

التحديات السيبرانية وتأثيرها على أمن الدول:

" دراسة في استخدام الفضاء السيبراني ضد دول المواجهة: الكيان الصهيوني أنموذجا "

د. مكّي دراجي ود. الصادق جرایة

جامعة الوادي

ملخص:

بالرغم من التسهيلات التي أتاحتها ثورة التكنولوجيا والاتصال للأفراد والدول في شتى المجالات، إلا أنها أفرزت من جهة أخرى، جوانب سلبية تتعلق بتنامي التهديدات في الفضاء السيبراني التي تمس بشكل أساسي الأمن الوطني للدول، وتزداد هذه التهديدات خطورة في ظل وجود عدو يمتلك هذه التكنولوجيا ويطورها باستمرار، كحالة الكيان الصهيوني، الذي أصبح في السنوات الأخيرة يمزج في عقيدته الأمنية بين مفاهيم الحرب التقليدية والحرب الإلكترونية (الحرب الهجينة)، مما يمكن أن يؤثر كل ذلك بشكل سلبي على أمن دول المواجهة خاصة (إيران، فلسطين ولبنان) في فضاء لا تمتلك فيه معظم هذه الدول المقومات الكافية لحماية أمنها السيبراني.

الكلمات المفتاحية: التهديدات الأمنية، الأمن، الأمن السيبراني، الفضاء السيبراني.

Abstract

Despite the facilities provided by the technology and communication revolution for individuals and countries in various fields, it has also produced negative aspects related to the growth of threats in cyberspace that primarily affect the national security of countries. These threats become more dangerous in the presence of an enemy that possesses this technology and is constantly developing it, such as the case of the Zionist entity, which in recent years has begun to combine in its security doctrine the concepts of traditional warfare and electronic warfare (hybrid warfare), which could all negatively affect the security of the confrontation states, especially (Iran, Palestine and Lebanon) in a space where most of these countries do not have the sufficient capabilities to protect their cyber security.

Keywords: Security threats, Security, Cyber security, Cyberspace.

1. مقدمة:

يشهد العالم في الآونة الأخيرة اهتماما كبيرا بالحروب ذات الطابع الإلكتروني، ويعود ذلك إلى التقدم التكنولوجي السريع في مجال الاتصالات وتبادل المعلومات، الذي أدى إلى تزايد الاعتماد على البنية الرقمية والإنترنت في مختلف جوانب الحياة. كما يعد الفضاء السيبراني من البيئات الجديدة لمفهوم القوة والتعبير عنها، وهو من المفردات الحديثة المستخدمة في حقل العلاقات الدولية، كما أصبح يمثل أحد الفواعل الرئيسية في المجتمع الدولي في شقه الصراع، وتتميز هذه البيئة بتقنياتها ذات المستوى العالي غير المتوفرة عند جميع الفاعلين الدوليين، حيث تستخدمها الدول الكبرى بما يحقق لها بعض المكاسب الأمنية، وعليه دخل مصطلح الأمن السيبراني ضمن حسابات كثير من الدول، وذلك للحفاظ على أمنها الوطني، حيث تم الربط بين الفضاء السيبراني والأمن الوطني من خلال اعتماد كثير من الدول مبدأ الحكومة الإلكترونية، ونتيجة لذلك أصبح المحتوى المعلوماتي العسكري، الأمني، الفكري، السياسي، الاجتماعي والاقتصادي موجود في الفضاء السيبراني، مما عرض هذه الدول لخطر ما يعرف بالتهديدات السيبرانية.

أدرك الكيان الصهيوني منذ وقت مبكر أهمية الفضاء السيبراني في تحقيق التنمية والأهداف الإستراتيجية، للحفاظ على أمنه من جهة، ولفرض هيمنته وسيطرته على دول المواجهة من جهة أخرى، حيث يعود اهتمام الجيش الصهيوني بالمجال السيبراني إلى سنة 2009 حين اعتبره حيزا عملاقا جديدا ومهما، وفي سنة 2015 أعلن رئيس أركان الجيش الصهيوني تأسيس سلاح رابع إلى جانب سلاح الجو والبر والبحر وهو سلاح السيبر.

وعليه يمكن طرح الإشكالية التالية:

ما هو أثر التهديدات السيبرانية على أمن الدول؟ وكيف يستخدم الكيان الصهيوني الفضاء السيبراني للتأثير على دول المواجهة؟

أهمية الدراسة:

تكتسب هذه الدراسة أهميتها العلمية والعملية من خلال طبيعة الموضوع الذي تعالجه، باعتبار أن الأمن السيبراني تحول إلى ظاهرة حديثة في المجتمع الدولي، تحظى باهتمام أغلب دول العالم، فنحن نعيش الآن في ظل الثورة التكنولوجية، والتي لم تعد تأثيراتها إيجابية فقط، ولكن أضحت لها آثار سلبية جسيمة، أدت إلى انتهاء عصر احتكار القوة.

الحقل المعرفي للدراسة:

تندرج هذه الدراسة ضمن حقل الدراسات العلمية المختصة في مجال الأمن والدفاع، كون الأمن السيبراني أضحت من الأبعاد الأساسية والجديدة للأمن، بل أصبح ممارسة الدفاع عن أجهزة الكمبيوتر، والخوادم، والأجهزة المحمولة، والأنظمة الإلكترونية، والشبكات، والبيانات من الهجمات الخبيثة ضمن أولويات الدراسات الأمنية الحديثة، خاصة مع زيادة الخسائر الناتجة عن الهجمات الإلكترونية، وما يعنيه ذلك من تهديدات على الأمن الوطني للدول.

منهجية الدراسة:

استخدمت الدراسة منهجين أساسيين هما: المنهج التحليلي الذي يفسر العلاقة بين متغيرات الدراسة الرئيسية، ويربط بين مفاهيمها: التهديدات السيبرانية وأمن الدول، وتأثير التهديدات السيبرانية الصهيونية على أمن دول المواجهة، ومنهج دراسة الحالة الذي من خلاله تم تسليط الضوء على التهديدات السيبرانية الصهيونية على دول المواجهة (فلسطين، إيران، لبنان).

وللإجابة على الإشكالية الرئيسية المطروحة أعلاه، تم تقسيم الدراسة إلى المحاور الأساسية التالية:

المحور الأول: التطور المفهومي للأمن السيبراني.

المحور الثاني: تأثير الهجمات السيبرانية على الأمن الوطني للدول.

المحور الثالث: أثر التهديدات السيبرانية الصهيونية على دول المواجهة.

2. التطور المفهومي للأمن السيبراني:

شهد مفهوم الأمن إجمالاً عدة تطورات، على ضوء الأحداث المتسارعة التي شهدتها المجتمع الدولي والعلاقات الدولية في فترة الحرب الباردة، إلا أن مزيداً من التركيز أخذ يبرز بصورة أكثر وضوحاً بعد نهاية الحرب الباردة في العام 1990م، فقد كان لهذه التطورات انعكاسات وآثار واضحة على مفهوم الأمن بأبعاده ومستوياته المختلفة، علمياً وإقليمياً، عسكرياً واجتماعياً، اقتصادياً وسياسياً، وحتى ثقافياً، فقد تغير مفهوم الأمن التقليدي إلى مفهوم جديد متجاوزاً الأسس التي كان يقوم عليها، لا سيما القوة العسكرية في التعامل مع الأخطار والتحديات التي كانت تواجه الدول، وذلك عبر إدراك أهمية وضرورة التركيز على منظومة أمنية شاملة من شأنها حماية الدولة والأفراد من التهديدات المتعددة والمتنوعة.

1.2. المفهوم التقليدي والحديث للأمن:

يرجع مفهوم الأمن بجذوره التاريخية إلى القرن السابع عشر، خاصة بعد إبرام معاهدة الصلح "وستفاليا" عام 1648م التي أنهت الحروب الدينية في أوروبا، وأبرزت مفهوم الأمن القومي الذي يعرفه "تريجر" على أنه: (ذلك الجزء من سياسة الحكومة الذي يستهدف خلق الظروف المواتية لحماية القيم الحيوية) (عاشور، 2017)، كما ارتبط مفهوم الأمن ومنذ البداية بالقدرات والإمكانات العسكرية التي تحقق الردع، ومن ثم الأمن، إذ يعرفه على هذا الأساس "والتر ليبمان" في قوله: (أن الأمة تبقى في وضع آمن إلى الحد الذي لا تكون فيه عرضة للتضحية بالقيم الأساسية، إذا كانت ترغب بتفادي وقوع الحرب، وتبقى قادرة على صون هذه القيم عن طريق انتصارها في الحرب) (الصادق، 2022، الصفحات 09-10).

