الترميز الدولي / ISSN (P) :2710-2653
ISSN (E) :2960-253X /
رقم الايداع الوطني / 2375 /2019

تاريخ استلام البحث : ٢٠٢٥/١١/١٤
تاريخ قبول البحث : ٢٠٢٦/٢/٢١
تاريخ النشر : ٢٠٢٦/٣/٣٠

الامن السيبراني دراسة في تطور أجيال الحروب

Cybersecurity: A Study in the Evolution of Generations of Warfare

م.م حسين سلام حسين
Assist Lecturer Hussein Salam Hussein

حسين صبري خلف
Hussein Sabri Khalaf

جامعة المستنصرية – كلية العلوم السياسية
Al-Mustansiriya University - College of Political Science

slamhsynhsyn317@gmail.com
hussein_sabri@uomustansiriyah.edu .iq

الباحثة شيماء عباس حسين
Shaimaa Abbas Hussein

جامعة بغداد –كلية العلوم السياسية
University of Baghdad - College of Political Science
Shaimaa.abbas1201d@copolicy.uobaghdad.edu.iq

IRAQI
Academic Scientific Journals
https://iasj.rdd.eedu.iq/journals/journal/view/229

الملخص :

يتناول البحث تطور أجيال الحروب وتأثير الأمن السيبراني على الأمن القومي. يبدأ بتعريف أجيال الحروب، حيث انتقلت من أشكال تقليدية تعتمد على المواجهات المباشرة إلى أساليب أكثر تعقيدًا تعتمد على التكنولوجيا الحديثة. يُبرز البحث أهمية الأمن السيبراني كعنصر حيوي لحماية البنية التحتية الحيوية والمعلومات الحساسة، حيث إن الهجمات السيبرانية يمكن أن تؤدي إلى عواقب وخيمة تهدد استقرار الدول.
كما يشير إلى ضرورة تطوير استراتيجيات شاملة لمواجهة التهديدات السيبرانية، تتضمن التعاون الدولي وتبادل المعلومات. بالإضافة إلى ذلك، يُشدد على أهمية رفع الوعي المجتمعي حول مخاطر الفضاء السيبراني، وتعزيز التعليم والتدريب في هذا المجال. في الختام، يؤكد البحث أن الاستثمار في الأمن السيبراني أصبح ضرورة حتمية لضمان مستقبل آمن ومستقر للأجيال القادمة.
الكلمات المفتاحية : أجيال الحرب ، الأمن السيبراني ، الهجمات السيبرانية ،الأمن القومي

Abstract

It is necessary to explore the generations of warfare that will shape cybersecurity at the national level. This begins by defining the generations of warfare, ranging from early, and reconstruction-based warfare to more serious, technology-driven warfare. The research highlights the importance of cybersecurity as an optional element for controlling sensitive data, as the combination of cybersecurity and cyberattacks can have dire consequences for the stability of nations.

It also points to the need to develop all aspects of cybersecurity, including international cooperation on information security. Furthermore, it emphasizes the importance of raising community awareness about cybersecurity and effective educational outreach in this field. At the conference, the research determined that investing in cybersecurity has become an absolute necessity to ensure a secure and stable future for future generations.
Keywords: Generations of warfare, cybersecurity, cyberattacks, national security

المقدمة :

يُعدّ الأمن السيبراني ركيزة أساسية في الحروب الحديثة مع تحوّل الفضاء الرقمي إلى ساحة رئيسية للصراعات. ومع تزايد الاعتماد على التكنولوجيا الرقمية، أصبحت حماية البيانات والمعلومات الحساسة ضرورة ملحّة. وتتعرض الدول والمؤسسات لتهديدات سيبرانية متزايدة، مثل الفيروسات والبرمجيات الخبيثة

والهجمات الموزعة، التي لا تقتصر آثارها على الأفراد بل تمتد إلى البنى التحتية الحيوية كأنظمة الطاقة والنقل والاتصالات، مما يجعل تبنّي استراتيجيات فعّالة للأمن السيبراني أمرًا حيويًا.

تُبرز دراسة الأمن السيبراني تحوّل طبيعة الحروب من الصراعات التقليدية إلى الحروب الرقمية المعتمدة على تكنولوجيا المعلومات. ويسهم التطور التقني، ولا سيما الذكاء الاصطناعي وتحليل البيانات الضخمة، في صياغة استراتيجيات حديثة قائمة على المعلومات. وتتطلب مواجهة التهديدات السيبرانية بناء أنظمة حماية متقدمة تشمل جدران الحماية والتشفير ونظم كشف التسلل. وتواجه الدول النامية تحديات تتعلق بنقص الموارد وضعف البنية التحتية والوعي المجتمعي، مما يستدعي تعزيز التعاون الدولي. كما تفرض الحروب الإلكترونية تبنّي تقنيات متقدمة كالتشفير الكمي، إلى جانب تطوير استراتيجيات مرنة قادرة على التكيّف مع تطور الذكاء الاصطناعي وإنترنت الأشياء والحوسبة السحابية.

تتجاوز التهديدات السيبرانية الحدود الجغرافية، مما يفرض ضرورة تعزيز التعاون الدولي عبر تبادل المعلومات والخبرات لمواجهة المخاطر المشتركة. كما يُعدّ التعاون بين القطاعين العام والخاص عنصرًا أساسيًا في دعم الأمن السيبراني. ويُسهم رفع الوعي المجتمعي، من خلال برامج تدريب تستهدف مختلف الفئات ولا سيما الشباب وطلبة المدارس، في تقليل فرص التعرض للهجمات السيبرانية.

أهمية البحث :

١- فهم العلاقات بين الأمن السيبراني والحروب الحديثة: يساهم البحث في توضيح كيف يؤثر تطور أجيال الحروب على استراتيجيات الأمن السيبراني، مما يساعد في فهم ديناميكيات الصراع في العصر الرقمي.

٢- تسليط الضوء على التهديدات السيبرانية: يُبرز البحث التهديدات المتزايدة التي تواجهها الدول نتيجة الاعتماد على التكنولوجيا، مما يعزز الوعي حول أهمية الأمن السيبراني.

٣- تقديم حلول عملية: يسعى البحث إلى تقديم توصيات واستراتيجيات لتعزيز القدرات الدفاعية السيبرانية، مما يفيد صانعي القرار في تطوير سياسات فعالة.

٤- تحليل التحديات في الدول النامية: يناقش البحث التحديات الخاصة التي تواجهها الدول النامية في مجال الأمن السيبراني، مما يسهم في صياغة استراتيجيات مناسبة لهذه السياقات.

إشكالية البحث :

تتمثل إشكالية البحث في دراسة تأثير تطور أجيال الحروب على الأمن السيبراني، وكيفية ارتباط الأمن السيبراني بالأمن القومي في ظل التحديات المتزايدة التي تواجهها الدول. يتناول البحث كيفية تطور

استراتيجيات الحروب نتيجة للتطور التكنولوجي، وكيف أصبحت الفضاءات الرقمية ساحة جديدة للصراع. كما يُطرح سؤال حول فعالية التدابير المتخذة لحماية البنية التحتية الحيوية من الهجمات السيبرانية، خاصة في الدول النامية.

فرضية البحث:

يفترض البحث أن الأمن السيبراني أصبح عنصرًا حيويًا في استراتيجيات الأمن القومي، وأن الفشل في مواجهة التهديدات السيبرانية يمكن أن يؤدي إلى تأثيرات سلبية على استقرار الدول وأمنها. كما يُفترض أن التقدم التكنولوجي المستمر يشكل تحديًا، مما يستدعي تطوير استراتيجيات مرنة وفعالة للتصدي لهذه التهديدات.

منهجية البحث:

اعتمدنا في الدراسة على المنهج الاستقرائي من خلال دراسة الواقع وقراءة المجريات الاحداث والمتغيرات لما تتطلبة الدراسة ، وأيضا المنهج الوصفي من خلال وصف الحالة (موضوع الدراسة) وصفا دقيقا .

المبحث الأول

الاطار المفاهيمي وتطور أجيال الحروب

المطلب الأول: ماهية اجيال الحرب

سيتم في البداية تفكيك مصطلح أجيال الحرب ، إذ سيتم أولا تحديد المقصود بمصطلح الجيل (الأجيال) والمقصود أيضا بمفهوم الحرب، ليتم بعدها إعادة الجمع (إعادة التركيب بين المصطلحين وتحديد المقصود بأجيال الحرب.

مفهوم الجيل (Generation): الأجيال من جمع جيل ، وهو مصطلح يستخدم في الغالب في علم الاجتماع، فقد كتب عالم الاجتماع المجري كارل مانهايم عام ١٩٢٣ مقالا مطولا بعنوان مشكلة الأجيال (The Problem of Generations) تحول فيما بعد لنظرية شهيرة عُرفت بـ نظرية الأجيال أو علم اجتماع الأجيال. يقسم مانهايم الأجيال وفقا للأحداث والظواهر الاجتماعية المصاحبة لمواليد تلك الفترة، فيرى أن تلك الأحداث، بلورث سمات تلك الأجيال، وساهمت في تكوين شخصياتهم. الأجيال كالتالي: سار علماء الاجتماع المعاصرون على هذا النهج وتتبعوا تطور الأجيال، ووفق هذا التصنيف، يمكن تقسيم الى :

- جيل الألفية أو جيل y: وهو جيل الأفراد الذين ولدوا في الفترة من بداية الثمانينات إلى بداية التسعينات وربما لمنتصف التسعينات.

- جيل z: وهو جيل مواليد منتصف التسعينات إلى منتصف الألفية الثالثة، أي عام ٢٠٠٥ تقريبا .

يحدد الجيل في فترة زمنية معينة، وتسمى هذه الفترة بالمرحلة الإنتقالية الطبيعية، يطلق إسم الجيل بعد انقضاء العديد من السنوات، وخاصة في متوسط عمر حياة الآباء فور ولادتهم، وحياة أبناهم كذلك عند ولادتهم، أي أن الجيل هو تلك الفترة الانتقالية من الآباء إلى الأبناء، حدد الجيل في ٣٣ سنة أي ما يعادل ثلث قرن من الزمان، وسمي بالفترة الانتقالية الطبيعية، لانتقال الصفات الوراثية من الآباء إلى الأبناء . أي أن الجيل هو مرحلة تاريخية تستغرق حوالي ٣٠ سنة (ربع قرن تتميز بكونها تشهد سلسلة من الأحداث و التطورات التي تصبح تميز تلك المرحلة عن بقية المراحل السابقة و ربما اللاحقة. (فريح ٢٠٢١،٥٤٤)

مفهوم الحرب : تعرف الحرب بانها هي استخدام العنف المسلح المنظم بين الجماعات الإنسانية ، وأيضاً تعرف بأنها الوسيلة الأكثر قسرا للدولة لتحقيق أهدافها، ويقال أنها تستخدم لإنجاز السياسة الوطنية، ويعرفها العالم الالماني كلاوز فيتز بأنها الاستمرار بالسياسة ولكن بوسائل أخرى، كذلك هي عملية قديمة قدم الانسان، ففي المجتمعات القديمة كانت الحرب ظاهرة مألوفة من أجل اشباع الحاجات المختلفة . وفي ضوء ذلك هل تعد فكرة الحرب استمرار للسياسة فكرة مقبولة في الوقت الحالي؟ لا يمكن اطلاقا القبول بهذه الفكرة في العصر الراهن ، بسبب تعقد الحروب وصعوبة السيطرة على مجرياتها، فإشعال الحرب عملية سهلة، ولكن السيطرة على نتائجها وحدودها أمر غير ممكن حاليا؛ بسبب التطورات الحاصلة في الأسلحة والقدرة التدميرية، واتساع حدودها، وعدم وجود طرف ممكن أن يسيطر على غيره بسهولة ، وقد أثبتت الحربين العالميتين ذلك، وبالتالي؛ لا يمكن أن يتم الاعتماد على الحرب بشكل مطلق، لتحقيق أهداف السياسة الوطنية للدول، كونها ستأتي بنتائج سلبية. فقد تؤدي بعض الحروب إلى أن يتم إنشاء دول جديدة، على أثر تفكك دولة أو مجموعة من الدول، كحصول بعض الدول على الاستقلال بعد حرب معينة، كتفكك الاتحاد السوفيتي، والدولة العثمانية، وبالتالي، فإن الدول الجديدة التي تأسست تعد وليدة الحرب، وبالمقابل؛ فإن هذه الحروب أدت إلى إنهاء دول تدميرها، كالاتحاد السوفيتي والدولة العثمانية في المثال السابق. اما أهداف الدول من الدخول في الحروب هي :

١- وضع أهداف أطراف النزاع موضع التطبيق، فلكل طرف هدفا معينا من الدخول في الحرب، وبالتالي يسعى إلى تحقيقه . وأيضا تطمين حماسة الرأي العام بشرعية الأهداف المعلنة للحرب .

