الامن السيبراني وتأثيره على الامن القومي للدول

م.م شهد عدنان صالح
الجامعة المستنصرية/ كلية العلوم السياسية
shahad1993@uomustansiryah.edu.iq

الملخص:

يشهد العالم اليوم العديد من التحولات والتغيرات في المجالات كافة، نتيجة التطور التكنولوجي الهائل لا سيما في المعلومات والاتصالات، مما أدى إلى إيجاد بيئة جديدة للتفاعل بين الافراد والمجتمعات من جهة والدول من جهة اخرى في بيئة مليئة بالمخاطر والتهديدات والصراع وشكلت تهديداً خطيراً للمجتمع وللدولة، إذ تغيرت مفاهيم القوة والصراع والحرب وارتبطت طبيعتها بالأمن السيبراني فظهور التهديدات الناجمة عنه كشكل جديد من أشكال التهديد الذي يعتمد على استخدام التقنيات الرقمية الحديثة لتحقيق أهداف متعددة، فقد اصبحت العديد من الفواعل الدولية مصدر خطر يهدد أمن المجتمعات بنشر أفكارها وقيمها على شبكات التواصل الاجتماعية، من خلال تجنيد أكبر عدد ممكن من الأفراد وتعليمهم كيفية اختراق المواقع الإلكترونية وغيرها من الجرائم الالكترونية مثل التسلل والتجسس على الشبكات الحساسة وإرسال رسائل تهديد إلى الدول لقبولها، لذلك عملت الدول ومن اجل حماية امنها القومي بتأسيس العديد من الهيئات والمؤسسات المدنية والعسكرية، ووضع الاستراتيجيات الخاصة بها وسن التشريعات القانونية لمواجهة تهديدات الامن السيبراني، فضلاً عن تعزيز التعاون الإقليمي والدولي لحماية الدول من الهجمات السيبرانية .

الكلمات المفتاحية : الامن السيبراني، الامن القومي، التطور التكنولوجي، الدولة.

تاريخ الاستلام :4 /1/ ٢٠٢٥	تاريخ القبول: 14/٥/ ٢٠٢٥	تاريخ النشر: ١/٦/ ٢٠٢٥

Cybersecurity and its Impact on the National Security of Countries

Assist lecturer Shahad Adnan Saleh
Al-Mustansiriya University/College of Political Sciences
shahad1993@uomustansiryah.edu.iq

Abstract:

Nowadays, the world is witnessing many transformations and changes in all fields, as a result of the tremendous technological development, especially in information and communications, which has led to the creation of a new

environment for interaction between individuals and societies on the one hand and countries on the other hand in an environment full of risks, threats and conflict and which has constituted a serious threat to society and the state, as the concepts of power, conflict, and war have changed and their nature has been linked to cyber security. The threats resulting from it have emerged as a new form of threat that depends on the use of modern digital technologies to achieve multiple goals. Many international actors have become a source of danger that threatens the security of societies by spreading their ideas and values on social media networks. By recruiting the largest possible number of individuals and teaching them how to hack websites and other electronic crimes such as infiltration and spying on sensitive networks and sending threatening messages to countries to accept them, so countries worked, in order to protect their national security, by establishing many civil and military bodies and institutions, and developing their own strategies. Enacting legal legislation to confront cyber security threats , as well as strengthening regional and international cooperation to protect countries from cyber-attacks.

Keywords: cybersecurity, national security, technological development, the state.

Receipt: 4/1/2025	Acceptance: 14/5/2025	Publication: 1/6/2025

المقدمة:

أسهمت التحديات الجديدة بعد انتهاء الحرب الباردة في تفتت دول واختفائها وظهور دول أخرى، وفي تنامي التحديات الافتراضية بعد أن أدت الثورة المعلوماتية الحديثة إلى تأكل السيادة القومية للدول، ومن ثم تهديدها للأمن القومي من خلال الهجمات والحروب السيبرانية التي أصبحت من سمات القرن الحادي والعشرين، فنتيجة للتقدم والثورة التكنولوجية الهائلة في أمن المعلومات والبيانات اصبح من الضروري في الوقت الحالي الاهتمام بترصين هذا الأمن شأنه شأن الأمن العسكري والاقتصادي، وقد تزايدت اهمية الامن السيبراني في المؤسسات الحكومية وغير الحكومية حتى اضحى من العناصر الرئيسة في استراتيجية الأمن القومي للدولة، والركيزة الاساسية التي تعمل على ضمانها جميع الدول التي تسعى الى تأمين المتطلبات الاساسية لتحقيق أمنها بشكل مستمر، وكذلك تحديد السبل والأليات التي تسهم في مواجهة مقومات وتحديات الامن السيبراني، وفي ظل التوسع الكبير في استعمال تكنولوجيا المعلومات فقد ارتفعت معدلات الرقابة والتجسس ليس على الافراد فحسب، بل على المؤسسات اثر تزايد عمليات الابتزاز والجرائم الإلكترونية، مما عرّض خصوصيات وحياة المجتمع وامن المؤسسات للخطر.

أهمية البحث:

تبيع أهمية الدراسة من أهمية الدراسات الاستراتيجية والأمنية في العلاقات الدولية، إذ تحاول إيصال فكرة مفادها ضرورة الحفاظ على الامن عبر معرفة مهدداته الجديدة وربطها بالتطورات والتحولات الحاصلة في البيئة الأمنية، إذ لم تعدّ الدولة بمقدورها عزل نفسها عن التفاعلات السياسية التي تمس أمنها بطريقة مباشرة او غير مباشرة، فلم يعد التهديد العسكري الخارجي هو المصدر الوحيد لأمن المجتمع فالدولة الان أصبحت تواجه انماطاً عديدة من مصادر التهديد لاسيما تلك التي تعتمد على التكنولوجيا لتهديد الأمن.

أشكالية البحث:

أن اشكالية الدراسة تكمن في أن الامن السيبراني أحد التحديات الرئيسة التي يتحتم على الدول مواجهتها في الوقت الراهن لا سيما مع تزايد اعتماد المجتمعات على شبكة المعلومات الدولية والتكنولوجيا المتقدمة مما يسهل عملية تهديدها ، فضلاً عن كونه أحد الوسائل الذي يستعمل في الصراعات بين الدول لقلة كلفته وعدم خضوعه لمعايير الصراعات التقليدية، وتم وضع مجموعة من التساؤلات للإجابة عنها وهي كالآتي:

١. ما مفهوم الامن السيبراني ؟
٢. ما هي مصادر تهديد الامن السيبراني؟
٣. ما هي ابعاد الامن السيبراني ؟
٤. الآفاق المستقبلية لتأثير الامن السيبراني على الامن القومي للدول؟

فرضية البحث:

تقوم ان فرضية الدراسة على وجود علاقة طردية بين الخطر واستعمال التكنولوجيا بمعنى كلما زاد اعتماد الدول على التكنولوجيا المتطورة في ظل تزايد تهديدات الامن السيبراني اصبح الأمن القومي لها في خطر، مما ينعكس على الأمن المجتمعي.

منهجية البحث :

تعتمد الدراسة على المنهج التحليلي النظمي الذي سيتم من خلاله تحليل وفهم طبيعة الامن السيبراني ومصادره ومدى تأثيرها في الأمن القومي للدول . وكذلك تعتمد الدراسة على المنهج الاستشرافي من اجل دراسة تأثير مستقبل تهديدات الامن السيبراني .

المبحث الاول

الامن السيبراني المفهوم ومصادر التهديد

أن الدفاع عن الأنظمة والشبكات والبرامج ضد التهديدات الرقمية يسمى بـ (الأمن السيبراني) وغالباً ما تركز هذه الاعتداءات الإلكترونية على الوصول إلى البيانات الحساسة لحذفها أو تعديلها من أجل ابتزاز أموال المستخدمين أو تعطيل عمليات الشركة الروتينية، لذا فقد تم تقسيم المبحث إلى مطلبين:-

المطلب الاول

مفهوم الامن السيبراني

أن لفظة سايبر (cyber) لفظة يونانية الأصل مشتقة من كلمة (kybernetes) وتعني الشخص الذي يدير دفة السفينة، وتستعمل مجازاً لتعبر عن المتحكم(Wiener 1989 , 15) ، وهناك من يرجع أصلها إلى منتصف القرن العشرين والذي استعملها عالم الرياضيات الأمريكي (Norbert Wiener) للتعبير عن التحكم الآلي(De Franco 2014, 40).