إن تطور مفهوم الأمن ارتبط بشكل وثيق بتطور أبعاده، ففضلاً عن البعد العسكري الذي يهتم بضرورة تعزيز القدرات العسكرية للدولة كمّاً وكيفاً، هناك أبعاداً أخرى أضفت الطابع الحديث لمفهوم الأمن وهي:

أ- **البعد الاقتصادي:** يعنى البعد الاقتصادي للأمن بتطوير اقتصاد الدولة في شتى القطاعات، حتى لا تكون تابعة لدولة أخرى تهيمن عليها، والأمن من المنظور الاقتصادي يعني التنمية والازدهار واستقرار الاقتصاد والاكتفاء الذاتي والرفاهية (المطيري، صفحة 42).

ب- **البعد السياسي:** ومن متطلبات تحقيق هذا البعد على المستوى المحلي، هو تحقيق الاستقرار السياسي على مستوى الجبهة الاجتماعية والمؤسسات السياسية للدولة، أما على المستوى الخارجي فيعني قدرة على الاندماج في النسق الدولي لتحقيق أهدافها الوطنية من خلال سياستها الخارجية (نجيدة، 2023، صفحة 13).

ت- **البعد الاجتماعي:** المقصود بالأمن في بعده الاجتماعي كونه الحالة التي يكون فيها الإنسان محمياً ضد- أو بعيد عن- خطر يتهدهده، ويتمثل في حالة الهدوء والاستقرار والوثام والاتفاق والانسجام داخل المجتمع الإنساني، وفي العلاقة بين شرائحه وأفراده وقواه المتعددة والمختلفة، كما أن أسوء ما يمكن أن يشعر به الإنسان هو الخوف على نفسه أو ماله أو عرضه من داخل مجتمعه، خاصة في ظل التزايد الكبير للجريمة بشتى أنواعها (الصادق، 2022، صفحة 20).

ث- **البعد الثقافي:** والمقصود بالأمن في بعده الثقافي، قدرة الدولة على توفير الحماية المطلوبة للثقافة بهدف تحقيق حرية الإبداع من جهة، والحفاظ على مكتسبات الشعوب الثقافية والفنية والدينية من جهة أخرى (كوش، 2002، صفحة 22).

ج- **البعد البيئي:** يتركز الأمن في بعده البيئي على ضرورة حماية البيئة والموارد الطبيعية من النضوب والانقراض، والنقص الناجم من المخاطر والملوثات والجرائم المعتمدة التي ترتكب في حق تنمية المصادر والموارد الطبيعية والإخلال بالتوازن البيئي (المشعل، 2011، صفحة 01).

ح- **البعد السيبراني:** يعد هذا البعد من أحدث أبعاد الأمن، فالتطور التكنولوجي الهائل في العصر الراهن أصبح مصدر خطر على الأمن الوطني للدول خاصة مع انتشار الهجمات السيبرانية، ونتيجة لهذه الأخطار الإلكترونية المتصاعدة بدأت الدول في الاهتمام بأمنها الإلكتروني وصار واحداً من أهم أبعاد الأمن.

2.2. مفهوم الأمن السيبراني:

يعتبر الأمن السيبراني من أكثر التحديات خطورة على الدول في القرن الـ 21، خاصة بعدما أصبحت الحدود الجغرافية والسيادة الوطنية على المحك جراء الثورة الهائلة في تكنولوجيا المعلومات والاتصالات، التي سهلت في شقها السلبي من عمليات نصب والاحتيال، التخطيط للعمليات الإرهابية، قرصنة المؤسسات الاقتصادية والتجارية، نشر

الفكر المتطرف من خلال وسائل التواصل الاجتماعي المتعددة، وكلها جرائم ذات بعد إلكتروني أصبحت تمس بشكل عميق مقومات وأسس الأمن الوطني للدول.

1.2.2. تعريف الأمن السيبراني:

يرجع أصل كلمة "ساير" "Cyber" إلى اللفظ اليوناني الأصل المشتق من كلمة "kybernetes" والذي يعني الشخص الذي يدير دفة السفينة، حيث تستخدم مجازا للتعبير عن المتحكم (مني، 2017، صفحة 32). ويعرف "الاتحاد الدولي للاتصالات الأمن السيبراني" على أنه: مجموعة من المهمات، مثل تجميع وسائل، وسياسات، وإجراءات أمنة، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية والمؤسسات والمستخدمين. كما يعرف بأنه مجموعة الأدوات والسياسات، والمفاهيم الأمنية والضمانات الأمنية، والمبادئ التوجيهية ونهج إدارة المخاطر، والإجراءات والتدريب، وأفضل الممارسات وسبل الضمان والتكنولوجيات، التي يمكن استخدامها جميعا في حماية البيئة السيبرانية (الاتحاد الدولي للاتصالات ITU، 2010، صفحة 01).

وقد عرف NIST الأمن السيبراني على أنه: حماية الأصول المعلوماتية من خلال معالجة التهديدات التي تتعرض لها المعلومات، التي يتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات (national institute of standards and technology, 2018).

ويعرف الأمن السيبراني أيضا، على أنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنية 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 (الهيئة الوطنية للأمن السيبراني، 2022، صفحة 03).

ويرتبط الأمن السيبراني بشكل وثيق بمفهوم القوة السيبرانية، التي تعني القدرة على القيام بنشاط سيبراني مؤثر في الفضاء السيبراني، أو القدرة على استخدام الفضاء السيبراني لتحقيق مجموعة من الأهداف، والتأثير على الأحداث، وتعرف أيضا على أنها الموارد البشرية والمادية المتاحة ضمن بيئة استراتيجية يمكن استخدامها لإحداث تأثير في هذا الفضاء الإلكتروني.

2.2.2. مقومات الأمن السيبراني:

لكي يتجسد الأمن السيبراني لا بد من توفر مجموعة من الشروط والعناصر، يكمل بعضها البعض في الوظائف والأدوار، ومن أهم هذه العناصر نذكر ما يلي:

أ- أساسيات الأمان: ويقوم هذا العنصر على ما يلي: (الهيئة الوطنية للأمن السيبراني، 2022، الصفحات 5-7)

- **السرية:** هي الحفاظ على خصوصية البيانات ومنع الإفصاح عنها للأشخاص غير المصرح لهم، ويتم عن طريق حماية البيانات والخصوصية، التحكم بالوصول إلى المعلومات.
 - **السلامة:** وتعني دقة وتطابق البيانات في كل مراحلها من تخزين واسترجاع ونقل، وأن يتم التعديل عليها من قبل الأشخاص المصرح لهم.
 - **توفر البيانات:** وتعني ضرورة توفر المعلومات بشكل دقيق، بالإضافة لاكتشاف ضعف وبطء النظام عند حدوثه، وبالتالي العمل على تخفيف الضغط على النظام.
 - **الهوية الشخصية:** وهي كل ما يدل على يخص بعينه، حيث هناك نوعين من الهوية الشخصية: (الهوية الحقيقية، الهوية الإلكترونية).
 - **الأثر الرقمي:** وهي البيانات التي تدل على الشخص إما بشكل مباشر أو غير مباشر.
 - **ملفات الارتباط (Cookies):** هي ملفات برمجية نصية صغيرة جدا تخزن في جهاز المستخدم عند زيارته لموقع ما بحيث تسهل عملية تصفح المواقع وتعتبر هذه الملفات نصية غير تنفيذية لذلك التصنيف ولا تعامل على أنها برامج خبيثة بالرغم من أنها أول ما يتم سرقة من قبل المخترقين لمعرفة حساباتك وكلمات المرور الخاصة بك.
 - **حالات المعلومات:** وتعني التأكد من حالة المعلومات المخزنة والبيانات المعالجة والمنقولة.
 - **الاحتياطات:** للحفاظ على الأمن السيبراني يجب أخذ جملة من الاحتياطات منها (الهيئة الوطنية للأمن السيبراني، 2018، صفحة 18):
 - تطوير واعتماد برامج للتوعية بالأمن السيبراني من خلال قنوات متعددة دوريا، من أجل تعزيز الوعي بالأمن السيبراني، تهديداته ومخاطره، وبناء ثقافة إيجابية حوله.
 - التعامل الآمن مع خدمات البريد الإلكتروني خصوصا مع رسائل التصيد الإلكتروني.
 - التعامل الآمن مع الأجهزة المحمولة ووسائل التخزين.
 - التعامل الآمن مع خدمات تصفح الإنترنت.
 - التعامل الآمن مع وسائل التواصل الاجتماعي.
3. تأثير الهجمات السيبرانية على الأمن الوطني للدول.

تطورت التهديدات والجرائم السيبرانية الموازية مع التطور الكبير والمتسارع الذي لقطاع الخدمات الإلكترونية، حيث بدأت هذه التهديدات بجرائم سيبرانية يقوم بها أفراد ومنظمات إجرامية، كالاختراق والتجسس وسرقة الأموال، وتطورت إلى تخويف وابتزاز المجتمعات وإرهابهم عن طريق الانترنت، لتصل إلى أخطر أنواع الصراع بين الدول وتهديد أمنها القومي، حيث ظهر هذا جليا في استعمال الأسلحة السيبرانية عالية التأثير في شن حروب سيبرانية مدمرة.