٢- الحصول على موقف ملائم من الدول المحايدة، والعمل على عدم السماح لهم قدر الامكان بالانتقال إلى الجبهة الأخرى. كذلك إقناع العدو وشعبه، بأن السلام هو البديل الأفضل بكثير من الاستمرار في الحروب.

اما طبيعة الحرب فتقسم الى ، الحرب بوصفها معركة مادية فهي أصبحت شاملة، ولم تعد أثارها محدودة النطاق، ولم يعد هناك استثناء في الاستهداف فليس كل استخدام محدود للقوة يعتبر حرب، والحرب بالمعنى المادي قديمة جدا، وباتت لا تميز بين هدف دون أخر، بل أصبح الشعوب كلها أهدافا في الحروب، وأصبح نطاقها أوسع بكثير، وباتت الدول تجند كافة امكانياتها المادية والتكنولوجية الحديثة، وأصبح هجف الحرب إخضاع العدو نفسيا، واضعافه قبل المواجهة المسلحة .

وأيضا الحرب بوصفها وضعا قانونيا : إذ تلعب الحروب دورا رئيسا في التأثير على بعض المعاهدات والاتفاقيات المعقودة بين الدول، فقد تلغي معاهدات معينة، وقد تنشأ عنها معاهدات جديدة، وإن قيام الحرب بالمعنى القانوني، يتطلب اعلان الحرب من قبل الدول المتحاربة وغالبا لا تعلن الدول بأنها في حالة حرب، أو إنها بدأت الحرب على دولة أخرى، خوفا من التبعات السياسية والقانونية، فاستخدام القوة في العلاقات الدولية أمرا محظورا وفقا لقواعد القانون الدولي . وبالتالي، فإن الحرب ليست مواجهة مادية فقط، إنما هي علاقة قانونية بين أطرافها. اما هي أسباب الحرب هي : (اسباب الاقتصادية ، اسباب السياسية ، اسباب النفسية والاجتماعية ، اسباب الدينية والأيديولوجية) . (عدوان، د.ت) وفي نفس السياق هنالك تصنيف للحروب وفقا لأسبابها منها :

١- الحروب لأسباب قومية وتتضمن حروب الاستقلال والتحرير الوطني : تقوم بها شعوب البلاد غير المستقلة أو التي استقلت حديثا اما للحصول على استقلالها او للمحافظة عليه ضد أي عدوان خارجي ، حروب لأغراض الاقليم ، حروب لا هداف اقتصادية، حروب المزايا الاستراتيجية .
٢- الحروب لأهداف اجتماعية وتشمل : الحروب الأهلية : والتي تقام لدعم او اضعاف نظام سياسي قائم والحروب لإبقاء او تغير النظام الاجتماعي القائم ، حروب الدول : وهى الحروب التي تدار بين الدول لتحقيق اهداف اقتصادية او استراتيجية او لمد اقليم تحت سلطة ما ، أو الحروب لأهداف أيدولوجية .
٣- الحروب لأهداف مختلطة : وهو ذلك التصنيف الذي تتدرج تحته تصنيف الحروب الي حرب سياسية ، اقتصادية ، واجتماعية ، وايدولوجية ، وذلك كما يلى : حروب اقتصادية والتي تقام لتحقيق مكاسب و موارد اقتصادية او لتأمين حاجة الدولة إلى الأسواق الخارجية ، حروب اجتماعية : وهى الحروب التي تقوم بين جماعات اجتماعية مختلفة في الدولة او طبقات أو منطقة معينه ، الحروب السياسية : وهي التي تنتج من الصراع الذي ينشأ بين وحدات مختلفة سياسيا ، الحروب الايدولوجية : وتنتج بفعل الاختلاف والتصادم بين جماعات مختلفة حول رؤيتهم للدولة والمجتمع والحكومة ،

الحروب الخاطفة : مفهوم عسكري يستخدم في العمليات الهجومية. تعتمد الحرب الخاطفة على استخدام عنصر المفاجأة والهجوم منها : الحرب الوقائية الضربة الاستباقية او الهجوم المسبق) الغزو ، والتدخل تقديم المعونة. (محمود، ٢٠١٩، ١٥٩)

اما مفهوم الحرب في اذهان العديد من الرؤساء الأمريكان عبر تأريخها الطويل فينطلق من كون الحرب ضرورة لأمريكا وضرورة لتثبيت مكانة الرئيس بين ساسة بلاده، وإن الحرب هي الوسيلة التي تكشف فيها الأمم موارد قوتها الداخلية والخارجية. أما في مفهوم الاسلام للحرب، فإن الاسلام يقدم لنا موقفاً لحضارة دينية لم تعرف في خبرتها التاريخية تناقضاً بين النظرية الاخلاقية والممارسة السياسية، لهذا نظر الاسلام الى الحرب باعتبارها ظاهرة تنجز وظيفة جهادية لها طبيعة مقدسة، ذلك ان أساس الاستراتيجية بمعناها الشامل في الفكر الاسلامي هو السلم وإقامة علاقات ودية مع الشعوب والأمم الاخرى التي تريد السلام أو تقبل به، انطلاقا مما دعى اليه القران الكريم في سورة البقرة، في الآية ٢٠٨ (يا أيها الذين آمنوا أدخلوا في السلم كافة)، إن الحرب في الاسلام هي حرب دفاعية حرب غير عدوانية تهدف الى حماية العقيدة ومحاربة الكفر والفساد والضلال، وان الحرب هي جزء من مفهوم وقيمة عليا هي الجهاد في سبيل العقيدة، حيث يأخذ الجهاد صيغ واشكال مختلفة من اجل حماية العقيدة ونشرها. (ولد خيري ٢٠٢٤) وإن انواع الحروب التي تشنها جيوش الدول وتتدرب من اجل القتال عليها بقصد تنفيذ غايات واغراض تلك الدول من الحرب هو(محدود، عامة، حروب الامن الداخلي، الحروب الثورية) (كنبر ٢٠٢١)، ليس هذا فقط فهنالك أشكال للحروب منها :

١. الحرب الأهلية: نزاع داخلي بين فئات معينة في دولة واحدة.
٢. الحرب الاستعمارية: صراع بين الدول للاستحواذ على الأراضي والموارد في مناطق جديدة.
٣. حرب الاستقلال: قتال من أجل التحرر من السيطرة الاستعمارية أو الاحتلال.
٤. حرب الاستنزاف: نزاع يهدف إلى استنزاف موارد العدو ببطء.
٥. الحرب الاقتصادية: استخدام الوسائل الاقتصادية لإضعاف العدو، مثل العقوبات والحصار.
٦. حرب الإبادة: محاولة منهجية للقضاء على مجموعة معينة من الناس.
٧. حرب الخلافة: صراعات على السلطة بين خلفاء أو زعماء سياسيين.
٨. حرب بالوكالة: نزاع يتم فيه استخدام أطراف ثالثة للقتال بالنيابة عن الدول المتنازعة. (شوا ٢٠٢٤)

المطلب الثاني: ماهية الأمن السيبراني

الأمن السيبراني هو مجموعة من الإجراءات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والمعلومات من الهجمات الإلكترونية والتهديدات المحتملة. يتجاوز الأمن السيبراني مجرد الدفاع عن البيانات؛ فهو يشمل أيضًا حماية البنية التحتية الحيوية التي تعتمد عليها الحكومات والشركات والمجتمعات.

كذلك يمكن أيضا تعريف الأمن السيبراني بأنه مجموعة من الممارسات والتقنيات التي تهدف إلى حماية المعلومات والأنظمة من الوصول غير المصرح به، التلاعب، أو التدمير. يتضمن ذلك استخدام أدوات وتقنيات متعددة لضمان سلامة البيانات وسرية المعلومات. اما العناصر الأساسية للأمن السيبراني هي :

١. حماية البيانات: ضمان سرية وسلامة المعلومات الحساسة.

٢. إدارة الهوية والوصول: التحكم في من يمكنه الوصول إلى الأنظمة والمعلومات.

٣. تحديد التهديدات: التعرف على التهديدات المحتملة وتحليلها.

٤. استجابة الحوادث: تطوير خطط للتعامل مع الهجمات السيبرانية والتقليل من آثارها.

٥. التوعية والتدريب: تعزيز الوعي بالأمن السيبراني بين الأفراد والمؤسسات.

اذن فالأمن السيبراني ليس مجرد خيار، بل ضرورة ملحة في عالم يزداد فيه الاعتماد على التكنولوجيا. يجب على الحكومات والشركات والأفراد العمل معًا لتعزيز الأمن السيبراني وضمان حماية المعلومات والبنية التحتية الحيوية. (مجموعة مؤلفين ٢٠٢٢، ٥–٦)

الأمن السيبراني : اللغة والاصطلاح

أولاً: الأمن السيبراني لغة : الأمن في اللغة العربية يعني ضد الخوف، وهو حالة الطمأنينة. وقد ورد في القرآن الكريم في عدة مواضع، مثل قوله تعالى: "الذي أطعمهم من جوع وآمنهم من خوف". في المعجم الوسيط، يُعرَّف الأمن بأنه اطمئنان الشخص دون خوف. أما كلمة "سايبر" (cyber)، فهي يونانية الأصل وترتبط بمصطلح "kybernetes" الذي يعني القيادة أو التحكم عن بُعد. في القواميس، تعرف السايبر بأنها علم الضبط، وتستخدم لوصف الفضاء الذي يضم الشبكات المحوسبة، حيث تشتق منها صفة السبرانية (cybernetic) التي تعني علم التحكم الأوتوماتيكي.

ثانياً : الأمن السيبراني اصطلاحاً : تحديد مصطلحات الأمن السيبراني يُعتبر تحديًا كبيرًا، حيث يتعرض الباحثون لتعقيدات تجعل من الصعب الاتفاق على تعريفات واضحة. يُعرف الأمن السيبراني بأنه مجموعة من السياسات والإجراءات والتقنيات المستخدمة لحماية البيئة السيبرانية، بما في ذلك أمن المعلومات والاتصالات. وفقًا لتقرير الاتحاد الدولي للاتصالات، يشمل الأمن السيبراني جميع الوسائل

اللازمة لحماية المعلومات من الهجمات والجرائم. ويُعتبر الأمن السيبراني سلاحًا استراتيجيًا للحكومات والأفراد، حيث أصبحت الحروب السيبرانية جزءًا لا يتجزأ من التكتيكات الحديثة.

أهمية وجود الأمن السيبراني ، تتطلب التحديات التي تواجه المجتمع وجود أطر تشريعية وتنظيمية تتناسب مع التطورات التكنولوجية ، اذا ان الأمن السيبراني أصبح قضية دولية تتطلب استراتيجيات مرنة متناسبة مع المتغيرات المستمرة. ويجب أن يتجاوز الاهتمام بالأمن السيبراني الأبعاد التقنية ليشمل الثقافية والاجتماعية والاقتصادية والعسكرية. (طارش وإبراهيم ٢٠٢٠، ١٥٧)

أهمية وأهداف الأمن السيبراني جزءًا أساسيًا من حياة الأفراد والمجتمعات، حيث يشمل حماية المعلومات والبيانات من التهديدات المختلفة. يتطلب هذا الأمر وعياً كبيراً بكيفية تأمين المعلومات، خاصةً في ظل تزايد الهجمات الإلكترونية ، تتزايد أهمية الأمن السيبراني بسبب:

١. حماية الأفراد: يجب حماية الأسر، وخاصة الأطفال، من الاحتيال عبر الإنترنت.
٢. حماية المعلومات المالية: ضمان سلامة المعلومات المالية التي تؤثر على الوضع المالي للأفراد.
٣. فرص العمل والتعلم: يوفر الإنترنت فرصاً كبيرة، مما يجعل حماية المعلومات أكثر ضرورة.
٤. تحديات الموارد: يواجه الأفراد والمؤسسات تحديات مثل محدودية الموارد وضعف المهارات في مجال الأمن السيبراني.

أهداف الأمن السيبراني تتمثل الأهداف الأساسية للأمن السيبراني في :

١. السرية: ضمان أن الأشخاص المصرح لهم فقط يمكنهم الوصول إلى المعلومات.
٢. النزاهة: التأكد من أن التغييرات في النظام تتم بواسطة أشخاص أو عمليات مصرح بها فقط.
٣. التوفر: ضمان أن المعلومات والنظام متاحة للأشخاص المرخص لهم فقط.

