الامن السيبراني ودوره في تعزيز الامن القومي للدول

م.د زينة عبد الامير عبد الحسن ابراهيم/كلية الاسراء الجامعة

الملخص:
يُعدُّ الامن السيبراني للدول احدى العوامل الاسياسية لحماية امنها ومستقبل بلادها ، فاصبح هذا الامن يضاف الى حدود الدولة الرئيسية (الحدود البرية – الحدود البحرية – الحدود الجوية) ، لما له من دور رئيسي وفاعل في حماية الدولة وتعزيز استقرارها وسيادتها على اراضيها ، فاصبحت الدول في اغلب تفاعلاتها تنطلق في فضاء الكتروني واسع ، وتقوم بالكثير من اعمالها على المستوى الداخلي والدولي في نطاق هذه الفضاء الذي اصبح يمثل جزء لا يمكن التقليل منه او تحييده على صعيد حياة الافراد والدول ، الا ان هذا المجال الالكتروني المهم وما يحملة من فرصة على صعيد الدول وانشطتها واعمالها التي باتت تتم بشكل اسرع وبجهد اقل يحمل معه العديد من التحديات للدولة ، فقد شكل هذا الفضاء بيئة جديدة للقيام بعدد غير محدد من الجرائم الالكترونية الخطيرة التي تهدد امن الدول وسلامتها وسلامة مؤسساتها وبناها التحتية بالاضافة الى الجرائم الى ترتكتب بحق الافراد والجرائم المنظمة الموجه لاستهداف الشباب والاطفال وهو ما فرض على الدول التركيز بشكل كبير على بناء منظومة الامن السيبراني ووضع ستراتيجية لها قادرة على تحقيق اهداف الدولة والاستفادة من هذا الحيز الجديد بمزاياه الفريدة و في ذات الوقت قادرة على وضع حد للتحديات والجرائم التي من الممكن ان توجد في اطاره .

الكلمات المفتاحية : (الامن ، الفضاء الالكتروني ، المعلومات ، الامن السيبراني ، الامن القومي).

Abstract:

The cyber security of states is one of the main factors to protect their security and the future of their country. This security has become added to the main state borders (land borders - sea borders - air borders), because of its key and active role in protecting the state and enhancing its stability and sovereignty over its lands. Most of its interactions are launched in a wide electronic space and do a lot of its work at the internal and international levels within the scope of this space, which has become a part that cannot be minimized or neutralized at the level of the lives of individuals and countries, but this important electronic field and the important opportunity it holds at the level of countries and their activities

And its work, which is now taking place faster and with less effort, but it brings with it many challenges for the state This space has created a new environment for carrying out an unspecified number of serious electronic crimes that threaten the security and safety of countries and the safety of their institutions and infrastructure, in addition to crimes committed against individuals and organized crimes directed at targeting youth and children, which forced states to focus heavily on building a cybersecurity system And developing a strategy for it that is capable of achieving the state's goals and taking advantage of this new space with its unique advantages, while at the same time able to put an end to the challenges and crimes that may exist within it.

Keywords: (security, cyberspace, information, cybersecurity, national security).

مقدمة :