1.3. أشكال التهديدات السيبرانية.

بداية، تجدر الإشارة إلى أن المقصود بالهجوم السيبراني هو ذلك الفعل الذي يقوض قدرات ووظائف شبكات الحاسوب، من أجل تحقيق هدف سياسي أو قومي. يمكن المهاجم من خرق الأنظمة والعبث بها، حيث تكون له القدرة على إغلاق أنظمة الدفاع الجوية وشبكات الكهرباء التي تهدد الأمن القومي، كما أنه هجوم يشنه المهاجمون بمساعدة أجهزة الكمبيوتر أو الشبكات المخترقة يمكن أن يؤثر على النظام ويسرق البيانات (سالم، 2022، صفحة 72)، والتهديدات السيبرانية بشكل عام هي كل هجوم ضار يهدف الوصول بشكل غير قانوني إلى بيانات معينة، أو يعمل على تعطيل العمليات الرقمية أو إتلاف المعلومات.

ويمكن حصر أشكال التهديدات السيبرانية فيما يلي:

أ- الإرهاب السيبراني:

يعرف "جيمس لويس" الإرهاب السيبراني على أنه: (استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل: الطاقة والنقل والعمليات الحكومية، أو بهدف تهريب حكومة ما أو مدنيين) (A.Lewis, 2002, p. 51)، وهو ذلك الهجوم غير المشروع، أو التهديد بالهجوم المنظم من طرف الجماعات الإرهابية باستخدام الوسائل الإلكترونية على البنى التحتية وأنظمة المعلومات والشبكات وأجهزة الكمبيوتر، بدوافع سياسية أو دينية وعقائدية، يهدف إلى التخريب وتدمير البنية التحتية، من خلال العديد من الطرق، منها: اختراق أنظمة الكمبيوتر، نشر الفيروسات أو تعطيل الأنظمة الإلكترونية (حامد، 2024، صفحة 268).

ب- الحروب السيبرانية:

تتميز الحرب السيبرانية عن الحرب التقليدية، في أن المفهوم التقليدي للحرب، ينطوي على استخدام الجيوش النظامية ويسبقها إعلان واضح لحالة الحرب وميدان قتال محدد، بينما تبدو هجمات الفضاء الإلكتروني غير محددة المجال وغامضة الأهداف، كونها تتحرك عبر شبكات المعلومات والاتصالات العابرة للحدود الدولية، إضافة إلى اعتمادها ما يمكن وصفه بأسلحة إلكترونية جديدة تلائم طبيعة السباق الإلكتروني لعصر المعلومات، حيث يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات، وعليه فإن أحد معايير التمييز بين الحرب السيبرانية والحرب التقليدية يمكن أن يكون بالاستناد إلى طبيعة السلاح المستخدم، وبالتالي يمكن القول أن الحرب السيبرانية هي الحرب التي تستخدم فيها الأسلحة غير التقليدية وفقا لآثار المترتبة على استخدام هكذا نوع من الأسلحة والمتمثلة بالتدمير واسع النطاق (سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، 2018، صفحة 83).

وعليه، يطلق على الحروب السيبرانية بالحروب الذكية، وهي أقوى من أي هجوم بري أو جوي، وأكثر ذكاء وأقل تكلفة، فهي لا تحتاج إلى معدات حربية ولا جنود، لكنها تحتاج إلى قدرات علمية عالية، فهي تتضمن كل هجوم

افتراضي يجري بدوافع سياسية على أجهزة العدو الإلكترونية وشبكات الإنترنت وأنظمة المعلومات الخاصة به، لتعطيل منظوماته المالية وأنظمته الإدارية، وذلك من خلال سرقة قواعد معلوماته السرية أو تعديلها لتقويض الشبكات العنكبوتية والمواقع ونظام الخدمات.

ت- القرصنة الإلكترونية:

تتضمن القرصنة الإلكترونية عمليات الاختراق والتجسس، فالاختراق بشكل عام يعني القدرة لهدف معين والدخول على الأجهزة بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بها بهدف التطفل على خصوصيات الآخرين وإلحاق الضرر بهم (الحمداني، 2014، صفحة 13)، والتجسس الإلكتروني هو الدخول إلى شبكة المعلومات أو نظام المعلومات للحصول على محتوى إلكتروني غير متاح للجمهور بمس الأمن الوطني للدولة أو علاقاتها الخارجية، أو السلامة العامة أو الاقتصاد الوطني (العدوان، 2019، صفحة 469).

ث- الخداع الإلكتروني:

ويشتمل هذا السلاح الرقمي على عدة وسائل، كالتقليد الصوتي، التشويش الإلكتروني، الخداع ونشر الشائعات، انتحال الشخصيات افتراضيا، الابتزاز الإلكتروني (حامد، 2024، صفحة 269).

خ- هجمات الحرمان من الخدمة:

إن الهدف من هجمات الحرمان من الخدمة هو إجبار النظام الإلكتروني المستهدف على الاستجابة لعدد كبير من الطلبات والأوامر الخدمية بشكل يفوق قدرته، مما يعوقه عن تقديم الخدمات المطلوب منه تقديمها. غير أن هذه الهجمات تعد تقليدية نوعا ما، إذ قد لا تستطيع إحداث تأثير كبير في الأنظمة أو المواقع المجهزة للاستجابة لكم ضخم من الأوامر، مما يستدعي شكلا أكثر تعقيدا من هذه الهجمات، وهو ما يعرف بهجمات الحرمان من الخدمة الموزعة. في هذا النوع من الهجمات يتم إصدار كم هائل من طلبات الخدمة من قبل عدد كبير من الأجهزة الإلكترونية -وليس جهازا واحدا فقط كما هو الحال في هجمات الحرمان من الخدمة التقليدية -حتى تغرق جهاز الخصم بالأوامر، حيث تتوقف قدرته عن العمل، وتتم هذه الهجمات من خلال القيام أولا باختراق مجموعة كبيرة من أجهزة الحاسب الآلي، وتحميل برامج عليها لئتم استخدامها لاحقا في شن هجوم على الخصم بشكل متزامن، من خلال إرسال إشارة بدء إلى هذه البرامج الموجودة على كافة الأجهزة التي تم اختراقها (al, 2001, p. 37).

2.3. انعكاسات التهديدات السيبرانية على الأمن الوطني للدول:

يعتبر الفضاء السيبراني ميدان المعركة الرئيسي لما يطلق عليه بـ "الجيش السيبراني"، ولكنه ليس الميدان الوحيد، فكما تقاوت القوات المسلحة في الميادين الأربعة التقليدية: الأرض والبحر والجو والفضاء الخارجي، فإن الجيش السيبراني تقاوت في جميع الميادين مشتركة، إلى جانب قتالها في الميدان الخامس الافتراضي وهو الفضاء السيبراني (خليفة، تهديدات

الأمن الإقليمي العربي في الميدان الخامس: نحو إستراتيجية للحماية، 2021، صفحة 03). ومن هنا تظهر خطورة التهديدات السيبرانية على الأمن الوطني للدول كونها وتهديدات ذكية وشاملة لشتى الميادين والمجالات، وعليه يمكن تقسيم مستويات التهديدات السيبرانية لأمن الدول إلى ما يلي:

أ- المستوى العسكري والأمني:

سببت الحروب السيبرانية العديد من المخاطر والتهديدات على الأمن الوطني للدول، سواء من خلال أساليب عملها مثل التجسس الإلكتروني والهجوم الإلكتروني أو من خلال النتائج المادية التي تخلفها، فعلى المستوى العسكري أدت الحروب إلى تصاعد المخاطر السيبرانية خاصة مع قابلية المنشآت الحيوية في الدولة للهجوم، وبالتالي التأثير في وظائف تلك المنشآت والتحكم في تنفيذ هذه الهجمات يعد أداة استراتيجية، كما لعبت الحروب السيبرانية دورا هام في عسكرة الفضاء الإلكتروني، وبالتالي تصاعدت القدرات في سباق التسلح السيبراني، وتبني سياسات دفاعية سيبرانية في مجال تطوير أدوات الحرب الإلكترونية داخل الجيوش الحديثة، عملت الحروب الإلكترونية على اختراق المخططات العسكرية للدولة، مما ساعد على التعرف على طبيعة القوة العسكرية للدولة وتكتيكها العسكري، وبالتالي ذلك يساعد على التحكم في مواجهة الدول المستهدفة سواء في ميدان الحرب التقليدي أو في الفضاء الإلكتروني (إبراهيم، 2023).