يُعتبر الأمن السيبراني عنصرًا حيويًا في حماية البيانات والمعلومات، مما يتطلب استراتيجيات فعالة لإدارة المخاطر. يجب أن تتعاون الحكومات والمنظمات لتوفير بيئة آمنة للجميع في ظل التهديدات المتزايدة. (سلمان ٢٠٢١، ١٥٨–١٦٠)

وبات صناع القرار في الولايات المتحدة الأمريكية، والاتحاد الأوروبي، وروسيا والصين والهند، يصنفون الأمن السيبراني كأولوية في استراتيجية سياستهم الدفاعية الوطنية، وقد اعلنت اكثر من ١٣٠ دولة عن تخصيص اقساماً وسيناريوهات خاصة بالحروب والهجمات السيبرانية ضمن فرق الامن الوطني، فالدول اليوم تسعى الى تطوير استراتيجيتها للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة الخاصة بها وردع الجريمة السيبرانية عن طريق انشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات بالاضافة الى

خلق قدرات وطنية الادارة الحاسب الآلي . فوظيفة الأمن السيبراني هي ليست حماية المعلومات فقط وانما يشمل كل جزء رقمي في الفضاء الالكتروني وخلق حالة من السرية والنزاهة فيه . (العلي ٢٠١٩، ٥٧)

المطلب الثالث: تطور أجيال الحروب

خلال المراحل التاريخية التي مرت بها الشعوب في صراعاتها تطورت أجيال الحروب المتعاقبة لتلبي الإحتياجات المتزايدة لإدارة تلك الصراعات في شتى أنحاء العالم وبذلك إنتقلت أجيال الحروب عبر السنين من مرحلة إلى أخرى في تطور طبيعي حمل أفكاراً ورؤى أدت إلى تحديث كل منظومة الحرب من تدريب الأفراد إلى نوعية السلاح المستخدم إلى النظريات والخطط العسكرية المتبعة فيها ومن هذا المنطلق صنف خبراء الفكر العسكري الحروب تصنيفاً دقيقاً حسب الفترات التي دارت فيها وكذلك بحسب المعدات التي إستخدمت فيها ، فكانت حروب الجيل الأول وهكذا تباعاً وأختص كل جيل من الحروب بنوع معين من التكتيكات والعمليات ونوعية الأسلحة والمعدات المستخدمة فيها. هذه الاستمرارية في الحروب جعلت الخبراء العسكريون يعملون على تطوير آلياتها حتى تتوافق مع الزمان والمكان والتطور التقني والفني الذي بات يفرض نفسه على نوعية الحروب وبالتالي قسمت الحروب ومعداتها إلى أجيال متعاقبة يتوقف فهمها على طبيعة العمليات العسكرية التي تجرى فيها وطبيعة الأرض وأيضاً طبيعة الخصم. (الأنصاري، ٢٠٢١) وهنا يجب القول بأن أجيال الحروب غير محددة بزمن وعدد سنين بل هي رهن لطبيعة الحرب ذاتها وتطورها الذي عادة ما يصاحب التطور الفكري والتقني للأمم والشعوب وبذلك قسمت الحروب إلى أجيال محددة كان آخرها الجيل الرابع والذي ذاع صيته مؤخراً سنتناول بالوصف في هذا المقال سمات كل جيل من أجيال الحروب بحسب تسلسلها بما يعطي نبذة موجزة عن مراحل تطور الحروب عبر اجيالها المتعاقبة.

١- **حروب الجيل الأول** : أطلقت تسمية الجيل الأول من الحروب على الحروب التقليدية التي دارت رحاها بين جيشين على أرض واحدة وفي ميدان محدد تكون فيها المواجهات المباشرة بين الخصمين في جبهة واحدة بشكل تصادمي وهذا الجيل من الحروب سمته الرئيسية بروز مقومات الفروسية والشجاعة والإقدام على مستوى القادة والأفراد والقادة وتسمى أيضاً بالقتال الخطي والتلاحمي . نفذت خلال حروب الجيل الأول عدد محدود من العمليات العسكرية وحققت نجاحات كبيرة كعمليات المناورة والإلتفاف لتطويق الخصم وضربه في أجنحته للقضاء عليه وتدميره بدأت هذه النوعية من الحروب مبكراً مع تطور محدود وعرفتها البشرية منذ القدم وأستمرت حتى فترة ما قبل الحرب العالمية الثانية.

٢- **حروب الجيل الثاني** : وامثالها حرب العصابات أو الحرب الثورية ، أي التي تكون بين جيش نظامي وقوات غير نظامية ، الا ان الادوات المستخدم كانت اسلحة ومواجهات مباشرة ، في ميادين تتباين بين ساحات مواجهة مباشرة وفي المدن والتجمعات البشرية ، هدف المجموعات المقاتلة يكون بلوغ هدف تحرير الارض او تحقيق ضغط على الجيوش النظامية ، وكان التكتيك الاستراتيجي المعمول به هو إستنزاف العدو من خلال عمليات المناورة من جهات متعددة والتركيز على الساحات الخلفية للمعارك ، وخلال هذه المرحلة حلت القوة النارية محل القوة البشرية التي استثمرت الهجمات المشتتة بمجموعات صغيرة ذات قوة نوعية. (Van Der Klaauw 2021, 72)

٣- **حروب الجيل الثالث:** ظهرت حروب الجيل الثالث من وحي نظرية الردع بالشك وهي نظرية سياسية عسكرية ظهرت في الولايات المتحدة الأمريكية عقب انهيار الاتحاد السوفييتي السابق وهي تعني عملياً الضربة الاستباقية وشن الحرب ضد ما من شأنه أن يهدد الأمن القومي الأمريكي أو السلم العالمي على حد تعبير الإدارة الأمريكية. ويطلق عليها كذلك حرب المناورات وهي إستراتيجية طورت سابقاً من قبل الألمان في الحرب العالمية الثانية وأستخدمت ضد بريطانيا بقصفها المتواصل بالطائرات وصواريخ V٢ وتميزت العمليات الخاصة بحروب الجيل الثالث بالمرونة والسرعة في الحركة واستخدم فيها عنصر المفاجأة وأيضاً الضرب بشدة وراء خطوط العدو ويستخدم فيها عادة سلاح الطيران والقاذفات الإستراتيجية البعيدة المدى والصواريخ الموجهة على وجه الخصوص ولعل ما شاهده وسمع العالم عنه في حرب العراق الثانية يلقي كثيراً من الضوء على نوعية هذه الحروب وتصاحبها في العادة حملات إعلامية مركزة .

٤- **حروب الجيل الرابع** : تسمية الجيل الرابع أطلقها الأمريكان في الحرب على المنظمات الإرهابية وحسب المفهوم الأمريكي يكون طرفيها جيش نظامي لدولة ما مقابل لا دولة أو خصم على صورة خلايا خفية منتشرة في أنحاء العالم وقد اتفق الخبراء العسكريين على أن حرب الجيل الرابع هي حرب امريكية النشأة والصناعة طورت من قبل قيادة الجيش الأمريكي وأسموها بـالحرب اللا متماثلة. هذه النوعية من الحروب نشأت عندما وجد الأمريكان أنفسهم يحاربون كياناً لا يعتمد وطناً له ولا دولة ولا جيش نظامي بل تنظيم يحمل طابع ديني أو سياسي بأيدلوجية محددة تنتشر حول العالم ويمتلك إمكانيات جيدة لضرب مصالح حيوية لدول أخرى لإضعافها أمام الرأي العام العالمي ، ومثال على هذه التنظيمات : تنظيم القاعدة بمختلف فروعه ، حزب الله ، أنصار الشريعة ، تنظيم الدولة داعش وآخرها جماعة الأخوان المسلمين والتي صنفت مؤخراً في عدد من الدول كتنظيم إرهابي وفي هذا

الجيل من الحروب تستغل وسائل الإعلام التقليدية والحديثة إلى جانب العمليات الإستخبارية للقيام بدور كبير لإضعاف الخصم والتأثير عليه ومثالها الحرب على الإرهاب التي قادتها أمريكا في العراق وفي اليمن وفي أفغانستان وفي باكستان بضربات ماحقة وستقودها أينما إستشعرت الخطر على أمنها ومصالحها . (الأنصاري ٢٠٢١)

٥- **حروب الجيل الخامس** : يطلق عليها بالحرب الهجينة (حروب الهايبرد) ، وتتمثل بوصف حروبها بانها غير نظامية ، تستخدم فيها مفاهيم الحرب الشعبية أو الثورية بوسائل الحرب الحديثة ، مستغلة التكنولوجيا المتقدمة، ولا توجد فيها مراكز قيادة للطرف غير الظاهر والذي يمكن إستهدافه وتحقيق النصر عليه ، وأكثر صوره تماس هي مع مجموعات عقائدية مسلحة وجماعات الجريمة المنظمة والمافيات ، ان حروب هذا الجيل هي حروب مفتوحة تتداخل في بعض الأحيان عملياته دون قيود أخلاقية وتستخدم فيه وسائل القوة المتوفرة المسلحة وغير المسلحة كافة الإجبار الخصوم للخضوع الإرادة من يشن الحرب أو يستمر بها هذه الحرب هي مزيج من الحروب الحركية وغير الحركية الموجهة بالاشخاص والتكنولوجيا. وتتميز حروب الجيل الخامس بتكتيكات الحروب الدعائية وأساليب الخداع الجماهيري التي تستغل الرموز الثقافية والمشاعر الدينية كوسيلة لخلق دعم سياسي من خلال نشر معلومات متلاعب بها وموجهة لتفكيك الهوية وخلق سوء الفهم لتغييب الروابط الاجتماعية واشاعة الصدامات المجتمعية داخل العقيدة الواحدة ، وأطلق عليها بحروب الهايبرد أي حروب منصات الفضاء الالكتروني الموجهة المدمجة بالوسائل التقليدية من خلال الدول المالكة للتقنية ، وسميت كذلك بالحروب الصامتة التي تستند بتحقيق النتيجة المرجوة من دون استخدام العنف من خلال التلاعب بالثقافة على مستوى اللاوعي للمجتمعات. وتعد الحرب الجوية عن بعد أحد أبرز أشكال حروب الجيل الخامس والسادس التي تشكل أسس الاستراتيجية الحربية الأمريكية التي تقوم عملياتها من خلال توجيه طائرات الدرونز وكذا الحال في حروب الاغتيالات الصامتة التي تقوم بها (إسرائيل) في الكثير من الاحيان والتي تمثل الدول الرائدة في استراتيجيات توجيه الضربات الذكية الموجهة من بعد والتي تستخدم في عمليات التصفية ، أن هذه الاجيال تركز على تطويع التكنولوجيا واستخدام ادوات حروب مدمجة والتي تتم برمجتها الكترونياً ، وواحدة من تطبيقاتها هو القتل الدقيق للقيادات التي تصفها بالإرهابية او الاشخاص الذين يشكلون خطراً وتهديداً محتملاً لمصالح من يلجأ الى استخدامها ومن امثلتها عملية اغتيال العالم النووي الايراني محسن فخري زاده في طهران والذي مثل نقلة نوعية في تكنولوجيا الاختراق المعلوماتي التي جمعت بين العمل الميداني

الموجه بشبكات الاقمار الصناعية وتكنولوجيا توجيه الأسلحة فائقة التطور . (Quresh 2019, 209–212) وكذلك (Rudolf 2014, 36–38)