يُعدُّ الفضاء الالكتروني ونظم المعلومات والاتصالات الالكترونية احدى اوجه التفاعلات والاتصالات الاساسية للدول ، ففي عالم تحول الى قرية صغيرة اصبحت هذه النظم الالكترونية تشكل جانب كبيرة منها ، وبالتالي باتت الدول اليوم متجه الى زيادة تفاعلاتها عبر هذا الفضاء الالكتروني ومواكباً لعالم متطور ، بالاضافة الى ان الجزء كبير من التفاعلات الدولية اصبحت تتم عن طريق هذا الفضاء . وكأي مجال مهم وحيوي وذا مردود كبير على مصالح واهداف الدول ، فان جانب الخطر والتهديد فيه يتناسب مع تلك الاهمية ، فبات الفضاء الالكتروني يشكل احدى اوجه التهديد الذي من الممكن ان تتعرض اليها الدول بصورة تختلف عن الطرق التقليدية ، وهو ما فرض على الدول ضرورة التصدي لها ومنعها من التوسع والاضرار بمصالح حيوية وحساسة تمس امن وسلامة الدول والافراد ، خاصة وان الفضاء الالكتروني اصبح يمس كافة جوانب التفاعلات الدولية سياسياً وامنياً واقتصادياً وعسكرياً . وقد جاء الامن السيبراني لحماية هذه الشبكة المهمة وتامين مصالح الافراد والدول من عصابات منظمة ومجرمين اصبحوا يمارسوا هذه الجرائم بصورة الكترونية مسببين ضرر كبير للامن والسلم سواء على نطاق الافراد او بصورة اشمل ليضم امن الدولة وسلامتها ، كالحالة مع جرائم التجسس وسرقة المعلومات والقرصنة الالكترونية وتخريب البنى التحتية والاحتيال الالكترونية وانتحال الشخصية والارهاب الكتروني وغيرها من الجرائم التي تقع في نطاق هذا المجال ، والتي اصبح من الضروري اي تضع الدول كافة التدابير وتتخذ جميع الاجراءات لوقف تلك الاعمال الاجرامية في هذا المجال الحيوي والمهم .

اهمية الموضوع :

تنبع اهمية الموضوع من كون الفضاء الالكتروني ونظم المعلومات الحديثة اصبح اليوم هي احدى مجالات عمل الدولة المهمة وان تامينها وسلامة هذا الفضاء والنظم يعد من حدود وسلامة امن الدول ، وبما ان اليوم جزء كبير من نشاطات وعمل الدولة اصبح يتم من خلال هذا الفضاء المعلوماتي الالكتروني وان معلومات مهمة وحساسة تتعلق بامن الدولة باتت تتواجد وتحفظ فيه ، فان حماية هذه النظم والمعلومات وسلامتها تعدى احدى التحديات الخطيرة التي تقع على عاتق الدولة ، فحماية الفضاء اللكتروني من جرائم خطيرة ربما تقع في نطاق يعد احد الاسس لحماية الامن القومي للبلاد .

اشكالية البحث :

تتمثل اشكالية البحث في ان الفضاء الالكتروني قد فتح مجالاً جديداً امام اشكال من الجرائم غير التقليدية والخطيرة في ذات الوقت تتم هذه العمليات من قبل جماعات واشخاص مجهولين الهوية ومنتسبين الى جهات متعددة على الصعيد الداخلي والخارجي ، وهو ما فرض جهداً اضافية على الحكومة اضافياً ، خاصة فيما يتعلق بالارهاب الالكتروني وجرائم التجسس الالكتروني وسرقة هياكل البنى التحتية المعلوماتية المهمة .

فرضية البحث :

تنطلق فرضية الدراسة من مدى قدرة الحكومات على تعزيز الامن السيبراني لها وبما يسمح للبلاد من الاستفادة من هذا المجال الواسع الحديث ومن توفره من فرصة لتدعيم الامن والاستقرار وتوفير الفرص الاقتصادية الاستثمارية وتعزيز مجال التعاون وكذلك فان تعزيز ودعم هذا المجال سيمكن الدولة من الحد من تاثير تهديدات كبيرة على امنها وسلامتها القومية .

ولاثبات هذه الفرضية او نفيها او تعديلها فسوف يتم الاجابة على التساؤلات الاتية :

اولاً : ما المقصود بالامن السيبراني ؟

ثانياً : ما اهمية الامن السيبراني ؟

ثالثاً : ما هي العلاقة التراتبطة بين الامن السيبراني والامن القومي ؟

رابعاً : التاثير للامن السيبراني على الامن القومي ؟

هيكلية البحث :

انضوت هيكلية البحث في مبحثين رئيسين تضمن الاول التعريف بالامن السيبراني ومدى اهميتة وجاء المبحث الثاني ليسلط الضوء على العلاقة الترابطية للامن السيبراني وكذلك تاثير الامن السيبراني على الامن القومي بالاضافة الى الخاتمة والاستنتاجات .