وهذا يعني أن مصطلح سايبر يعني الفضاء السيبراني الذي ظهر مع ظهور الانترنت واستعمال الرقمنة، وظهر الأمن السيبراني أو الالكتروني حديثاً بمعنى مجمل القوانين السياسية والنصوص والأدوات والمفاهيم وميكانيزمات الأمن وطرق تسيير الأخطار والممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات والاتصالات المستعملة في حماية الدول والمنظمات والأشخاص، وعُرفَ (الامن السيبراني) بأنه الحالة المرغوب فيها لعمل أنظمة الاتصالات والمعلومات التي تمنحها القدرة على المقاومة والتصدي لكل ما ينجم عن الفضاء السيبراني، والذي من شأنه أن يعرض المعلومات المخزنة أو المعالجة أو المنقولة التجسس أو للتلف أو التغيير(رضوان ٢٠١٦، ١٤).

لذا أصبحت معظم الدول ينتابها القلق حالياً من تعرض أمنها القومي للهجمات السيبرانية، لا سيما أن تقنيات المعلومات والاتصالات قد رفعت مستوى التهديدات من خلال اتاحتها لمصادر جديدة متعددة، فضلاً عن الإمكانات الهائلة لتحقيق هذا الخطر مقابل انخفاض نسبة المخاطر وإمكانية اكتشاف الجهة المنفذة للهجوم نتيجة للتنسيق المتبادل بين إدارات الأمن والاقتصاد، والترابط الذي يجمع بين أمن الفضاء السيبيراني والامن القومي، ويعتقد ضابط الأمن القومي الأمريكي السابق (مايكل مكونيل)، أن الإنترنت زاد من عدد التهديدات التي يتعرض لها النظام بطريقة غير مسبوقة(موسى ٢٠٠٢، ٢٣) ، وقدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني بأنه: جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بالأشكال جميعها الإلكترونية والمادية من مختلف الجرائم والهجمات والتخريب والتجسس والحوادث(Ventre

2011, 103) ، وكذلك عرَّفه الإعلان الأوروبي بأنه: قدرة النظام المعلوماتي على مقاومة الحوادث أو محاولات الاختراق غير المتوقعة، التي تستهدف البيانات، ووفقاً لدراسة الاتحاد الدولي للاتصالات بعنوان (اتجاهات إصلاح الاتصالات لعام ٢٠١٠-٢٠١١) فإن الأمن السيبراني عبارة عن مجموعة من المهام التي تشمل جمع أدوات وإجراءات وإرشادات وسياسات وطرق إدارة المخاطر والتدريب وأفضل الممارسات والاستراتيجيات الأمنية، ويمكن استعماله لحماية البيئة السيبرانية فضلاً عن أصول الشركات والأفراد(جبور ٢٠١١، ٤)، فالأمن السيبراني يمكن فهمه بأنه عملية حماية الأنظمة والبرامج والشبكات ضد الهجمات الرقمية، وتهدف هذه الهجمات السيبرانية عادةً للوصول إلى المعلومات الحساسة لتغييرها أو تدميرها؛ بغرض الاستيلاء على اموال المستخدمين أو مقاطعة عمليات الأعمال العادية. ويمثل تنفيذ تدابير الأمن السيبراني تحدياً كبيراً نظرًا لوجود عدد أجهزة يفوق أعداد الأشخاص كما أصبح المهاجمون أكثر ابتكاراً (Bologna and at el 2013, 40) ، كما يُعرف الامن السيبراني بأنه اتخاد إجراءات ووضع معايير اللازمة لمنع وصول المعلومات المطلوبة أو حماية تلك المعلومات من وقوعها في أيدي جهات معادية عبر الشبكة المعلوماتية(Libicki 2007, 114) ، ويختلف الأمن السيبراني عن الأمن المعلوماتي لكون الأول يتجاوز حدود الأمن المعلوماتي التقليدي أي حماية مصادر المعلومات فقط إلى حماية الأشخاص(طاجين ٢٠١٨، ٣٤٣) ، وعليه يمكن تعريف الأمن السيبراني بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات المعلومات والاتصالات، ويضمن إمكانيات تقليل الخسائر والأضرار التي ينتج عنها في حال مواجهة المخاطر والتهديدات، ويسمح بإعادة الاوضاع إلى ما كانت عليه لتجنب إيقاف عجلة الإنتاج وتقليل الأضرار(بنك الإسكندرية ٢٠٠٣، ٢٤) .

المطلب الثاني

مصادر تهديد الامن السيبراني

أن تهديد سواء كان حركياً أو سيبرانياً له فواعله ووسائله الخاصة، إلا أن تهديدات الامن السيبراني لها العديد من الخصائص المتميزة منها سهولة التنفيذ وقلة التكلفة وعابرة للحدود ومتعددة الاطراف، إذ بات الامن السيبراني مجال جديد للنزاع ليس بين الدول فقط، ولكن أيضاً بين الأفراد والاطراف الاخرى من غير الدول بسبب التكاليف المنخفضة نسبياً، فقد حدد (جوزيف ناي) ثلاثة أطراف لها القدرة على استعمال الهجمات السيبرانية والتعامل معها وهي: الدول والأفراد والأطراف الأخرى، لذا سنقسم المطلب إلى فقرتين، الاولى للدول والثانية للفواعل من غير الدول(ناي الأبن ١٩٩٧، ٢٢) :

اولاً: الفواعل من الدول

تعدّ الدولة أهم طرف في مجال تنفيذ الهجمات السيبرانية لما تتمتع به من قدرات مادية وبشرية وبنيوية وقانونية(بلفرد ٢٠١٦، ١٥٧) ، فجميع الأطراف لها القدرة والدافع للمشاركة في الصراعات والحروب في الفضاء السيبراني لضمان بقائها وتحقيق مصالحها الخاصة، فمن المنطقي أن تكون الدول جاهزة بشكل كامل للأنشطة في الفضاء السيبراني، بالنظر إلى حقيقة أن الأعداء المحتملين من الدول والأطراف من غير الدول سيتصرفون وفقا لذلك، وعليه إذا لم تتمكن الدول من القيام بأنشطة في هذا المجال الجديد فلن تكون قادرة على ضمان مصالحها الحيوية في المستقبل(Graham. Howard & Olson 2011 , 23-24) ، وبناءً على ذلك فإن الدولة بما تتوفر لها من إمكانيات بشرية ومادية وتكنولوجية تعد الطرف الرئيس في تنفيذ هجمات سيبرانية مثل قيام روسيا عام ٢٠٠٧ بشن هجمات سيبرانية على إستونيا مما أدى إلى توقف وتدمير المواقع الإلكترونية الرسمية الاستونية(Knapp 2018, 110) ، وكذلك قيامها بشن هجوم سيبراني على جورجيا عام ٢٠٠٨ استهدف مواقع رسمية حكومية منها الموقع الرسمي للرئيس الجورجي، ومواقع إعلامية، كما تم حجب موقعي (CNN) و (BBC) في جورجيا(إيه كلارك و كنيك ٢٠١٢، ٣٣).

ثانياً: الفواعل من غير الدول

أن الدور الذي تؤديه الفواعل من غير الدول في مجال الفضاء السيبراني يفوق دورها في أي مجال اخر، من حيث قدرتها على التفاعل أو التأثير في أمن الدول، ويرجع ذلك الى العديد من العوامل أبرزها انخفاض تكلفته وعدم وجود حواجز تعوق قدرتها على اداء دوراً بارزاً فيه، فالأدوات التكنولوجية والتقنية اللازمة للقيام بتهديدات سيبرانية يمكن الوصول اليها بسهولة عبر شبكة الانترنت، مما يمكّنها من امتلاك القدرات السيبرانية الهجومية بتكلفة منخفضة تمكنهم من شن تهديدات سواء على الدول أو الفواعل الاخرى من غير الدول، على الرغم من أن الدول لا تزال هي الفاعل الاكثر قوة وقدرة على شن تهديدات سيبرانية من الفواعل من غير الدول ومن هذه الفواعل هي: الشركات المتعددة الجنسية، المنظمات غير الحكومية، الافراد(Brenner & Clarke 2010, 249).