٦- **حروب الجيل السادس :** يمكن أن نطلق عليها تسمية الحرب عن بعد وهي حرب تعتمد التقنية عالية الدقة لإدارة وسائطها القتالية التي تدار عن بعد أسلحتها ومعداتها ذكية ، وهذا التصنيف يعتبر الأحدث في أجيال الحروب أطلقته روسيا باعتبار أن هذا النوع من الحروب لا يعتمد على الاتصال بشكل مباشر بالخصم و بمعنى آخر أنها حرب تدار بشكل كامل عن بعد وتتسع دائرتها لتشمل كل ما هو معني بمفهوم الحرب سواء كانت أسلحة أو إمكانيات بدءا من الأسلحة النووية التكتيكية إلى إدارة الصراع الاقتصادي والمعلوماتي الى استهداف الأفراد أنفسهم عن بعد سواء كانوا فرادى أو مجموعات وقد صاغ مصطلح "الجيل السادس للحرب" لأول مرة الجنرال الروسي فلاديميرسليبتشينكو عند استخدام أنظمة تسليح عالية الدقة يمكنها أن تجعل من تسليح وتنظيم الجيوش التقليدية أمور عفا عليها الزمن . وأخطر ما في حروب الجيل السادس هو استهدافها للإنسان وعقله وعواطفه واستغلال كل ما في الطبيعة من حوله كسلاح يدار ويسيطر عليه كمشاريع التحكم في الطبيعة "مشروع هارب" وأيضاً تصرفات الكائنات الحية وغيرها من المشاريع المتطورة التي تستهدف إلحاق أكبر ضرر بالجنس البشري واستغلال الحشرات والطيور والأسماك وغيرها من الكائنات كأدوات للتجسس والسيطرة . من سمات حروب الجيل السادس البراعة العالية في استخدام الوسائط القتالية والتفوق في تحقيق الأهداف والمصالح والسيطرة على الآخرين بأقصر الطرق واقل الخسائر وبذلك ستغدو معها كل تلك الترسانات من الأسلحة والمعدات وكأنها أسلحة شخصية لن تستطيع الجيوش إستخدامها مطلقاً . وبذلك أعتقد بأن أجيال الحروب ستستمر في التقدم بصورة مضطردة وستشمل في صورها الجديدة أنواع متعددة سابقة وحديثة متداخلة من فنون القتال وأنواعه وستستغل كل ما تصل إليه التقنية والتطور العلمي في مختلف المجالات ولذلك فحروب المستقبل ستكون غير محددة بنوع ونمط قتالي معين عرفه العالم من قبل ، الغاية فيه تبرر الوسيلة وهدفها الاسمى هو سحق الخصم حتى قبل أن يستعد للحرب والسيطرة على العالم ومصادر الماء والطاقة فيه بالقوة العسكرية المطلقة. لم يتفق العالم وخبراء السياسة والعسكر على مقومات معينة تحدد أجيال الحروب وتركت لإجتهاد المحللين فهناك من لايزال يعتقد بأن الحروب و الأعمال العدائية والنزاعات المسلحة لا تزال ضمن الجيل الرابع وشخصياً أعتبر بأن الأمر قد تجاوز في تسارع كبير نحو الجيل السادس من الحروب التي بدأت وسائطه المعتمدة على التفوق التقني والذكاء الصناعي في الدخول للمناوبات القتالية

والخدمة العملية في كثير من الجيوش وقد تداخلت فيها أجيال الحروب حتى أمتزج قديمها بجديدها في تطور فكري عسكري مستمر متناسق مع التطور العلمي الذي يسابق الزمن وظهرت نتائج ذلك في تدريب المقاتلين وحرفيتهم العالية والتطور النوعي في دقة الوسائط القتالية المستخدمة من الأسلحة الذكية والطائرات بدون طيار والمركبات المسيرة الغير مأهولة وأسلحة الفتك ذات الدقة العالية وتطور عمليات القيادة والسيطرة عبر الأقمار الصناعية. (Alderman 2015)

٧- **حرب الجيل السابع** : ستشمل القدرات العسكرية الاستراتيجية مع الامكانيات التقنية البرمجية التي تم التعبير عنها بتمثيلها بحرب آلية بالكامل ، إذ ستقوم على تكتيكات مبرمجة ومنظمة وفق معادلة حربية) من خلال إغلاق أنظمة الاتصالات التجارية والعسكرية الخاصة بالعدو وشبكات الطاقة ومرافق المياه واستخدام منظومة الكترونية متقدمة وأسلحة إلكترونية واستراتيجية مزودة بتقنيات النبض الكهرومغناطيسي التي تؤدي الى تعطيل المجالات الحيوية في عصر المعلوماتية لتدمير الاقتصاد والنظام المصرفي الالكتروني والتحكم بالمجال الجوي بواسطة أسراب من منصات الاسلحة المستقلة (الطائرات بدون طيار (والتحكم بالموانئ والسواحل بواسطة أسراب من سفن سطحية وطوربيدات ذكية ، فضلاً عن أنظمة جمع المعلومات الاستخباراتية عبر الاقمار الصناعية وهو ما يعني إخضاع العدو دون قتال ، والتي ستكون مدخلاً لحروب الجيل الثامن المستقبلية ، والتي ستكون أكثر تطوراً عن حروب الجيل السابع التي من المفترض أنها ستكون حرب آليات متبادلة ومتكاملة بشكل آخر يشير اليها بإعتبارها (حرب العوالم) والتي تستنبط من الخيال العلمي تطبيقات واقعية محتملة لتطور الجيل السابع، بالتالي فإن حروب الجيل الثامن سيكون فيها الانسان خارج دائرة محاور الحرب وستكون الآلات هي الموجهة والمسيرة للحروب وستقوم بإداء وظائفها دون عوائق ، مما عد حروب الجيل السابع والثامن ضرب من الخيال بإعتبار أن العالم اليوم ما زال في حاجة ملحة إلى إستيعاب حروب الجيل الخامس والسادس، التي يصعب تفسيرها من حيث عدها وسيلة أو غاية سياسية ، قبل الانتقال الى تطوير اجيال حروب المستقبل في الجيلين السابع والثامن. (سعدون ٢٠٢٢، ١٥٠)

ختاماً كل أجيال الحروب وتطورها عبر التاريخ لم تكن لتثني جيوش الدول الصغيرة التي قد لا تملك التقنية والعتاد الحربي المتطور عن أن تقوم بأداء مهامها وواجباتها ، لأن مهمة الدفاع عن الأرض والعرض مهمة وطنية مشرفة تقدسها الأديان وتبذل فيها المهج والأرواح ويتسابق فيها الجميع لنيل مرتبة الشهادة التي لا تعدلها مرتبة ويبقى الإيمان والعقيدة والمعنويات دافعاً مهماً للدفاع والذوذ عن الأوطان مهما تفوق الخصم ومهما تطورت أجيال الحروب.

المبحث الثاني

انعكاس الامن السيبراني على الامن القومي للدول

المطلب الأول: خصائص الامن السيبراني

مع التطور التكنولوجي الهائل الذي يشهده العالم في العصر الحديث، أصبح الاعتماد على أنظمة المعلومات والتقنيات الرقمية أمرًا ضروريًا في مختلف جوانب الحياة، سواء في القطاع الحكومي أو الخاص أو حتى على المستوى الشخصي. غير أن هذا الاعتماد المتزايد أدى إلى ظهور تحديات جديدة تتعلق بحماية المعلومات والأنظمة من التهديدات السيبرانية المتزايدة والمتطورة باستمرار. من هنا، برزت أهمية الأمن السيبراني كعنصر أساسي لضمان سلامة البيانات والمحافظة على الخصوصية وحماية البنية التحتية الرقمية من الهجمات والاختراقات . الامن السيبراني مجموعه من الخصائص التي تميزه عن غيرة من المجالات وهي كما يأتي :

١- الثقة وعدم الثقة : يستخدم جدار الحماية لتصفية البرامج والتأكد من أمانها. يتم التعامل مع جميع البرامج على أنها غير موثوقة حتى يتم التحقق من مصدرها وأمانها. هذا يساعد في منع البرامج الضارة من اختراق النظام.

٢- الحماية من التهديدات الداخلية : تتعلق هذه الخاصية بحماية الأجهزة من المخاطر الناتجة عن المستخدمين الذين قد يكون لديهم معرفة محدودة بأمان المعلومات. يمكن أن يؤدي جهل المستخدم إلى السماح بتفعيل برامج غير موثوقة، مما يتطلب أنظمة حماية سريعة للكشف عن هذه التهديدات.

٣- الحماية من التهديدات الخارجية : تشمل هذه الخاصية بناء جدران حماية قادرة على تصفية المخاطر القادمة من الإنترنت، مثل الفيروسات والبرمجيات الخبيثة. الهدف هو حماية النظام من الهجمات التي تستهدف البيانات الحساسة.

٤- رؤية شاملة : تهدف هذه الخاصية إلى توفير رؤية واضحة للمستخدمين حول نقاط القوة والضعف في أنظمتهم. من خلال التحليل المستمر، يمكن اكتشاف الثغرات التكنولوجية بسرعة، مما يساعد على اتخاذ إجراءات تصحيحية.

٥- مراقبة مستمرة : يعمل نظام الأمن السيبراني على مراقبة الشبكة بشكل دائم. لا تقتصر عملية المراقبة على فترات زمنية معينة، بل تستمر على مدار الساعة لاكتشاف أي خلل أو نشاط غير معتاد.

٦- لامتثال للسياسات والقوانين : تتطلب هذه الخاصية الالتزام بالقوانين والسياسات المتعلقة بأمان المعلومات. يهدف ذلك إلى حماية البيانات الحساسة ومنع الوصول غير المصرح به أو إساءة استخدام المعلومات.

٧- التنوع : يجب أن يتضمن نظام الأمن السيبراني حلولاً متعددة للتعامل مع أنواع مختلفة من التهديدات. هذا يعني أنه يجب أن يكون قادرًا على تحليل واكتشاف والتعامل مع مجموعة متنوعة من الهجمات التي قد تهدد سلامة المعلومات. (دون مؤلف ٢٠٢٣)

٨- السرية (Confidentiality): تعني حماية المعلومات من الوصول غير المصرح به أو الكشف عنها لأشخاص أو جهات غير مخوّلة. تُستخدم وسائل مثل التشفير وكلمات المرور وتقنيات إدارة الهوية للتحكم في صلاحيات الوصول وضمان عدم تسرب البيانات.

٩- السلامة (Integrity): تشير إلى المحافظة على دقة واكتمال المعلومات والبيانات أثناء تخزينها أو نقلها أو معالجتها، بحيث لا يتم تعديلها أو حذفها من قبل جهات غير مخوّلة. تُستخدم تقنيات مثل التواقيع الرقمية والهاشات (Hashing) للكشف عن أي تغيير غير مصرح به.

١٠- التوافر (Availability): تعني ضمان أن تكون الأنظمة والمعلومات متاحة للمستخدمين المصرح لهم عند الحاجة، دون تعرضها لانقطاع أو تعطيل متعمد أو غير متعمد. تشمل الإجراءات هنا صيانة الأنظمة، وتخطيط استمرارية الأعمال، وحماية الشبكات من هجمات (حجب الخدمة) DDoS.

١١- المصادقة (Authentication): تعني التأكد من هوية المستخدمين أو الأنظمة أو الأجهزة قبل السماح لهم بالوصول إلى الموارد أو المعلومات. تشمل وسائل المصادقة كلمات المرور، والبطاقات الذكية، والتحقق الثنائي (FA٢)، والبيانات الحيوية مثل بصمة الإصبع.

١٢- عدم التنصل (Non-repudiation): تعني ضمان عدم قدرة الأطراف المشاركة في عملية معينة من إنكار القيام بها لاحقًا. يتم تحقيق ذلك غالبًا من خلال التوقيعات الرقمية والسجلات الإلكترونية التي تثبت صحة العمليات والإجراءات.

١٣- المساءلة (Accountability): تعني القدرة على تتبع وتحديد الجهة المسؤولة عن القيام بأي إجراء داخل النظام، مما يسهل كشف الأنشطة المشبوهة أو غير القانونية. يتم ذلك من خلال تسجيل الأحداث (Log files) ومراقبة الأنشطة باستمرار.

وفي نفس السياق ، تلعب خصائص الأمن السيبراني دورًا جوهريًا في حماية المعلومات والأنظمة من المخاطر والتهديدات المتزايدة، وتُسهم في بناء الثقة بين المستخدمين ومزودي الخدمات الرقمية. كما تساعد المؤسسات على الامتثال للمعايير واللوائح الدولية والمحلية، والمحافظة على سمعتها، وتجنب الخسائر المالية الناتجة عن الهجمات السيبرانية. يمثل الأمن السيبراني حجر الأساس في حماية الأنظمة الرقمية والمعلومات الحساسة من التهديدات المتنوعة. وتعد خصائص الأمن السيبراني، مثل السرية والسلامة والتوافر والمصادقة وعدم التنصل والمساءلة، عناصر رئيسية لا غنى عنها لأي منظومة معلوماتية حديثة. لذلك، يجب على المؤسسات والأفراد إدراك أهمية هذه الخصائص وتطبيق أفضل الممارسات والإجراءات لتعزيز حماية بياناتهم وأنظمتهم ضد الهجمات السيبرانية المتزايدة. (مصطفى، ٢٠٢٤)

عناصر الأمن السيبراني :

يعتبر الأمن السيبراني جزءًا أساسيًا من عالم التكنولوجيا الحديثة، حيث يعمل على حماية الأنظمة الإلكترونية والشبكات من التهديدات السيبرانية. يتضمن الأمن السيبراني عدة عناصر رئيسية يجب أخذها بعين الاعتبار:

١- أمن التطبيقات : يتعلق أمن التطبيقات بحماية البرمجيات والتطبيقات الخاصة بالمؤسسات. من الضروري التأكد من أن البرمجيات المستخدمة تتوافق مع معايير الأمان المعتمدة وخالية من الثغرات. يتم ذلك من خلال إجراء فحوصات واختبارات أمان للتأكد من عدم وجود نقاط ضعف يمكن أن يستغلها المهاجمون.

