث عن سبل لمواجهتها حتى أنها أصبحت من الأولويات في إستراتيجيات الدول.

لذلك تدرك إسرائيل أن الهجمات الإلكترونية الموجهة إليها تتحقق في حالة طرف يملك قدرات كبيرة في المجال السيبراني والتي تمكنه من القيام بمثل هذه التهديدات والاختراقات ضدها.

فالذي يجعلها تدرك كل تلك المخاطر والتهديدات يرجع أساسا إلى حقيقة معرفتها بأن تلك الهجمات تمارس على نطاق واسع، ويمكن أن تحقق أهدافا إستراتيجية وتكتيكية لأن إسرائيل دولة محوسبة تعتمد كل قطاعاتها على الأنظمة الإلكترونية.

وأن مثل هذا التهديدات سيشل كل القطاعات الموجودة في الدولة لذلك كان لزاما عليها اتخاذ إستراتيجية وموقف هجومي متبعة في ذلك مبدأ الأسبقية في توجيه الضربات ضد أعدائها في فضائها الإلكتروني.

المطلب الأول : استخدام الفيروسات والبرامج الخبيثة

الفرع الأول : استخدام فيروس (ستاكسنت) وفيروس (فيلمر) ضد إيران

أصبحت الحرب الإلكترونية جزءا لا يتجزأ من إستراتيجية إسرائيل الهجومية حيث تقوم بتوظيف الفضاء الإلكتروني في الجهد الحربي ضمن إستراتيجية شاملة اعتمدتها فهو يمثل إحدى المجالات الإستراتيجية العملياتية.[1]

ويمكن تنفيذ الهجمات أوعمليات جمع المعلومات الاستخباراتية في الفضاء الإلكتروني باستخدام البرمجيات الخبيثة التي أصبحت أسلحة الفضاء السيبرانية في السياق العسكري وهي غالبا عبارة عن هجوم برمجي "Soft Ware" من خلال شبكة القرصنة (Hacking)، وهذا الشكل من أشكال الهجمات يستقطب جل الاهتمام الإعلامي ومن الضروري تقسيم أسلحة الفضاء الإلكتروني إلى أسلحة معقدة شديدة التأثير تهدف إلى إحداث تأثير إستراتيجي وأسلحة منخفضة التأثير تهدف إلى إلحاق الضرر محدود بقصد إحداث

[1]- فيصل محمد عبد الغفار، **مرجع سابق**، ص 164.

الارتباك والإضرار بالسمعة، وتعتبر الفيروسات الإلكترونية والرقمية أحد أهم الأسلحة التقنية التي دأبت إسرائيل على استخدامها في حروبها الإلكترونية نظرا لقوتها وضمان فاعليتها في التأثير على البيئات الرقمية المعلوماتية التي تستهدفها.[1]

يعد فيروس (ستاكسنت) نموذجا هاما لأسلحة الفضاء السيبراني الشديدة التأثير ومصممة لتحقيق تأثير إستراتيجي والذي تم تطويره كأهم سلاح رقمي من الدرجة العسكرية.[2]

ويمثل الهجوم الذي قامت به إسرائيل والذي تعرض له المفاعل النووي الإيراني في سنة 2010م حدثا تأسيسيا في مجال حرب الفضاء السيبراني، وشكل مرحلة جديدة في تطور استعمال الفضاء الإلكتروني في مجال القتال باستخدام فيروس "ستاكسنت" الذي كان عبارة عن دودة حاسوب تهدف إلى التخريب.

وقد لعبت الوحدة 8200 دورا أساسيا في مهاجمة إيران إلكترونيا، فهي تشتهر أيضا بقدرتها على إنتاج البرامج الضارة أوالخبيثة والفيروسات وهي المسؤولة عن الهجوم الذي استهدف أنظمة الكومبيوتر التي تشغل منشآت تخصيب اليورانيوم النووية الرئيسية في إيران بفيروس "ستاكسنت" الذي قام بتصميميه كل من الولايات المتحدة الأمريكية وإسرائيل وهذا يظهر مدى التعاون الكبير بين الدولتين في مجال الفضاء السيبراني الدفاعي والهجومي معا.

حيث أستخدم هذا الفيروس في إطار موجة من الهجمات الرقمية على إيران وعطل نحو100 من أصل 5000 جهاز طرد مركزي ويعتبر أول هجوم إلكتروني يستخدم فيه هذا النوع من الأسلحة لإلحاق دمار مادي.[3]

ويمثل فيروس"ستاكسنت" بداية حقبة جديدة في سباق التسلح في مجال الأمن السيبراني لأنه وللمرة الأولى في تاريخ العلاقات الدولية يتم اكتشاف هجوم إلكتروني يهدف إلى تدمير جزء من البنية التحتية الحرجة للدولة كما يعتبر الهجوم الأول الذي حظي باهتمام عالمي بسبب غرضه الفريد كسلاح إلكتروني.[4]

---

[1]- وليد غسان سعيد جعلود، **مرجع سابق**، ص 164.

[2]- جون باسيت، "**حرب الفضاء الالكتروني: التسلح وأساليب الدفاع الجديدة** "، (أبو ظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2014)، ص ص 58–59.

[3]- محمد بلال أحمد عايش حبيب، ومحمود صلاح جاد الله أبو ركبة، "**بحث بعنوان: الصراع النووي الإيراني الإسرائيلي: المخاطر والتحديات**"، (الجامعة: الإسلامية، كلية التجارة ، قسم الاقتصاد والعلوم الإنسانية، 2012)، ص 78.

[4] - Boldizar Bencsath and others, **" The Cousins of Stuxnet: Duqu,Flame and Gauss",** Journal future internet , (Novembre 2012), p 971.

يقوم هذا الفيروس بمهاجمة أنظمة التحكم الصناعية المستخدمة على نطاق واسع في مراقبة الوحدات التي تعمل آليا ولا يعمل بشكل عشوائي وإنما بشكل محدد جدا.

إذ يقوم بعد احتراق الأجهزة والحواسيب بالتفتيش عن علامة فارقة تتعلق بأنظمة صنعتها شركة "سيمتر" الألمانية وعندما يجدها يقوم بتفعيل نفسه ويبدأ بالعمل على تخريب وتدمير المنشأة المستهدفة من خلال العبث بأنظمة التحكم، وقد تتعددت المنشآت التي يستطيع مهاجمتها من خطوط نقل النفط إلى محطات توليد الكهرباء وحتى المفاعلات النووية وغيرها من المنشآت الإستراتيجية الحساسة إضافة إلى صعوبة القضاء عليه[1] وقد ظهر أيضا في ماليزيا ودول متعددة وأصاب هذا الفيروس حوالي 45 ألف حاسب آلي في أنحاء العالم، 60% منها في إيران و18% في إندونيسيا.

كما أنه في سنة 2012م تعرض الشرق الأوسط بشكل عام وإيران بشكل خاص إلى هجمة جديدة عبر فيروس اللهب (Flame) بإختراق منظومات حواسيب إيرانية حساسة وأنظمة التشغيل الرقمية أدى إلى تعطيل 189 حاسوب وبنوك للمعلومات، أستخدمت في هذا الفيروس تقنيات تشفير متعددة من خلال مسح البيانات من الأجهزة التي تهاجمها وبشكل دوري وآمن حتى لا يترك أي أثر لها كما أن التجسس وجمع المعلومات هما أبرز صفات هذا الفيروس.

وهومن أكثر الفيروسات تعقيدا وصعوبة في الاكتشاف لتسلله في أشكال عدة، ومصمم لسرقة المعلومات من الأنظمة المستهدفة والملفات المخزنة داخل أنظمة الحواسيب، والمحتويات التي تعرضها شاشة الكومبيوتر وحتى المحادثات الصوتية، يستهدف هذا الفيروس الأنظمة المحوسبة في الشرق الأوسط لأنه يهدد أمن البنية التحتية النووية ويهاجم بقوة أنظمة التحكم الصناعية ويتسبب في فقدان كم هائل من المعلومات والبيانات في أنظمة الحواسيب المتضررة وإستغلال بعض الثغرات ونقاط الضعف الموجودة فيها. [2]

إضافة إلى إيران استهدف فيروس (فليمر) بعض الدول في الشرق الأوسط منها: لبنان، فلسطين، والإمارات العربية المتحدة وسوريا .

---

[1]– إيهاب خليفة، "**ما هو فيروس ستاكسنت**"، تم تصفح الموقع يوم : 26 مارس 2018. الرابط: http://books.google.dz/book?id=t Tewdg AA QBAJ&pg=PA11&lpg.

[2]– إيمان الزبيدي، "**سيمانتك تكشف عن خطر فيروس فليمر الذي يستهدف مناطق الشرق الأوسط**"، تم تصفح الموقع يوم : 13 أفريل 2018. الرابط: http:/www.tech-wd.com/wd /2012/06/01/w32-flamer

تفوق قوة فيروس (لهب) أو(فليمر) نظيره (ستاكسنت) بحوالي 20 إلى 40 مرة وله قدرة لاسلكية في نطاق الموجات القصيرة أوماتسمى بتقنية البلوتوث.

لذلك تقوم إسرائيل في إستراتيجيتها الهجومية بالتشويش على شبكة الكهرباء والإنترنت والشبكة الخليوية وموجات الطوارئ الخاصة بالشرطة وأجهزة الأمن الأخرى، وتطوير أنظمة قتالية إلكترونية متطورة تتيح لها تشويش الأنظمة الدفاعية الإيرانية.[1]

الفرع الثاني : اختراق منظومة التحكم الإلكتروني في سوريا

تمكنت أجهزة الاستخبارات الإسرائيلية "الموساد" وهيئة الأركان العامة للجيش الإسرائيلي التابعة لشعبة الاستخبارات العسكرية الإسرائيلية "أمان" عن طريق الوحدة 8200 وبالتعاون مع الاستخبارات المركزية الأمريكية من الوصول إلى معلومات تؤكد النشاط النووي في سوريا، حيث بدأ التأكيد على هذه المعلومات بعد زرع برنامج (حصان طروادة) في جهاز كومبيوتر نقال خاص بمسؤول سوري في لندن، ليخضع لمراقبة "الموساد" في سنة 2006م، بعد زرع هذا البرنامج أصبح بالإمكان تشغيل برنامج الباب الخلفي الذي يمكن "الموساد" من مراقبة تحركاته ولكن الأهم من ذلك هوتمكن "الموساد" بواسطة هذا البرنامج من نسخ كل المعلومات الموجودة على جهاز الكومبيوتر التي تتعلق بمفاعل "دير الزور".

أدى ذلك إلى اتخاذ تدابير من قبل الحكومة الإسرائيلية كما حرصت على إطلاع الولايات المتحدة الأمريكية على الأدلة التي جمعتها ومارست ضغوطا على المسؤولين الأمريكيين لاستخدام أقمار صناعية تجسسية مع التركيز على منطقة (دير الزور)، وإستخدمت كذلك إسرائيل قمرها الصناعي (أوفيك 7).[2]

نجحت أجهزة الاستخبارات الإسرائيلية في إقناع الطرف الأمريكي بضرورة شن هجوم على المفاعل لتدميره وبذلك أقدمت على التسلل إلكترونيا إلى منظومة التحكم المسؤولة عن توجيه الدفاعات الجوية السورية وتمكنت أنظمة الحرب الإلكترونية الإسرائيلية وأجهزة التشويش المتطورة من تحييد الدفاعات الجوية السورية الصاروخية مما أدى إلى التشويش على الرادارات واستحالة الرؤية.

ما سمح للطائرات الإسرائيلية بإصابة الهدف وتفجير المفاعل النووي السوري لأن إسرائيل لن تسمح بامتلاك من يهدد بقائها أسلحة نووية.

---

[1]- محمد بلال أحمد عايش حبيب، ومحمود صلاح جاد الله أبو ركبة، **مرجع سابق**، ص 79.

[2]- د م، "**إسرائيلي يكشف تفاصيل الغارة على دير الزور**"، تم تصفح الموقع يوم : 26 مارس 2018. الرابط:
alakhbar.spiru.la/node/43031

مع التقدم التقني الكبير وتطور وسائل وأجهزة الاتصالات أصبح اقتحام المواقع وأنظمة التحكم الإلكترونية وتدميرها وتغيير محتواها هوالسائد في تعامل دوائر الأمن والاستخبارات الإسرائيلية، لمنع الدول التي تعتبرها معادية لها والتي تشكل تهديدا على وجودها من امتلاك قدرات تكنولوجية معلوماتية وعسكرية وأمنية فضلا عن نظرتها المستقبلية ورغبتها في أن تكون قوة إقليمية في المنطقة.

المطلب الثاني : التعامل مع مواقع التواصل الإجتماعي

أحدثت التكنولوجيا تطورا سريعا وتغييرا كبيرا في مجال الاتصال والتواصل فوجود شبكة الانترنت زاد من أهمية هذا التغير وجعله يلامس جميع نواحي الحياة الاجتماعية، كما أثرت على طريقة التعامل بين الأفراد والمجتمعات والتواصل فيما بينهم وأصبحت وسيلة سهلة لنقل الأخبار وانتشارها ومساحة للتعبير عن الآراء والتوجهات.

ومع الانتشار الواسع لمواقع التواصل الاجتماعي تزايدت المخاوف من حقيقة الجهات الخفية المسؤولة عن هذه المواقع والمستفيدة من المعلومات التي ينشرها المشتركون على صفحاتهم مع تعاظم الدور الاستخباراتي الإسرائيلي.