١. الشركات المتعددة الجنسية

تمتلك هذه الشركات موارد تفوق قدرة بعض الدول ولا ينقصها سوى شرعية ممارسة القوة، التي تعدّ حكراً على الدول مثل شركات، مايكروسوفت (Microsoft) وجوجل (Google) وآبل (Apple) المنتشرة فروعها في مختلف دول العالم وتمتلك قواعد من البيانات العملاقة(طاجين ٢٠١٨، ٢١) ، وتستطيع من خلالها استكشاف واستغلال الأسواق والتأثير في اقتصاديات الكثير من الدول وفي قوة الدولة الاقتصادية والناعمة، وكذلك التلاعب بالبيانات والتصنيفات الدولية الخاصة بالاقتصاديات والأسواق، إذ أن معظم الدول تتجه إلى

جذب هذه الشركات الدولية لإيجاد استثمارات جديدة بها لارتفاع عوائدها الاقتصادية جراء تصدير التكنولوجيا (Lohr 2010, 44).

٢. المنظمات غير الحكومية

لا تقتصر مصادر تهديد الامن السيبراني على الدول فقط، وانما تشمل الفواعل من غير الدول لا سيما المنظمات غير الحكومية، وان كانت لا تمتلك نفس القدرات للقيام بتهديدات سيبرانية معقدة، فربما تقتصر قدراتها على مهاجمة أهداف ذات اهمية أقل نسبياً كالمواقع الالكترونية، فهذه التهديدات المعقدة الموجهة لأهداف على درجة كبيرة من الاهمية كنظم الاتصالات الدفاعية لابد أن تتم من خلال اجهزة الاستخبارات التابعة للدول والتي تمتلك من الامكانات ما يؤهلها لخرق البيانات المشفرة الخاصة بهذه الانظمة، إذ أن بعض هذه المنظمات هي صغيرة تسعى لتحقيق ارباح سريعة قبل أن يتم اكتشافها من قبل الحكومات ومعاقبتها، فيما يعمل البعض الاخر على المستوى العالمي ويحظى بحماية بعض الدول، كما ان هذه المنظمات تتخذ من الفضاء الالكتروني مجالاً لعملها، ولعل أخطر أنواع هذه المنظمات هي المنظمات الاجرامية وتنقسم الى نوعين: منظمات اجرامية تقليدية تقوم باستعمال الفضاء السيبراني في القيام بهجماتها، ويتمثل النوع الثاني في الجماعات الاجرامية الالكترونية ويمثل الفضاء السيبراني المجال الوحيد لعملها(Seib 2008, 79).

٣. الأفراد

أسهمت تكنولوجيا الاتصالات والمعلومات والانترنت الفاعلين من غير الدول من الافراد في امتلاكهم للقوة السيبرانية وتأسيس شركات عالمية غير خاضعة لسيطرة الدولة، فقد وفر الفضاء السيبراني بيئة مناسبة لتواصل الأفراد (عبد الحي ٢٠١٩ ، ٥١) .

المبحث الثاني

ابعاد الامن السيبراني ومستقبل تهديده للأمن القومي للدول

تختلف الجرائم السيبرانية عن الجرائم التقليدية من حيث طبيعتها ووسائلها؛ فقد أدى التطور السريع في مجال تقنيات المعلومات والاتصالات وشبكة الإنترنت إلى ظهور هذه الجرائم؛ عن طريق هجمات واختراقات للنظم المعلوماتية، لغرض تدميرها أو الحصول على معلومات سرية، فقد اتسمت الجرائم السيبرانية بطابع السرية وعابرة للحدود الاقليمية او الزمنية وتسبب أضراراً فورية للضحايا، لذلك فقد تجاوز جرائم الامن السيبراني مفهومها التقني لتشمل الأبعاد الاستراتيجية والامنية، لذا تم تقسيم المبحث إلى مطلبين، الاول يتناول ابعاد الامن السيبراني، أما الثاني يتحدث عن مستقبل تهديدات الامن السيبراني على الامن القومي للدول .

المطلب الاول

ابعاد الامن السيبراني

أولاً: البعد العسكري:

تعد الحروب السيبرانية من أبرز معالم الصراعات السياسية والاقتصادية بين الدول، فمن الناحية النظرية يقصد بالحرب السيبرانية الأنشطة الخبيثة بواسطة شبكة الإنترنت المدعومة من قبل دولة ما، والتي تستهدف البنية التحتية أو الشبكات الصناعية والأبحاث والمنشآت والمؤسسات الحكومية وهي قادرة على تعطيل تشغيل البنية التحتية الحيوية مع الحد من خطر اندلاع صراع أو حرب جيوسياسية، وسواء أكان الهجوم السيبراني مرتبطاً مباشرة بمؤسسة حكومية أم لا، فقد تكون له عواقب مدمرة لا سيما إذا استهدف منشأة حيوية(موقع مونت كارلو الدولية ٢٠٢٠).

فالإرهاب السيبراني هو محاولة خبيثة ومتعمدة من فرد أو منظمة لاختراق نظام العمل الخاص بفرد أو مؤسسة(Cisco 2024) ، ويمكن التمييز بين نوعين من الإرهاب السيبراني، يشير الاول إلى الإرهاب السيبراني الخاص والذي يتعلق بالهجمات المباشرة على البنية التحتية للمراد استهدافه لتحقيق أهداف مختلفة، في حين يشير الثاني إلى الإرهاب السيبراني الهجين والذي يستعمل فيه المهاجم الادوات السيبرانية في مختلف الانشطة، مثل: الدعاية، والحرب النفسية وتجنيد أعضاء جدد وجمع الاموال والتبرعات والتخطيط لهجمات فعلية(البهي ٢٠١٩).

لذا يعد الإرهاب السيبراني يعد أخطر أنواع الإرهاب إذ انه يؤثر على الأمن القومي للدولة المستهدفة من خلال توظيف تقنيات المعلومات الواسعة لقرصنة المعلومات الاستخباراتية واستخراج البيانات، وجمع الأموال والتوظيف والتعبئة والتدريب عن بعد مثل التدريب على استعمال تقنيات الهجوم ومهاراته، ومشاركة المعلومات، ونشر الأدلة(غرابوسكي ٢٠٠٦، ٣٣٨) ، فقد أكد تقرير المخاطر العلمية الصادر عن المنتدى الاقتصادي العالمي عام ٢٠١٩ أن الإرهاب السيبراني أصبح واقعاً لا مفر منه، ويصف التقرير الهجمات السيبرانية بأنها تتسبب في اضطرابات جيوسياسية أو أضرار اقتصادية كبيرة، أو قد تؤدي إلى فقدان الثقة بشبكة الإنترنت على نطاق شاسع، وتتمثل الهجمات الإرهابية واسعة النطاق بأفراد أو جماعات غير الحكومية ذات أهداف سياسية أو دينية أو اجتماعية تهدف إلى إلحاق أضرار بشرية أو مادية واسعة النطاق، وكشف تقرير ايضاً عن مخاطر عميقة للهجمات السيبرانية، إذ ان له صلة وثيقة بانهيار البنية التحتية للمعلومات المهمة، والاخطر من ذلك أمكانية اطلاق اسلحة الدمار الشامل من خلال استعمال البرامج التخريبية الخبيثة وفيروسات البرامج، فضلاً عن حجب الخدمات والأعمال الاستخباراتية التجسسية على الشبكة وغيرها(ذو

الهدى ٢٠٢٠) ، إذ كشفت دراسة حديثة في مجال تكنولوجيا المعلومات والاتصالات عن أن الجرائم السيبرانية كلفت العالم ما يقارب من (٦) مليار دولار عام ٢٠٢١ ، وهذا ضعف المبلغ عام ٢٠١٥ الذي كان (٣) مليار دولار وهذه التكاليف نابعة من الآثار الكثيرة والأضرار التي خلفتها هذه الجرائم لا سيما سرقة البيانات أو تدميرها وسرقة الأموال والملكية الفكرية والاختلاس والاحتيال، والتحقيق الجنائي والاختلالات التجارية واختراق الأنظمة والإضرار بالسمعة(Jurgens& Del Cin 2024, 24) ، فضلاً عن أن الهجمات السيبرانية قد تكون مدعومة ومكرسة من قبل جهات أو حتى دول لأغراض هجومية أو استخباراتية(شحرة ٢٠١٨، ٩).