المبحث الاول : التعريف بالامن السيبراني واهميته

يُعدُّ الامن السيبراني اليوم من القضايا المهمة والحساسة في أمن الدول وسلامتهم ، خاصة وان جانب كبير من الحياة العملية اليوم انتقل الى جانب المعلومات ونظم الحاسوب ، وبالتالي فان الامن السيبيراني اصبح يمثل جانب من عمل الدول وميدانٍ تحقق فيه تطورها ونموها .

المطلب الاول : التعريف بالامن السيبراني

يقصد بالامن السيبراني هو امن حماية المعلومات الرقمية والانظمة والشبكات الالكترونية ضد الهجمات الرقمية ، وتهدف هذه الهجمات الى الوصول الى معلومات مهمة وحساسة والقيام بتغييرها او تدميرها او استخدام للاحتيال على الافراد او تخريب الاعمال التي تتم من خلالها ، وقد زادت هذه الاعمال بسبب ازدياد مجال وفاعلية جانت نظم المعلومات الرقمية ودخولها في مجالات الاعمال كافة بالاضافة الى ازدياد اعداد المستخدمين والاجهزة المستخدمة الى اصبحت تفوق اعداد الاشخاص واصبح المستخدمين لها اكثر ابتكاراً .[١]

فالامن السيبراني هو عبارة عن مجموعة من الوسائل التقنية والادارية والتنظيمية والتي تعمل من خلالها الدول على حماية نظم المعلومات والبيانات التي اصبح مفتوحة على عدد من الدول الاخرى ضمن ما يعرف بالفضاء الالكتروني والعمل على حماية تلك المعلومات وعدم السماح الوصول اليها من قبل اشخاص غير مصرح لهم بذلك ، من اجل ضمان استمرارية عمل نظم المعلومات وتعزيز سرية وخصوصية البيانات فيها ، وضمان امن معلومات الاشخاص والحد من الجرائم الالكترونية التي من الممكن ان تقع ضمن هذا الفضاء .[٢] وكذلك دعم العمليات التشغيلية والمحافظة على سرية وسلامة الاصول الملعوماتية ودقتها وتوافرها .[٣]

وتُعرف ايضاً بانها مجموعة الاجراءات التي تتخذها الاجهزة الامنية او الاجهزة المعنية الاخرى الغرض منها حماية امن المعلومات وسريتها ، ومنع الاختراقات الفايروسية من اجل ضمان

---

[١] Cisco ، ماهو الامن السيبراني ، الموقع الرسمي ل Cisco ، شبكة المعلومات الدولية (الانترنيت) ، تاريخ الاقتباس ٢٥-٤-٢٠٢٢ ، https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html

[٢] الجمهورية اللبنانية الهيئة المنظمة للاتصالات National Internet Safety Lebbanon، الموقع الرسمي للهيئة ، شبكة المعلومات الدولية (الانترنيت) ، تاريخ الاقتباس ٢٥-٤-٢٠٢٢ ، http://www.tra.gov.lb/Cybersecurity-AR

[٣] الضوابط الاساسية للامن السيبراني ، الهيئة الوطنية للامن السيبراني ، المملكة العربية السعودية ، ٢٠١٨ ، ص١٩ .

حماية المعلومات والبيانات المهمة والبنى التحتية المعلوماتية وضمان وصولها بشكل سليم الى كافة المؤسسات والافراد المستفيدين منها ، والسعي في عدم وقوعها بيد الاصدقاء او الاعداء على حد السواء . حيث يمثل هذا الجانب الامني هاجساً كبيراً امام الحكومات والدول ، خاصة مع تعدد مصار التهديد والجهات التي تقف ورائه ووقوعها في اغلبها خارج سيادة الدولة .[٤]

وهو أيضاً مجموعة من الاجراءات المتخذة من قبل الدول من اجل الدفاع ضد الهجمات السيبرانية ونتائجها ، التي تتمثل في اتخاذ التدابير المطلوبة . وقد عرفت وزارة الدفاع الامريكي " البنتاغون " الامن السيبراني بانه " جميع الاجراءات التنظيمية اللازمة لضمان حماية امن المعلومات بجميع اشكالها المادية الالكترونية ، من مختلف الجرائم : الهجمات ، التخريب ، التجسس والحوادث " ، وقد عرف الاعلان الاوربي ان الامن السيبراني هو " قدرة النظام السيبراني على مقاومة محاولات الاختراق التي تستهدف البيانات " .[٥]