٢- أمن الشبكات : يتعلق أمن الشبكات بحماية البنية التحتية والأنظمة المتصلة بها. بعد تأمين نقاط الدخول إلى الشبكة، يمكن حماية المعلومات المخزنة والمرسلة عبر طرق مؤمنة. تشمل هذه العملية تطبيق إجراءات الحماية مثل جدران الحماية (firewalls) وتحديد الأدوار والصلاحيات للمستخدمين. والأمن السيبراني يوفر حلولاً فورية تساعد في السيطرة على البيانات ومنع سرقة المعلومات. تقدم "النور أون لاين" خدمات متكاملة لأمن الشبكات، بما في ذلك حماية الشبكات من الهجمات ورصد الحركة وتحليل التهديدات.

٣- الأمن التشغيلي : يتعلق الأمر بضمان استمرارية وثبات عمل الأنظمة والخدمات التكنولوجية. يتضمن ذلك تنفيذ احتياطات للتعامل مع الانقطاعات الطارئة أو الأعطال، بالإضافة إلى تحديث البرمجيات والأجهزة بشكل دوري لحمايتها من التهديدات الجديدة.

٤- أمن التعافي من الكوارث : يشير أمن التعافي من الكوارث إلى الخطط والإجراءات اللازمة للتعامل مع الحوادث السيبرانية. يتضمن ذلك إنشاء نسخ احتياطية للبيانات وتطوير استراتيجيات لحماية واستعادة الأنظمة بعد الكوارث.

٥- أمن المعلومات : يتعلق أمن المعلومات بحماية سرية وسلامة المعلومات الحساسة. يجب تنفيذ سياسات صارمة لإدارة وحماية المعلومات، بما في ذلك تحديد حقوق الوصول وتشفير البيانات. (موقع النور اون لاين ٢٠٢٥)

٦- إدارة الهوية والوصول : تتعلق هذه العنصر بتحديد من يمكنه الوصول إلى المعلومات والأنظمة. يجب تنفيذ سياسات قوية للتحكم في الوصول، مثل استخدام المصادقة متعددة العوامل (MFA) وتحديد صلاحيات المستخدمين بناءً على أدوارهم.

٧- الأمن السحابي : يشمل هذا العنصر حماية البيانات والتطبيقات المخزنة في السحابة. يجب أن تتضمن استراتيجيات الأمن السحابي تشفير البيانات، ومراقبة الوصول، وتقييم مخاطر مزودي الخدمات السحابية.

٨- الأمن الفيزيائي : يتعلق هذا العنصر بحماية البنية التحتية المادية التي تحتوي على الأنظمة والمعلومات. يشمل ذلك تأمين المرافق، واستخدام أنظمة المراقبة، وتقييد الوصول إلى مناطق حساسة.

٩- التوعية والتدريب : يعتبر التدريب والتوعية جزءًا أساسيًا من الأمن السيبراني. يجب على المؤسسات تقديم برامج تدريبية للموظفين لزيادة الوعي حول التهديدات السيبرانية وكيفية التعامل معها بشكل صحيح.

١٠- استجابة الحوادث : تتضمن إنشاء خطط وإجراءات للتعامل مع الحوادث السيبرانية عند حدوثها. يشمل ذلك تحديد فرق الاستجابة، وتوثيق الحوادث، وتحليل الأسباب الجذرية لتفادي تكرارها.

١١- تقييم المخاطر : يشمل تقييم المخاطر تحليل التهديدات المحتملة وتحديد نقاط الضعف في الأنظمة. يجب إجراء تقييمات دورية لتحديث استراتيجيات الأمان بناءً على المخاطر الجديدة.

١٢- الامتثال والتقارير : تتطلب العديد من الصناعات الالتزام بمعايير ولوائح معينة تتعلق بالأمن السيبراني. يجب على المؤسسات التأكد من الامتثال لهذه القوانين، وإجراء تقارير دورية حول حالة الأمن.(Exabeam, n.d.) ، بهذه العناصر، يمكن تحقيق مستوى عالٍ من الأمان السيبراني وضمان حماية فعالة للأنظمة والمعلومات.

المطلب الثاني: فرضيات الامن القومي

بات كل حديث عن الأمن القومي في العالم المعاصر يتخطى مفهوم تخوم ميدان الحرب و الأمن الدفاعي و الإستراتيجيات العسكرية ليتصل بميادين الاقتصاد و الاجتماع و الثقافة . ففي التعريف الحديث لأمن القومي ، لم تعد المؤسسة العسكرية هي الجهة المنوطة بمهمة حماية ذلك الأمن وتحقيق المصالح القومية العليا أو صيانتها ، بل غدت تشاركها الدور نفسه، المؤسسات الاقتصادية و المدنية والحق أن هذا التوسيع لدائرة مفهوم الأمن لم يكن حصيلة ترف نظري لدى المشتعلين في حقل الإستراتيجيا، بمقدار ما أتى يعبر عن التمفصل الموضوعي للمستويات العسكرية و الاقتصادية والاجتماعية في تكوين نسيج الأمن الخاص بمجتمع أو امة في عالم جديد نزاع إلى تحقيق الترابط والتداخل بين مستويات بالنظام الاجتماعي .

قبل عقود قليلة خلت ، كان مجتمع ما يستطيع أن يضمن لنفسه إشباعا أمنيا ذاتيا من خلال تطوير قدرته على حماية سيادته وترابة في الاستباحة الخارجية ، و لم يكن يكلفه ذلك أكثر من تطوير بنيته التحتية العسكرية وقدراته الميدانية على القتال أو الدفاع . و المفهوم من ذلك أن معنى الأمن تطابق حينه مع معنى السيادة الترابية ، فكان أن أوكلت مهمة حراسة تلك السيادة إلى جهاز من الدولة خاص بأداء المهمة عينها هو الجيش و من يتفرع عنه من أجهزة ملحقة كالمخابرات و مراكز الدراسات الإستراتيجية . (زروقي ٢٠١٣، ٢٣١)

يتم فيما يلي تقديم تعريف إجرائي لمفهوم الأمن القومي وذلك من خلال التعريف اللغوي والاصطلاحي للكلمتين اللتين يتكون منهما المفهوم:

١- التعريف اللغوي والاصطلاحي المفهوم الأمن:

الأمن في اللغة هو نقيض الخوف والفعل الثلاثي أمن أي حقق الأمان. قال ابن منظور : أمنت فأنا أمن، وأمنت غيري أي ضد أخفته، فالأمن ضد الخوف، والأمانة ضد الخيانة، والإيمان ضد الكفر، والإيمان بمعنى التصديق، وضده التكذيب، فيقال أمن به قوم وكذب به قوم". " وقد ورد المفهوم في القرآن الكريم بقوله تعالى: فليعبدوا رب هذا البيت الذي أطعمهم من جوع وآمنهم من خوف. تتفق معظم الأدبيات التي قامت بتعريف مفهوم الأمن على أن المفهوم يشير عموماً إلى تحقيق حالة من انعدام الشعور بالخوف، وإحلال شعور الأمان ببعديه النفسي والجسدي محل الشعور بالخوف والشعور بالأمان قيمة إنسانية كونية مرغوبة لا تقتصر على فئة اجتماعية معينة أو مرتبطة بمستوى الدخل، فالفقير مثل الغني يحتاج إلى الشعور بالأمان ويسعى إلى تحقيقه وإن اختلفت درجات المتمتع به، ونظراً لصعوبة تحقيق الأمان الكامل، فقد أصبح ينظر للأمن على أنه مسألة نسبية مرهونة بالسعي لتعزيز أفضل الشروط لتوافره."

٢- التعريف اللغوي والاصطلاحي لمفهوم القومية:

المادة اللغوية لكلمة القومية هي (ق. و.م)، والقوم يعني الرجال دون النساء، وهو لفظ جمعي لا واحد له، وربما يدخل النساء فيه على سبيل التبع، وجمع القوم أقوام. أما الفعل الثلاثي منها قام، والرباعي .أقام، ومنها يأتي معني الارتباط بالمكان، والقوم هم الجماعة التي ترتبط بمكان ما وتقيم فيه. وعندما يوجد قوم من الناس في أرض واحدة ويمارس أفراده الحياة بثقافة واحدة توجد بينهم علاقات أخرى قوية تدور حول المصلحة المشتركة والتضامن والنسب، وعلاقات اجتماعية تجعلهم بدأ واحدة. وتلك الروابط هي التي توجد ما يسمى بالقومية. (عبد الرحمن ٢٠٢٠)

أهداف الأمن القومي :

تقوم منظومة العلاقات الدولية على ركيزتين أساسيتين: المصلحة الوطنية والقوة. تُعتبر القوة المفتاح الرئيسي في العلاقات الدولية وفقاً للمدرسة الواقعية، وتعتمد بشكل كبير على المصلحة الوطنية، التي تُعبر عن القيم والمصالح الوطنية للدولة. يُعتبر تحقيق المصلحة الوطنية الهدف الأساسي للدول، وهو المفتاح في السياسة الخارجية.

١- تحقيق المصلحة الوطنية : تُعتبر المصلحة الوطنية من العوامل الحاسمة في السياسات الخارجية، حيث يفكر صناع القرار في تأثير قراراتهم على الأمن القومي. تُعد المصلحة والأمن القومي المرتكز الأساسي الذي يُبنى عليه اتخاذ القرارات السياسية، سواء في الحرب أو السلم. التدخل في قرارات أي دولة يتعلق بسياستها الوطنية يُعتبر انتهاكاً للقوانين الدولية، إلا أن كثيراً من الدول تتجاهل ذلك عندما تتعارض مصالحها مع مصالح الآخرين.

٢- التأثير على سلوك الدول :يهدف السلوك الاستراتيجي إلى تغيير معادلة السيطرة على منطقة معينة. في ظل التغيرات السياسية العالمية، يصبح تحقيق هذا الهدف معقداً، خاصة أن القوة النوعية لكل دولة تؤثر في توازنات القوى. الولايات المتحدة، على سبيل المثال، لم تعد المتحكم الأوحد في منطقة الشرق الأوسط، حيث ظهرت قوى جديدة تسعى للسيطرة والنفوذ.

٣- التوسع في نفوذ الدولة خارجياً: تُعتبر ظاهرة الصراع الدولي بين القوى العظمى من العوامل المؤثرة على الأمن والسلام الدوليين. تسعى القوى الكبرى إلى إدارة الشؤون الدولية وتحقيق مصالحها الذاتية. يشمل هذا التنافس السيطرة على المناطق الاستراتيجية، مثل الشرق الأوسط وغرب آسيا، حيث تسعى الدول إلى

وعليه ،تختلف أهداف الأمن القومي بين الدول، لكن جميعها تسعى للحفاظ على أمنها القومي من خلال توظيف إمكانياتها العسكرية والاقتصادية والسياسية . إن فهم هذه الأهداف يساعد على تحليل السياسات الدولية والتفاعل بين الدول. (حسن ٢٠١٤، ٣٠٤)

فرضيات الأمن القومي :

يُعتبر الأمن القومي أحد المفاهيم الأساسية في السياسة الدولية، حيث يشير إلى مجموعة من السياسات والاستراتيجيات التي تتبناها الدول لحماية مصالحها وأمنها من التهديدات الداخلية والخارجية. يتضمن هذا المفهوم جوانب متعددة تشمل الأمن العسكري، الأمن الاقتصادي، الأمن الاجتماعي، والأمن البيئي. في هذا البحث، سوف نستعرض فرضيات الأمن القومي التي تشكل الأساس لفهم كيفية حماية الدول لمصالحها وأمنها، مع تقديم تحليل معمق لكل فرضية وأهميتها في السياق العالمي الراهن.