ثانياً: البعد الاجتماعي

تتجسد التهديدات السيبرانية في تأثير المخاطر الاجتماعية وفي تشكيل بنية المجتمع ابرزها زيادة الجرائم المستحدثة واستهداف الأمن القومي وهز الثقة في الحكومة واجهزة الدولة المختلفة عبر تهديد البنى التحتية والقيم والأخلاق، كما أن انتشار المخاطر في مختلف الدول يجعلها تنتشر وتتمدد دون القدرة على إخضاعها للسيطرة بواسطة العولمة وانسيابية التدفق وتخطي الحدود القومية التي عملت على توسيع نطاق عدم الأمان المصطنع، ومع تفاقم المخاطر مقابل الفرص فإن مجتمع المخاطر بات يعيش حالة من الشك وعدم الأمان وفقدان اليقين بإمكاناته ومقدرته على مواجهة تلك المخاطر والتحكم فيها(بك ٢٠١٣، ٢٣).

لقد جاء في تقرير الاتحاد الدولي للاتصالات عام (ITU)٢٠١٠ المتعلقة بالأبعاد الاجتماعية، أن الثورة الرقمية غيرت كيفية التعامل التجاري وعمل الحكومات، وأدت العولمة والتقدم التكنولوجي إلى إضعاف البنى التحتية وجعلها هدفا محتملاً لهجمات سيبرانية، إذ تواجه البلدان مخاطر حقيقية؛ تمكّن الأعداء من استغلال مواطن الضعف التي تعاني منها أنظمة المعلومات الدقيقة، من خلال تعطيل البنى التحتية وتهديد الامن القومي لهذه البلدان(تقرير ITU قطاع تنمية الاتصالات ٢٠١٠) ، ومع الاعتماد المتزايد على الأنظمة المعلوماتية والأجهزة المرتبطة بالشبكة الدولية للمعلومات وتشعب طبيعتها يزداد عدد المتصلين بالفضاء السيبراني وتزداد احتمالات الاعتداءات والجريمة (جبور ٢٠١٢، ٤) ، وتسهل سبل التجسس الاقتصادي التي تؤثر في سير عمل الحكومة مثل الفيروسات وهجمات منع الخدمة وسرقة البيانات التي تقوض مصداقية تكنولوجيا المعلومات والاتصالات وقدرة المجتمعات على العمل(تورية ٢٠٠١، ٢) ، ومن المتوقع أن ترتفع التحديات والمخاطر مستقبلاً لاسيما بعد أن أوضح تقرير (Council Advisory Over scan Security) عام ٢٠١٦، أن الهجوم السيبراني على شركة أرامكو السعودية كلفها تغيير (٥٠) ألف قرص صلب لأجهزتها الحاسوبية، ولم تستطع استعمال الإنترنت لمدة (٥) اشهر تقريباً، وأشار تقرير شركة نورتون الأمريكية

(سمنتك) في آب ٢٠١٦ عن وجود (٢٦٢,٥٣٨) ضحية لهجمات سيبرانية، كما ذكر التقرير أن ما يقارب من (٨٥%) من السكان تعرضوا لهجمات سيبرانية(عالم ٢٠١٨، ١) ، إذ أن مفهوم الحرب السيبرانية لا يشمل استهداف القدرات والأنظمة العسكرية فحسب، بل وايضاً استهداف البنى التحتية الحيوية للمجتمع بما في ذلك الشبكات الذكية وحيازة البيانات التي تسمح لها بالعمل والدفاع عن نفسها ومن ثم يؤدي النزاع السيبراني إلى عواقب تهدد البنية التحتية للمعلومات(جبور ٢٠١٢، ١٦).

تزداد أهمية الأمن السيبراني بوصفه يشمل الجوانب التعليمية والاجتماعية والإنسانية والاقتصادية، ومثالاً لقدرة الدولة على حماية مصالحها وشعبها في مختلف المجالات، كونه يرتبط ارتباطاً وثيقاً بسلامة مصادر الثروة المعلوماتية والقدرة على الاتصال والتواصل، وهو المحور الذي يتكون حوله الإنتاج والإبداع، والقدرة على المنافسة(جبور ٢٠١٢، ٧) ، فلقد ازداد اهتمام دول العالم بدور المؤسسات التربوية نظرا لدورها في إعداد المعلمين بشكل يمكّنهم من التعامل والتطورات التكنولوجية كافة التي من المتوقع ان تصل إلى آفاق أبعد، وما يتطلبه هذا التعامل من ادراك وافي بالأمن السيبراني، إذ هناك مسؤولية مزدوجة تقع على عاتق المعلمين في عصر الثورة المعلوماتية يتعلق الأول منها بضرورة الوعي بالأمن السيبراني بوصفه من الأمور اللازمة لكل مستخدم للإنترنت بشكل عام، أما الثاني يتعلق بدور المعلم المهم في إعداد الطلبة وتوعيتهم بمخاطر الأمن السيبراني وانتهاكاته(المنتشري و حريري ٢٠٢٠، ٢٩).

ثالثاً: البعد القانوني

تتمثل المخاطر القانونية بشكل رئيس في غياب الإطارين التشريعي والتنظيمي الملائمين للتعامل مع نتائج الأعمال القانونية وغير القانونية، والتي تتم في الفضاء السيبراني، ويتطلب النشاط التجاري والاقتصادي تحديداً واضحاً للحقوق والواجبات، فمستخدمو هذه التقنيات عبر الفضاء السيبراني بحاجة إلى إطار يؤمن حماية استخدامهم، ففي حالة غياب الأطر التشريعية تؤثر الجرائم السيبرانية على عمليات معلوماتية متعلقة بحقوق الانسان، وتدفع إلى العنف وتؤدي إلى اضرار اقتصادية خطيرة، فضمان إدارة مخاطر الأمن السيبراني على نحو ممنهج يسعى لحماية الأصول التقنية والمعلوماتية وفقاً للسياسات والإجراءات التنظيمية والمتطلبات التشريعية(جبور ٢٠١٢، ٦) ، ومن هذا المنطلق تتمثل المخاطر القانونية في غياب الأمن القانوني أو تناقض الأحكام والقوانين وتنازع الأنظمة القانونية، فيؤدي إلى ارتفاع منسوب المخاطر مع عدم وجود ملاحقة فاعلة، تتلاءم وطبيعة الأعمال والجرائم والاعتداءات السيبرانية، العابرة للحدود وللأنظمة القانونية، وتعد المخاطر التي يتعرض لها الأفراد والدول مخاطر كبيرة وغير مقيدة بالأطر القانونية النافذة التي لا تواكب العصر السيبراني بالقدر الكافي لتشمل النزاع السيبرانى، وعدم تعارض القوانين والتشريعات(تورية ٢٠٠١، ٥).

رابعاً: البعد الاقتصادي

أن الإطار القانوني والأساليب التوعوية وتنظيم العمل المشترك للحد من الهجمات لا تطبقها الدول التي تتصيد المعلومات والبيانات لاسيما البيانات المتعلقة بالبرامج العسكرية والأمنية والنووية، إذ لا بد من إيجاد تقنيات حديثة في الوصول إلى القراصنة وأصحاب الخبرة في كيفية الوصول إلى شبكات البيانات والمعلومات الخاصة بالدول والشركات والافراد للقضاء على الهجمات السيبرانية، وكذلك لابد من التعاون بين الدول على أساس الاحترام المتبادل لسيادة وامن كل منها، وعدم التدخل في شؤونها أو التجسس على انشطتها السياسية والاقتصادية والعسكرية، فأن التطور المستمر في تكنولوجيا الاتصالات وزيادة الاتصال من دون حدود يجعل أمن المعلومات قضية معقدة عابر للوطنية، إذ قدرت شركة الأبحاث (PWC) عن حدوث (١٧٧,٣٠٠) هجوماً سيبرانياً حول العالم عام ٢٠٠٧، فيما ارتفع العدد إلى (٥٩٤) مليون ضحية للهجمات السيبرانية في جميع أنحاء العالم عام ٢٠١٤ بمعدل (١٨) ضحية في الثانية الواحدة و (١,٥) مليون ضحية يومياً، وارتفع عدد ضحايا الهجمات السيبرانية عام ٢٠١٧ بمعدل (٥٤%) مقارنة بعام ٢٠١٤ بمعدل (٣,٥) مليون ضحية يومياً(الصحفي و العسكول ٢٠١٩، ٤٩٥).