ومن أمثلة ذلك، العديد من الهجمات الإلكترونية التي شهدتها السنوات الماضية على بعض البنى التحتية الحرجة والمؤسسات العسكرية، مثل محطات الطاقة النووية، كما في قيام فيروس "ستاكسنت" بتعطيل حوالي ألف من أجهزة الطرد المركزي في منشأة لتخصيب اليورانيوم في "ناتانز" في وسط إيران في عام 2010، فضلا عن تعرض أنظمة الكمبيوتر لشركة كوريا الجنوبية للطاقة المائية والنووية التي تديرها الدولة لهجمات إلكترونية في ديسمبر 2014، واتهمت الولايات المتحدة الأمريكية روسيا بالتورط في شن هجمات إلكترونية على شبكات كمبيوتر في عدة محطات طاقة نووية (خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية، 2017، صفحة 56، 57).

ب- المستوى الاقتصادي:

بالرغم من أن التكنولوجيا والابتكار تعد من الركائز الأساسية للاقتصاد، ووسيلة متاحة لمواجهة العديد من المصاعب والتحديات الاقتصادية، بل سهلت الحصول على الخدمات وتخفيض كلفتها، إلا أن ذلك ترافق مع ارتفاع التهديدات الناجمة عن محاولات اختراق الأنظمة الإلكترونية بهدف الاستيلاء على البيانات أو تعطيل الخدمات أو الابتزاز المالي، مما يتسبب كل ذلك في الإضرار بالإنتاجية، والمساس بصناعة المؤسسات الاقتصادية وفقدان ثقة المتعاملين.

ومن أبرز الأمثلة عن التهديدات السيبرانية في المجال الاقتصادي ما تعرضت له عدة شركات اقتصادية من هجمات سيبرانية استهدفت بياناتها عبر أسلوب الاختراق، ومن ذلك ما تعرضت له "شركة EBAY" الأمريكية من

سرقه لـ 140 مليون دولار من حسابها المصرفي، كذلك الهجوم السيبراني الكبير الذي تعرضت له شركة الطيران البريطانية سنة 2018 الذي أدى إلى تدهور قيمة أسهم الشركة المسيرة في البورصة (دراعو، 2022، صفحة 116).

ت- المستوى السياسي:

لا يقتصر تأثير التهديدات السيبرانية على البنى التحتية العسكرية والاقتصادية فقط، بل يتعدى ذلك ليشمل المجالات السياسية من خلال عمليات الاختراق والتجسس التي تطل أجهزة ومؤسسات سياسية حكومية، والحصول على معلومات وبيانات رسمية واستخدامها بغرض الضغط على الدول وابتزازها، أو من خلال استخدام تقنيات الهندسة الاجتماعية وبث الإشاعات لتأليب الرأي العام وزعزعة الاستقرار داخل الدولة.

وقد خلفت الهجمات السيبرانية آثار كبيرة على البنية المجتمعية والسياسية للعديد من دول العالم، بل استطاعت هذه العمليات تقسيم الدول مذهبيا وطائفيا وعرقيا، وذلك من أجل تحقيق هدف هذه الظاهرة المتمثلة بضرب المؤسسات والأفراد لتهديد الأمن الاجتماعي والسياسي للدولة، حيث أخذت الدول على عاتقها القيام بما هو ممكن من أجل تحقيق السلام والاستقرار داخل مجتمعاتها، من خلال الدعوة إلى ضرورة مواجهة التهديدات السيبرانية، الأمر الذي يستدعي ضرورة العمل على تنسيق الجهود المشتركة بين الدول، من أجل مكافحة التهديدات السيبرانية من خلال قاعدة معلومات وبرامج عمل مشتركة للقضاء عليها، عبر محاربة الفكر المتطرف الذي اخذ ينتشر، والعمل على تحقيق أكبر قدر ممكن من التعاون الدولي لحصر هذه الظاهرة والحد من انتشارها، ومن ثم إعادة نشر السلام والمحافظة على الأمن والسلم الدوليين والاستقرار في المجتمع الدولي (يوسف، 2013، صفحة 53).

ومن أمثلة التهديدات السيبرانية في هذا الجانب، ما تعرضت له جمهورية استونيا عام 2007 من هجوم سيبراني مستقل بذاته موجه من روسيا الاتحادية، وذلك عن طريق إغراق المواقع الالكترونية بسيل من البيانات غير اللازمة، حيث وجهت ما يقارب من مليون حاسبة من عدة نقاط في العالم، واستهدفت المواقع الحكومية والصحف والجامعات والمستشفيات والمصارف وخدمات الإطفاء و الإسعاف، وذلك بمهدف إسقاط وشل الحكومة الإستونية (سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، 2018، الصفحات 88-89)، ومن ذلك أيضا، التدخل السيبراني الروسي في الانتخابات الأمريكية لسنة 2016، من خلال استخدام تقنيات الهندسة الاجتماعية وهجمات التصيد بالرمح، في محاولة للتأثير على مجريات العملية الانتخابية في الولايات المتحدة الأمريكية (عنان، 2024).

ث- المستوى الفكري والثقافي:

وتؤثر الهجمات السيبرانية في هذا المجال في ما يطلق عليه بالغزو الثقافي أو الفكري، ومثل هذه العمليات تهدف إلى سلخ الخصم عن هويته من خلال التسلل لأفكاره عن طريق إرسال رسائل لاستدراجه للوصول للنتيجة المطلوبة، وهي

تطبيع هوية الخصم على طبع المهاجم، وتتم بأشكال مختلفة أهمها وسائل التواصل الاجتماعي، ونتيجة للعولمة والثورة المعلوماتية قد يؤدي ذلك للانحلال في القيم العميقة للبنية الاجتماعية وفقا لرأي "فرانسيس فوكاياما". (إبراهيم، 2023)

4 . أثر التهديدات السيبرانية الصهيونية على دول المواجهة:

يشكل تطوير القدرة الصهيونية على العمل في ميدان الحرب السيبرانية مقوما رئيسيا من مقومات الحفاظ على الأمن، كما أن المصلحة القومية والموقع الجيوسياسي للكيان الصهيوني يحتمان عليه التفوق في المجال السيبراني، باعتباره جزء لا يتجزأ من قدرته على حماية نفسه من الهجمات التقليدية والسيبرانية، وكذلك من قدرته الرادعة في منطقة الشرق الأوسط وخارجها.

ويعتمد الكيان الصهيوني على قدراته التكنولوجية، وتقدمه في صناعة البرمجيات على خلق ديدان الحاسوب، فيروسات، برامج خبيثة، يشن بها هجمات على دول وأطراف يعتبرها معادية (Baram, 2013)، كما نجح بفضل هذا التقدم في اقتحام أسواق عالمية، وفي مقدمتها السوق الأمريكية، إلى درجة تصل إلى تحذير الخبراء الأمريكيين من الغزو الصهيوني لسوق الاتصالات والتكنولوجيا في أمريكا.

1.1. القدرات السيبرانية الصهيونية (مواطن القوة والضعف):

أصبح الأمن السيبراني هدفا أساسيا للكيان الصهيوني منذ سنة 2010، حين تم إطلاق ما يسمى بـ (المبادرة السيبرانية الوطنية) تحت إشراف مجلس البحث والتطوير في وزارة العلوم، وعلى إثره تم إنشاء مكتب سيبراني صهيوني (INCB) سنة 2011 (الجلاد، 2021، صفحة 31). كما أسس الكيان الصهيوني سنة 2016 ما يسميه (السلطة الوطنية للدفاع في مجال السايبر)، وهي هيئة تقوم بتنسيق عملية الدفاع عن المجال السيبراني الصهيوني، والردع عند حصول هجمات سيبرانية على الكيان ومصلحته، ورسم صورة شاملة للتعاون الاستخباراتي مع الجهات المختصة، وتم إخضاع هذه الهيئة لسلطة رئيس هيئة السايبر (القومية) (Tabansky, 2016).