فالامن السيبراني هو تلك الاجراءات والسياسات المتبعة من قبل الدول والمتعلقة بحماية امن وسلامة المعلومات والبيانات ومنع الاشخاص غير المخولين من الوصول اليها ومحاولة تخريبها او تغييرها او ممارسة اي نوع من انواع الجرائم الالكترونية من خلالها .

المطلب الثاني : اهمية الامن السيبراني

أن وجود التكنولوجيا اضحى امراً ضروري واساسي ، لاعطاء المؤسسات والافراد ادوات الامن السيبراني من اجل حماية انفسهم من خطر الهجمات السيبرانية ، وتتضمن الحماية في جوانب رئيسة هي الاجهزة الطرفية واجهزة الكومبيتر والاجهزة الذكية والموجهات والشبكات . وضمن عالم اليوم التكنولوجي المتصل فان وجود الامن السيبراني مهم جداً ، فعلى صعيد الافراد يمكن ان تُسفر الهجمات السيبرانية من اختراق المعلومات الشخصية والاطلاع عليها ، انتحال الشخصية ، العمليات التخريبية والاحتيال وفقدان المعلومات الشخصية كالصور العائلية وغيرها ، فالاعتماد على بنية من الامن السيبراني ضروري فمحطات الطاقة والمستشفيات وشركات الاتصالات والمعلومات والنظم المالية والمصرفية كلها اليوم تعتمد على نظم المعلومات وشبكة كبير من تكنولوجيا المعلومات التي من المهم جداً حمايتها من خلال انظمة الامن السيبراني ، فوصول عصابات الاختراق الالكتروني او الهكرز الذين اصبحوا يوظفون التكنولوجيا بطريق محترفة للوصول الى المعلومات والبيانات المهمة يعتبر من الجرائم الخطيرة التي اصبح من

---

[٤] علي زياد العلي ، المرتكات النظرية في السياسة الدولية ، دار الفجر للنشر والتوزيع ، ط١ ، القاهرة ، ٢٠١٧ ، ص٢٢٤.

[٥] الامن السيبراني ، الموسوعة السياسية ، شبكة المعلومات الدولية (الانترنيت) ، تاريخ الاقتباس ، ٥-٥-٢٠٢٢ ، https://political-encyclopedia.org/dictionary/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A

الضروري على الدول أن تهياة لها كافة الامكانات المادية والبشرية للتصدي لها، لما تشكله من خطورة على امن المجتمع وسلامته .[٦]

ويمكن تلخيص أهمية الامن السيبراني بالاتي :[٧]

١- تقديم الحماية الكاملة لامن المعلومات والبيانات وعدم السماح للاشخاص غير المخولين بالاطلاع او العبث بها .
٢- المحافظة على المعلومات وتجانسها وسلامتها .
٣- السماح بتوفير وفرة من المعلومات والبيانات وجاهزيتها للاستخدام في اي وقت يتم الحاجه فيه اليها .
٤- حماية الاجهزة الالكترونية ونظم المعلومات من الاختراق ككل .
٥- اكتشاف نقاط الخلل والضعف في الانظمة الالكترونية ومعالجتها حتى لا يتم استغلالها واختراقها .
٦- توفير بيئة العمل الامنة لجميع مستخدمي شبكة المعلومات الدولية (الانترنيت) .

ومن الناحية العملية فقد ارتبطت اهمية الامن السيبراني مع تزايد الهجمات الالكترونية والتي حدثت بسبب عاملين رئيسيين : [٨]

الاول والذي يمثل بظهور اجهزة الكومبيتر منذ خمسينيات القرن الماضي كادارة لمعالجة وحفظ المعلومات رقمياً (Digital) ، مع تزايد عمل الشركات الخاصة والعامة لتطوير وحدة المعالجة المركزية (CPU) ، وذلك لتسهيل المهام المكلفة بها ، وقد تطور هذا المجال في العقود اللاحقة ، بحيث اصبح جهاز الكومبيتر اساسي في عمل الشركات الخاصة والعامة بالاضافة الى دخوله الى الحياة اليومية للافراد .