إذ أدى الاعتماد المتزايد للشركات العامة والخاصة على تقنيات وشبكات الويب لأنظمة الإدارة المالية الخاصة بها إلى زيادة تعرضها للهجمات السيبرانية، مع تتعدد أهداف هذه الهجمات منها السرقة أو تدمير الأصول المالية أو سرقة الملكية الفكرية أو غيرها من المعلومات المهمة الأخرى المتعلقة بالشركات أو عملائها أو شركائها في العمل، ويتضمن الاستهداف بشكل خاص الشركات العاملة في الصناعات الحيوية ، ومن المتوقع أن تصل تكلفة هذه الهجمات إلى (٦) تريليون دولار بحلول عام ٢٠٢٥، إذ تعد تهديدات الأمن السيبراني من أبرز خمسة تهديدات تواجه الاقتصاد العالمي ومن أكثر عشرة تهديدات تواجه الشركات ومستقبلها التي لا تفقد ثقتها وسمعتها لدى الأطراف المختلفة والمستثمرون والعملاء والموردون فحسب، بل وحتى صناعتها التي تنتمي إليها الشركة بأكملها، وقد أشارت دراسة إلى أن العديد من الدراسات أكدت الآثار الاقتصادية السلبية على الشركات وعلى سمعتها نتيجة الهجمات السيبرانية التي تتعرض لها وتمتد هذه الآثار إلى الصناعة بأكملها فيما يعرف بـ (أثر العدوى)(Gwebu et al.,2014 ; Hinz et al 2015; Higgs et al,2016).

المبحث الثاني

مستقبل تهديد الامن السيبراني للأمن القومي للدول

يواجه العالم اليوم ثورة نوعية يقودها الذكاء الاصطناعي والطابعات ثلاثية الأبعاد والعملات الافتراضية، وغيرها من التقنيات الذكية، التي من شأنها أن تغير ليس هياكل الإنتاج وخصائص المجتمعات وموازين القوة فحسب، بل أيضاً المنظور المعرفي للبشر اتجاه الأشياء، فالبشرية أصبحت في طور التحول نحو جيل جديد من المجتمعات ينذر بظهور مجتمع فائق الذكاء تكون فيه الآلة على حساب الإنسان، نتيجة ظهور الفضاء السيبراني والشبكة العنكبوتية في الحياة البشرية، فسهولة استعمالها ورخص تكلفتها اسهم في قيامها بأدوار مختلفة في الحياة البشرية، سواء كانت سياسية أو اقتصادية أو عسكرية أو معلوماتية وغيرها من المهام التي يمكن أن تقوم بها، ونتيجة لهذا التقدم التكنولوجي فأن تهديدات الامن السيبراني سوف تشكل التحدي الحقيقي في المستقبل المنظور، لما لها من اثار امنية على الامن القومي للدول.

المطلب الاول

تزايد فرص تهديد الامن السيبراني للأمن القومي للدول

بات العالم اليوم يدرك نوع جديد من الحرب الخفية التي تشنها الدول على بعضها البعض، على الرغم من عدم وجود معالم لهذه الحرب، إلاّ أنها أسفرت عن تزايد الهجمات السيبرانية على المستوى العالم بسبب توافر العديد من الفرص التي تزيد من استعمال هذه التهديدات على النحو الآتي:-

اولاً: استعمال التهديدات السيبرانية كأداة جديدة لتعزيز المكانة الدولية

سعت العديد من الدول والفاعلين من غير الدول إلى اداء دور فاعل ومؤثر في النظام الدولي من خلال استعمال التهديدات السيبرانية كسلاح جديد في العلاقات الدولية يمكّنهم من التأثير وتحقيق مصالحهم الخاصة دون الحاجة إلى استعمال الأدوات التقليدية للسياسة الخارجية أو خوض الحروب، أو الجمع بين الادوات السيبرانية والتقليدية لزيادة تأثيرها وتعزيز مكانتها الدولية في المستقبل (شفيق ٢٠١٦، ١٩١) .

ثانياً: إطلاق سباق التسلح السيبراني

اسهم الاهتمام الأمني بالبنى التحتية الحيوية لا سيما أنظمة الدفاع القومي وصناعات أنظمة التحكم وشبكات الاتصالات، في تزايد سباق الدول لزيادة قدراتها السيبرانية في الدفاع والهجوم في إطار من التنافسية التي يحكمها التطور السريع في الأسلحة السيبرانية والحاجة إلى وجود الخبرات والعناصر المؤهلة لقيادة تلك الهجمات (Craig and Valeriano 2016, 141-142) ، وتجلى ذلك من خلال زيادة الإنفاق على الأمن

السيبراني نتيجة لزيادة اعتماد الدول على التكنولوجيا المتقدمة في ادارة جميع مرافقها الحيوية، وسوف يفرض هذا الاعتماد على التكنولوجيا تحديات ومخاطر يدفع بالدول الى السعي الى التسلح لمواجهة التهديدات المتزايدة في المستقبل (Fischer 2016 , 5).

ثالثاً: دخول الأمن السيبراني ضمن السياسات الدفاعية للدول

أصبح الأمن السيبراني جزء لا يتجزأ من سياسات الدفاع الداخلية والخارجية للدول، وهو ما اسهم في تدشين هذا المجال على أجندة الأمن الدولي، لتفادي التهديدات السيبرانية المتنامية التي تهدد البنى التحتية للدول، بسبب ارتباط العالم المتزايد بالفضاء السيبراني، فغياب الأمن السيبراني ضمن السياسات الدفاعية سيؤدي إلى زيادة التهديدات السيبرانية(Ebert and Maurer 2017).

رابعاً: توتر واحتقان العلاقات الدبلوماسية بين الدول بسبب التدخل السيبراني في الشؤون الداخلية

تسفر التهديدات السيبرانية عن إحداث نوع من الخلافات والتوتر في العلاقات الدولية، ويمكن الاستشهاد بذلك من خلال قيام إسرائيل بهجوم سيبراني تمكّن من اختراق مفاعل نطنز النووي في إيران، فضلاً عن منشآت نووية إيرانية أخرى عبر إدخال برنامج فايروسي مُعقد يحمل الاسم المشفر (ستوكسنت) إلى الاجهزة الحاسوبية الخاصة بالتحكم في أجهزة الطرد المركزي لتخصيب اليورانيوم، وتسبب ذلك الهجوم في إحداث فوضى وإخراج هذه الاجهزة عن نطاق السيطرة (Ebert and Maurer 2017).

خامساً: صعوبات تطبيق القانون الدولي على التهديدات السيبرانية

اثارت الحروب والتهديدات السيبرانية الجدل والنقاش حول مدى عدّها حرباً تنطوي على استعمال القوة ومن ثم يمكن تطبيق معايير القانون الدولي عليها، أو أنها مجرد صراعات في الفضاء السيبراني لم تصل بعد إلى مرحلة الحرب، لذلك تتركز الجهود على تطوير قواعد ونصوص القانون الدولي من اجل احتواء الهجمات السيبرانية وتصنيفها ضمن الأعمال العدائية التي تنطوي على استعمال القوة، وسد الثغرات في القوانين النافذة ووضع المعايير القابلة للتطبيق، لكن لا توجد حتى الآن قواعد وقوانين تعمل على تحجيم استعمال الهجمات السيبرانية أو تحديد نطاقها أو خضوع مرتكبيها للعقاب، وفي ظل غياب القواعد والقوانين الدولية فأن فرص تزايد هذه تهديدات السيبرانية ستكون عالية جدا، إذ سيشكل خطراً فعلياً على مستقبل الأمن الدولي(Schreier 2015, 27-28).