- **فرضية الاستقرار الداخلي** ، تعتبر فرضية الاستقرار الداخلي من الركائز الأساسية التي يعتمد عليها الأمن القومي. فاستقرار الدولة سياسياً واجتماعياً يسهم بشكل كبير في تعزيز قدرتها على مواجهة التهديدات. عندما تكون المؤسسات السياسية قوية وتعمل بشكل فعال، فإنها تستطيع إدارة الأزمات الداخلية وتجنب الفوضى. على سبيل المثال، يمكن أن تؤدي الأزمات الاقتصادية أو الاضطرابات الاجتماعية إلى زعزعة الاستقرار، مما يفتح المجال للتدخلات الخارجية. لذا، تسعى الحكومات إلى تعزيز الاستقرار من خلال تنظيم الانتخابات، تعزيز المشاركة السياسية، وتوفير الخدمات الأساسية مثل التعليم والرعاية الصحية. علاوة على ذلك، تلعب الثقافة الوطنية والهوية دوراً مهماً في تعزيز الاستقرار. فالتنوع الثقافي يمكن أن يكون مصدر قوة، ولكن إذا لم يُدار بشكل جيد، قد يؤدي إلى النزاعات. وبالتالي، يجب على الحكومات العمل على بناء مجتمع متماسك يعزز من الوحدة الوطنية.
- **فرضية التهديدات الخارجية** ، تتعلق فرضية التهديدات الخارجية بتقييم المخاطر التي قد تواجه الدولة من الخارج. تشمل هذه التهديدات العسكرية، مثل الهجمات من دول معادية، وكذلك التهديدات الاقتصادية مثل الحصار أو العقوبات. على سبيل المثال، شهدت العديد من الدول في المنطقة العربية تهديدات عسكرية أدت إلى تدخلات خارجية في شؤونها. تتطلب هذه الفرضية من الدول تطوير استراتيجيات شاملة لمواجهة التهديدات المحتملة. يتضمن ذلك تعزيز القدرات العسكرية، من خلال تحديث الأسلحة وتدريب القوات المسلحة، بالإضافة إلى بناء تحالفات مع دول أخرى لتبادل المعلومات والتعاون في مجالات الأمن. عندما تقيّم الدول التهديدات الخارجية بشكل دوري، تستطيع أن تتخذ قرارات مدروسة حول كيفية

التعامل معها. على سبيل المثال، قد تقرر بعض الدول الاستثمار في التكنولوجيا العسكرية المتقدمة كوسيلة لتعزيز قوتها الدفاعية.

- **فرضية التعاون الدولي** ، تعتبر فرضية التعاون الدولي من العناصر الأساسية في الأمن القومي، حيث أن التهديدات العالمية مثل الإرهاب، تغير المناخ، والأوبئة تتطلب استجابة جماعية. التعاون بين الدول يمكن أن يتخذ أشكالاً متعددة، مثل التحالفات العسكرية، الاتفاقيات التجارية، أو التعاون في مجالات الأمن السيبراني. تُظهر التجارب التاريخية أن الدول التي تتعاون في مجالات الأمن تستطيع تحقيق نتائج أفضل في مواجهة التهديدات. على سبيل المثال، أدت الاتفاقيات الدولية المتعلقة بالحد من انتشار الأسلحة النووية إلى تقليل المخاطر العالمية. يمكن أيضاً أن تشكل المنظمات الدولية، مثل الأمم المتحدة، منصة لتعزيز التعاون بين الدول وتنسيق الجهود لمواجهة الأزمات. كما أن التعاون في مجال تبادل المعلومات الاستخباراتية يعد أداة فعالة لمكافحة الإرهاب والجريمة المنظمة.(د.م ٢٠٢٥) وكذلك (عبد الحسين ٢٠٢٤، ٧٠٢-٧٠٤)
- **من ثم فرضية التنمية الاقتصادية** ،ترتبط فرضية التنمية الاقتصادية ارتباطاً وثيقاً بالأمن القومي، حيث أن التنمية المستدامة تسهم في تعزيز الاستقرار والأمن. عندما تكون الدولة قادرة على توفير فرص العمل وتحسين مستوى المعيشة، فإنها تقلل من احتمالية حدوث الاضطرابات الاجتماعية. تعتبر التنمية الاقتصادية أيضاً عاملاً مهماً في تعزيز القدرات الدفاعية. فالدول التي تتمتع باقتصاد قوي تستطيع أن تستثمر في الدفاع والتكنولوجيا، مما يساهم في تعزيز الأمن القومي. علاوة على ذلك، فإن الفقر والبطالة يمكن أن يؤديان إلى زيادة الجريمة والعنف، مما يعكس ضرورة تنفيذ سياسات اقتصادية فعالة تدعم النمو وتحقق الاستقرار. ومن هنا، يجب على الحكومات التركيز على تطوير استراتيجيات تنموية شاملة تغطي جميع القطاعات.
- **وأخيرا فرضية التكنولوجيا والأمن** ، تعتبر التكنولوجيا عاملاً مهماً في تعزيز الأمن القومي، حيث أن التطورات التكنولوجية توفر أدوات جديدة لمواجهة التهديدات. ومع ذلك، فإن هذه التكنولوجيا قد تخلق تهديدات جديدة، مثل الهجمات السيبرانية التي تستهدف البنية التحتية الحيوية. تُظهر التجارب أن الدول التي تستثمر في تطوير قدراتها التكنولوجية تتمتع بميزة تنافسية في مجال الأمن. التكنولوجيا الحديثة تتيح للدول جمع وتحليل البيانات بشكل أكثر فعالية، مما يعزز من قدرتها على الاستجابة للتهديدات. (عبد الحي ٢٠٢٣)

علاوة على ذلك، يجب أن تكون هناك استراتيجيات لحماية المعلومات الحساسة والأنظمة الحيوية من الهجمات السيبرانية. الاستثمار في الأمن السيبراني يعد ضرورة ملحة في عصر تزايد الاعتماد على التكنولوجيا. في الختام، يُمكن القول إن فرضيات الأمن القومي تمثل الأساس لفهم كيفية حماية الدول لمصالحها وأمنها. من خلال التركيز على الاستقرار الداخلي، تقييم التهديدات الخارجية، تعزيز التعاون الدولي، دعم التنمية الاقتصادية، والاستثمار في التكنولوجيا، يمكن للدول تعزيز أمنها القومي. ومع ذلك، فإن التحديات المستمرة تتطلب استجابة فعالة واستراتيجيات مرنة لضمان استقرار وأمن الدول في عالم متغير.

المطلب الثالث: اثر الامن السيبراني على الامن القومي

في السنوات الأخيرة، أصبح الأمن السيبراني يحتل أهمية قصوى في سياسات الدول واستراتيجياتها الوطنية، حيث أضحى الفضاء الرقمي جزءًا لا يتجزأ من حياة الأفراد والمؤسسات، بل وركيزة أساسية في إدارة شؤون الدولة الحديثة. هذا التطور الهائل في مجال تكنولوجيا المعلومات والاتصالات أدى إلى ظهور نوع جديد من التهديدات، وهو التهديد السيبراني، الذي لا يقتصر أثره على الأفراد أو المؤسسات فحسب، بل يتعدى ذلك ليصل إلى الأمن القومي للدول بشكل مباشر وحساس. فقد شهد العالم تصاعدًا ملحوظًا في وتيرة الهجمات الإلكترونية، سواء تلك التي تستهدف البنية التحتية الحيوية أو المؤسسات الحكومية أو حتى القطاعات الاقتصادية، مما جعل الأمن السيبراني يشكل خط الدفاع الأول عن الدولة ومصالحها العليا في العصر الحديث.ولفهم هذا التأثير العميق للأمن السيبراني على الأمن القومي، يجب أولًا أن ندرك طبيعة العلاقة بين الاثنين. فالأمن القومي يشمل الحفاظ على سيادة الدولة وحماية مصالحها الاستراتيجية، وضمان استقرار المجتمع وسلامة مواطنيه من جميع أنواع التهديدات، سواء كانت عسكرية أو اقتصادية أو اجتماعية أو حتى معلوماتية. وقد أدى الاعتماد الكبير على الأنظمة الرقمية والشبكات الإلكترونية في إدارة مرافق الدولة ومؤسساتها، إلى جعل الفضاء السيبراني ساحة جديدة للصراع بين الدول والجماعات، وبالتالي أصبح الأمن السيبراني ضرورة وطنية تماثل في أهميتها الدفاع العسكري التقليدي. وأحد أبرز مظاهر أثر الأمن السيبراني على الأمن القومي يتمثل في حماية البنية التحتية الحيوية للدولة. ففي عصرنا الحالي، أصبحت قطاعات مثل الكهرباء والمياه والنقل والاتصالات والصحة والتعليم والإدارة الحكومية تعتمد بشكل شبه كامل على نظم الحوسبة والشبكات الرقمية. أي هجوم سيبراني ناجح على هذه القطاعات قد يؤدي إلى شلل تام في وظائفها الحيوية، ما ينعكس سلبًا على حياة المواطنين ويهدد استقرار المجتمع والدولة. على سبيل المثال، يمكن لهجوم إلكتروني على شبكات الكهرباء أن يعطل الإمداد بالطاقة في مدن كاملة، مسببا خسائر اقتصادية هائلة وتهديدًا مباشرًا للأمن القومي. وفي حالات كثيرة، أعلنت بعض الدول عن تعرضها لهجمات سيبرانية

متكررة استهدفت منشآتها الحيوية، ما دفعها إلى رفع درجة التأهب ووضع خطط استجابة طارئة لمثل هذه التهديدات. (Protecting Critical Infrastructure in Modern Society 2024)

ولا يقتصر أثر الأمن السيبراني على البنية التحتية فقط، بل يمتد ليشمل حماية أسرار الدولة والمعلومات الحساسة. فالحكومات ومؤسساتها تحتفظ ببيانات ضخمة تتعلق بالأمن والدفاع والسياسة الخارجية والاقتصاد، وأي اختراق لهذه المعلومات أو تسريبها قد يعرض الدولة لخطر التجسس أو الابتزاز أو حتى التدخل الخارجي في شؤونها. وقد شهدنا في السنوات الأخيرة تصاعدًا في عمليات التجسس الإلكتروني التي تنفذها بعض الدول أو الجماعات المنظمة بهدف جمع معلومات استخباراتية عن الدول المستهدفة، مما يشكل تهديدًا صريحًا للأمن القومي ويؤثر على اتخاذ القرار السيادي. ومن الجوانب الأخرى التي تظهر فيها أهمية الأمن السيبراني للأمن القومي، تصاعد ظاهرة الحروب السيبرانية بين الدول. فقد أصبحت الفضاءات الرقمية ميدانًا جديدًا للصراع والعداء، حيث تستخدم بعض الدول الهجمات الإلكترونية كأداة لتحقيق أهداف سياسية أو عسكرية أو اقتصادية دون اللجوء إلى المواجهة العسكرية المباشرة. في هذا السياق، يمكن للهجمات السيبرانية أن تعطل أنظمة الدفاع الجوي أو نظم الاتصالات العسكرية أو حتى الأنظمة المصرفية والمالية، ما يؤدي إلى نتائج كارثية تفوق في بعض الأحيان أضرار الحروب التقليدية. وهذا ما جعل العديد من الدول تخصص موارد هائلة لبناء قدرات دفاعية سيبرانية، بل وإنشاء وحدات عسكرية متخصصة في الحرب الإلكترونية ضمن جيوشها النظامية. ولا يمكن إغفال الأثر الاقتصادي للأمن السيبراني على الأمن القومي، حيث أصبحت الهجمات الإلكترونية على القطاع المالي تمثل تهديدًا خطيرًا لاستقرار الاقتصاد الوطني. فقد شهدت بعض الدول حوادث كبرى تم فيها اختراق أنظمة البنوك أو البورصات مما أدى إلى خسائر مالية ضخمة وفقدان الثقة في النظام المالي، الأمر الذي قد يؤدي إلى زعزعة الاستقرار الاقتصادي والاجتماعي. كما أن عمليات الاحتيال الإلكتروني وسرقة البيانات المالية أصبحت من أكثر الجرائم انتشارًا في العصر الرقمي، ما يتطلب تعزيز سبل الحماية الرقمية ومتابعة التطورات في مجال الأمن السيبراني بشكل مستمر. إضافة إلى ذلك، فإن الأمن السيبراني أصبح ضروريًا لحماية المجتمع من مخاطر الشائعات والمعلومات المضللة التي تنتشر عبر وسائل التواصل الاجتماعي والمنصات الرقمية. يستخدم بعض الفاعلين، سواء كانوا أفرادًا أو جماعات أو حتى دولًا، الفضاء السيبراني لنشر معلومات كاذبة أو تحريف الحقائق بهدف التأثير على الرأي العام أو إثارة الفوضى أو زعزعة الثقة في الدولة ومؤسساتها. وتكمن خطورة هذا النوع من الهجمات في سرعة انتشارها وصعوبة السيطرة عليها، ما يتطلب من الجهات المعنية تطوير أدوات فعالة لرصد ومكافحة هذه الظواهر، ورفع وعي المواطنين بأهمية التحقق من مصادر المعلومات وعدم الانجرار