الثاني : تمثل في دخول شبكة المعلومات الدولية (الانترنيت) وتزايد المعلومات المشتركة المنتقلة من خلالها والذي احدث نقل نوعية مهمة في حياة البشرية من خلال نقل وتبادل المعلومات من خلال تلك الشبكة ، وقد تسارعت وتيرة استخدام شبكة المعلومات الدولية الانترنيت لاحداث تغيرات وتطورات نوعية في المجال الامني والعسكري وهو ما فتح المجال امام مفاهيم جديدة كالحالة مع سباق التسلح السيبراني والحروب الالكترونية .

لذلك فان الامن السيبراني هو ضرورة لكل دولة تسعى لحماية امنها وسلامته مجتمعها حيث ان اهمية هذا الجانب المعلوماتي والتكنولوجي اصبح لا يقل عن جانب اخر ممكن اي يؤثر على امن وسلامة الدولة كالحالة مع الجانب الاقتصادي والسياسي والعسكري ، فاتجاه العالم اليوم نحو التعامل والتعاون الكترونياً ضمن ما يعرف بالفضاء الالكتروني جعل من الامن السيبراني

---

[٦] Cisco ، مصدر سبق ذكره .

[٧] قاسم بشان التميمي ،الامن السيبراني واهميته في نشر الوعي المجتمعي ، معهد ابرار معاصر طهران ، شبكة المعلومات الدولية (الانترنيت) ، تاريخ الاقتباس ٢٨-٤-٢٠٢٢ ، https://tisri.org/ar/?id=mkl6y9sj

[٨] الموسوعة السياسية ، مصدر سبق ذكره .

من ضروريات التي يجب ان تسعى الدول لتوفير كافة الموارد المادية والبشرية لدعمها وجعلها في مستوى متقدم .

المبحث الثاني : الامن السيبراني والامن القومي للدول

ان التدعيات التي شهدها العالم ومنذ خمسينات القرن العشرين ودخول التكنولوجيا الجانب العملي في حياة الدول واستمرار تزايد وتيرة استخدامها الى ما وصل الى انتهاج عدد من الدول نمط الحكومة الالكترونية والتي تعمل من خلالها على ادارة الدولة ومؤسساتها كافة من خلال نظم المعلومات والحاسوب ادى الى ان يكون امن الدول واستقرارها وتقدمها الاقتصادي والسياسي وحتى العسكري يرتبط بشكل كبير بامن معلوماتها ونظم التكنولوجيا فيها .

المبحث الاول : الترابطية بين الامن السيبراني والامن القومي

تبرز العلاقة بين الفضاء الالكتروني والامن القومي للدول مع التوسع في استخدام نظم المعلومات والتكنولوجيا واتجاه عدد كبير جداً من الدول لتبني نمط الحكومات الالكترونية واتساع نطاق مستخدمي نظم المعلومات سواء على الصعيد المعاملات الحكومية او من جانب شخصي ، ففي هذه الحالة (الحكومة الالكترونية) تصبح نظم المعلومات القومي امام تحدٍ كبير وهو خطر تعرض تلك المعلومات المهمة والحساسة الى التهديد [٩]من خلالها انكشافها على الفضاء الالكتروني او احتمال تعرضها لهجمات الالكترونية ، فضلاً عن التعرض الى الدعاية المغرضة والمضللة ونشر الاشاعات او الدعوة لاعمال تخريبية او عنف ودعم المعارضة لنظام الحكم وتقديم الدعم المالي والمعنوي الكترونياً وهو بمجلها تمثل تحدياً كبيراً لامن الدولة . وان هذا الاعتماد الكبير على جانب المعلومات والتكنولوجيا التي هي اليوم احدى الجوانب التي لا يمكن الاستغناء عنها ، والتي جعلت الامن القومي عرضة لجملة من التحديات الجديدة ، كالحالة مع شركات الطاقة والنقل والموصلات والتجارة الالكترونية والخدمات الحكومية ومؤسسات الدولة المالية ومؤسساتها الامنية ، كل هذا جعل امكانية الوصول الى تلك المعلومات من الجرائم الخطيرة التي من الممكن ان تتعرض لها اي دولة . وقد جعل الفضاء السيبراني جميع تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة تعرف بالبنية التحتية القومية للمعلومات وهي التي ترتبط بدورها بالبنية التحتية الكونية للمعلومات ، وهو ما جعل الامن العالمي يتعلق بمدى قدرة المجتمع الدولي بتوفير انظمة حماية فعالة جدا ومطورة امام اي هجمات الكترونية ممكن ان تعرض امن الدول وسلامتها للخطر .[١٠]