ويعد موقع (الفيس بوك) ساحة خلفية للاستخبارات الإسرائيلية مهمته الحقيقية تجنيد العملاء والجواسيس[1] بحيث تستفيد إسرائيل من التكنولوجيا التفاعلية والمعلوماتية لتحقيق الأهداف خاصة وأنها تدرك خطورة مواقع التواصل الاجتماعي وتأثيرها عليها لذلك استغلت هذه المواقع في مجال التجسس والمراقبة.[2]

أصبحت مواقع التواصل الاجتماعي بمثابة أداة فعالة تتيح لإسرائيل وأجهزتها الاستخباراتية الحصول على معلومات من الشباب العربي وخاصة الفلسطينيين في مختلف شؤونهم بما يخدم تجنيد البعض لخدمة أهدافها وأجهزتها، فهي أحد أهم الأدوات التي تهدف إلى الإيقاع بالشباب العربي والإسلامي ودفعه للعمالة مع وحداتها الاستخباراتية وتعد الوحدة 8200 أهمها.

ومن جهة أخرى أدى إقبال الشباب الإسرائيلي على هذه المواقع إلى تجنيد الآلاف منهم ليشكلوا أكبر جيش إلكتروني لنشر الفكر الصهيوني والتوغل في أعماق العالم العربي والإسلامي واستهداف الناشطين لأهداف استخباراتية.

---

[1]–حسنين شفيق، "**الإعلام الجديد والجرائم الإلكترونية: التسريبات...التجسس الإلكتروني...الإرهاب**"، (القاهرة: دار فكر وفن للطباعة والنشر والتوزيع، 2015)، ص 159.

[2]– شدان يعقوب خليل أبويعقوب، **مرجع سابق**، ص 51.

وفي ذات الإطار أنشأت المخابرات الإسرائيلية عددا من المواقع الإلكترونية باللغة العربية بهدف تجنيد جواسيس جدد وظهر ذلك عبر مواقع صرحت بذلك علانية وأخرى عملت لنفس الغاية ولكن بصورة غير مباشرة مقابل مساعدات مالية.[1]

أسس الجيش الإسرائيلي في سنة 2008م وحدة عسكرية تتخصص بالإعلام الاجتماعي وأنشأ أول قناة له على "اليوتوب"، كما شكلت جميع المؤسسات الرسمية الإسرائيلية وحدات إعلام اجتماعي فعالة للدفاع عن الدولة الإسرائيلية.

كما تقوم بتجنيد منظم للمؤسسات الأكاديمية والطلاب الجامعيين لشن حروب إلكترونية وحملات إعلامية، بالإضافة إلى ذلك تقوم المؤسسات الحكومية بتدريب هؤلاء الطلاب ليكونوا سفراء لإسرائيل على هذه المواقع خاصة إذا كانوا يجيدون أكثر من لغة لتمنحهم بذلك المنح الدراسية والهبات المادية والمحفزات الأخرى التي تشجعهم على خدمة دولتهم.

أقامت وزارة الخارجية الإسرائيلية وحدة إعلام اجتماعي جديدة تتألف بالأساس من خريجي الوحدة العسكرية للتجسس الإلكتروني 8200 حيث تعمل على متابعة كلمات مفتاحية "تحريضية" على شبكات التواصل الاجتماعي.[2]

أنشأت إسرائيل وحدة تجسس ومراقبة إلكترونية لرصد تحركات ومراسلات الشباب العربي عبر وسائل التواصل الاجتماعي واستطاعت بذلك أجهزة المخابرات وعلى مدار السنوات السابقة أن تنفذ عمليات الاغتيال ضد عناصر المقاومة الفلسطينية عن طريق هذه المواقع.[3]

---

[1]- أحمد حامد سليمان خضير، "**دور إسرائيل والمتعاونين معها من الفلسطينيين في تمزيق النسيج السياسي للشعب الفلسطيني**"، مذكرة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية السياسية، (جامعة: النجاح الوطنية، كلية الدراسات العليا، 2014)، ص 74.

[2]- نديم ناشف،" **شبكات التواصل الاجتماعي في خدمة الاحتلال**"، تم تصفح الموقع يوم : 27 مارس 2018. الرابط: https://www.arab 48. com/

[3]- شدان يعقوب خليل أبويعقوب، **مرجع سابق**، ص 52.

ولابد من الإشارة إلى أن إسرائيل تبرم مجموعة من الشراكات السرية الكبرى في مجال التكنولوجيا المعلوماتية مثل "غوغل" و"آبل" و"ياهو" وغيرها حيث تتيح لها الولوج إلى قواعد معلومات ضخمة ومهمة، وبعض الشركات التي ترفض الشراكة أولا تستطيع دوائر التجسس الوصول إليها تقوم الوكالة بمحاولات لاختراقها لتحصل على المعلومات التي في قاعدة بياناتها أوتعمل على عرقلة عملها في الشبكة الدولية بحيث يبقى الإقبال مركزا على الشركات المرتبطة بالمؤسسة الأمنية الإسرائيلية.[1]

أنشأ جهاز الأمن الداخلي الإسرائيلي المخابرات العامة "الشاباك" وحدة "هاتساف" (Hatsav) سنة 2003م، تم تكليف الوحدة بإبقاء الإعلام العربي تحت الرقابة الإسرائيلية وتزويد المخابرات العسكرية بالمعلومات الهامة من خلال "الفيس بوك" و"تويتر" حيث تقوم هذه الوحدة بمراقبة كل ما يجري على الصفحات العربية بما في ذلك التنصت على المكالمات التي تتم عبر "الفيس بوك" والمحافظة على النشطاء الذين يؤثرون على مستخدمي "الفيس بوك" و"التويتر".

قامت إسرائيل بمهاجمة المواقع وذلك من خلال حجب بعض الصفحات والتي من أبرزها "صفحة الانتفاضة الفلسطينية الثالثة" الصفحة التي أغلقت حساب نحونصف مليون مستخدم بعد ضغوط إسرائيل على إدارة "الفيس بوك" بحجة أن محتوى الصفحة ينطوي على دعوات لقتل اليهود الإسرائيليين واستخدام العنف.[2]

كما تم غلق بعض حسابات قادة "حماس" على "الفيس بوك" بما في ذلك حساب القائد حسام بدران المسؤول عن الكتلة الإسلامية في جامعة الخليل وعزت روشق.

كما تم حجب صفحات الأخبار الفلسطينية بما في ذلك (وكالة أنباء الوطن) تحت ذريعة التحريض على الكراهية، وقد اعتبرته وسائل الإعلام الفلسطينية اعتداءا على حرية التعبير وتدخل صارخ في وسائل الإعلام.

لقد أصبحت الانترنت وبالتحديد مواقع التواصل الاجتماعي ساحة للنزاعات والصراعات إذ أنها تنطوي على التجسس وقرصنة بيانات الأمن القومي الحساسة التي يمكن أن تشكل تهديدا للدول عند التلاعب بها.[3]

---

[1]- عبد الوهاب محمود الزيدي، "**التجسس الإسرائيلي الإلكتروني على الدول العربية**"، العدد 58، مركز الدراسات الإستراتيجية والدولية، (جامعة: بغداد)، ص 144.

[2]- Said Abu Mualla, **"Palestinian-Israeli Cyber Conflict : An Analytical Study of the Israeli Propaganda on Face book, Adraei's page as an example"**, journal of Arab American university (Arabic language and Media Department, Faculty of Arts, November 2017), p 58.

[3] -Said Abu Mualla, **Op-cit**, p 59.

المطلب الثالث: الهجمات الإلكترونية المضادة

رغم امتلاك إسرائيل العديد من المقومات الإلكترونية والمعلوماتية مضاف إليها تمتعها بفضاء تكنولوجي عالي الحصانة والمتانة ومواكب لكل ماهوجديد في عالم التقنيات والإلكترونيات.[1]

إلا أن ذلك لم يمنعها من التعرض إلى العديد من الهجمات الإلكترونية التي أدت إلى اختراق وإيقاف العديد من مؤسساتها البارزة من طرف قراصنة الانترنت.

وردا على ذلك قامت بشن عدد من الهجمات الإلكترونية كرد فعل على الإختراقات التي تعرضت لها، كالهجوم الذي نفذته مجموعة تطلق على نفسها إسم (آي دي إف) (IDF) في إشارة إلى قوات الدفاع الإسرائيلية (Israel Defense Forces)، من خلال مهاجمتها مواقع إلكترونية استطاعت بها اقتحام البورصة المركزية في العاصمة السعودية الرياض وتعطيله بشكل كامل ردا على اقتحام الموقع الإلكتروني لشركة الطيران الإسرائيلية "العال" وموقع البورصة الإسرائيلية وموقع بنك "ليؤمي" مما أدى إلى تعطيل تلك المواقع بشكل كامل[2]، إضافة إلى مواقع الخطوط الجوية السعودية وبورصة أبوظبي وغيرها.

كما أعلن قراصنة الحاسوب الإسرائيلي في 2012/01/17م أنهم ردوا على الهجوم السعودي (OX.Omer) باختراق موقع بورصة الأوراق المالية في السعودية وأبوظبي وتخريبه عبر إغراق الموقع بطلبات الدخول ومنع من يريد الدخول إلى هذا الموقع.[3]

شنت إسرائيل هجمات إلكترونية على الفضاء الإلكتروني الفلسطيني وذلك عبر توجيه كم هائل من الرسائل على خوادم المواقع الإلكترونية الفلسطينية مما أدى إلى عدم استيعابها لهذه الرسائل وبالتالي تعطيلها، علاوة على اختراقها للترددات المنطلقة من محطات التلفزيون الفلسطيني، فبتاريخ 2012/2/29م قامت إسرائيل بمصادرة معدات محطتين تلفزيونيتين في الضفة الغربية مدعية أن ترددها تشوش على اتصالات مطار بن غورين.[4]

كما قامت مجموعة القراصنة الإسرائيليين المسماة "الذرة" بنشر 4800 بطاقة ائتمان لمواطنين من بعض الدول العربية في 2012/01/19م، بما فيها الأرقام السرية والرموز وأرقام الحماية ونوع البطاقة

---

[1]- وليد غسان سعيد جعلود، **مرجع سابق**، ص 206.

[2]- "**ملفات ساخنة، حرب التحكم الآلي سلاح الحرب الخامس**"، **مرجع سابق**، ص 201.

[3]- المكان نفسه.

[4]- وليد غسان سعيد جعلود، **مرجع سابق**، ص 247.

وتاريخ صلاحيتها حيث صرحت هذه المجموعة أنهم حصلوا على هذه المعلومات جراء اختراقهم لأحد البنوك السعودية الكبيرة ونشر آلاف العناوين الإلكترونية وحسابات فيس بوك لمواطنين في بعض هذه الدول[1]، وقيام قراصمة الانترنت الإسرائيليين في 2015/04/09م بتسريب سجل السكان الفلسطينيين الذي يحتوي على معلومات عن 4 ملايين فلسطيني وبنشر معلومات شخصية عن 700 موظف في السلطة الفلسطينية من بينهم وزراء في الحكومة وصحفيين.

وشرعت إسرائيل بالقيام بمحاكاة هجمات إلكترونية ضخمة تفترض فيها تعرضها لهجوم إلكتروني فمثلا قامت رئاسة الحكومة الإسرائيلية ومجلس الأمن القومي الإسرائيلي وبعض الوزارات المختلفة بتنفيذ عملية افتراضية أطلق عليها اسم "إطفاء الأنوار" تتمثل في تعرض المرافق الإسرائيلية لهجوم إلكتروني كبير للتدرب على كيفية التعامل مع هذه الهجمات.[2]

تستغل إسرائيل كل ما يصدر من تقنيات حديثة في عمليات التجسس التي تقوم بها لذا أدرجت في إستراتيجيتها أنظمة الهاتف المحمول التي اجتاحت العالم وخاصة العربي ووظفت أجهزة تنصت ومراقبة فائقة التطور تعمل على نظام (أيشلون) الأمريكي المتطور والذي بإمكانه التقاط موجات الهواتف العادية والخليوية في آن واحد، هذا في الوقت الذي أسهمت فيه وسائل حل الشيفرات بواسطة العقول الإلكترونية في الوقت الراهن في تجاوز الكثير من العقبات السابقة.[3]

وتنشئ محطات خاصة بذلك مبرمجة لتمييز الكلمات وأرقام الهواتف من خلال المحادثات الهاتفية والرسائل الإلكترونية والبيانات التي يتم التقاطها وإرسالها عبر الأقمار الصناعية، ولهذه المحطات القدرة على جمع المعلومات الإلكترونية ورصد اتصالات الحكومات والمنظمات والشركات والأفراد على حد سواء، ويتم إرسال المعلومات التي يتم جمعها لترجمتها وتحويلها إلى وكالات أخرى من بينها أجهزة الأمن الإسرائيلية.[4]

يمكن اعتبار مخاطر عمليات القرصنة والاختراق على هذه المواقع أنها توازي الحرب العسكرية لأنها تصل إلى الأماكن الحساسة للدولة كالقواعد العسكرية والمطارات والبنوك وقد تؤدي إلى خسائر فادحة وتأثير هذه العمليات يعتمد على الجهة المتعرضة للاختراق سواء حسابات مصرفية أو مواقع عسكرية وأمنية وتعتبر تهديدا للأمن القومي للدول.

1- "**ملفات ساخنة، حرب التحكم الآلي سلاح الحرب الخامس**"، **مرجع سابق**، ص 201.

2- وليد غسان سعيد جعلود، **مرجع سابق**، ص 248.

3- عبد الوهاب محمود الزيدي، **مرجع سابق**، ص 148.

4- المكان نفسه .