ومن بين أهداف الكيان الصهيوني من تطوير قدراته السيبرانية، هو بناء شبكات تجسس محلية وإقليمية بغرض جمع المعلومات وتبادلها مع الدول الأخرى، وتشير مصادر أكاديمية عديدة، بأن الكيان يركز في عمليات تجسسه على "تكنولوجيا التجسس" للحصول عليها واستخدامها أو توفيرها للحلفاء، ولتحقيق ذلك يتم توظيف أفراد في كبرى الشركات الغربية، لإنتاج أجهزة التجسس المتطورة ليقوموا هم أنفسهم فيما بعد للتجسس لصالح الكيان الصهيوني، ومن ثم استخدام المعلومات المتحصل عليها أو مشاركتها مع الحلفاء (الحي، 2022، صفحة 14)، وهذا ما يبرر تركيز الكيان في كثير من المخططات على تفوقه التقني، وبالتالي فهو يقدم هذا التفوق كمجال للتعاون مع دول الإقليم (المطبعة) كالإمارات العربية المتحدة مثلا، والدول الأخرى كإثيوبيا وغيرها من الدول الإفريقية التي تعاني من ضعف في الجانب التكنولوجي،

لكن في حقيقة الأمر أن هذا النوع من التعاون وفي هذا المجال بالتحديد إنما هو منفذ واضح للاختراق الصهيوني لهذه الدول، وتعتبر هذه الاستراتيجيات كنوع من التغلغل الصهيوني في هذه الدول والمناطق ومن ثم السيطرة عليها. وتظهر الإمكانيات السيبرانية الصهيونية فيما يلي:

- الوحدة 8200:

هي وحدة نخبة تابعة لجهاز الاستخبارات العسكرية الصهيونية (أمان Aman)، وهي ركن أساسي للمخابرات العسكرية في الكيان الصهيوني، تسعى لإنتاج أفضل المواهب التكنولوجية على مستوى العالم، وهي المسؤولة عن جمع المعلومات الاستخبارية المشفرة SIGINT، أي من الإشارات الإلكترونية وأنظمة الاتصالات الأخرى التي تستخدمها الأهداف الأجنبية والمحلية، من خلال الرصد، والتنصت، والتصوير، والتشويش، ثم يتم تحليل هذه البيانات لتقييم التهديدات المحتملة للأمن الصهيوني (عبتاني، 2019، صفحة 15).

- الوحدة لهاية 433:

تعمل الوحدة 433 في شرطة الكيان الصهيوني على كشف الجرائم المحلية والدولية، والفساد العام، وتحتوي على مجموعة من الأقسام وهي ثمانية: وحدة التحقيق في الاحتيال، وحدة التحقيق في الجرائم الدولية، وحدة إنفاذ الاقتصاد الصهيوني، وحدة كشف وملاحقة لصوص السيارات، الوحدة 33، الوحدة السيبرانية، والوحدة 105، وتشكل هذه الأقسام ستة فرق عمل تخضع للجنة دائمة للتقييم والإشراف، ويظهر ضمن عمل الوحدة دورها البارز في الملاحقات الأمنية من بينها التجسس (صفوري، 2024).

- جهاز C4I:

يتولى مسؤولية الاتصال وتنظيم القدرات الصهيونية، ويتم تعيين ضابط ذو رتبة عالية من جهاز الاستخبارات الصهيوني في مركز الشفرة والأمن المعلوماتي، وتكون لديه المسؤولية لجمع المعلومات حول قدرات خصوم الكيان الصهيوني في مجال القرصنة الإلكترونية، ويقوم هذا الضابط بفتح شفرة الاتصالات المنقولة من شبكات الشن-بيت والموساد والجيش الصهيوني، ولدى الجهاز نفسه فرق عمل تقوم بفحص الشفرة لتأمين الدفاع الافتراضي للكيان (محمود، الهجمات عبر الإنترنت، 2013، صفحة 28).

- سلاح الاتصالات الإلكترونية (هتيشكوف):

تم إنشاء داخل هذا الجهاز ما يسمى بـ "دائرة الدفاع السيبراني"، حيث أن أكثر أنشطتها مصنفة سرية. وتمكن هذه الدائرة قوات الجيش الصهيوني من تنفيذ عمليات برية، وجوية، وبحرية، في عصر يعتمد فيه الجيش أكثر من أي وقت مضى، على تكنولوجيا الحواسيب. وتعمل الدائرة بالتعاون مع معظم وحدات النخبة في الجيش الصهيوني، مستخدمة

تشكيلة من الوسائل التكنولوجية المتطورة في سبيل تعطيل هجمات الخصم السيبرانية، كما يتضمن هذا الجهاز برنامجا يشتمل على دورات تدريبية لتعزيز مهارات أفراد الجيش في مجال الدفاع السيبراني (برعام، 2013، صفحة 14).

وتعزيزا لهذه القدرات أنشأ الكيان الصهيوني مؤخرا - سنة 2022- ما أطلق عليه بـ "القبة السيبرانية"، وهي عبارة عن نصح استباقي جديد وموسع للتنبؤ وصد الهجمات السيبرانية على مستوى الكيان بأكمله، دون أن يقتصر على قطاع أو مجال بعينه، ومن المفترض أن تعمل هذه القبة على تحديد التهديدات وحماية الأنظمة من مختلف المخاطر السيبرانية، بالإضافة إلى شن هجمات انتقامية مضادة ضد المهاجمين والقراصنة من قبل القيادة لجيش الدفاع الصهيوني، أي أنها لن تكتفي بالدفاع فقط، بل تتعدى ذلك إلى الإمداد بمعلومات دقيقة حول طبيعة المهاجم ومكان تواجده إما لإحباط هجومه أو لتوجيه ضربة انتقامية ضده (البهي، 2022).

لكن، وبالرغم من القدرات الهائلة التي يمتلكها هذا الكيان في المجال السيبراني، إلا أن هناك مواطن ضعف أفرزتها مواجهاته مع الخصوم، ففي 24-25 أبريل 2020 تعرضت عدة منشآت تابعة لمصلحة المياه في الكيان الصهيوني إلى هجوم إلكتروني إيراني كان الهدف منه تعطيل أجهزة الحواسيب التي تتحكم في توزيع المياه المعالجة، ومضخات الكلوريد والمواد الكيميائية المستعملة في عملية المعالجة، وحسب صحيفة "فوكس نيوز" الأمريكية فإن الإيرانيين اعتمدوا استخدام خوادم أمريكية للإضرار بالبنية التحتية المائية للكيان (الميموني، 2020، صفحة 74).

ومن جهة أخرى، فقد شنت مجموعات ناشطة في مجال القرصنة (وكلاء سيبيرانيون) يظهرهم الدعم والتضامن مع القضية الفلسطينية، ومنشأها دول إسلامية وعربية، منذ تاريخ الحرب الجارية ضد الفلسطينيين في قطاع غزة (07 أكتوبر 2023)، العديد من الهجمات السيبرانية وكانت أغلبها في شكل هجمات رفض الخدمة الموزعة ضد منصات ومواقع الإنترنت، وتشويه مواقع إلكترونية صهيونية، وتسريب البيانات لمختلف المؤسسات التي تعتبر أهدافا رفيعة المستوى وعظيمة القيمة.

ومثال ذلك، الأنشطة التي تمت ملاحظتها في بداية الحرب، المتمثلة في شن هجمات نشر الخوف من خلال المجال السيبراني، إذ استغلت مجموعة قرصنة مؤيدة للقضية الفلسطينية يطلق عليها اسم Anon Ghost ثغرة أمنية في واجهة برمجة (API) الخاص بتطبيق الإنذار الصاروخي الصهيوني Red Alert وأرسلت تحذيرات صاروخية زائفة إلى المستخدمين. وتمكن المهاجمون من الوصول إلى خادم يقوم بتشغيل اللوحات الإعلانية الذكية في تل أبيب، وقاموا بتغيير الإعلانات التجارية إلى محتوى مؤيد للمقاومة الفلسطينية، بالإضافة إلى لقطات من حرق (علم) الكيان الصهيوني. كما أن هذه الهجمات السيبرانية استطاعت أن توقف أكثر من 100 موقع، من بينها الموقع الإلكتروني الرسمي لجهاز مخابرات الكيان (محمود، البعد السيبراني في الحرب الإسرائيلية على غزة، 2023).

2.4. استخدام القوة السيبرانية الصهيونية ضد دول المواجهة وآليات الوقاية منها:

يلجأ الكيان الصهيوني لاستخدام القوة السيبرانية في حروبه ضد الدول والأطراف المعادية كونها أقل تكلفة من عناصر القوة التقليدية التي تتطلب مستوى عالي من الإنفاق المادي والبشري، بل أدركت دوائر صناعة القرار داخل الكيان أهمية الحرب الهجينة (المزج بين الحرب التقليدية والحرب السيبرانية) في إلحاق الضرر بالخصم، والتأثير في البنية الأساسية لأمنه. ومن نماذج الهجمات السيبرانية الصهيونية ضد دول المواجهة نذكر ما يلي:

4.2. 1. الهجمات السيبرانية الصهيونية ضد إيران:

في خضم الصراع الدائر بين دولة إيران والكيان الصهيوني، أقدم هذا الأخير في شن العديد من الهجمات السيبرانية على إيران بهدف ضرب البنية التحتية لمختلف منشآتها الحيوية، ومن ثم التأثير على أمنها الوطني، ومن ذلك، الهجوم الإلكتروني الذي شنته الولايات المتحدة الأمريكية والكيان الصهيوني في نوفمبر 2010 لإيقاف إنتاج اليورانيوم كجزء من البرنامج النووي الإيراني، وكان من خلال فيروس يسمى "Virus Stuxnet"، تم تحميله على وصلة تخزين "USB stick"، مما أدى إلى تدمير 1000 وحدة تخصيص، كما تسبب الهجوم في الحد من قدرات إيران النووية، الأمر الذي أدى بإيران آنذاك في البحث عن سبل تطوير وحماية أمنها السيبراني (الميموني، 2020، صفحة 76).