---

[٩] **Kenneth Geers , Strategic Cyber Security , CCDCOE , USA , 2011 , p9 .**

[١٠] عادل عبد الصادق ، الاقتصاد الرقمي وتحديات السيادة السيبرانية ، المركز العربي لابحاث الفضاء الالكتروني ، القاهرة ، ٢٠٢٠، ص١٥ .

وقد امتدت هجمات الفضاء الالكتروني والتطور الكبير الذي جرى عليه الى امكانية توظيفها من قبل دول وجماعات منظمة خاصة للنيل من مراكز ومؤسسات حيوية لدى الدول كالحالة مع استهداف المنشأت العسكرية للدول ، خاصة في ظل اعتماد الدول في اغلب منشأتها الحيوية على التكنولوجيا المتطورة ونظم المعلومات . وهو ما دفع الدول الى تعظيم عناصر قوتها من خلال الاعتماد المتزايد على مزايا الفضاء الالكتروني ، وظهر ما يعرف بالاستراتيجية السيبراني التي تعمل من خلالها الدول على توظيف الفضاء الالكتروني لتحقيق اهدافها وغاياتها واحراز التقدم والتطور الذي تتميز به عن غيرها من الدول .[١١]

عمل انفتاح العالم على الفضاء الالكتروني في تغير طبيعة وخصائص الامن والقوة والصراع في المشهد الدولي ، سواء على المستوى التطبيقي او النظري ، واصبح له ثأثيرات وشواهد في العلاقات بين الدول ، والذي يتم عبر متغيرات ثلاثة :[١٢]

البعد الاول : حيث ان الامن السيبراني لم يعد مقتصراً على البعد التقني بل تمدد الى ابعاد اخرى مع تراجع سيادة الدولة في ظل هذه المتغيرات الجديدة ، وتزايد العلاقة بين الامن والتكنولوجيا بصفة عامة ، مع تزايد فرص تعرض المصالح الوطنية للخطر ، وقد فرضت تلك التطورات اعادة النظر في مفهوم الامن القومي للدول ، والذي يعمل على حماية قيم المجتمع الاساسية ، وابعاد مصادر التهديد عنها ، وابعاد اي خطر ممكن اي يعترض تلك القيم او يهاجمها . كذلك فان تحول الفضاء الالكتروني الى ساحة عالمية عابرة لحدود الدول . ادى الى ان يكون هناك ارتباط عضوي بين الامن السيبراني الداخلي للدولة وامن الفضاء الالكتروني وهو ما يمثل اسس الامن الجماعي العالمي ، خاصة مع وجود تهديدات مشتركة لجميع الفاعلين في مجتمع المعلومات العالمي .

البعد الثاني : فقد فتح الفضاء الالكتروني المجال لبروز نوع جديد من القوة وهي القوة السيبرانية ، حيث اصبح التفوق في هذا المجال من اوجه قوة الدولة الاساسية ويوفر لها تنفيذ عمليات ذات فاعلية في الارض والبحر والجو والفضاء . وفي هذا السياق فقد اسهم في تدعيم القوة الناعمة ، حيث بات الفضاء الالكتروني مسرحاً لشن هجمات تخريبية ترتبط بنشر المعلومات المضللة والحرب النفسية وتاثير في توجهات الرأي العام والنشاط الاستخباراتي ، وهو ما دفع الدول الى زيادة انفاقها علي سياسات الدفاع الالكتروني وحماية شبكاتها الوطنية من خطر التهديدات . وايجاد مؤسسات الوطنية متخصصة في الامن السيبراني .