أدت الهجمات الإلكترونية بين إسرائيل والأطراف الأخرى التي تقوم بشن الهجمات ضدها خاصة الجانب العربي إلى تشديد عملية الرقابة على الاتصالات الإلكترونية لديهم وقيامها باختراقات مضادة للأجهزة التقنية في الجانب الآخر وإنشاء وحدات أمنية لمواجهة تلك المخاطر.

تعتبر إسرائيل من أكثر الدول المتطورة في مجال الاختراقات وذلك للصناعات الإلكترونية والرقمية التي تنتجها لأن عملية اختراق المواقع الإلكترونية هي بالدرجة الأولى إسرائيلية-أمريكية، بحيث وظفت هذه التكنولوجيا في عملياتها واعتمدت عليها بشكل كبير منذ سنة 1989م وذلك لما تملكه من تفوق في هذا المجال بسبب الدعم الأمريكي والغربي لها.

لقد أصبح الفضاء السيبراني بمثابة مجال قتال جديد يضاف إلى المجالات البحرية والجوية والبرية التي يخوضها الجيش الإسرائيلي لتصبح شبكة الانترنت ساحة معركة حقيقية وليست مجرد ذراع إضافية بل اتجاهات ذات أبعاد يتفوق على جميع أذرع الجيش وتكمن مهمته في التأكد من أن جميع أسلحته مستعدة لهذا العصر.

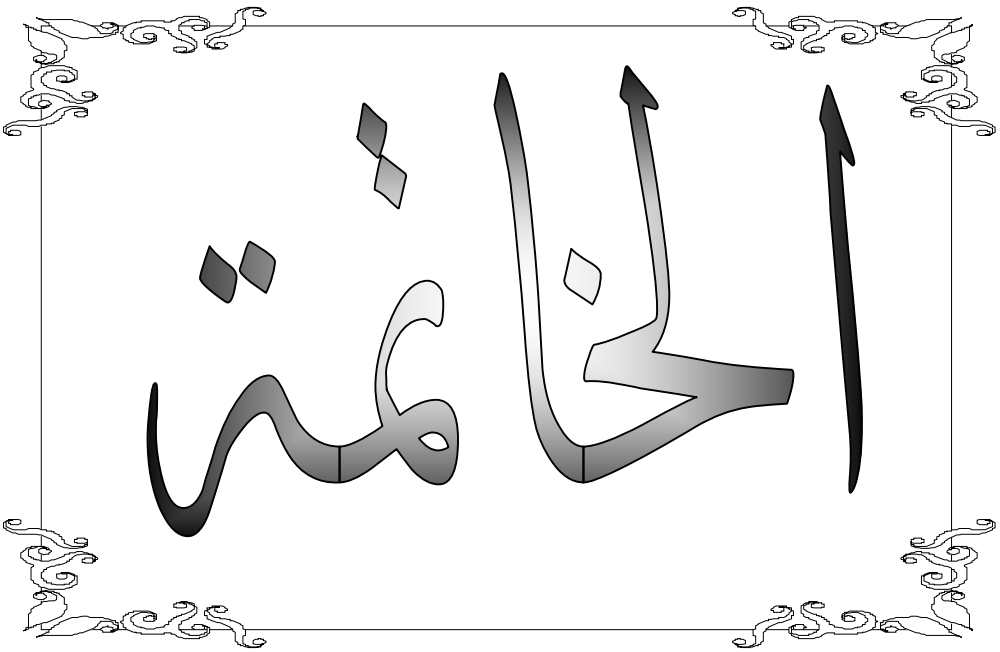
لذلك تعمل إسرائيل على تعزيز قدراتها الدفاعية والهجومية في مجال الحرب الإلكترونية لمواجهة التهديدات المتنامية التي تشكل تحديا وجوديا لها في فضائها السيبراني، نظرا لتعاظم وتيرة المخاطر التي تشكلها هذه التهديدات الأمر الذي يدعو قادة الجيش الإسرائيلي إلى تغييرات جذرية ومنح الجهات المختصة صلاحيات أكبر في مجال التصدي لها وتعزيز أمنها السيبراني.

خلاصة الفصل الثالث

تتعرض إسرائيل إلى العديد من الاختراقات الإلكترونية من مصادر عدة تهدف إلى استهداف منظومتها الإلكترونية والوصول إلى اجهزتها الحساسة أوالسيطرة على كبرى المؤسسات والشركات الحيوية فيها ردا على سياساتها المنتهجة خاصة تجاه القضية الفلسطينية وسياسات التطبيع المتبعة من العديد من الدول العربية.

كانت لهذه الهجمات والاختراقات الإلكترونية تأثيرات على كافة المجالات في إسرائيل مست العديد من الجوانب و التي برزت خاصة في الجانب الأمني و السياسي وكذلك الاقتصادي والاجتماعي بسبب اعتماد إسرائيل على التكنولوجيا الإلكترونية والتقنية في إدارة منشآتها الحيوية.

أصبحت إسرائيل أمام حرب لا تقل في خطورتها عن الحرب التقليدية، استخدم فيها الفضاء الإلكتروني كمجال جديد للقتال من الناحية الإستراتيجية والعملياتية، ولأن إسرائيل تدرك مدى خطورة التهديدات السيبرانية على أمنها القومي سخرت لذلك كافة الموارد واتخذت مجموعة من التدابير والخطوات لمواجهة هذه التهديدات وحماية فضائها السيبراني من خلال الاعتماد على شبكة محكمة ذات قواعد وإجراءات صارمة وعلى استراتيجية ترتكز على مبدأ الهجوم والرد ضد كل ما يهدد أمنها وهي بذلك تعتبر أبعادا مناسبة لمفهوم الأمن السيبراني في إسرائيل.


الخاتمة

من المؤكد أن إسرائيل انتهجت إستراتيجيات أمنية لمواجهة التهديدات السيبرانية التي تتعرض لها، نظرا لوجودها في محيط يتسم بالصراع والعداء التاريخي.

وهذا ما يثبت لنا فرضية أن إحاطة إسرائيل بدول أو أطراف معادية لها أدى إلى اتساع دائرة التهديدات السيبرانية ضدها.

وعلى هذا الأساس فقد تم دراسة هذا الموضوع الذي تتمحور إشكاليته حول مدى نجاح الإستراتيجية الأمنية الإسرائيلية في التصدي للتهديدات السيبرانية التي تواجهها في ظل المقاربة الإسرائيلية للحفاظ على أمنها القومي.

الإجابة عن الإشكالية

لقد تمت معالجة الإشكالية على امتداد ثلاث فصول، وتبين لنا أن إسرائيل تتعرض بشكل دائم للتهديدات السيبرانية وهذا ما ينعكس سلبا على أمنها القومي ويتضح ذلك فيما يلي:

- التخوف من أن تمس هذه التهديدات البنى التحتية في إسرائيل مما يؤدي إلى شل قطاعاتها الحيوية وأبرز مؤسساتها.

- تتجه إسرائيل نحو تفعيل استراتيجياتها واتخاذ مجموعة من التدابير والخطوات وإيجاد حلول لمشاكل حماية أمنها السيبراني.

إختبار الفرضيات

سيتم أيضا في إطار الخاتمة الوقوف على نتائج اختبار الفرضيات والتي تم التوصل فيها إلى ما يلي:

الفرضية الأولى: تبين لنا أن إسرائيل تواجه أعداء لها دوافع كثيرة لإلحاق الضرر بها سواء أكانت دولا أو منظمات أو أفراد معاديين أدى إلى اتساع دائرة التهديدات السيبرانية ضدها، فالبيئة الإستراتجية في مجال الفضاء السيبراني تختلف عن البيئة الإستراتيجية التقليدية التي اعتادت إسرائيل عبرها تحديد دوائر العداء الجغرافية كما أن العلاقة بين مجال الفضاء السيبراني والجغرافي تتعلق بالانتشار الجغرافي لبنية الحواسيب والشبكات، وأن التعامل مع معيار الزمن في المجال السيبراني يختلف عن التعامل العادي مع الزمن نظرا لسرعة انتشار هذه التهديدات، لذلك يخلق مجال الفضاء الإلكتروني فرصا أمنية جديدة ويتيح الفرصة للاستعانة بحلفاء بصورة مختلفة وفقا لقدراتهم ومكانتهم في هذا المجال.

الفرضية الثانية: استفحال التهديدات السيبرانية وتعدد مصادرها هو تحدي عويص يؤثر على الأمن القومي الإسرائيلي في كافة المجالات سواء الاقتصادية (استهداف البنوك، مواقع البورصة وحتى حسابات الأفراد

الشخصية)، سياسيا وأمنيا (التشكيك في قدرات إسرائيل الأمنية وبالتالي التشكيك في القادة السياسيين) واجتماعيا ونفسيا (انتشار الذعر والهلع بين الإسرائيليين).

الفرضية الثالثة: لا يمكن الاعتماد على المقاربة الأمنية الإسرائيلية فقط بل لا بد من وجود تعاون وتنسيق على المستوى المحلي والدولي للتصدي للتهديدات السيبرانية، من خلال تفعيل التعاون بين القطاع الحكومي والقطاع الخاص والقطاع الأمني والعسكري، وتشجيع الشراكات الدولية خاصة مع الدول الكبرى التي تدعم إسرائيل مثل الولايات المتحدة الأمريكية وبعض الدول الغربية.

الفرضية الرابعة: تزايد حدة التهديدات السيبرانية وتصاعد وتيرتها يؤثر سلبا على فعالية ونجاح الإستراتيجية الأمنية الإسرائيلية المنتهجة، فرغم ما تتمتع به إسرائيل من قوة إلكترونية جعلها من الدول الرائدة عالميا بحيث حققت إنجازات كبرى في مجال الأمن السيبراني، إلا أن تشابك هذه التهديدات وتعقدها وسرعة إنتشارها مع عدم وضوح مصدرها والأطراف الفاعلة فيها يؤثر سلبا على فعالية الإستراتيجية التي تنتهجها إسرائيل في الحد من هذه التهديدات مما يبرز مجموعة من التحديات خاصة مع تنامي قدرات من تخشاهم إسرائيل كإيران وحزب الله اللذان يعتبران عدوان إستراتيجيان يهددان أمنها القومي.

أبرز النتائج

إنطلاقا مما تم دراسته يمكننا استنتاج ما يلي:

- الإستراتيجية هي اتخاذ كل التدابير اللازمة بعد دراسة وتخطيط من طرف دولة أو مجموعة من الدول على المدى المتوسط أو البعيد، ويمكن القول أن الأمن والإستراتيجية متلازمان فلا يمكن تحقيق إستراتيجية دون أمن ولا أمن دون إستراتيجية، لذا فهذه الأخيرة تحتاج لنجاحها إلى مقومات مختلفة في مختلف المجالات وإمكانيات اقتصادية وعسكرية وسياسية وتكنولوجية؛

- الأمن السيبراني هو مجموعة الأدوات والسياسات ومفاهيم الأمن والضمانات الأمنية، ومناهج إدارة المخاطر والإجراءات والتدابير التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستخدمين من المخاطر والتهديدات السيبرانية والهدف من ذلك هو الحد من الخسائر والأضرار والحيلولة دون وصول هذه الأضرار إلى خسائر دائمة تعيق حركة الإنتاج وديمومته؛

- لقد أصبحت العلاقة بين الأمن والتكنولوجيا علاقة متزايدة مع إمكانات تعرض المصالح الإستراتيجية ذات الطبيعة الالكترونية إلى أخطار وتهديدات الكترونية، تؤدي إلى تحول الفضاء الالكتروني لوسيط ومصدر لأدوات للصراع المتعدد الأطراف؛

- يعبر التهديد عن كل عملية تنفذ من طرف وحدة معينة تؤثر على وحدة أخرى بالسلب سواء أكان مصدرها من داخل أو خارج الدولة وبغض النظر عن طبيعتها (الاقتصادية، سياسية، ثقافية، بيئية وحتى تكنولوجية)، يتميز هذا المفهوم بالنسبية والحركية كما أن المفهوم خلافي متداخل مع تهديدات أخرى ويتميز بسرعة الانتشار؛

- أصبحت التهديدات السيبرانية أحد أهم التحديات التي يتحتم على الدول مواجهتها خلال الفترة الحالية، خاصة مع تزايد الاعتماد على شبكات الانترنت والحواسيب لإلحاق الضرر بها عن قصد ، كما تتنوع أشكال ومصادر هذه التهديدات حيث يصبح بإمكان فرد أو مجموعة أفراد في أي مكان من العالم أن يحاول بشكل سري اختراق الأنظمة التي تحتوي على معلومات حيوية أو شن هجمات على البنى التحتية الحيوية ؛

- بالرجوع إلى مرتكزات العقيدة الأمنية الإسرائيلية يمكن القول أن عوامل التاريخ والأيديولوجيا هي التي رسمت العقيدة الأمنية الإسرائيلية وهي تعكس قناعات ثابتة بأن الأمن ما هو إلا تعبير عن تلك الحالة التي تشكل قوة الدولة؛

- من بين العوامل التي تساهم في تطور المقاربة الأمنية الإسرائيلية دور العولمة والثورات التكنولوجية في مجالات الاتصالات، السايبر والفضاء الخارجي، وما لا يلاحظ أن العقيدة الأمنية الإسرائيلية تحاول التكيف مع ما هو مستجد من تهديدات أمنية خاصة تلك التي تتعلق بالتهديدات السيبرانية والتكنولوجية التي أصبحت هاجسا يهدد أمن الدول؛