كما استخدم الكيان الصهيوني فيروسات طورها سنة 2012 (Flame, Duqu)، إذ أن فيروس Flame تم تطويره بشكل مشترك من قبل الكيان الصهيوني والولايات المتحدة الأمريكية، لكي يقوم بجمع المعلومات الإستخباراتية للمساعدة في إبطاء البرنامج النووي الإيراني (Reuters, 2012)، كما استخدم الكيان الصهيوني فيروس Duqu من أجل جمع المعلومات عن المحادثات الجارية بين الصين وفرنسا وروسيا والمملكة المتحدة والولايات المتحدة الأمريكية وأوروبا حول القدرات النووية الإيرانية (Gibbs, 2015).

كما قام الكيان الصهيوني في 18 ماي 2020 بشن هجوم سيبراني على "ميناء الشهيد رجائي" المطل على مضيق هرمز، تسبب في تعطيل الحركة الملاحية، حيث تم من خلال هذا الهجوم التسلل إلى العديد من أنظمة التشغيل وتدميرها (الميموني، 2020، الصفحات 74-75). كما تم أيضا تنفيذ هجوم إلكتروني صهيوني "ستوكس نت" في 07 جوان 2022 على مصنع الصلب في إيران، وقد أعلنت جماعة تدعى "بريداتوري سبارو" أي العصفور المفترس مسؤوليتها عن الهجوم وأنها تسببت بالحريق الخطير في المصنع (تيدي، 2022).

4.2.2. الهجمات السيبرانية الصهيونية ضد فلسطين:

أصبحت الحرب الإلكترونية من الأدوات الرئيسية التي يستخدمها الكيان الصهيوني لتحقيق أهداف إستراتيجية دون التورط في مواجهة مكشوفة مع الأطراف المستهدفة، وفي فلسطين، تعكف مخابرات الكيان الصهيوني منذ سنوات على توظيف مواقع التواصل الاجتماعي في تجنيد عملاء عبر استخدام هويات مزيفة، وتؤكد المعطيات التي تقدمها

الأجهزة الأمنية الفلسطينية، أنه بالاستناد إلى التحقيقات التي أجريت مع أشخاص اعترفوا بالتعاون مع الكيان، أن نسبة كبيرة من هؤلاء أسقطوا في برائن العمالة مع الكيان بعد إقامة علاقات افتراضية مع رجال مخابرات قدموا أنفسهم على أنهم فلسطينيون عبر مواقع التواصل الاجتماعي (العفار، 2016، صفحة 163)، كما تعمل الوحدة 8200 على ابتزاز الفلسطينيين من خلال المعلومات الشخصية والخاصة والتي تقوم بجمعها عنهم من خلال اعتراض المحادثات الهاتفية الخاصة والرسائل النصية والبريد الإلكتروني، وذلك بغرض إجبارهم على التعاون معها (عيتاني، 2019، الصفحات 29-30).

كما أن الكيان الصهيوني يعتمد في كل مواجهة مع الفلسطينيين، إلى استخدام الطائرات الاستطلاعية بأشكال وأنواع وأحجام مختلفة، خاصة في قطاع غزة، كما أن هذه الطائرات المخصص بعضها للتصوير وآخر للمراقبة والتنصت وتلك المزودة بالصواريخ، الغرض منها تنفيذ عمليات الاغتيال والقصف الدقيق لشخصيات من حركة المقاومة الفلسطينية، بهدف التأثير عليها وإرباكها ومن ثم إضعافها (القدس العربي، 2016).

كما يستخدم الكيان الصهيوني برامج التجسس السيبراني ضد الفلسطينيين، منها برامج بيجاسوس Pegasus spyware، حيث يمكن لهذا البرنامج الصهيوني الذي طوره شركة أن أس أو NSO Group Technologies الصهيونية الخاصة، قراءة الرسائل والاستماع وحتى تسجيل المكالمات، وكذلك التقاط الصور عن بعد، وهو ما أكدته تقارير منظمة العفو الدولية Amnesty International. ففي 18 نوفمبر 2021 منظمة العفو الدولية ومنظمة سيترز لاب المتخصصة في مراقبة أمن الإنترنت بأن الهواتف المحمولة الخاصة بستة نشطاء حقوقيين فلسطينيين في الضفة الغربية المحتلة قد تعرضت للإختراق باستخدام برامج التجسس بيجاسوس، كما قامت منظمة "هيومن رايتس ووتش" بإصدار بيان تدين فيه الكيان الصهيوني معتبرة أن هذا الهجوم جزء من اعتداء أوسع على المجتمع المدني الفلسطيني، وما يؤكد ضلوع الكيان الصهيوني في هذا العمل، أن ثلاثة من المدافعين الحقوقيين المستهدفين ينتمون إلى جماعات المجتمع المدني الفلسطينية البارزة التي صنفها السلطات الصهيونية على أنها "منظمات إرهابية". (هيومن رايتس ووتش، 2021)

وفي الحرب الأخيرة على قطاع غزة (07 أكتوبر 2023)، شن الكيان الصهيوني العديد من الهجمات السيبرانية ردا على الهجمات السيبرانية للمقاومة الفلسطينية، التي مست قطاعات حيوية في الكيان، وقد شملت هذه الهجمات الصهيونية ثلاث قطاعات فلسطينية - في شكل هجمات سيبرانية موزعة لحجب الخدمة باستخدام HTTP- وهي المواقع الإلكترونية المصرفية بنسبة 76 % من مجموع الهجمات، ونسبة 24 % مست قطاع الإنترنت، كما طالت هذه الهجمات قطاع الإنتاج الإعلامي بنسب صغيرة (Omer Yoachimik, jorge pacheco, 2023).

كما يستخدم الكيان الصهيوني الفضاء السيبراني مدعوما بالخوارزميات، من خلال الضغط على الشركات الكبرى التي تسيطر على هذا الفضاء لتقييد المحتوى الداعم للقضية الفلسطينية والمقاومة عبر منصات التواصل الاجتماعي، وتطبيقات الذكاء الاصطناعي Deepfake أي (التزييف العميق)، منها جثة الطفل المحروق، وبث العديد من الرسائل

عبر الكلمات والصور والفيديوهات لخلق حالة تعاطف دولي وتوجيه الرأي العام العالمي عبر دعايات تصف الفلسطينيين بالجرمين والإرهابيين، وتصف ما حدث في السابع من أكتوبر 2023 بـ "الحرق النازية".

كما أن الكيان الصهيوني يحظى بدعم الهند في حربه السيبرانية ضد الفلسطينيين، وهذا راجع لتطور العلاقات الدبلوماسية والعسكرية بين الكيان الصهيوني والهند، فضلا عن علاقة مجموعات سيبرانية هندية بمؤسسات ناشئة صهيونية التي تشكل مزودا لها، إذ قام فريق "القوة السيبرانية الهندية (Indian Cyber Force)" بشن هجمات على العديد من المؤسسات الفلسطينية، مثل البنك الوطني وشركة الاتصالات "paltel.ps"، كما زعموا أيضا إسقاطهم لموقع حماس الإلكتروني "Hamas.ps"، وشنهم هجوم سيبراني على مزود الإنترنت الفلسطيني في قطاع غزة وإيقافه (يورونيوز، 2023).

3.2.4. الهجمات السيبرانية الصهيونية ضد لبنان:

شملت الهجمات السيبرانية الصهيونية دولة لبنان أيضا في العديد من المحطات، ففي 07 جانفي 2024 تعرضت شاشات عرض الرحلات في مطار رفيق الحريري الدولي ببيروت للاختراق، وظهرت عليها رسالة تطالب (حزب الله) بعدم جر لبنان إلى حرب مع الكيان الصهيوني، كما أدى هذا الهجوم السيبراني على المطار إلى تعطيل نظام جر وتفتيش الحقائق (محيط، 2024).

كما طالت عمليات القرصنة المؤسسات العامة للدولة اللبنانية منها الاختراق السيبراني للموقع الإلكتروني لمجلس النواب اللبناني في 08 جانفي 2024 الذي أدى إلى تجميده فيما بعد، يليه اختراق موقع وزارة الشؤون الاجتماعية اللبنانية، حيث أصدرت الجهة المخترقة بيانا تبنت فيه هذه العملية، وأعلنت أن الهدف من الهجوم هو "الاحتجاج على تردي الأوضاع الاقتصادية والاجتماعية في لبنان" (Transparency News، 2024)، والواضح أن الهدف من هذه الهجمات السيبرانية على المؤسسات الهيكل الرئيسية للدولة اللبنانية هو خلق انقسامات الغرض منها زعزعة الاستقرار داخل المجتمع اللبناني، وخلق جبهة اجتماعية لبنانية معارضة لحركة المقاومة، الأمر الذي يخدم إستراتيجية الكيان الصهيوني في محاولاته لإبعاد حزب الله كحركة مقاومة من المواجهة، وإدخال لبنان ضمن قائمة الدول العربية المطبوعة مع الكيان الصهيوني.