خلف الأخبار الكاذبة. (طبيعة العلاقة بين الأمن السيبراني والنمو الاقتصادي الرقمي في دول العالم. د.ت)، في مواجهة هذه التحديات المتزايدة، أصبح على الدول أن تضع الأمن السيبراني في قلب استراتيجياتها للأمن القومي، وأن تتبنى سياسات متكاملة لتعزيز قدرتها على التصدي للتهديدات السيبرانية. ويشمل ذلك تطوير التشريعات والقوانين التي تجرم الهجمات الإلكترونية وتحدد المسؤوليات والعقوبات، وتعزيز التعاون بين القطاعين العام والخاص في مجال حماية المعلومات، إضافة إلى الاستثمار في التعليم والتدريب لرفع كفاءة الكوادر البشرية المتخصصة في مجال الأمن السيبراني. كما أن التعاون الدولي أصبح ضرورة ملحة في ظل الطبيعة العابرة للحدود للتهديدات السيبرانية، حيث تتطلب مواجهة هذه التهديدات تبادل المعلومات والخبرات مع الدول الأخرى والمنظمات الدولية، وتوحيد الجهود لملاحقة المجرمين السيبرانيين أينما وجدوا. ولا يقل أهمية عن ذلك، العمل على رفع مستوى الوعي المجتمعي حول مخاطر الفضاء السيبراني وأهمية حماية البيانات الشخصية والمؤسساتية، إذ أن الكثير من الهجمات تبدأ من نقاط ضعف بشرية ناجمة عن قلة المعرفة أو الإهمال. لذا، يجب تنفيذ حملات توعية مستمرة تستهدف جميع شرائح المجتمع، مع التركيز على العاملين في القطاعات الحيوية والحساسة. كما ينبغي تحديث الأنظمة التقنية باستمرار، واستخدام أحدث وسائل الحماية الإلكترونية، بما في ذلك أنظمة كشف الاختراق والاستجابة السريعة، والتشفير المتطور، والمراقبة الدائمة للشبكات. (سليمان د.ت)

ومن الجدير بالذكر أن العلاقة بين الأمن السيبراني والأمن القومي ليست علاقة أحادية الاتجاه، بل هي علاقة تبادلية متداخلة، إذ يؤثر كل منهما في الآخر بشكل مباشر. فالتقصير في حماية الفضاء السيبراني يضعف مناعة الدولة أمام التهديدات الإلكترونية، بينما يعزز الأمن السيبراني القوي من قدرة الدولة على الحفاظ على استقرارها وأمنها في جميع المجالات. ولهذا السبب، باتت العديد من الدول تصنف الأمن السيبراني كأولوية وطنية من الدرجة الأولى، وتخصص له موارد وميزانيات ضخمة، وتسعى إلى بناء تحالفات دولية لضمان أمنها الرقمي. يتضح لنا أن الأمن السيبراني أصبح ركيزة أساسية من ركائز الأمن القومي في العصر الحديث، ولا يمكن لأي دولة أن تحقق أمنها واستقرارها دون الاهتمام الجاد بحماية فضائها الرقمي ومعلوماتها الحيوية. فالتحديات التي يفرضها العصر الرقمي تتطلب استجابة شاملة تشمل جميع المستويات: التشريعية والتنظيمية والتقنية والبشرية، كما تتطلب تضافر الجهود بين جميع مؤسسات الدولة والمجتمع، وتعزيز التعاون الإقليمي والدولي لمواجهة خطر الهجمات السيبرانية الذي لا يعترف بالحدود الجغرافية. إن الاستثمار في الأمن السيبراني لم يعد خيارًا بل ضرورة حتمية من أجل حماية الأوطان وضمان مستقبل آمن للأجيال القادمة في عالم يتغير بوتيرة متسارعة ولا حدود فيه للتحديات.

ومع ازدياد التداخل بين العالم الواقعي والعالم الافتراضي، باتت التهديدات السيبرانية أكثر تنوعًا وتعقيدًا من أي وقت مضى. ولم تعد الهجمات الإلكترونية مقتصرة على محاولات اختراق بسيطة أو عمليات احتيال فردية، بل أصبحت هناك مجموعات منظمة مدعومة أحيانًا من دول أو جهات قوية، تمتلك القدرة على تنفيذ هجمات معقدة تستهدف شبكات بأكملها وتؤثر على قطاعات حيوية في الدولة. فعلى سبيل المثال، شهدت الولايات المتحدة الأمريكية وأوروبا في السنوات الأخيرة هجمات سيبرانية واسعة النطاق، مثل الهجوم الشهير المعروف باسم "هجوم رانسموير واناكراي" الذي وقع عام ٢٠١٧، حيث أصاب مئات الآلاف من الأجهزة حول العالم، بما في ذلك نظم المستشفيات وشركات الاتصالات والمصانع الكبرى. تسببت تلك الهجمات في تعطيل خدمات أساسية وخسائر مالية ضخمة، وأبرزت مدى هشاشة الفضاء الرقمي أمام هجمات من هذا النوع، وأكدت أن الأمن القومي أصبح مرتبطًا ارتباطًا وثيقًا بقدرة الدولة على حماية بنيتها الرقمية. (دون مؤلف، ٢٠٢٥) ، وفي السياق العربي، لم تعد المنطقة بمنأى عن هذه التهديدات، بل أصبحت أهدافًا متكررة للهجمات السيبرانية، سواء لدوافع سياسية أو اقتصادية أو حتى إجرامية. فقد تعرضت بعض الدول العربية لهجمات استهدفت منشآت نفطية ومؤسسات حكومية، مما أدى إلى تعطيل بعض الخدمات الأساسية لفترات زمنية متفاوتة، وكشف عن الحاجة الماسة لبناء منظومات دفاعية سيبرانية متطورة وقادرة على الاستجابة السريعة لأي تهديد. كما أن التحديات الأمنية في المنطقة لا تقتصر فقط على الهجمات الخارجية، بل تشمل أيضًا الجرائم الإلكترونية المحلية، كعمليات الاحتيال وسرقة البيانات والتلاعب بالمعلومات، الأمر الذي يشكل ضغطًا إضافيًا على أجهزة الأمن الوطني ويستلزم تعاونًا وثيقًا بين جميع الهيئات والمؤسسات. (CyberTalents, 2022)

التحدي الأكبر الذي يواجه معظم دول العالم في مجال الأمن السيبراني هو مواكبة التطورات السريعة في أساليب الهجوم والدفاع، إذ أصبح المهاجمون أكثر ذكاءً وقدرة على التكيف مع إجراءات الحماية الجديدة، وغالبًا ما يستخدمون تقنيات متقدمة مثل الذكاء الاصطناعي والتعلم الآلي لتطوير برمجيات خبيثة قادرة على تجاوز أنظمة الدفاع التقليدية. من جهة أخرى، تواجه الدول صعوبة في إيجاد وتدريب الكوادر البشرية المؤهلة لمواكبة هذا التطور، حيث أن خبراء الأمن السيبراني أصبحوا عملة نادرة في السوق العالمية، وتتنافس الدول والشركات الكبرى على استقطابهم وتطوير مهاراتهم. من الجوانب المهمة أيضًا، أن الأمن السيبراني لا يتعلق فقط بالتقنيات والبرمجيات، بل يمتد ليشمل الأبعاد القانونية والاجتماعية والثقافية. فوجود تشريعات واضحة وقوانين رادعة للجرائم الإلكترونية يعد أحد أهم الأسس لبناء منظومة أمنية فعالة. كما أن تعزيز ثقافة الأمان الرقمي لدى الأفراد والمؤسسات يعتبر خط الدفاع الأول ضد محاولات الاختراق، إذ تشير الدراسات إلى أن

نسبة كبيرة من الهجمات السيبرانية تبدأ من ثغرات بشرية مثل فتح رسائل بريد إلكتروني مجهولة المصدر أو استخدام كلمات مرور ضعيفة أو مشاركة معلومات حساسة دون وعي بخطورتها. لذا فإن الاستثمار في التوعية والتدريب لا يقل أهمية عن الاستثمار في شراء أحدث الأنظمة التقنية. ومن الحلول التي لجأت إليها العديد من الدول، إنشاء مراكز وطنية للاستجابة للطوارئ السيبرانية، وهي جهات متخصصة تعمل على رصد التهديدات السيبرانية وتحليلها، والاستجابة السريعة لأي حادث اختراق أو هجوم محتمل. كما أن بعض الدول أنشأت وحدات عسكرية متخصصة في الدفاع السيبراني ضمن جيوشها، وأصبحت تدريبات الحروب السيبرانية جزءًا من الاستعدادات الدفاعية الوطنية. هذا بالإضافة إلى التعاون الدولي الذي أصبح عنصرًا أساسيًا في مواجهة التهديدات العابرة للحدود، من خلال تبادل المعلومات والخبرات والمساعدة التقنية، والتنسيق في إجراءات تعقب المجرمين السيبرانيين وتقديمهم للعدالة. (BitSight, 2025) ، على صعيد آخر، تدرك الدول اليوم أن الحفاظ على الأمن القومي في العصر الرقمي يتطلب تطوير منظومة متكاملة تجمع بين الحماية التقنية والقانونية والبشرية، وتراعي في الوقت ذاته خصوصية كل دولة واحتياجاتها الفريدة. فعلى الرغم من وجود تحديات مشتركة، إلا أن لكل دولة خصوصيتها في البنية التحتية الرقمية ونقاط ضعفها، ما يستلزم حلولًا مصممة خصيصًا لمواجهة التهديدات المحتملة. كما أن الاستثمار في البحث العلمي وتطوير منتجات وطنية في مجال الأمن السيبراني أصبح من الأولويات، ليس فقط بهدف الحماية بل أيضًا لتعزيز السيادة الرقمية وتقليل الاعتماد على الحلول الأجنبية التي قد تشكل هي بذاتها مصدرًا للتهديد. ولا يمكن إغفال الدور المتنامي للقطاع الخاص في حماية الأمن السيبراني الوطني، إذ أن معظم البنية التحتية الرقمية الحيوية، مثل شبكات الاتصالات والبنوك والطاقة، تدار من قبل شركات خاصة أو بالتعاون بين القطاعين العام والخاص. لذا فإن بناء شراكات استراتيجية بين الدولة وهذه الجهات أصبح ضرورة لا غنى عنها، لضمان تبادل المعلومات بشكل فوري وفعال، وتوحيد الجهود في مواجهة الهجمات الإلكترونية التي تستهدف المصلحة الوطنية العليا. يجدر التنبيه إلى أن التقدم التكنولوجي المستمر، مثل إنترنت الأشياء والتوسع في استخدام الذكاء الاصطناعي والحوسبة السحابية، ضاعف من حجم التهديدات السيبرانية، حيث أضاف طبقات جديدة من التعقيد وأوجد نقاط ضعف جديدة يمكن استغلالها من قبل المهاجمين. هذه التطورات تستدعي يقظة دائمة واستثمارًا مستمرًا في تطوير الأنظمة والكوادر البشرية، ووعيًا مجتمعيًا بأهمية الأمن الرقمي كجزء لا يتجزأ من الأمن القومي. من الواضح إذًا أن الأمن السيبراني لم يعد مجرد خيار أو ترف تقني، بل أصبح ضرورة وطنية وأحد أعمدة الأمن القومي، تتوقف عليه سلامة الدولة واستقرارها ومستقبلها في عالم يتسم بالتنافسية الشديدة والتغير السريع. وفي عالم يسير نحو مزيد من الترابط الرقمي والانفتاح المعلوماتي، فإن قدرة الدول على

تأمين فضاءها السيبراني ستحدد إلى حد كبير مكانتها ووزنها على الساحة الدولية، وستبقى حماية الأمن السيبراني تحديًا متجددًا يتطلب الجدية والاستثمار والتخطيط طويل الأمد.