- تولي إسرائيل اهتمام كبيرا بالقطاعات التكنولوجية والتقنية منذ مطلع الخمسينات من القرن الماضي، لأنها تدرك أن بامتلاكها منظومة أمنية ذات دلالات معلوماتية قادرة على حسن توجيه إمكانياتها سيبقيها في طليعة معرفة الأحداث التي تجري في العالم وكيفية توظيفها بصورة تخدم الجانب الإسرائيلي؛

- تصنف إسرائيل في مصاف الدول المتقدمة تكنولوجيا وإلكترونيا لما تتوفر عليه من مستويات عالية في هذا المجال، حيث يتكون الفضاء الإلكتروني الإسرائيلي من العديد من المقومات للحفاظ على أمنها من الهجمات الإلكترونية الآخذة بالتوسع ضدها؛

- تتعرض إسرائيل إلى العديد من الهجمات والاختراقات الإلكترونية المستمرة من أطراف مختلفة من أبرزها مجموعة "الأنونيموس" الدولية، إيران، حزب الله وحركة حماس وحتى فئات الشباب من مختلف الجنسيات خاصة العربية والإسلامية بحيث استطاعت هذه الأطراف ضرب العمق الإسرائيلي والوصول إلى القطاعات

الحساسة في إسرائيل لكن رغم ذلك لا يمكن الجزم بأثر هذه التهديدات على إسرائيل لأنها تجيد إخفاء أضرارها وعدم الإفساح عن خسائرها؛

- تدرك إسرائيل أن للأمن السيبراني دور مهم في حماية أمنها القومي، فهو قد يؤثر على أمنها كليا إذا ما تعرضت للانكشاف أوالاختراق الأمر الذي يكلفها الكثير من الخسائر المادية والمعنوية أيضا، وهذا ما جعلها تضعه ضمن حساباتها الإستراتيجية وعقيدتها الأمنية سواء من خلال إتخاذ تدابير دفاعية أو الإعتماد على الهجوم والرد المباشر على كل الإعتداءات الموجهة ضد فضائها الإلكتروني؛

- ورغم ما تتمتع به إسرائيل من قدرات ومزايا في مجال الفضاء السيبراني إلا أنها في الوقت نفسه تواجه عدة تحديات ومخاطر تتمثل فيما يلي :

صعوبة تحديد مكان وهوية المهاجم، وقدرة المهاجمين على شن هجمات سريعة جدا؛

كذلك إسرائيل ليست الطرف الوحيد في المنطقة الذي يمتلك قدرات سيبرانية أوقدرات على استخدام الوسائل التكنولوجية على الصعيدين المدني والعسكري؛

صعوبة تطبيق سياسة الردع في المجال السيبراني.

التوصيات

- تتميز التهديدات السيبرانية بالديناميكية والتعقيد وسرعة الإنتشار، فهي تستلزم تفعيل العديد من السياسات الإستراتيجيات لمواجهتها، والاعتماد على تقنيات أكثر تطورا وكذلك تسخير الموارد اللازمة لذلك والتي يمكن من خلالها التصدي لهذه التهديدات، ومن خلال ذلك وضعت الباحثتان مجموعة من التوصيات المتمثلة فيما يلي:

- بناء وتشريع قواعد قانونية دولية لمراقبة ومعاقبة المهاجمين بحيث تكون أحد الوسائل الفعالة لمواجهة هذه التهديدات.

- زيادة الوعي الثقافي والتكنولوجي الإنساني بمخاطر التهديدات السيبرانية.

- العمل على زيادة وتحسين المستوى الفني والتقني لإدارة الأجهزة والشبكات الإلكترونية لحمايتها من مخاطر التهديدات السيبرانية.

- توسيع مجال التنسيق والتعاون بين الدول، من خلال عقد المؤتمرات والندوات الدولية لزيادة الوعي حول مخاطر هذه التهديدات.

لكن رغم ما تتمتع به إسرائيل والدول الكبرى من مقومات في مجال الأمن السيبراني إلا أنه من الصعب أن تصل دول العالم إلى تحقيق أمن سيبراني مطلق، حيث تبقى درجة حماية وحصانة الفضاء الإلكتروني لدول العالم نسبية فمن يعمل أكثر على هذه الحصانة يحمي نفسه بشكل أكبر عبر هذا الفضاء.


قائمة المصادر والمراجع

أولا: المصادر

1- la rousse dictionnaire de français .

2-Oxford dictionaries language.

ثانيا: قائمة المراجع

1- المراجع باللغة العربية

1- الكتب

1- أبو سعدة، محمد."**مؤسسات الإعلام الصهيوني: خريطة أولية**"، المعهد المصري للدراسات السياسية والإستراتيجية، 2016.

2- أبوسويرح، منذر، سلامة. "**الاستخبارات الإسرائيلية: البناء التنظيمي ووسائل التجسس**"، د ب ن، د د ن، 2016.

3- أبوعامر، عدنان، عبد الرحمان، **مترجما**، "**مراكز البحث العلمي في إسرائيل، السياسات، الأهداف، التمويل**"، بيروت: مركز نماء للبحوث والدراسات، 2013.

4- البعلبكي، منير. والبعلبكي، رمزي منير. "**المورد الحديث**"، لبنان: دار العلوم للملايين.

5- الحسينة، سعيد، **مترجما**، "**جواسيس ليمتد: شركات وصناعات متطورة يديرها أسياد الاستخبارات الإسرائيلية**"، بيروت: الدار العربية للعلوم، 2005.

6- الحلبي، تحسين. "**الشركات الخاصة الإسرائيلية للخدمات الأمنية الدور والأخطار**"، دمشق: مركز دمشق للأبحاث والدراسات، 2016.

7- الخضرا، ديما، **مترجما**،"**نظريات العلاقات الدولية: التخصص والتنوع**"، الدوحة: المركز العربي للأبحاث ودراسة السياسيات، 2016.

8- الطويل، رواء، زكي. "**الأمن الدولي وإستراتيجيات التغيير والاصلاح**"، الأردن: دار أسامة للنشر والتوزيع، 2012.

9- العتوم، نبيل. "**الجيش الالكتروني الايراني**"، الأردن: دار عمار للنشر والتوزيع، 2015.

10- - الفولي، عبد الفتاح، محمد، عبد الفتاح. "**التحديات إنشاء الحكومات الإلكترونية : دراسة في أمن المعلومات من وجهة نظر الأمن القومي العربي**"، القاهرة: دار الخبرة للبحوث والتدريب، د س ن.

11- المومني، محمد، حسين. وشلبي، سعد، شاكر. **"المؤسسة العسكرية في النظام السياسي الإسرائيلي"**، الأردن: دار الحامد للنشر والتوزيع، 2013.

12- النيرب، باسل، يوسف. **"الإعلام الإسرائيلي....ذراع الجلاد"**، الرياض: مكتبة الملك فهد الوطنية للنشر، 2010.

13- إيفين، شموئيل. وغرانيت، عاموس. **"المخابرات الإسرائيلية...إلى أين؟"**، بيروت: مركز باحث للدراسات، 2009.

14- باسيت، جون. **"حرب الفضاء الالكتروني: التسلح وأساليب الدفاع الجديدة"**، أبو ظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2014.

15- بامفلح، فاتن، سعيد. **"حماية أم المعلومات في شبكات المكتبات– دراسة حالة أم القرى"**، جامعة الملك عبد العزيز، د س ن .

16- برعام، جيل. **"تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في إسرائيل"**، مؤسسة الدراسات الفلسطينية، د م ن، د س ن.

17- بويغارة، ياسمينة. **"الجريمة الإلكترونية"**، جامعة: الأمير عبد القادر للعلوم الإسلامية.

18- جبور، منى، الأشقر. **"الأمن السيبراني: التحديات ومستلزمات المواجهة"**، جامعة الدول العربية: المركز العربي للبحوث القانونية والقضائية، 2012.

19- حسين، خليل. وعبيد، حسين. **"الإستراتيجيا"**، بيروت، منشورات الحلبي الحقوقية، 2013.

20- حمدونة، رأفت، خليل. **"القدرة العسكرية الإسرائيلية 2017"**، مركز الأسرى للدراسات والأبحاث الإسرائيلية، 2017.

21- حيدر، رندة. **"العقيدة الأمنية الإسرائيلية وحروب إسرائيل في العقد الأخير"**، إشراف وتحرير: أحمد خليفة، بيروت: مؤسسة الدراسات الفلسطينية، د س ن.

22- د م. **"ملفات ساخنة: حرب التحكم الآلي سلاح الحرب الخامس"**، الأردن: دار الجليل للنشر والتوزيع، 2013.

23- رفيق، عادل، **مترجما**، **"الجيوبوليتكس السيبراني والاستقرار في الشرق الأوسط"**، المعهد المصري للدراسات، 2018.

24- زكريا، فؤاد. **"التفكير العلمي"**، الطبعة الثالثة، الكويت: المجلس الوطني للثقافة والفنون،، 1978.

25- سامية، أبو النصر. **"الإعلام والعمليات النفسية في ظل الحروب المعاصرة وإستراتيجية المواجهة"**، القاهرة: دار النشر للجامعات، 2010.

26- شعبان، أحمد، بهاء. **"العلم والسيطرة: كيف استخدمت إسرائيل تقدمها العلمي والتكنولوجي لبسط هيمنتها على منطقتنا؟"**، القاهرة: الهيئة العامة لشؤون المطابع الأميرية، 2015.

27- شفيق، حسنين. **"الإعلام الجديد والجرائم اللاكرتونية: التسريبات...التجسس الإلكتروني...الارهاب"**، القاهرة: دار فكر وفن للطباعة والنشر والتوزيع، 2015.

28- شفيق، نوران. **" تأثير التهديدات الالكترونية على العلاقات الدولية –دراسة في أبعاد الأمن الالكتروني"**، القاهرة: المكتب العربي للمعارف، 2016.

29- صادق، عباس، مصطفى. **"الإعلام الجديد: المفاهيم والوسائل والتطبيقات"**، الأردن: دار الشروق للنشر والتوزيع، 2008.

30- عبد الغفار، فيصل، محمد. **"الحرب الإلكترونية"**، الأردن: الجنادرية للنشر والتوزيع، 2016.

31- عبد الكريم، إبراهيم. **"الصناعات العسكرية الإسرائيلية: المحددات–البنية–الصادرات"**، أبوظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2004.

32- عبد الهادف، عادل. **"الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي"**، المركز العربي لأبحاث الفضاء الإلكتروني، 2017.

33- عقلي، بدر. **"الموساد، الشاباك، أمان وأسلحة الدمار الشامل الإسرائيلية"**، عمان: دار الجليل للنشر والتوزيع، 2009.

34- عكروم، ليندة. **"تأثير التهديدات الجديدة على العلاقات بين دول شمال وجنوب المتوسط"**، الأردن: دار إبن بطوطة للنشر والتوزيع، 2011.

35- عنتباوي، منذر. **"أضواء على الإعلام الإسرائيلي"**، بيروت: مركز الأبحاث، 1968.

36- عون، ميشال. **"دراسة موجزة عن الإستراتيجية"**، الرابية، 2008.

37- فؤاد، عباس، إبراهيم. **"الموساد تحت المجهر"**، القاهرة: دار المنار للطباعة والنشر، 2010.

38- فهمي، محمد، عبد القادر. **"المدخل في دراسة الإستراتيجية"**، عمان: دار مجدلاوي للنشر والتوزيع، 2009.

39- فهمي، محمد، عبد القادر. "**المدخل إلى دراسة الإستراتيجية**"، عمان: دار مجدلاوي للنشر والتوزيع، 2010.

40- قوجيلي، سيد، أحمد. "**تطور الدراسات الأمنية ومعضلة التطبيق في العالم العربي**"، أبوظبي: مركز الإمارات للدراسات والبحوث الإستراتيجية، 2012.

41- محارب، محمود. "**إسرائيل والحرب الإلكترونية**"، معهد الدوحة: المركز العربي للأبحاث ودراسة السياسات، (أوت 2011).

42- محمود، خالد، وليد. " **الهجمات عبر الانترنت: ساحة الصراع الإلكتروني الجديدة**"، الدوحة: المركز العربي للأبحاث ودراسة السياسات، 2013

43- مراد، علي، عباس."**الأمن والأمن القومي: مقاربات نظرية**"، الجزائر: ابن النديم للنشر والتوزيع، 2017.

44- منصور، جوني. ونحاس، فادي. "**المؤسسة العسكرية في إسرائيل: تاريخ، واقع، إستراتيجيات وتحولات**"، فلسطين: المركز الفلسطيني للدراسات الإسرائيلية، 2009.

45- نيوف، صلاح. "**مدخل إلى الفكر الإستراتيجي**"، الدنمارك: الأكاديمية العربية المفتوحة، د س ن.

46- وراد، ضياء، **مترجما**، "**الكون الرقمي: الثورة العالمية في الإتصالات**"، المملكة المتحدة: مؤسسة هنداوي سي آي سي للنشر، 2017.

1-2- المذكرات والرسائل

1- أبو يعقوب، شدان، يعقوب، خليل. "**أثر مواقع التواصل الاجتماعي على الوعي السياسي بالقضية الفلسطينية لدى طلبة جامعة النجاح الوطنية**"، مذكرة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية المستدامة، (جامعة: النجاح الوطنية، كلية الدراسات العليا، 2015).

2- الجيش، محمد، إسماعيل، محمد. "**الأوضاع الداخلية في إسرائيل وأثرها على حرب 1967**"، مذكرة مقدمة لنيل شهادة الماجستير في التاريخ الحديث المعاصر، (الجامعة: الإسلامية،كلية الآداب، قسم التاريخ والآثار، 2008).