سادساً: صعوبة معرفة الطرف المعتدي

تكمن مخاطر التهديدات السيبرانية في صعوبة تحديد هوية الجهة المنفذة للهجمات السيبرانية في الكثير من الحالات ظل غياب التشريعات الدولية التي تلزم الدول أو المؤسسات بعدم القيام بمثل هذه الأنشطة ووضعها تحت طائلة القانون الدولي، مما يعني عدم القدرة على ملاحقتها قانونياً بخلاف الحرب التقليدية،

وهذا سيؤدي الى إعطاء فرصة للطرف المعتدي للقيام بالمزيد من الهجمات السيبرانية(Trujillo 2014, 45).

المطلب الثاني: تراجع فرص تهديد الامن السيبراني للأمن القومي للدول

أن ردع التهديدات السيبرانية على اختلاف أنواعها وآثارها، وما شهده العالم المعاصر من متغيرات متباينة أثرت في الدول المتقدمة والنامية على حد سواء، يؤكد الحاجة إلى اتخاذ اجراءات وانتهاج سياسات رادعة للتهديدات السيبرانية على النحو الآتي:

اولاً: بلورة استراتيجية خاصة للردع بالاستيعاب

تتضمن هذه الاستراتيجية تبني خطط للتعامل مع الهجمات السيبرانية في حالة حدوثها، تشمل التخفيف من حدتها، وعدم تأثر البنى التحتية والخدمات الرئيسة والمعلومات المهمة للأمن القومي، وابرزها(Trujillo 2014, 45):-

١. إنشاء مجسات إلكترونية ونظم إنذار مبكر

تركز على حماية المرافق والبنى التحتية الحيوية التي قد تتعرض للهجمات السيبرانية، وتساعد في اكتشافها فور وقوعها مباشرة، مما يسهل عملية تفادي المخاطر الناجمة عنها.

٢. إنشاء نسخ احتياطي (Back up) للبيانات المهمة

تبني استراتيجية شاملة لإنشاء نسخ احتياطية من بيانات مواطني الدولة سواء كانت هذه البيانات تخص القطاع الحكومي أو الخاص، ويتم تحديث هذه النسخة يومياً، من خلال مزامنة البيانات الموجودة بالأنظمة السيبرانية في مختلف المؤسسات، مع نظام أرشفة وحفظ البيانات الرئيسة، وفي حال تدمير بعض البيانات جراء هجمات إلكترونية يمكن الرجوع الى النسخ الاحتياطية .

٣. تشفير البيانات الرئيسية

تشفير البيانات الحيوية والحساسة والمهمة لا سيما البيانات العسكرية والمراسلات السرية، وفي حال تعرضها للهجمات السيبرانية وسرقتها يصبح من الصعب على الطرف المعتدي فهم ما بداخلها، وحتى يكتسب الطرف المعتدى عليه بعض الوقت من أجل المناورة، إما باكتشاف هذا الطرف ومفاوضته أو الإعلان المسبق عنها(Libicki 2009, 7) .

ثانياً: إيجاد نظم إلكترونية بديلة للخدمات

سعت العديد من الدول في الآونة الاخيرة الى ايجاد نظم الكترونية بديلة لاستعمالها كبدائل عن الأنظمة السائدة في عملية التواصل الآمن بين المستخدمين، من اجل بناء منتظم خالٍ من التهديدات السيبرانية مثل

النظام الضوئي، أو ما يسمى بالحوسبة الضوئية، من خلال التواصل المبني على تقنية الضوء والاستعاضة عن الترانزستورات السيبرانية، وفي هذا النظام يكون التبادل بين المستخدمين أكثر أماناً وفرص اختراقه ضئيلة أن لم تكن منعدمة، وكذلك التواصل عبر تقنية (DBS) (Direct Broadcasting Satellite) الأقمار الصناعية للبث التلفزيوني، إذ ترسل اقماراً تدور في مدارات معينة والتي تسبب بعكس الموجات الكهرومغناطيسية الأقل من (٣٠) ميجاهرتز، والتي يمكن ربطها بمحطة أرضية تكون المركز الثابت لتحديد التردد المعين وتسمح بتواصل آمن ومستقر كإشارات البث التلفزيوني' كما يمكن استعمال (hub) بالتعاون مع شبكات تزويد الخدمة بمختلف انماطه المتعددة، فيكون هناك سيطرة مركزية من قبل مزود الخدمة، ولا يسمح بمرور أي تهديد وتنعدم فيه فرص الاختراق الأمني(Hardesty 2013).

ثالثاً: تطبيق طرق ووسائل جديدة للردع السيبراني

يتطلب الردع السيبراني تطبيق طرق وأساليب جديدة، واعادة تكييف مفاهيم الردع التقليدية، إذ لا يمكن معرفة الهدف من الهجمات دون معرفة الخصم واهدافه، لذلك فأن عملية الردع لن تنجح وسيتم تكرار سرقة المعلومات مستقبلًا، اذا لم يتم الرد على مصدر الهجوم ولن يكون الردع ممكنًا لتآكل مصداقيته، لذا تتعدد الخيارات والسبل المقترحة للردع، ولعل منها على النحو الآتي(Denning 2015, 13-15) :

١. الردع السلبي

يعدّ الأقل تعقيدًا من خلال عدم الرد على الخصم، لكن مع الاعتراف بأن الأمن السيبراني وإجراءاته المتبعة غير كافية، مما يتطلب تطوير الأنظمة الأمنية بشكل مستمر، مما يؤدي إلى تحسن تدابير الأمن السيبراني أو الردع السلبي ويرفع من تكاليف أي هجوم الكتروني في المستقبل، أو تقليل فرص حدوثه.

٢. الاحتجاجات الدبلوماسية

عبر طرد مسؤولي الدولة المشتبه بها في هجمات سيبرانية، على الرغم من سريان قواعد المعاملة بالمثل على ذلك الأمر، مما يؤدي إلى الاضرار بسمعة الدولة في المحافل الدولية وسيجعل الدولة المعتدية تفكر بعلاقاتها ومصالحها قبل القيام بأي تهديد سيبراني .

٣. التدابير القانونية

اتخاذ إجراءات قانونية ضد الدولة المشتبه بها، والتزام جميع الدول الاخرى بقمع ومنع وبكافة الوسائل القانونية أي انشطة متعلقة بالتهديدات السيبرانية، وتوفير التدابير القانونية لتطوير ومواءمة الآليات القانونية للحد من هذه التهديدات، وزيادة فعالية التعاون العابرة للحدود لمنع الانشطة المشبوهة والتحقيق فيها .

٤. العقوبات الاقتصادية

تعزيز العقوبات الاقتصادية ضد الدولة المعتدية مما يجبر هذه الدولة سبب وجيه لتغيير سلوكها، نتيجة التداعيات المحتلة للاعتماد المتبادل وارتباط اقتصاديات الدول مع بعضها البعض في شبكة مترامية الأطرافة ومتداخلة المصالح من شأنه ردع الدول الساعية لشن هجمات سيبرانية تفادياً لتعرض مصالحها للخطر(Stevens 2015, 148).

٥. الانتقام في الفضاء الافتراضي

من خلال التهديد بالانتقام لردع الاختراقات السيبرانية المستقبلية، والتلويح بسرقة ونشر معلومات الخصم واستهداف بنيته التحتية، مما يجعل الخصم يعدل عن تهديداته السيبرانية.

٦. الانتقام العسكري:

يمكن اللجوء الى هذا الخيار في حال أسفرت الهجمات السيبرانية عن نتائج كارثية، دون تحديد الطرف المهاجم بدقة والرد عليه عبر الفضاء السيبراني، مما يؤدي إلى اللجوء إلى التهديد باستعمال القوة العسكرية، أو استهداف اهداف حيوية للطرف المعتدي(Glaser 2011, 5).

الخاتمة:

يعدّ مفهوم الامن السيبراني مفهوماً جديداً على العلاقات الدولية في القرن الحادي والعشرين، ويشير الى الاساليب التي تعتمد على تكنولوجيا المعلومات، لذا فأن التحكم في مؤسسات الدولة الحديثة معلوماتياً اضحى قادرا على اصابة الدول الكبرى بالشلل التام والعجز امام هذه التهديدات، ويشكل هذا المفهوم جزءا لا يتجزأ من الجيل الخامس من الحروب غير المتماثلة والتقليدية التي تشنها دول أو مجموعات او افراد وتستعمل التكنولوجيا المتطورة لتحقيق مصالحها الخاصة، كما بات الفضاء السيبراني، والتقدم التكنولوجي المتسارع من اهم وسائل الصراع المستقبلية القادرة على حسم جوانب عديدة، فقد باتت تسود نظريات الجيوش الذكية القائمة على النوع لا الكم في الاستراتيجيات العسكرية الحديثة لا سيما النوع المتخصص القائم على أسس التكنولوجيا المتقدمة القادرة على تحقيق اعلى المكاسب بأقل التكاليف.