وقبل ذلك، تمكن الكيان الصهيوني في شهر أكتوبر 2023 من اختراق شبكات الاتصال اللبنانية، والتسلل إلى قاعدة البيانات، ما سهل عليه ضرب كثير من الأهداف بدقة، واغتيال قادة ميدانيين في تنظيم حزب الله، وهو ما جعل الدولة اللبنانية والحزب عاجزين أمام هذه الاختراقات، إذ يتلقى الكثير من سكان الجنوب اللبناني اتصالات مجهولة من أشخاص يتحدثون اللهجة اللبنانية، ويتنحلون صفة موظفين في مؤسسات رسمية، يزعمون أنهم بصدد إجراء إحصائيات

عن عائلات ومنازل لإيصال المساعدات لهم، لكنها في الحقيقة ليست كذلك، وإنما الغرض منها هو إستقاء معلومات عن كوادرات تنظيم حزب الله ومقاتليه، وأماكن وجودهم في قرى الجنوب عبر الاتصال بالسكان (الشرق الأوسط، 2024).

ولقد تعرضت حركة المقاومة اللبنانية (حزب الله) في الآونة الأخيرة (17-18 سبتمبر 2024)، إلى هجوم معقد يشبه إلى حد كبير بتورط الوحدة 8200 الصهيونية في تنفيذه، إذ تسبب الهجوم في انفجار الآلاف من أجهزة النداء وأجهزة الراديو المحمولة التابعة لحزب الله، وفي تصريح لرئيس سابق لجهاز استخبارات الكيان الصهيوني "داني ياتوم" يقول فيه: (أن الأجهزة المتفجرة كانت تهدف إلى إثارة الذعر والتوتر والصدمة داخل حزب الله، ما يدل على قدرة (إسرائيل) على اختراق أكثر خطوط الاتصال أماناً للمجموعة، كما أن هذه العملية ليست بمفردها، إنما عملية قد تبدأ حرباً أكثر حسماً في لبنان) (موريس، 2024، صفحة 09).

ولقد تعددت النظريات في تفسير كيفية وضع المتفجرات داخل الأجهزة، وفي السيناريو الأكثر احتمالاً، أن عملاء من الكيان الصهيوني قاموا بحشو البطاريات بالمتفجرات عندما تم تصنيع الأجهزة، بواسطة شركة وهمية حصلت على ترخيص باستخدام تكنولوجيا أجهزة النداء القديمة من شركة تايوانية. بينما يرى البعض الآخر، أن الأجهزة قد تم تعديلها في مرحلة ما بين تصنيعها وتوزيعها على قادة حزب الله وجنوده، ومن الممكن في ذات الوقت، أن هذه الانفجارات قد حدثت فقط من خلال رسالة قد أرسلت في الوقت نفسه إلى تلك الأجهزة (سانغر، 2024، صفحة 09).

إن هذه الهجمات السيبرانية التي يشنها الكيان الصهيوني على دول المواجهة (إيران، فلسطين ولبنان)، أظهرت بشكل جلي مدى خطورة التهديدات التي تعترض مقومات الأمن السيبراني لهذه الدول، ولمواجهة هذه التهديدات أصبح من الضروري التفكير في آليات واستراتيجيات عامة من شأنها أن تعزز الأمن السيبراني لدى هذه الدول.

خاتمة:

ساهمت تكنولوجيا المعلومات والاتصالات والوسائل الحديثة بشكل كبير في تسهيل العديد من مناحي الحياة، ونشاطات الإنسان اليومية، إلا أنه بالرغم من هذه المميزات التي أضافتها تلك التكنولوجيا لحياة الإنسان، فإنها تعتبر بمثابة أرض خصبة لكثير من التحديات التي تتركز المجتمع الدولي بأكمله، حيث دفعت المجتمعات ضريبة رقمنة حياتها بسبب تنامي تهديدات الأمن السيبراني.

وعليه، فإنه كلما زاد الارتباط بالوسائل التكنولوجية واستخدامها في شتى الميادين العسكرية والاقتصادية والسياسية والثقافية، كلما زادت مخاطر التهديدات السيبرانية، ويعتبر الكيان الصهيوني من الأطراف التي تسعى دائما إلى تعظيم مقومات القوة في الفضاء السيبراني، بحجة وجود دول عربية وإسلامية تهدد أمن ووجود هذا الكيان، لكن هذا التسابق الصهيوني - العربي والإسلامي في مجال امتلاك القوة السيبرانية وتوظيفها، يؤثر بشكل واضح على الكيان الصهيوني من جهة، وعلى أمن دول وأطراف المواجهة من جهة ثانية، خاصة في حالة تفوق طرف على الآخر في امتلاك الأسلحة السيبرانية النوعية والحديثة.

ونظرا لخطورة التهديدات السيبرانية الصهيونية، كونها تحتاج قطاعات حيوية لدول المواجهة (فلسطين، إيران ولبنان)، فإنه يتوجب على هذه الدول القيام بتعزيزات أكبر من أجل الوقاية من هذه التهديدات، ومحاولة التفكير في استراتيجية سيبرانية وطنية وعربية شاملة، من شأنها أن تعزز من صلابة البنية السيبرانية الهشة لبعض الدول خاصة فلسطين ولبنان، كما أنها سوف تعمل على الحد من تأثير هذه التهديدات على أمن هذه الدول.

الاقتراحات:

- ضرورة إنشاء أقسام خاصة في هذه الدول، لمواجهة الاختراقات والهجمات السيبرانية التي يشنها الكيان الصهيوني عليها، ويجب أن تتشكل هذه الأقسام من متخصصين، وكفاءات في مجال الأمن السيبراني، لتشكل في مجملها جهازا دفاعيا متكاملا لمقاومة هذه التهديدات.
- التنبيه لأهمية استعمال الوسائل والأجهزة التكنولوجية الأكثر تطورا المتعلقة بالفضاء السيبراني، والتركيز على أن تكون هذه الأجهزة والآليات غير مختزقة من طرف الكيان الصهيوني، وغير تابعة لشركات لها علاقة بالشركات الصهيونية المنتشرة في عدة دول من العالم، ولا يتحقق هذا الأمر إلا من خلال تطوير الصناعات المرتبطة بالتعاملات السيبرانية، وتحقيق الإكتفاء في مجال صناعة الشرائح والرقائق الإلكترونية.
- تأمين الشبكات على نحو يمنع من اختراقها، ومن طرق تحصين الشبكات الداخلية كذلك من الاختراق عملية التشفير، والتشفير يعني تحويل البيانات المكتوبة إلى أرقام أو رموز لا يمكن حلها إلا بالنسبة لمن يمتلك شفرة حل هذه

الرموز والأرقام، وتستخدم عملية التشفير في تداول النقود والبيانات عبر الشبكة في التجارة الإلكترونية وفي تداول غيرها من البيانات التي تتعلق بالأمن الوطني.

- أهمية التفوق في تقنيات الذكاء الاصطناعي واستخدامها في التعرف على الأنماط الخبيثة واستجابة التهديدات بسرعة أكبر، إذ يمكن لهذه التقنيات أن تساعد في تحسين دقة الكشف وتقليل الوقت اللازم للاستجابة.

- ضرورة التحديث المستمر للبنية التحتية للتأكد من أن جميع الأنظمة والبنية التحتية محدثة بأحدث التصحيحات الأمنية والبرامج، وكذلك تطبيق استراتيجيات دفاع متعددة الطبقات التي تشمل الجدران النارية، نظام كشف التسلسل، وبرمجيات مكافحة الفيروسات المتقدمة.

- العمل على تأهيل وتدريب المعنيين على طرق وآليات مجابهة المخاطر السيبرانية، فلابد من وضع سياسة رشيدة تستند على تدريب المختصين في هذه الدول.