3- الدبس، معتز، سمير. " **التطورات الداخلية وأثرها على حركة المقاومة الإسلامية (حماس)، 2000-2009**"، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، (جامعة: الأزهر، كلية الاقتصاد والعلوم الإدارية، قسم العلوم السياسية، 2010).

4- الفاعوري، أحمد، عواد، نويران. **"التحولات الإقليمية العربية وأثرها على نظرية الأمن الإسرائيلي (2006-2012)"**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، (جامعة: الشرق الأوسط، كلية الآداب والعلوم، 2011).

5- باسط، سميرة. **"الإستراتيجية الجزائرية لمكافحة الإرهاب 1999-2014"**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، العلاقات الدولية، تخصص دارسات إستراتيجية وأمنية، (جامعة الجزائر: كلية العلوم السياسية والعلاقات الدولية، قسم الع-د، 2014).

6- بودن، زكرياء. **"أثر التهديدات الإرهابية في شمال مالي على الأمن الوطني الجزائري وإستراتيجيات مواجهتها 2010-2014"**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية، تخصص علاقات دولية ودراسات إستراتيجية، (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، 2015).

7- بوطويل، نسيمة. **"الإستراتيجية الأمنية الأمريكية في منطقة شمال شرق آسيا: دراسة لمرحلة ما بعد الحرب الباردة"**، رسالة مقدمة لنيل شهادة دكتوراه العلوم في العلوم السياسية تخصص علاقات دولية، (جامعة: الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، 2010).

8- جلعود، وليد، غسان، سعيد. **"دور الحرب الإلكترونية في الصراع العربي الإسرائيلي"**، مذكرة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية السياسية، (جامعة: النجاح الوطنية، كلية الدراسات العليا، 2013).

9- حمزاوي، جويدة. **"التصور الأمني الأوروبي: نحوبنية أمنية شاملة وهوية إستراتيجية في المتوسط"**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، تخصص دراسات مغاربية ومتوسطية في التعاون والأمن، (جامعة: الحاج لخضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية 2011).

10- خضير، أحمد، حامد، سليمان، **" دور إسرائيل والمتعاونين معها من الفلسطينيين في تمزيق النسيج السياسي للشعب الفلسطيني"**، مذكرة مقدمة لنيل شهادة الماجستير في التتخطيط والتنمية السياسية ، (جامعة: النجاح الوطنية، كلية الدراسات العليا، 2014).

11- خلف، نصر، الدين، ديب، سعد. **"دور المؤسسة العسكرية الإسرائيلية في صناعة القرار السياسي الخارجي (السلطة الفلسطينية ولبنان نموذجا) 2000-2009"**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية، (جامعة: الأزهر، كلية الاقتصاد والعلوم الإدارية، 2012).

12- دلة، أمينة، مصطفى. **"الدراسات الأمنية النقدية"**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية، تخصص دراسات إستراتيجية، (جامعة: الجزائر3، كلية العلوم السياسية والإعلام، قسم العلوم السياسية والعلاقات الدولية، 2013).

13- شقور، رفقة، نبيل، مطلق. **"أثر حزب الله في تطوير فكر المقاومة وأساليبها في المنطقة العربية"**، مذكرة مقدمة لنيل شهادة الماجستير في التخطيط والتنمية السياسية، (جامعة النجاح الوطنية بنابلس، فلسطين، كلية الدراسات العليا، 2009.

14- قاسيمي، صافية. **"الفضاء السيبراني والأغورا الإلكترونية –إشكالية خلق فضاء عمومي افتراضي حسب المنظور الهابرماسي"**، (جامعة: الجزائر 03، كلية الإعلام والاتصال، د س).

15- لبدي، حنان. **"التحولات الدولية الراهنة وتأثيرها على الإستراتيجية الأمنية في منطقة الساحل الإفريقي"**، مذكرة مقدمة لنيل شهادة الماجستير في العلوم السياسية والعلاقات الدولية، (جامعة: محمد خيضر، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، 2015).

16- ماضي،محمد، محمد. **"الأمن القومي الإسرائيلي وأثره على الأمن الفلسطيني (1948-2012)"**، بحث مقدم لاستكمال متطلبات الحصول على درجة الماجستير في القيادة والإدارة، (أكاديمية: الإدارة والسياسة للدراسات العليا، 2015).

17- جبر، دينا، محمد. **"الإستراتيجية النووية الإسرائيلية (الثوابت والمتغيرات)"**، (جامعة بغداد: كلية العلوم السياسية، د س) .

1-3- المجلات والمؤتمرات

1- أبو عامر، عدنان، عبد الرحمان، **مترجما**، **"إستراتيجية الجيش الإسرائيلي"**، إعداد: الجيش الإسرائيلي، العدد 79، بيروت: مركز الزيتونة للدراسات والإستشارات، 2015.

2- الزيدي، عبد الوهاب، محمود. **"التجسس الإسرائيلي الإلكتروني على الدول العربية"**، مركز الدراسات الإستراتيجية والدولية، العدد 58، (جامعة: بغداد).

3- العوادي، أوس، مجيد، غالب. **"الأمن المعلوماتي السيبراني"**، سلسلة إصدارات مركز البيان للدراسات والتخطيط، (أوت 2016).

4- الفتلاوي، أحمد، عيسى، نعمة. **"الهجمات السيبرانية:" مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم المعاصر"**، (بحث مقبول للنشر في مجلة المحقق الحلي، جامعة الكوفة،كلية القانون، 2016).

5- بن مرزوق، عنترة. **"الأمن السيبراني كبعد جديد من السياسة الدفاعية الجزائرية"**، (محاضرات مقدمة لطلبة جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، د س).

6- حبيب، محمد، بلال، أحمد، عايش. وأبوركبة، محمود، صلاح، جاد الله. **بحث بعنوان: الصراع النووي الإيراني الإسرائيلي: المخاطر والتحديات"**، (الجامعة: الإسلامية، كلية التجارة ، قسم الاقتصاد والعلوم الإنسانية، 2012).

7- حسن، فاروق، فؤاد. **" مدخل إلى أمن المعلومات وتعريف الجرائم الإلكترونية وكيفية الحماية والاستخدام الأمثل للموارد المتوفرة للوصول إلى أقصى درجات الحماية في دوائر وزارة الداخلية العراقية"**، (وزارة الداخلية: المديرية العامة للاتصالات والمعلوماتية، قسم التدريب والتطوير، شعبة الدراسات والبحوث، د س) .

8- خليفة، ايهاب. **"القوة الالكترونية وأبعاد التحول في خصائص القوة"**، مجلة أوراق، العدد 12، (2014).

9- د م. **"تحليل للتطورات السياسية والأمنية"**، مجلة باحث للدراسات الفلسطينية والإستراتيجية، العدد 28، (نوفمبر 2016).

10-د م: **"الخطوات العامة لسياسة المعلومات في إسرائيل**، (د م ن، د س ن).

11-ربيع، محمد، يحي. **"إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشر ق الأوسط: دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الانترنت (2002-2013)"**، رؤى إستراتيجية، (يونيو 2013).

12-صفاء، خليل، كاظم. **"البرنامج النووي الإسرائيلي، الدوافع، الاتجاهات، المضامين والسيناريوهات المستقبلية"**، مجلة جامعة جيهان- أربيل العلمية، المجلد1، العدد 01، (حزيران 2017).

13-طويلة، جميل، حسين. **"البرمجيات الخبيثة"**، (دليل عملي لاستخدام البرمجيات الخبيثة وبرمجيات التجسس وإجراءات الوقاية والحماية منها).

14-غودي، ميشال. والهمامي، قيس. **"الاستشراف الإستراتيجي والمشاكل والمناهج"**، مجلة ليبسور، ط6، (2005).

15-قادير، إسماعيل. "**إدارة الحروب النفسية في الفضاء الإلكتروني: الإستراتيجية الامريكية الجديدة في الشرق الاوسط**"، الندوة الدولية: عولمة الإعلام السياسي وتحديات الامن القومي للدول النامية، (جامعة: الجزائر 03، كلية العلوم السياسية والعلاقات الدولية، د س).

16-ليتيم، فتيحة. وليتيم، نادية. "**الأمن المعلوماتي للحوكمة الإلكترونية وإرهاب القرصنة**"، مجلة الفكر، العدد 12، (دش، دس).

17-وتد، نضال، محمد. "**جنود السايبر**"، مجلة الراصد للشؤون الصهيونية، مركز غزة للدراسات والإستراتيجيات، (فيفري 2017).

18- مختار، محمد. "**Cyber Security: هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية**"، مجلة مفاهيم المستقبل، العدد 06، (يناير 2015).

19- د م، "**السفارة الأمريكية مطالبة بتوضيح مصير الهاركر PX1**"، السلام، 22 أوت، 2015، العدد 1323، الجزائر.

1-4- المواقع الإلكترونية

أ- المواقع باللغة العربية

1- الدريبي، فهد. "**ما هو الأمن السيبراني**"، تم تصفح الموقع يوم : 21 فيفري 2018. الرابط:
Https://www.fadvisor.net/blog/2017/11/what is Cyber security/

2- الديماني، مصطفى. "**الحرب الإلكترونية على إسرائيل: الأبعاد والدلالات**"، تم تصفح الموقع يوم : 17 مارس 2018. الرابط:

www.m.ahewar.org/s.asp?aid:381345§r=0

3- الزبيدي، إيمان. "**سيمانتك تكشف عن خطر فيروس فليمر الذي يستهدف مناطق الشرق الأوسط**"، تم تصفح الموقع يوم : 13 أفريل 2018. الرابط:

http:/www.tech-wd.com/wd /2012/06/01/w32-flamer

4-اللواتي، نسرين، فوزي. "**الفيس بوك أداة إسرائيلية للتجسس والتجنيد والمراقبة**"، تم تصفح الموقع يوم : 13 مارس 2018. الرابط:

Aitmag-ahram.org.eg/News/2068.aspx

5-الموسوعة العربية. "**علم الحياة (الحيوان والنبات)، الاستقلالية**"، تم تصفح الموقع يوم : 03 فيفري 2018. الرابط:

http;//www.arab_ency.com/détails.php? Full=18nid=113

6- النجاي، بشير. "**مستقبل تأثير الإستراتيجية الأمنية الإسرائيلية على الأمن العربي الراهن**"، تم تصفح الموقع يوم : 02 مارس 2018. الرابط:

www.ahewar.org/s.asp?aid=578455&r=0&u=&i=o&q=

7- أوأرتيمة، أحمد. "**المؤسسات الأكاديمية : حول جامعات إسرائيل والمشروع الصهيوني**"، تم تصفح الموقع يوم : 24 مارس 2018. الرابط:

https://arabi21.com/story/903760

8- أندراوس، زهير. "**شعبة الاستخبارات العسكرية "أمان"**، تم تصفح الموقع يوم : 10 مارس 2018. الرابط:

Https://www.raialyoum.com/index.php

9- بكري، سعد، علي، الحاج. "**الأمن السيبراني ومعضلة حمايته**"، تم تصفح الموقع يوم : 03 فيفري 2018. الرابط:

www.aleqt.com/2017/08/24/article.1241506.html

10- جارش، عادل. "**مقاربة معرفية حول التهديدات الأمنية الجديدة**"، مجلة العلوم السياسية والقانونية، (فيفري2017)، تم تصفح الموقع يوم 25 فيفري 2018. الرابط:

democraticac.de/?p=43831

11- جابر، شيماء. "**الاختراق وطرق الحماية منه**"، تم تصفح الموقع يوم : 26 فيفري 2018. الرابط:

Https://download-internet-PDF-ebooks.com/4926.Free-book

12- حسن، إجلال، عبد اللطيف. "**تكوين وحدات جيش الدفاع الإسرائيلي**"، تم تصفح الموقع يوم : 12 مارس 2018. الرابط:

www.alhasahisa.net

13- حواس ،مؤنس. **"ماذا يتعلم الأطفال في إسرائيل"**، تم تصفح الموقع يوم : 24 مارس 2018. الرابط:

https://www.youtube.com/watch?v=yxt9TDBbhbI

14- خليفة، إيهاب. **"التطبيقات الأمنية لـــ"قوة الفضاء الالكتروني"**، تم تصفح الموقع يوم : 22 مارس 2018. الرابط:

https://futureuae.com/ar/Mainpage/Item/851/cyber-power

15- خليفة، إيهاب. **" ما هو فيروس ستاكسنت"**، تم تصفح الموقع يوم : 26 مارس 2018. الرابط:

Tewdg AA QBAJ&pg=PA11&lpg

16- دبوق، يحي. **"إيران تخترق الحواسيب الإسرائيلي: ضباط وخبراء وعلماء نوويون"**، تم تصفح الموقع يوم : 19 مارس 2018. الرابط:

al-akhbar.com

17- د م. **"النظام القانوني للأمن الوطني الإلكتروني في ظل الثورة الرقمية"**، تم تصفح الموقع يوم : 22 فيفري 2018. الرابط:

www.univ-chlef.dz/fdsp/images/PDF/JE-DROIT-2017.PDF

18- د م. **"الحرب الالكترونية تؤرق إسرائيل"، تقارير وحوارات"**، تم تصفح يوم: 18 مارس 2018. الرابط:

www.aljazeera.net/reports and interviews/.