لقد تغيرت موازين القوى عسكرياً واقتصادياً، وأصبحت الاطراف الدولية من الدول وغير الدول القادرة على صناعة التكنولوجيا الحديثة وتطويرها الدور الأبرز والمؤثر في العلاقات الدولية على المستوى السياسي والاقتصادي والعسكري، وأثرت تلك المتغيرات الجديدة في المفاهيم التقليدية للقوة وتحولاتها وتطبيقاتها وأشكالها، فظهر نوع جديد من القوة يتمثل بالقوة السيبرانية التي تعتمد على البرمجيات الرقمية المرتبطة بالفضاء السيبراني، وادوات الاتصال الحديثة لتحقيق اهدافها، ونتيجة لذلك ظهرت العديد من المفاهيم الجديدة

التي تتلاءم وهذا النوع من القوة، مثل الصراع السيبراني والحرب السيبرانية والتجسس السيبراني والدبلوماسية السيبرانية وغيرها من المصطلحات التي تؤسس لهذا النوع الجديد من القوة ، الامر الذي دفع بالعديد من دول العالم على مواكبة التطورات العالمية في هذا المجال، وتسريع وتيرة استعدادتها لمواجهة هذا التحدي الجديد من اجل تحسين ادوات ووسائل الدفاع في الحيز الافتراضي الذي يشكل مصدر قوة لها، لكن في الوقت نفسه يكشف عن مواطن ضعف، إذ أن البنى التحتية الحيوية لعمل الدولة مثل الكهرباء والمواصلات والمياه وشبكات القيادة والسيطرة والتحكم العسكرية تعتمد جميعها على هذا التكنولوجيا المتقدمة، الامر الذي يشكل تهديداً وخطراً على امن الدول، وهذا ما يشجع اغلبية الدول في تطوير عقيدتها الأمنية لتتلاءم والمتغير الجديد، في محاولة منها لمواجهة التهديدات السيبرانية التي تتطور بسرعة، إذ تعدّ الجرائم والارهاب والحروب في الفضاء السيبراني من التحديات الأمنية الجديدة للامن القومي للدول .

المصادر باللغة العربية:

١. إيه كلارك ، ريتشارد و كنيك، روبرت. ٢٠١٢. حرب الفضاء الإلكتروني الخطر القادم على الأمن القومي وسبل مواجهته. ط١. أبوظبي: مركز الإمارات للدراسات والبحوث الاستراتيجية.

٢. بك ، أوليرش. ٢٠١٣. مجتمع المخاطر العالمي بحثاً عن الأمان المفقود. ترجمة: علاء عادل. القاهرة: المركز القومي للترجمة.

٣. بلفرد ، لطفي لمين. ٢٠١٦. الفضاء السيبراني: هندسة وفواعل. المجلة الجزائرية للدراسات السياسية. العدد(٥). المدرسة الوطنية العليا للعلوم السياسية. الجزائر.

٤. بنك الإسكندرية. ٢٠٠٣. النشرة الاقتصادية. المجلد الخامس والثلاثون. الإسكندرية. مصر.

٥. البهي، رغدة. ٢٠١٩. الإرهاب السيبراني: المفهوم والسمات و الأنماط. المركز المصري للفكر والدراسات الإستراتيجية. متاح على الرابط: https://www.ecsstudie.com/7141

٦. تقرير ITU قطاع تنمية الاتصالات. ٢٠١٠ .الاجتماع الإقليمي التحضيري للمؤتمر العالمي للتنمية الاتصالات ٢٠١٠ لمنطقة الدول العربية. دمشق– سوريا. (١٧–١٩ كانون الثاني) .

٧. تورية، حمدون إ. ٢٠٠١. البحث عن السلام السيبراني. الاتحاد الدولي للاتصالات. فريق الرصد الدائم لأمن المعلومات. الاتحاد العالمي للعلماء. ارتشه. صقلية– ايطاليا. (كانون الثاني).

٨. جبور ، منى الأشقر. ٢٠١١. الأمن في الفضاء السيبيري: الأمن المعلوماتي والأمن القانوني. لبنان: الفرع الفرنسي لكلية الحقوق والعلوم السياسية و الادارية.

٩. جبور ، منى الأشقر. ٢٠١٢. الأمن السيبراني: التحديات ومستلزمات المواجهة. اللقاء السنوي الأول للمختصين في أمن الفضاء السيبراني. جامعة الدول العربية. بيروت المركز العربي للبحوث القانونية والقضائية. (٢٧ – ٢٨ آب) .

١٠.ذو الهدى، سني. ٢٠٢٠. تهديد الإرهاب السيبراني وإمكانية تطبيق اتفاقية الجرائم السيبرانية. متاح على الربط التالي: https://imctc.org/arabic/ArticleDetail/Index/637285074665439022

١١.رضوان، ج. ٢٠١٦. الأمن السيبراني: أولوية في استراتيجيات الدفاع. مجلة الجيش. العدد (٦٠٣). مؤسسة المنشورات العسكرية. كانون الاول.

١٢.شحرة، أبو بكر. ٢٠١٨. بناء القدرات في الأمن السيبراني: الأمن السيبراني حروب الأرقام الصماء. العدد (٩٨). المجلة العربية . الرياض– السعودية.

١٣.شفيق ، نوران. ٢٠١٦. السياسة الدولية والاستراتيجية. التهديدات الالكترونية على العلاقات الدولية. ط١. القاهرة– مصر: المكتب العربي للمعارف.

١٤. الصحفي ، مصباح أحمد حامد و العسكول، سناء صالح. ٢٠١٩. مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمي. العدد (٢٨). كلية البنات للآداب والعلوم والتربية. جامعة عين شمس– مصر.

١٥.طاجين ، فريدة. ٢٠١٨. سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية: الواقع والتحديات. الملتقى الدولي الثاني حول سياسات الدفاع. كلية الحقوق والعلوم السياسية. جامعة قاصدي مرباح. الجزائر. ورقلة.

١٦.عالم ، محمد أسعد. ٢٠١٨. الهدم والتخريب تقنياً. المجلة العربية. العدد (٤٩٨) الرياض– السعودية.

١٧.عبد الحي ، صباح عبد الصبور. ٢٠١٩ . استخدام القوة الالكترونية في التفاعلات الدولية: تنظيم القاعدة نموذجاً. ج٢. اسطنبول– تركيا : المعهد المصري للدراسات السياسية والاستراتيجية.

١٨.غرابوسكي، بيتر. ٢٠٠٦. جرائم الحاسب الآلى: الابعاد العالمية في القيادة العامة للشرطة أبو ظبي شبكات الإنترنت وتأثيراتها الاجتماعية والأمنية. أبوظبي: مركز البحوث والدراسات الأمنية. القيادة العامة لشرطة .

١٩.المنتشري، فاطمة يوسف و حريري، رنده. ٢٠٢٠. درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية. العدد (١١٥). الرياض– السعودية: المؤسسة العربية للتربية والعلوم والآداب.

٢٠.موسى، أحمد جمال الدين.٢٠٠٢. النقود الالكترونية وتأثيرها على المصارف المركزية في إدارة السياسة النقدية. أعمال المؤتمر العلمي السنوي لكلية الحقوق. جامعة بيروت العربية. ج١. الجديد في التقنيات المصرفية. بيروت: منشورات الحلبي الحقوقية.

٢١.موقع مونت كارلو الدولية . ٢٠٢٠. ما هي خلفية استراتيجية الصين في الحرب السيبرانية؟ متاح على الرابط:
https://www.mc-doualiya.com/chronicles

٢٢.ناي الأبن ، جوزيف. ١٩٩٧.المنازعات الدولية مقدمة للنظرية والتاريخ. ترجمة: أحمد أمين الجمل ومجدي كامل. الطبعة العربية الأولى. القاهرة : الجمعية المصرية لنشر المعرفة والثقافة العالمية.