المراجع باللغة العربية:

أولا: الكتب:

1. الأشقر جبور منى. (2017). السيبرانية هاجس العصر. بيروت: المركز العربي للبحوث القانونية والقضائية.
2. الاتحاد الدولي للاتصالات ITU. (2010). تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني.
3. الهيئة الوطنية للأمن السيبراني. (2018). الضوابط الأساسية للأمن السيبراني. الهيئة الوطنية للأمن السيبراني.
4. الهيئة الوطنية للأمن السيبراني. (2022). الأمن السيبراني. منشآت.
5. بشرى حسين الحمداني. (2014). القرصنة الإلكترونية: أسلحة الحروب الحديثة. الأردن- عمان: دار أسامة للنشر والتوزيع.
6. جرایة الصادق. (2022). الفكر الأمني الإسرائيلي: المحددات، المقومات، سياسات التنفيذ. الجزائر: مطبعة منصور.
7. جيل برعام. (2013). تأثير تطور تكنولوجيا الحرب السيبرانية على بناء القوة في إسرائيل. مؤسسة الدراسات الفلسطينية. لبنان: مركز الزيتونة للدراسات والاستشارات.
8. خالد وليد محمود. (2013). الهجمات عبر الإنترنت. الدوحة: المركز العربي لأبحاث ودراسة السياسات.
9. دوبي كوش. (2002). مفهوم الثقافة في العلوم الاجتماعية. دمشق: منشورات اتحاد الكتاب العرب.
10. سرور جرمان سرور المطيري. (بلا تاريخ). تغير مفهوم الأمن القومي الكويتي ودلالاته في الفترة 1990-2013. القاهرة: دار المكتب العربي للمعارف.
11. فاطمة حسان عيتاني. (2019). الوحدة الإسرائيلية 8200 ودورها في خدمة التكنولوجيا التجسسية الإسرائيلية. لبنان: مركز الزيتونة للدراسات والاستشارات.
12. فيصل محمد عبد الغفار. (2016). الحرب الإلكترونية. عمان- الأردن: الجنادرية للنشر والتوزيع.
13. وليد عبد الحي. (يوليو 2022). الاقتصاد السياسي لمبيعات السلاح الإسرائيلي. ورقة علمية. مركز الزيتونة للدراسات والاستشارات.

ثانيا: المقالات:

1. أحمد بن علي الميموني. (أكتوبر 2020). الجبهة النشطة: تداعيات المواجهة السيبرانية بين إيران وإسرائيل. مجلة الدراسات الإيرانية، الصفحات 67-85.
2. إيهاب خليفة. (2017). تنامي التهديدات السيبرانية للمؤسسات العسكرية. إتجاهات الأحداث، الصفحات 54-57.

3. إيهاب خليفة. (2021). تحديات الأمن الإقليمي العربي في الميدان الخامس: نحو إستراتيجية للحماية. أوراق السياسات الأمنية، الصفحات 1-15.
4. حسام نجيدة. (ديسمبر، 2023). الأبعاد الجديدة لمفهوم الأمن. مجلة العلوم الإدارية والسياسية.
5. تينا الجلاد. (2021). الدبلوماسية السيبرانية الإلكترونية وأهميتها لإسرائيل. شؤون فلسطينية، الصفحات 24-43.
6. سليمة مصباح حامد. (2024). التهديدات السيبرانية وإنعكاساتها على الأمن القومي الليبي: التأسيس وآليات التحصين المعرفي. إقتصاد المعرفة، المقومات والآليات، ليبيا نموذجاً (الصفحات 256-280). ليبيا: كلية الإقتصاد والتجارة.
7. سليمان المشعل. (30 08، 2011). ثقافة وتطبيقات الأمن البيئي العالمي. المجلة الإقتصادية.
8. عبد الإله محمد النوايسة، ممدوح حسن العدوان. (2019). جرائم التجسس الإلكتروني في التشريع الأردني: دراسة تحليلية. مجلة علوم الشريعة والقانون، الصفحات 467-482.
9. عز الدين دراغو. (30 06، 2022). الآثار الإقتصادية والمالية للهجمات السيبرانية في ظل التحول الرقمي: النتائج، التجارب والحلول، مع الإشارة إلى حالة الجزائر. مجلة التكامل الإقتصادي، الصفحات 109-124.
10. قياتي عاشور. (01 12، 2017). الأمن القومي العربي: التحديات وسبل المواجهة. حولية كلية الآداب جامعة بني سويف، الصفحات 137-255.
11. يحي ياسين سعود. (2018). الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني. المجلة القانونية، الصفحات 80-108.

ثالثاً: الأطروحات:

1. صغير يوسف. (2013). الجرائم المرتكبة عبر الإنترنت . رسالة ماجستير، كلية الحقوق جامعة مولود معمري. الجزائر.

رابعاً: المؤتمرات:

1. ماجد صدام سالم. (01 12، 2022). الأمن السيبراني العراقي وأثره على قوة الدولة. مجلة العلوم التربوية والإنسانية.

خامساً: الجرائد:

1. ديفيد سانغر. (2024). الهجوم الإلكتروني الإسرائيلي على لبنان لم يحقق نتائج إستراتيجية. الأيام.
2. لوفداي موريس. (2024). هل ينقل هجوم "البيجر" المعركة بين إسرائيل وحزب الله إلى مرحلة جديدة. الأيام.

سادساً: المواقع الإلكترونية:

1. (22, 01, 2024). اختراق مواقع حكومية لبنانية يثير المخاوف. تم الاسترداد من: Transparency News: <https://www.transparency.news/news/322492>
2. القدس العربي. (23, 12, 2016). المقاومة الفلسطينية تكشف إفشال عشرات محاولات الاغتيال بعد اختراق منظومة طائرات الاستطلاع الإسرائيلية. تم الاسترداد من القدس العربي: <https://www.alquds.co.uk/>
3. إيهاب عنان. (23, 06, 2024). أمن سيبراني. الهندسة الاجتماعية سلاح الحروب السيبرانية الناعم. تم الاسترداد من المركز الأوروبي لدراسات مكافحة الإرهاب والاستخبارات: <https://www.europarabct.com>
4. الشرق الأوسط. (20, 1, 2024). الاختراق الإسرائيلي لشبكات الاتصالات يسهل اغتيالهم في لبنان. تم الاسترداد من صحيفة الشرق الأوسط: www.aawsat.com
5. جو تيدي. (12 جويلية, 2022). ماذا نعرف عن قرصنة "العصفور المفتاح" الذين أعلنوا مسؤوليتهم عن حريق مصنع في إيران. تم الاسترداد من BBC NEWS: www.bbc.com/arabic/middleeast-62124759
6. خالد وليد محمود. (16 نوفمبر, 2023). البعد السيبراني في الحرب الإسرائيلية على غزة. تم الاسترداد من الشرق: m.al-sharq.com
7. رغدة البهي. (03, 08, 2022). القبة السيبرانية الإسرائيلية: السمات والدوافع. تم الاسترداد من المركز المصري للفكر والدراسات الإستراتيجية: ecss.com.eg
8. مجد زياد، أنيس جميل صفوري. (14 أوت, 2024). الأمن السيبراني في أولويات الأمن القومي الإسرائيلي. تم الاسترداد من مركز دراسات الوحدة العربية: caus.org.lb
9. محمد عاطف إمام إبراهيم. (04 جويلية, 2023). الفضاء الإلكتروني وأثره على الأمن القومي للدول: الحروب الإلكترونية نموذجاً. تم الاسترداد من المركز العربي لأبحاث الفضاء الإلكتروني: https://accronline.com/article_detail.aspx?id=40264
10. مها محيط. (29, 01, 2024). بعد موجة اختراقات.. كيف يواجه لبنان الهجمات السيبرانية؟ تم الاسترداد من الشرف: <https://asharq.com/reports/78654>
11. هيومن رايتس ووتش. (8, 11, 2021). استخدام برنامج تجسس لاختراق المدافعين الحقوقيين الفلسطينيين. تم الاسترداد من <https://www.hrw.org/ar/news/2021/11/08/380353>
12. يورو نيوز. (14, 10, 2023). حرب بموازة المعارك بين غزة وإسرائيل.. هل تؤثر المواجهة السيبرانية على الصراع؟ تم الاسترداد من <https://arabic.euronews.com/2023/10/14/cyberspace-is-another-battlefield-between-israel-and-hamas>

المراجع باللغة الأجنبية:

Books:

1. Baram, G. (2013). The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case. *Military and Strategic Affairs*.
2. James A. Lewis. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Threats*. Center for Strategic and International Studies.
3. National Institute of Standards and Technology. (2018). *A Glossary of Key Information Security Terms*. National Institute of Standards and Technology

Articles:

1. Lech J. Janczewski et al. (2001). Handling Distributed Denial-of-Service Attacks. *Information Security Technical Report*, pp 37-44

Websites:

1. Omer Yoachimik, Jorge Pacheco. (2023, 10 23). Retrieved from Cyber attacks in the Israel-Hamas war: <https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/>
2. Gibbs, S. (2015, Jun 11). *Duqu 2.0: computer virus 'linked to Israel' found at Iran nuclear talks venue*. Retrieved from the Guardian: <https://www.theguardian.com/technology/2015/jun/11/duqu-20-computer-virus-with-traces-of-israeli-code-was-used-to-hack-iran-talks>
3. Reuters. (2012, June 19). *U.S., Israel developed Flame computer virus: newspaper*. Retrieved from Reuters: <https://www.reuters.com/article/net-us-usa-cyber-flame-idUSBRE85I1QQ20120619/>
4. Lior Tabansky. (2016). *Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy*. Cyber Research Center : www.ccdcoe.org