19- د م. **"هكذا اخترقت حماس جيش الاحتلال الإسرائيلي"**، تم تصفح الموقع يوم : 19 مارس 2018. الرابط:

www.aljazira.net/encylopedia/military/15/01/2017

20- د م. **"ماذا تعرف عن الجيوش الالكترونية"**، تم تصفح الموقع يوم : 19 مارس 2018. الرابط:

http://www.aljazeera.net/encyclopedia/conceptsandterminology/2017/7/5/

21- د م. **"الجيش الالكتروني يخترق المدونة الدولية للجيش الإسرائيلي"**، تم تصفح الموقع يوم : 19 مارس 2018. الرابط:

http://www.almayadeen.net/news/604561

22- د م. "**أخطر الهاكرز العرب على المستوى العالمي**"، تم تصفح الموقع يوم : 19 مارس 2018. الرابط:

https://www.ta3allamdz.com/2015/09/blog-post.html

23- د م. "**البنك الإسرائيلي يؤكد اختراق 15000 بطاقة إتمان من قبل هاكر سعودي**، " تم تصفح الموقع يوم : 19 مارس 2018. الرابط:

http://www.alyaum.com/article/3039850

24- د م. "**إسرائيل تتعرض لهجوم إلكتروني واسع ومئات المواقع بدأت تتساقط**"، تم تصفح الموقع يوم : 21 مارس 2018. الرابط:

https://video.alwatanvoice.com

25- د م. "**الإعلام الإسرائيلي: بنية، أدوات، أساليب عمل**"، مركز المعلومات الوطني الفلسطيني، تم تصفح الموقع يوم : 24 مارس 2018، الرابط:

http://info.wafa.ps/atemplate.aspx?id=8788

26- د م. "**إسرائيلي يكشف تفاصيل الغارة على دير الزور**"، تم تصفح الموقع يوم : 26 مارس 2018. الرابط:

alakhbar.spiru.la/node/43031

27- زقاع، عادل، **مترجما** ، "**مفهوم الأمن في نظرية العلاقة الدولية**"، تم تصفح الموقع يوم : 17 فيفري 2018. الرابط:

Bohothe.blogspot.com/2010/03/blog-spot-26.html.

28- سعادة، حنان، علي. "**الأمن السيبراني والأمن المعلوماتي**"، تم تصفح الموقع يوم : 20 فيفري 2018. الرابط:

http://ae.linkedin.com/sulse/D8A7D984D8A7

29- شفيق، نوران. "**أشكال التهديدات الإلكترونية ومصادرها**"، تم تفحص الموقع يوم : 17 مارس 2018. الرابط:

http://www.europarabct.com/

30- صوافطة، أشرف. "**أثر البحث العلمي على صناعة القرار السياسي، إسرائيل نموذجا**"، تم تصفح الموقع يوم : 14 مارس 2018. الرابط:

Democraticac.de/?p=25826

31- علي، إلهام، محمد. "**التجسس الالكتروني: سلاح إسرائيل الذهبي لمراقبة العرب**"، تم تصفح الموقع يوم : 24 مارس 2018. الرابط:

https://www.noonpost.org/content/13821

32- عبد الصادق، عادل. "**المجال الأعلى للأمن السيبراني خطوة في دعم إستراتيجية الأمن القومي**"، تم تصفح الموقع يوم : 23 فيفري 2018. الرابط:

www.accronline.com/article-detal.aspx?!d=20284.

33- عوف، ميرفت. "**الحرب الالكترونية تتأجج بين إسرائيل والمقاومة الفلسطينية فمن الأقوى؟!**"، تم تصفح الموقع يوم : 19 مارس 2018. الرابط:

http :www.sasapost.com/electronic-warfare.resistance.israel

34- عبد الصادق، عادل. "**الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي**"، تم تصفح الموقع يوم : 21 مارس 2018. الرابط:

http://accronline.com/article_detail.aspx?id=28395

35- كردي، علي، محمد، إبراهيم. "**المفهوم العسكري للإستراتيجية والتطور التاريخي**"، تم تصفح الموقع يوم : 15 فيفري 2018. الرابط:

Renanaonline.com/users/alihordi/posts/352158

36- محمد، محسن، وتد. "**إسرائيل تسعى للريادة التكنولوجية بحلول 2024**"، تم تصفح الموقع يوم : 12 مارس 2018. الرابط:

https://www.aljazeera.net/news/SC

37- مؤيد، سامر. "**الإستراتيجية من منظور وظيفي إجرائي**"، تم تصفح الموقع يوم : 17 فيفري 2018. على الرابط:

Fcdrs.com/mag/issue-6-2.html

38- ناشف، نديم. " **شبكات التواصل الاجتماعي في خدمة الاحتلال**"، تم تصفح الموقع يوم : 27 مارس 2018. الرابط:

https://www.arab 48. com/

39- وني، وسيم. "**الإعلام ودوره بالصراع مع الاحتلال الإسرائيلي**"، تم تصفح الموقع يوم : 10 مارس 2018. الرابط:

www.pm-news.net/news.php?extend.6189.7

ب- المواقع باللغة الأجنبية

*1- **"Cyber Threat Basics, Type of Threat intelligence and best practices"**,Web Site Visited in : 25 Februay 2018. Link: https://www.secure works.com/Blog/Cuber-threat basics.*

*2- **"Cyber Threat"**, Web sit Visited in : 25 February 2018. Link: it law.Wikia.com/Cyber-threat*

*3- "**Electronics security**", Web Site Visited in: 22 Februay 2018. Link: https://www.the freedictionary.com/electronics+security "*

*4 -**The U.S. Israël Stratégie Partmership**",Web Sit Visited in :24 March 2018. Link : http://www.mepc.org/future-us-israel-strategic-partnership.*

*5- **What is Cyber Threat? how to Explain Cyber Threat your CEO, Blog featured Article. How-to-Guides?"** , Web Site Visited in : 25 Februay 2018. Link: https://www.threatconnect.com/blog/how-to-Explain-Whati-is-a Cyber-threat/*

*6- **"9900: the Israel Satellite intelligence unit"**, Web Visited in : 09 March 2018. Link: https://i-hls.com/archives/22809.*

2- المراجع باللغة الأجنبية

2-1- باللغة الفرنسية

1- Danino, Olivier. ***"l'economie de la cybersecurité en Israél ",*** *Chaire de cybersécurité, Saint-cyr,Sogeti, Thales, 2017.*

2- Denece, Eric. et Elraîm, David. ***"Les Service Secrets Israéliens: Aman, Mossad et Shin Beth",*** *Paris, Edition Tallandier, 2014.*

*3- "**Paysage de Cyber Security et Investissements, Israël 2016**" , Rapport sur l'industrie de la cyber sécurité, (Département de la recherche cyber D13, Janvier 2017).*

2-2- المراجع باللغة الإنجليزية

1- Abu Mualla , Said. ***"Palestinian-Israeli Cyber Conflict : An Analytical Study of the Israeli Propaganda on Face book, Adraei's page as an example",*** *journal of Arab American university, (Arabic language and Media Department, Faculty of Arts, November 2017).*

*2-**"Autism In the IDF: the Solidiers of Intelligence Unit 9900"**, Israel Katters Issue, Number 81, (June 2014).*

3- Bencsath, Boldizar. and others. ***" The Cousins of Stuxnet: Duqu,Flame and Gauss",*** *Journal future internet ,(Novembre 2012).*

4-Cohen, Matthew. and Friesisch, Charles. ***"Israel and Cyberspace - Unique Threat and response"****, (international Studies Perspectives, August 2016).*

5-Couriel, Deborah, Housen. ***" National Cyber Organisation :Israël",*** *(Nato Cooperative Cyber defence : Centre Of Exellence, Tallinn, Estonia, 2017).*

6-Craigen, Dan, &Others. ***"Defining Cybersecurity"****, (Technology innovation Management Review, Octobre 2014).*

*7-**"Cyber Security landscape and investment Israel, 2016"**, (Cyber DB research department, January 2017).*

8-Klein, Hadas. ***"Global Cyber. Biweekly Report",*** *(The institute for National Security Studies, July 2016).*

9-Mahmoud, Khalid, Walid. ***" Cyberattacks, The Electronic Battlefield "****, Doha : Arab centre for Research and policy Studies, 2013.*

10-Ouwendijk, Heno. ***"Cybersecrity and Hemeland Secrity in Israel ",*** *Rijks-dienst voor ondernement, Nederland, 2015.*

11-Rousseau, Peter. ***"the history and impact of unit 8200 on Israel Hi-Tech Entrepreneurship"****, (Athesis presented to the Homors tutorial college, Ohio university, 2017).*

12-Shkedi, Daniel. ***" The Cybersecurity Sector in Israel "****, (Embassy of India, Tel Aviv, commercial wing, 2015).*

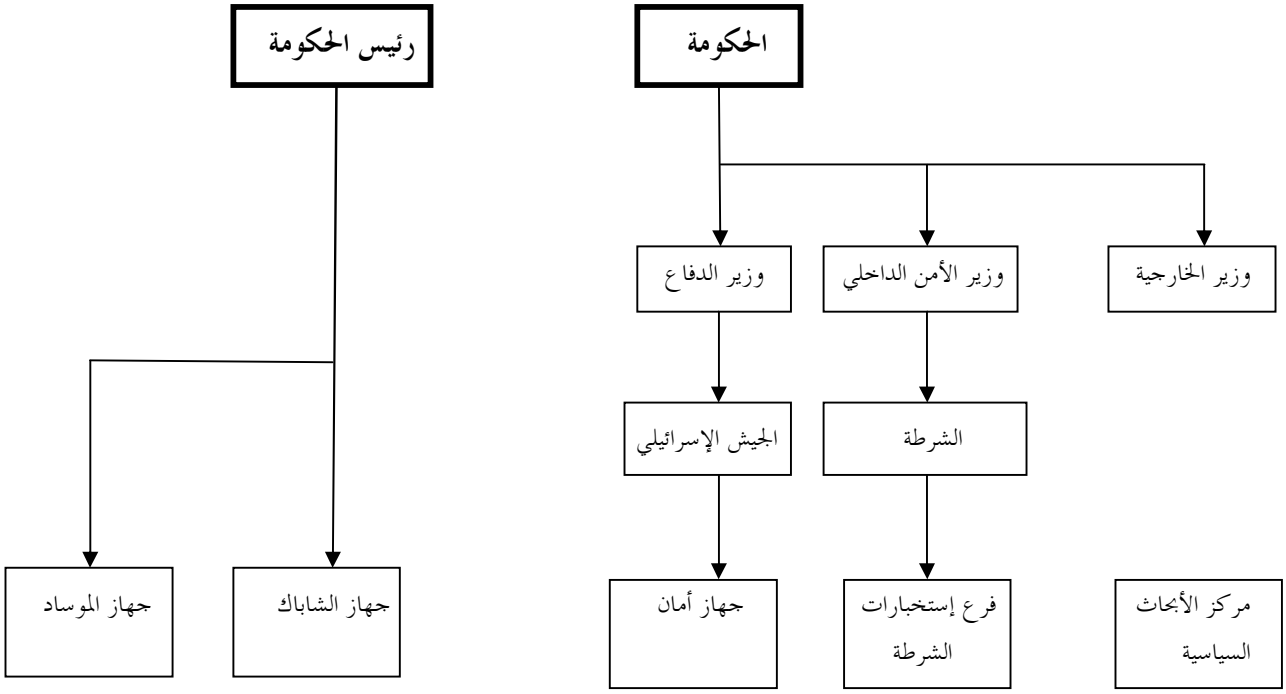
13-Taureck, Rita. ***"Securitization Theory and Securitization Studies"****, (university of institutional repository, 2006).*

14-Vaidya, Tavish. ***" Survey and*** **Analysis of Major** ***Cyberattacks : 2001-2013 "****, (Georgetown University, July 2015).*

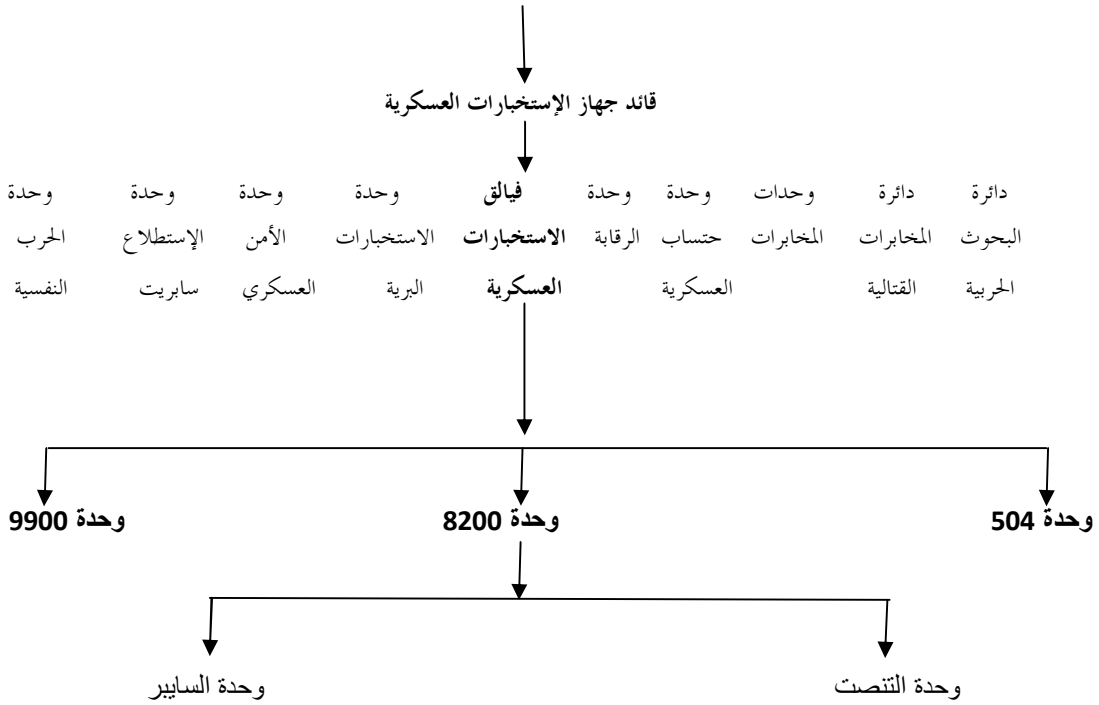
*15-"****Cyber Wellness Profile Isreal****", (ITU Statistics, Decembre 2013).*