المصادر باللغة الانكليزية:

1. Abdul-Hay, Sabah Abdul-Sabour. 2019. The use of electronic power in international interactions: Al-Qaeda as a model. Part 2. Istanbul- Turkey: The Egyptian Institute for Political and Strategic Studies.
2. Alam, Muhammad Asaad. 2018. Technical demolition and sabotage. The Arab Journal. Issue (498) Riyadh- Saudi Arabia.
3. Al-Bahi, Raghda. 2019. Cyber terrorism: concept, characteristics and patterns. Egyptian Center for Thought and Strategic Studies. Available at: https://www.ecsstudie.com/7141
4. Alexandria Bank. 2003. Economic Bulletin. Volume Thirty-Five. Alexandria. Egypt.
5. Al-Montashari, Fatima Youssef and Hariri, Randa. 2020. The degree of awareness of intermediate school teachers of cybersecurity in public schools in Jeddah from the teachers' point of view. Arab Journal of Specific Education. Issue (115). Riyadh - Saudi Arabia: Arab Organization for Education, Science and Arts.
6. Al-Sahafi, Misbah Ahmed Hamed and Al-Askoul, Sanaa Saleh. 2019. Level of Awareness of Cybersecurity among Secondary School Computer Teachers in Jeddah. Scientific Research Magazine. Issue (28). Girls College of Arts, Sciences and Education. Ain Shams University- Egypt.
7. Beck, Ulrich. 2013. The global risk community in search of lost security. Translated by: Alaa Adel. Cairo: National Center for Translation.
8. Belferd, Lotfi Lamine. 2016. Cyberspace: Engineering and actors. Algerian Journal of Political Studies. Issue (5). National Higher School of Political Science. Algeria.
9. Bologna, Sandro . Hämmerli, Bernhard& Gritzalis, Dimitris .2013. Critical Information. Infrastructure Security. Berlin; Springer.
10. Brenner, Susan W & Clarke, Leo L. 2010.Civilians in Cyber warfare: Casualties. Dallas: SMU Science & Technology Law Review.
11. Cisco.٢٠٢٤. What Are the Most Common Cyber Attacks. Available at the link: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
12. Craig ,Anthony and Valeriano, Brandon. 2016. "Conceptualising Cyber Arms Races". in: N.Pissanidis.H.Rõigas And M.Veenendaal (eds.). Cyber Power, 8th International Conference on Cyber Conflict. Nato Ccd Coe Publications. Tallinn.

13. Clark, Richard and Knick, Robert. 2012. Cyber warfare: the coming threat to national security and ways to confront it. 1st ed. Abu Dhabi: Emirates Center for Strategic Studies and Research.
14. De Franco, Joanna F . 2014.What Every Engineer Should Know about Cyber Security and Digital Forensics.Boka Raton: CRC press.
15. Dorothy,Deadening.2015. Rethinking the Cyber Domain and Deterrence, JFQ, 2nd Quarter .
16. Dhu al-Huda, Sunni. 2020. The Threat of Cyberterrorism and the Possibility of Applying the Cybercrime Convention. Available at the following link:https://imctc.org/arabic/ArticleDetail/Index/637285074665439022
17. Ebert, Hannes and Maurer, Tim . 2017.The Impact of Cybersecurity On International Relations. Carnegie Endowment for International Peace. (12 February). Available at the link: http://carnegieendowment.org/2019/01/11/international-relations-and-cyber-security-carnegie-contribution-to-oxford-bibliographies-pub-67672.
18. Fischer, Eric A.2016 . "Cyber security Issues and Challenges, In Brief, Congressional Research Service.
19. Glaser, Charles L. 2011.Deterrence of Cyber Attacks and U.S. National Security, Report GW-CSPRI, George Washington University. Washington. DC.
20. Grabowski, Peter. 2006. Computer crimes: Global dimensions in the General Command of Police Abu Dhabi Internet networks and their social and security impacts. Abu Dhabi: Center for Security Research and Studies. General Command of Police.
21. Graham, James. Howard ,Richard & Olson ,Ryan. 2011 . Cyber Security Essentials. Francis Group. an Informal business.
22. Gwebu et al.,2014 ; Hinz et al ,2015; Higgs et al,2016.
23. Hardesty, Larry . 2013 .MIT researchers build an all-optical transistor, Massachusetts Institute of Technology. Available at the link: http://phys.org/news/2013-07-mit-all-optical-transistor.html#jCp
24. ITU Telecommunication Development Sector Report. 2010. Regional Preparatory Meeting for the World Conference on Telecommunication Development 2010 for the Arab States Region. Damascus-Syria. (January 17-19).
25. Jabour, Mona Ashqar. 2011. Security in Cyberspace: Information Security and Legal Security. Lebanon: French Branch of the Faculty of Law, Political and Administrative Sciences.
26. Jabour, Mona Ashqar. 2012. Cybersecurity: Challenges and Requirements for Confrontation. The First Annual Meeting of Cybersecurity Specialists. League of Arab States. Beirut Arab Center for Legal and Judicial Research. (August 27-28).

27. Jurgens, Jeremy. Del Cin, Paolo . 2024.Cybercrime and the state of resilience, Global Cyber security Outlook 2024.World Economic Forum. (January) .
28. Knapp, Kenneth J . 2018.Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions, Published in the United States of America by Information Science Reference.
29. Libicki, Martin C . 2007. Conquest in Cyberspace: National Security and Information Warfare. New York: Cambridge University Press.
30. Libicki, Martin C. 2009.Cyber deterrence and Cyber war. RAND Cooperation. Santa Monica. CA.
31. Lohr, Steve . 2010.Global Strategy Stabilized IBM During Downturn. New York. Available at the link :ttps://www.nytimes.com/2010/04/20/technology/20blue.html
32. Monte Carlo International website. 2020. What is the background of China's strategy in cyber warfare? Available at:https://www.mc-doualiya.com/chronicles
33. Musa, Ahmed Gamal El-Din. 2002. Electronic money and its impact on central banks in managing monetary policy. Proceedings of the Annual Scientific Conference of the Faculty of Law. Beirut Arab University. Vol. 1. New in banking technologies. Beirut: Al-Halabi Legal Publications.
34. Nai, Joseph. 1997. International disputes: an introduction to theory and history. Translated by: Ahmed Amin Al-Gamal and Magdy Kamel. First Arabic edition. Cairo: The Egyptian Association for the Dissemination of Knowledge and Global Culture.
35. Radwan, J. 2016. Cybersecurity: A Priority in Defense Strategies. Army Magazine. Issue (603). Military Publications Foundation. December.
36. Schreier, Fred. 2015. “On Cyberwarfare”, Dcaf Horizon Working Paper. No. 7.
37. Seib, Philip .٢٠٠٨ .The AlQaeda media machine. Military Review. Army University Press. Kansas.
38. Shafiq, Nouran. 2016. International Policy and Strategy. Electronic Threats to International Relations. 1st ed. Cairo - Egypt: Arab Office for Knowledge.
39. Shahra, Abu Bakr. 2018. Building Capacities in Cybersecurity: Cybersecurity Wars of Deaf Numbers. Issue (98). Arab Magazine. Riyadh - Saudi Arabia.
40. Stevens, Tim . 2015.A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. Contemporary Security Policy. Vol.(33), No. (1). London.
41. Tajin, Farida. 2018. Malaysian defense policies in light of security threats to the digital environment: reality and challenges. The Second International Forum on Defense Policies. Faculty of Law and Political Science. University of Kasdi Merbah. Algeria. Ouargla.

42. Touria, Hamdoun E. 2001. The Search for Cyber Peace. International Telecommunication Union. Permanent Monitoring Team for Information Security. World Federation of Scientists. Arche. Sicily-Italy. (January).
43. Trujillo, Clorinda. 2014.The Limits of Cyberspace Deterrence. the Air War College. Air University. Alabama.
44. Ventre, Daniel.2011. Cyber attaque et cyber défense. Paris; La Voisier.
45. Wiener, Norbert. 1989. The Human Use of Human Beings: Cybernetics and Society. London: Free Association Books.