الخاتمة :

تتناول هذه الدراسة تطور أجيال الحروب وتأثيرها على مفهوم الأمن في العصر الحديث، حيث نرى كيف انتقلت الحروب من أشكالها التقليدية إلى أشكال أكثر تعقيدًا تعتمد على التكنولوجيا الحديثة. يُظهر هذا التحول كيفية تكيف المجتمعات مع التغيرات السياسية والاجتماعية والاقتصادية، مما يعكس أيضًا التحديات التي تواجهها الدول في الحفاظ على أمنها واستقرارها. الحروب تُدار بوسائل تقليدية تعتمد على المواجهات المباشرة بين الجيوش. ومع مرور الوقت، تطورت الأساليب إلى حروب الجيل الثاني والثالث، حيث بدأت تظهر تكتيكات جديدة مثل حروب العصابات والحروب بالوكالة. أما اليوم، فإن حروب الجيل الرابع والخامس تعتمد بشكل كبير على التكنولوجيا، مما يجعلها أكثر تعقيدًا وصعوبة في السيطرة عليها. هذه التحولات تستدعي إعادة تقييم استراتيجيات الدول في مجال الأمن والدفاع. في هذا السياق، يبرز الأمن السيبراني كجزء لا يتجزأ من الأمن القومي. إذ تعتمد الدول بشكل متزايد على البنية التحتية الرقمية في إدارة شؤونها اليومية. الهجمات السيبرانية التي تستهدف هذه البنية التحتية يمكن أن تؤدي إلى عواقب وخيمة؛ من تعطيل الخدمات الأساسية إلى تسريب معلومات حساسة. لذلك، أصبح من الضروري أن تتبنى الدول استراتيجيات شاملة تعزز من قدرتها على مواجهة هذه التهديدات.

يتطلب تعزيز الأمن السيبراني تكامل الجهود بين الحكومات والقطاع الخاص والمجتمع المدني. التعاون الدولي أصبح ضرورة ملحة لمواجهة التهديدات العابرة للحدود. من خلال تبادل المعلومات والخبرات، يمكن للدول تحسين استجابتها للهجمات السيبرانية. كما أن توعية المجتمع بأهمية الأمن الرقمي تعد خطوة أساسية لتعزيز الحماية. يجب أن تكون هناك حملات توعوية تستهدف جميع فئات المجتمع، مع التركيز على الشباب وطلبة المدارس، لتعليمهم أساليب الحماية وكيفية التعامل مع المخاطر المحتملة. علاوة على ذلك، يتطلب التطور التكنولوجي المستمر استثمارًا في البحث والتطوير في مجال الأمن السيبراني. يجب على الحكومات أن تخصص ميزانيات كافية لبناء قدرات دفاعية سيبرانية وتحديث أنظمتها بشكل دوري. هذا الاستثمار لا يقتصر على الجانب التقني فحسب، بل يشمل أيضًا تدريب الكوادر البشرية المتخصصة في هذا المجال، حيث أن نقص الخبرات والكفاءات يمكن أن يشكل عائقًا كبيرًا أمام قدرات الدول في مواجهة التهديدات. بالإضافة إلى ذلك، يجب أن تكون هناك تشريعات واضحة تحكم التعامل مع الجرائم السيبرانية.

القوانين يجب أن تشمل عقوبات رادعة للمخالفين، وتوفير حماية قانونية للمعلومات الحساسة. هذه التشريعات تعد بمثابة الإطار القانوني الذي يضمن حماية حقوق الأفراد والمؤسسات في الفضاء السيبراني.

يتضح أن الأمن السيبراني ليس مجرد خيار بل ضرورة حتمية. إن التهديدات المتزايدة التي تواجه الدول في العصر الرقمي تتطلب استجابة شاملة وفعالة. يجب أن تتعاون الدول على جميع الأصعدة، سواء كانت محلية أو دولية، لضمان حماية أمنها واستقرارها. إن الاستثمار في الأمن السيبراني هو استثمار في المستقبل، يضمن للأجيال القادمة بيئة آمنة ومستقرة.

الاستنتاجات :

١- تطور الحروب عبر الزمن: تم تصنيف الحروب إلى أجيال متعددة، كل منها يتميز بأساليب وتقنيات مختلفة. حروب الجيل الأول كانت تعتمد على المواجهات التقليدية، بينما تطور الجيل الرابع والخامس ليشمل حروبًا غير متماثلة تعتمد على التكنولوجيا.

٢- الأمن السيبراني كعنصر أساسي: يمثل الأمن السيبراني ضرورة ملحة لحماية البنية التحتية الحيوية والمعلومات الحساسة. الهجمات السيبرانية الحديثة يمكن أن تؤثر بشكل كبير على استقرار الدول، مما يستدعي تطوير استراتيجيات شاملة لمواجهتها.

٣- التعاون الدولي: يجب على الدول تعزيز التعاون الدولي لمواجهة التهديدات السيبرانية. هذه التهديدات تتجاوز الحدود الجغرافية، مما يتطلب تبادل المعلومات والخبرات بين الدول.

٤- توعية المجتمع: نشر الوعي حول الأمن السيبراني بين الأفراد والمؤسسات يعد خطوة أساسية لتعزيز الحماية. التعليم والتدريب يمكن أن يساعدا في تقليل المخاطر الناتجة عن السلوكيات غير الواعية.

٥- التكنولوجيا والتطور المستمر: تطور التكنولوجيا يستدعي استجابة مرنة وسريعة من الدول. الاستثمار في البحث والتطوير في مجال الأمن السيبراني يعد أمرًا حيويًا لمواجهة التحديات المستقبلية.

٦- تأثير الهجمات السيبرانية على الاقتصاد: الهجمات السيبرانية يمكن أن تؤدي إلى خسائر اقتصادية كبيرة، مما يتطلب من الدول تعزيز سبل الحماية الرقمية. يجب أن تكون هناك استراتيجيات لحماية القطاع المالي والبنية التحتية الحيوية.

٧- الاستجابة للطوارئ: إنشاء مراكز وطنية للاستجابة للطوارئ السيبرانية يمكن أن يساعد في التعامل مع الهجمات بسرعة وفعالية. هذه المراكز يجب أن تكون مجهزة بالتقنيات الحديثة والكوادر البشرية المدربة.

المصادر باللغة العربية:

١. الأنصاري، صلاح الدين الزيداني. ٢٠٢١ .*تطور أجيال الحروب* .موقع دفاع العرب. متاح على الرابط: https://defensearabia.com/

٢. حسن، عادل. ٢٠١٤. الأمن القومي في ظل المدارس الفكرية. مجلة الجامعة العراقية. العدد ٥٨، ج ٣.

٣. د.م. ٢٠٢٣. كل ما ترغب في معرفته عن الأمن السيبراني: مفهومه وخصائصه وأشهر أنواع التهديدات فيه. متاح على الرابط:https://www.e3melbusiness.com/blog/cyber-security

٤. د.م. ٢٠٢٥. الأمن القومي والاستراتيجية. العدد الخامس. متاح على الرابط:https://nsas.journals.ekb.eg وكذلك: عبد الحسين، أحمد. ٢٠٢٤. الأمن القومي: المفهوم وأهم استراتيجياته. مجلة الكلية الإسلامية الجامعة. العدد ٧٨.

٥. د.م. ٢٠٢٥. أنواع تهديدات الأمن السيبراني – أهم ٨ أنواع. متاح على الرابط: https://bakkah.com/ar/knowledge-center

٦. زروقي، إبراهيم. ٢٠١٣. الأمن القومي العربي: دراسة في المفهوم والأبعاد والمرتكزات. كلية العلوم الإنسانية والعلوم الاجتماعية، جامعة تلمسان.

٧. سعدون، عباس. ٢٠٢٢. التطور التكنولوجي وتأثيره على أجيال الحروب في العلاقات الدولية. مجلة تكريت للعلوم السياسية. العدد ٢٩.

٨. سلمان، مصطفى إبراهيم. ٢٠٢١ .*الأمن السيبراني وأثره في الأمن الوطني العراقي* .مجلة العلوم القانونية والسياسية، جامعة ديالى. المجلد العاشر، العدد الأول.

٩. سليمان، فهد عباس. د.ت. الأمن السيبراني وأثره على الفرد والمجتمع. متاح على الرابط: https://uokirkuk.edu.iq/Girls-Education-Coll

١٠. شوا، سعاد. ٢٠٢٤ .*الحرب: أسبابها وآثارها وتأثيرها على المجتمعات* .موقع كاف. متاح على الرابط: https://www.cappasande.de/%D8%A7%D9%84%D8%AD%D8%B1%D8%A8/

١١. طارش، أسعد، وإبراهيم، علي. ٢٠٢٠ .*الأمن السيبراني ودوره في انتشار ظاهرة الإرهاب في العراق بعد عام ٢٠٠٣* . مجلة مركز الدراسات الاستراتيجية والدولية، جامعة بغداد. العدد ٨٠.

١٢. طبيعة العلاقة بين الأمن السيبراني والنمو الاقتصادي الرقمي في دول العالم. د.ت. المجلة الأمريكية الدولية المحكمة للعلوم الإنسانية والاجتماعية. متاح على الرابط:https://iajphss.us/

١٣. عبد الحي، وليد. ٢٠٢٣. مستقبل التطور التكنولوجي العسكري وأثره على الاستقرار الداخلي. مركز الزيتونة للدراسات والاستشارات. متاح على الرابط:https://www.alzaytouna.net/2023/03/06/

١٤. عبد الرحمن، أسامة. ٢٠٢٠. الأمن القومي. موقع الموسوعة السياسية. متاح على الرابط:-https://political /encyclopedia.org/dictionary

١٥. عدوان، أركان إبراهيم. د.ت .*مفهوم الحرب* .جامعة الأنبار. متاح على الرابط: https://www.uoanbar.edu.iq/eStoreImages/Bank/13640.pdf

١٦. العلي، زياد علي. ٢٠١٩. *الصراع والأمن الجيوسبراني في السياسة الدولية: دراسة في استراتيجيات الاشتباك الرقمي*. عمّان: دار أمجد للنشر والتوزيع. ط١.

١٧. فريح، زينب. ٢٠٢١. *أجيال الحروب: دراسة في محددات تطور الأجيال الخمس للحرب*. مجلة دفاتر السياسة والقانون، جامعة البليدة، الجزائر. العدد ٢.

١٨. كنبر، نور عبود. ٢٠٢١. *مفاهيم في الحرب*. مركز النهرين للدراسات الاستراتيجية، مستشارية الأمن القومي العراقي. متاح على الرابط: https://www.alnahrain.iq/post/619

١٩. مجموعة مؤلفين. ٢٠٢٢. *تسليط الضوء على الحروب الحديثة في مجال العلاقات الدولية: مفهومًا ومضمونًا*. مركز البيدر للدراسات والتخطيط، العراق.

٢٠. محمود، علياء. ٢٠١٩. *الاتجاهات الحديثة في نظرية الحروب مع تطبيق على الحرب الأمريكية على أفغانستان*. مجلة البحوث المالية والمصرفية، الأردن. العدد الثالث، الجزء الأول.

٢١. مصطفى، تقى عثمان. ٢٠٢٤. التهديدات السيبرانية والعلاقات الأمريكية الروسية. المركز الديمقراطي العربي، برلين، ألمانيا. متاح على الرابط:https://democraticac.de/?p=99583

٢٢. موقع الجزيرة نت. ٢٠١٧. هجوم إلكتروني واسع يضرب شركات ومؤسسات بالعالم.. متاح على الرابط: https://www.aljazeera.net/news/2017/6/27

٢٣. موقع النور اون لاين . ٢٠٢٥. بحث كامل عن الأمن السيبراني. موقع النور أون لاين. متاح على الرابط: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

٢٤. ولد خيري، محفوظ. ٢٠٢٤. *أخلاق الحرب في الإسلام*. موقع إسلام ويب. تاريخ النشر ٢٠٢٤/٦/٥. متاح على الرابط: https://www.islamweb.net/ar/article-

المصادر باللغة الانكليزية:

1. Alderman, Ray. 2015. Looking toward 7th and 8th Generation Warfare. Military Embedded Systems, Oklahoma City. 7/7/2015. Available at: https://militaryembedded.com/unmanned/isr/looking-toward-7th-and-8th-generation-warfare
2. BitSight. 2025. What Is Cybersecurity Compliance? List of Regulations by Sector. Available at: https://www.bitsight.com/blog/what-is-cybersecurity-compliance.
3. CyberTalents. 2022. A Quick Guide to Cybersecurity Incidents and How to Avoid Them. Available at: https://cybertalents.com/blog/cybersecurity-incidents-what-are-they-and-how-to-avoid-them

4. Exabeam. n.d. The Twelve Elements of Information Security Policies. Available at: https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy
5. Protecting Critical Infrastructure in Modern Society.2024. Available at https://industrialcyber.co/analysis/critical-infrastructure-protection-in-modern-society
6. Quresh, Waseem Ahmad. 2019. Fourth- and Fifth-Generation Warfare: Technology and Perceptions. University of San Diego: San Diego International Law Journal. Vol. 21, Issue 1.
7. Rudolf, Peter. 2014. Killing by Drones: The Problematic Practice of U.S. Drone Warfare. Anonymous Killings by New Technologies? Ethics and Armed Forces.
8. Van Der Klaauw, Cornelis. 2021. Generations of Warfare: An Outdated Concept. The Three Swords Magazine. Vol. 37