الملاحق

الملحق رقم 01: بنية وتبعية أجهزة الإستخباراتية الإسرائيلية

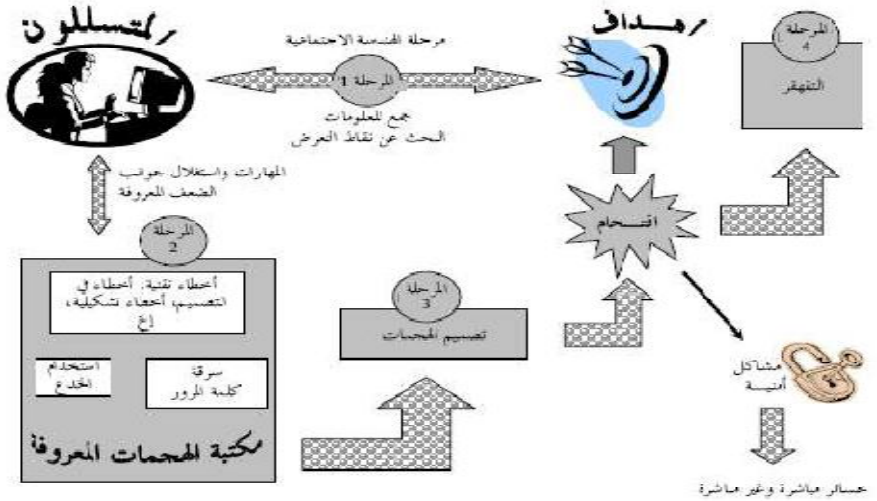


البناء التنظيمي لجهاز الإسنخبارات العسكرية "أمان".

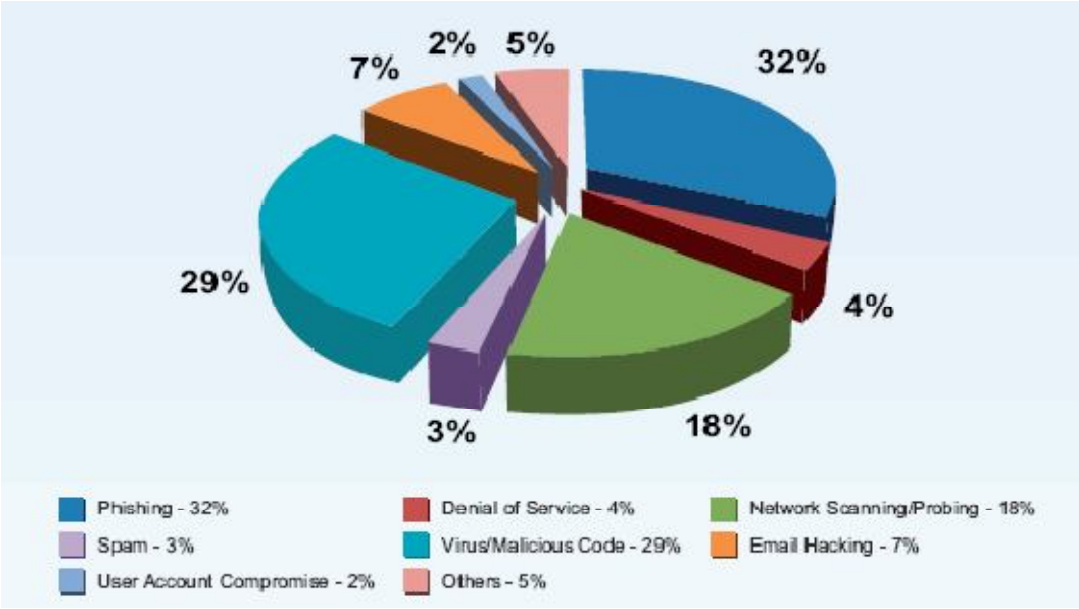


المصدر: منذر سلامة أبو سويرح، **مرجع سابق**، ص ص 103-104.

الملحق رقم 02: رسم توضيحي يمثل مراحل الهجمات السيبرانية



الملحق رقم 03: دائرة بيانية توضح نسب الهجمات السيبرانية على مستوى العالم



مخطط بياني يوضح نسب الهجمات السيبرانية على مستوى العالم

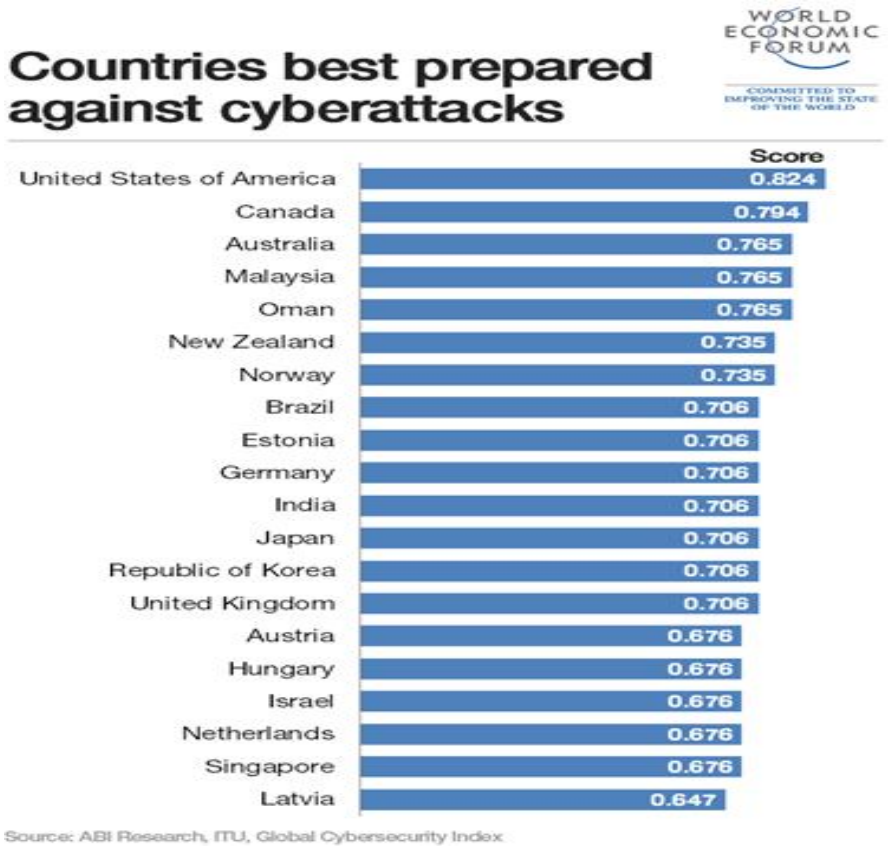
المصدر: أوس مجيد غالب العوادي، **مرجع سابق**، ص ص18-26.

الملحق رقم 04: جدول يوضح التوزيع العالمي لهجمات مواقع الإنترنت

الدول	الولايات المتحدة الأمريكية	الصين	المملكة المتحدة	إسرائيل	البرازيل	روسيا	أندونيسيا	ألمانيا	باكستان
مجموع الهجمات السيبرانية	%48,80	%20,98	%9,19	%2,15	%1,27	%0,97	%0,91	%0,84	%0,47

المصدر : http://democraticac.de/?p=30962

الملحق رقم 05: ترتيب أفضل الدول تأهبا للتهديدات السيبرانية



المصدر : http://resources.infosecinstitute.com/cyber-warfare-from-attribution-to-deterrence/

الملحق رقم 06: ترتيب إسرائيل في مؤشر الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية

الدولة	الرقم القياسي	الترتب العالمي
إسرائيل	**0,676**	**6**

الدولة	التدابير القانونية	التدابير التقنية	التدابير التنظيمية	بناء القدرات	التعاون	الرقم القياسي	الترتب الإقليمي
إسرائيل	**1,0000**	**0,6667**	**0,6250**	**0,7500**	**0,5000**	**0,6765**	**3**

المصدر : www.potomacinstitute.org/images/.../CyberReadiness_AR.pdf

الملحق رقم 07: ترتيب إسرائيل في مؤشر الأمن السيبراني

Global Rank	Score	Member State
Singapore	0.925	1
United States of America	0.919	2
Malaysia	0.893	3
Oman	0.871	4
Estonia	0.846	5
Mauritius	0.830	6
Australia	0.824	7
Georgia	0.819	8
France	0.819	8
Canada	0.818	9
Russian Federation	0.788	10
Japan	0.786	11
Norway	0.786	11
United Kingdom	0.783	12
Republic of Korea	0.782	13
Egypt	0.772	14
Netherlands	0.760	15
Finland	0.741	16
Sweden	0.733	17
Switzerland	0.727	18
New Zealand	0.718	19
Israel	0.691	20

المصدر : https://www.itu.int/dms_pub/itu.../D-STR-GCI.01-2017-PDF-E.pdf

الملحق رقم 08: ترتيب إسرائيل في قائمة الدول الأكثر إبتكارا في العالم

These are the world's most innovative countries

Based on Bloomberg's Innovation Index, 2018

	Country	Place change from 2017	Total score
1	South Korea	0	89.28
2	Sweden	0	84.70
3	Singapore	+3	83.05
4	Germany	-1	82.53
5	Switzerland	-1	82.34
6	Japan	+1	81.91
7	Finland	-2	81.46
8	Denmark	0	81.28
9	France	+2	80.75
10	Israel	0	80.64

Source: Bloomberg

المصدر: https://www.weforum.org/agenda/2018/02/

الملحق رقم 09: أفضل شركات التكنولوجيا العالية التقنية في إسرائيل

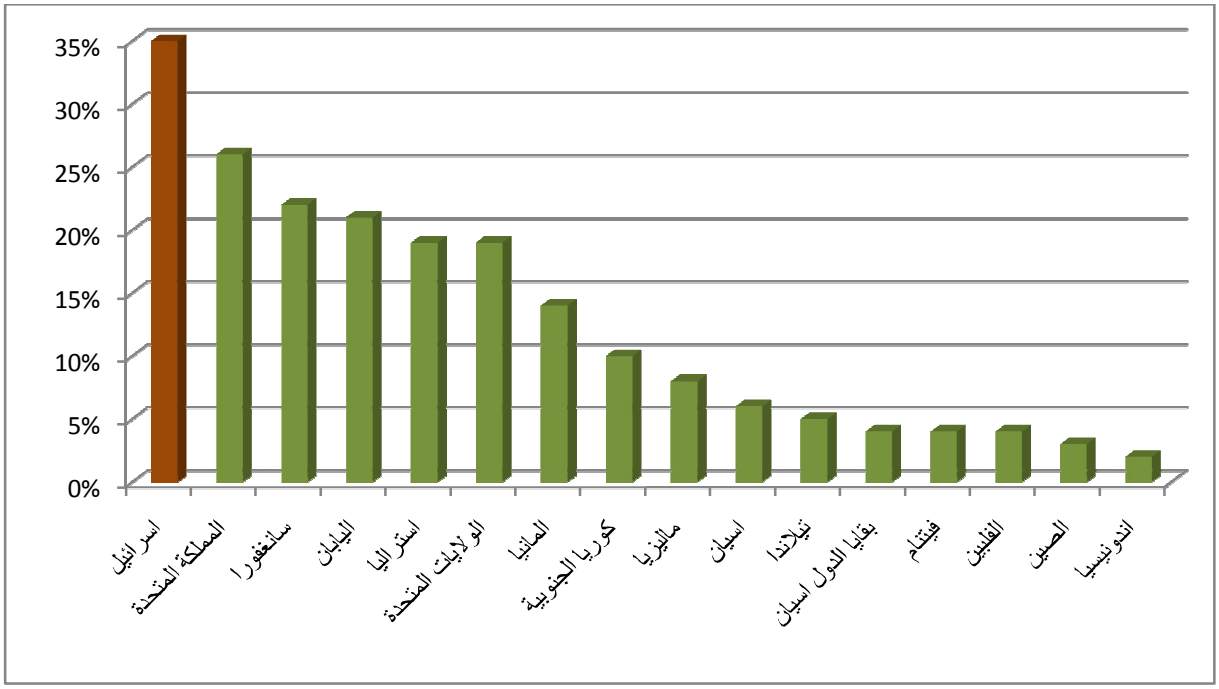
DUN'S100 2016

Best High Tech companies to work for

Rank 2016	Company
1	Google Israel
2	Facebook Israel
3	Intel
4	Apple Israel
5	Wix
6	Elbit Systems
7	HPE Israel
8	Microsoft Israel
9	I.A.I
10	Rafael
11	Amdocs
12	Ebay Israel
13	SimilarWeb
14	IBM Israel
15	Ironsource
16	Nova
17	Perion Network
18	Teva Pharmaceutical Industries
19	Outbrain
20	Mellanox Technologies
21	Panaya
22	Oracle Israel
23	Check Point Software
24	Taboola
25	Nice

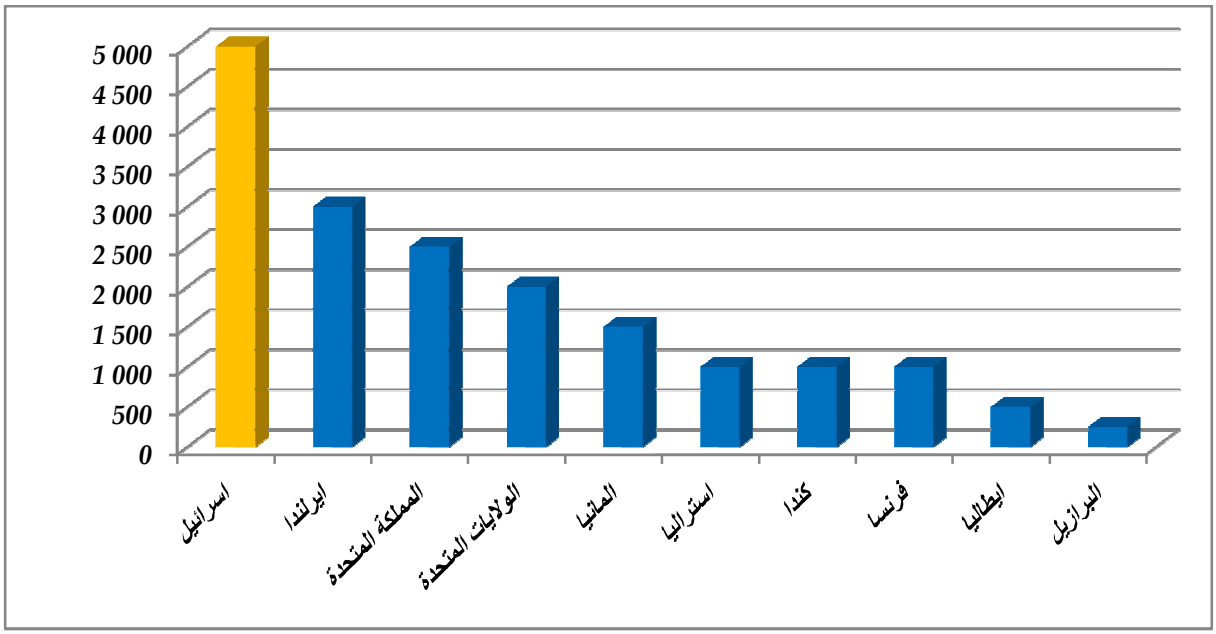
المصدر: https://www.similarweb.com/blog/best-private-company-in-israel

الملحق رقم 10: رسم بياني يوضح ترتيب إسرائيل في الاستثمار والإنفاق على الأمن السيبراني حسب تقرير الآسيان للأمن السيبراني



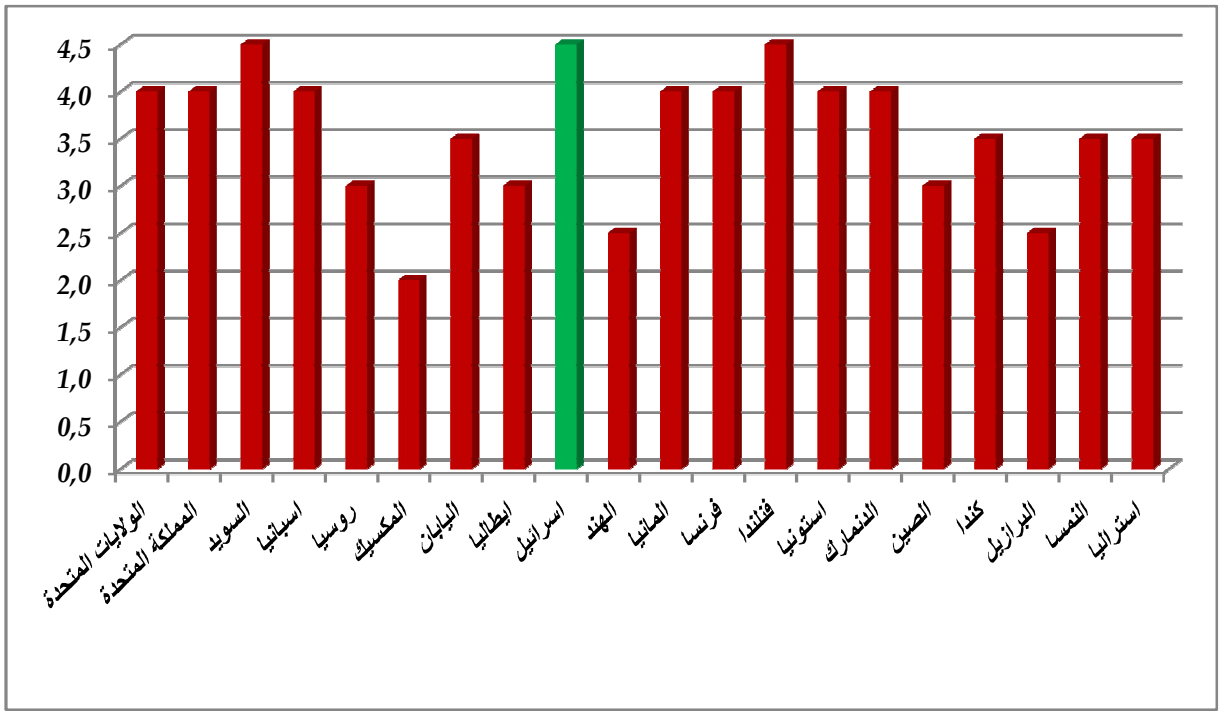
المصدر: http://www.businessinsider.sg/singapore-leads-asean-in-its-cyber-security-policies-but-the-region-needs-to-work-together-report/

الملحق رقم 11: رسم بياني يوضح ترتيب إسرائيل في طلب متخصصين في الأمن السيبراني



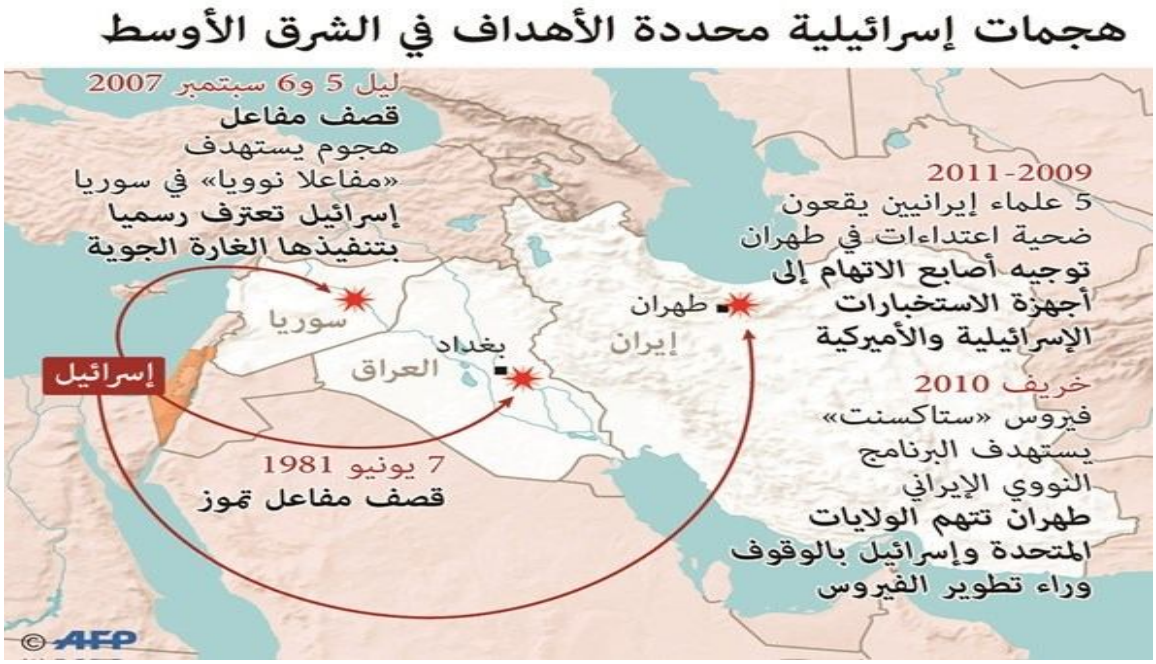
المصدر: https://www.cybintsolutions.com/category/cybint-news/cyber-intelligence/page/2/

الملحق رقم 12: رسم بياني يوضح تصنيف الدول بحسب قدرتها على الاستجابة لحالات الطوارئ السيبرانية



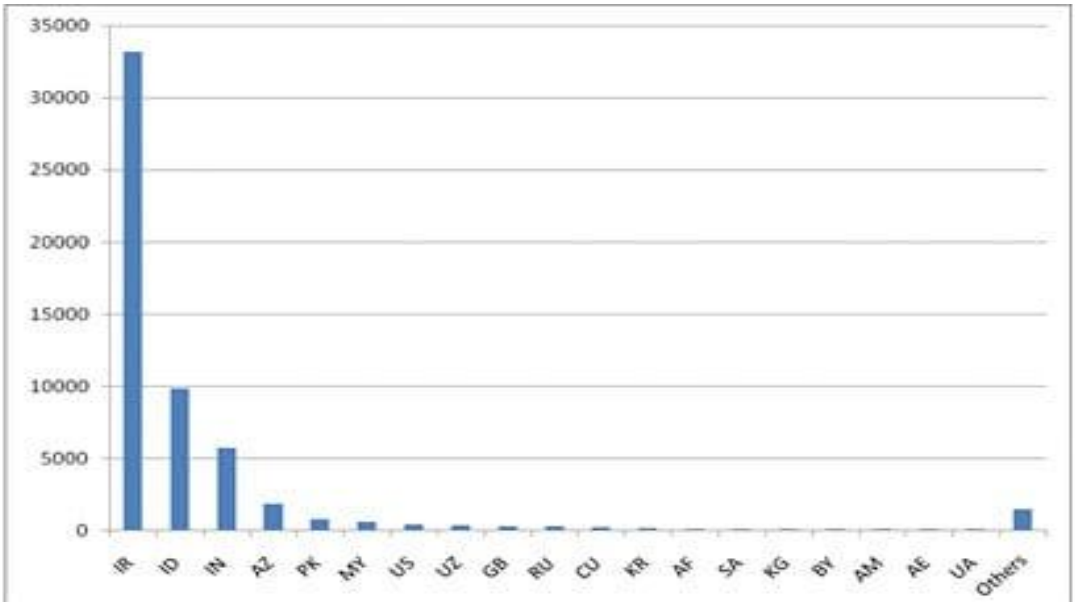
المصدر :ربيع محمد يحي، **مرجع سابق**، ص69 .

الملحق رقم 13: خريطة تبين أهم هجمات إسرائيل الإلكترونية في الشرق الأوسط



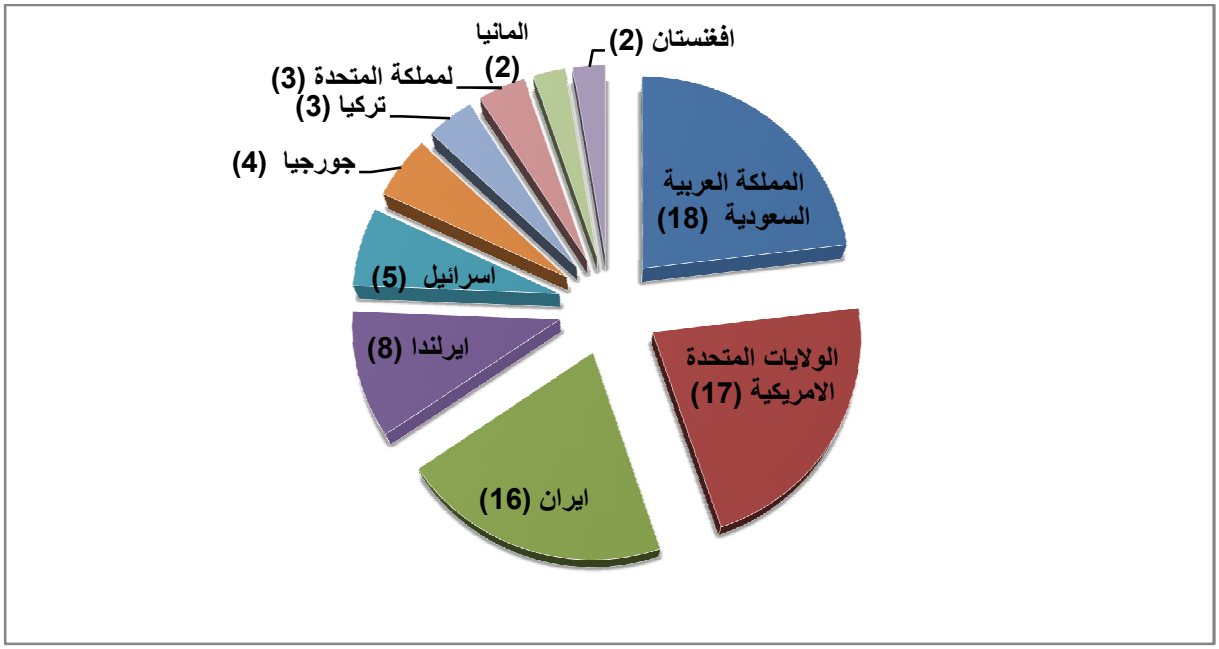
المصدر : http://www.alanba.com.kw/ar/arabic-international-news/syria-news/820409/22-03-

الملحق رقم 14: يوضح أهم أجهزة الكومبيوتر الإيرانية التي اخترقها فيروس "ستاكسنت"



المصدر: https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency

الملحق رقم 15: دائرة بيانية توضح توزيع الهجمات الإلكترونية ضد الأفراد في الدول



المصدر: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/