---

[١١] Greg Austin , Cyber Security in China : The next wave , Springer Briefs in Cyber Security , Australia , 2018 , p3 .

[١٢] عادل عبد الصادق ، مصدر سبق ذكره ، ص ١٧ وما بعدها .

البعد الثالث : والذي يتمثل في ان الفضاء الالكتروني قد اوجد نوع جديداً من مجالات الصراع بين الدول ، وهو الصراع الالكتروني والذي ينشأ نتيجة تعارض المصالح والقيم سواء كان ذلك بين الفواعل من الدول او غير الدول .

وتمثل التهديدات السيبرانية ، احد اهم واكثر الاخطار التي من الممكن ان تتعرض لها الدول كوجود محاولات لاتلاف او تعطيل شبكات الكبيومتر ونظم المعلومات ضعيفة التحصين ،[١٣] حيث ان طبيعة وتاثير التهديد السيبراني متنوعة وعديدة وعادة ما يبدأ ذلك التهديد مع محاولة استغلال حدوث خلل في شبكة المعلومات او وقوع حادث يسمح بحدوث خرق في شبكة المعلومات المهمة او الضوابط الامنية . وتتبع تلك العمليات القيام بهجوم الالكتروني الذي ينطوي على استخدام برمجيات وضارة وتغير الرموز البرمجة الرقمية والانظمة الرياضية او البيانات التي تضر بسرية وسلامة البيانات الهدف النهائي منها احراز اضرار تخريبة بالبنى التحتية الالكتروني والوصول الى معلومات مهمة وتقييد الخدمات الالكترونية او تحقيق المكاسب المادية .[١٤] وهي بمجملها تمثل خطراً كبيرة ممكن ان يتعرض له الامن القومي لاي دولة .

المطلب الثاني : تأثير الامن السيبراني على الامن القومي للدول

يُعدُّ الامن السيبراني اليوم عنصراً مهماً من عناصر امن الدولة ، لذك فقد راحت الدول تتنافس للحصول على مزايا اكثر للامن السيبراني وتعزيزه في مجالات الدفاع والهجوم ، وكذلك تبني استراتيجية وطنية للامن السيبراني تعمل من خلالها على اتباع سياسات فعاله ضمن الفضاء الالكتروني الرقمي تعمل من خلالها على دعم اهدافها السياسة والامنية وفي مختلف جوانب عمل الدولة والعمل على حفظ فرص النمو الاقتصادي في ظل تداعيات ما يعرف بالثورة الصناعية الرابعة والعلاقة القوية بين الامن الرقمي والاقتصاد الرقمي وما يؤسسه هذا من الثقة في الحكومة وسياستها المتبعة .[١٥]

ونتيجة لتزايد الترابط بين الامن والتكنولوجيا المعلومات والفضاء الالكتروني من جهة وتصاعد دور التطبيقات التكنولوجيا في الاقتصاد من جهة اخرى ، وظهور فجوة في الاستجابة لتقديم ستراتيجيات للامن السيبراني تتلائم مع تحديات الفضاء الالكتروني ، وما قدمه من تحديات خطيرة للامن القومي للدول ومنها تاثير ضعف الامن السيبراني على اقتصاد الدولة الرقمي ومؤسساتها المهمة وبالتالي فان لهذه العلاقة الطردية دور كبير في بناء الثقة في البيئة الرقمية والعرض الرقمي والطلب الرقمي والبنية التحتية المعلوماتية في وقت تتصاعد فيه التهديدات الرقمية ، في الوقت الذي تتجه فيه العديد من الحكومات للاستحواذ على مقدرات الثورة الصناعية

---

[١٣] Joseph Steinberg , Cyber Security , Dummies , Canada , 2020 , p5-p7.

[١٤] استراتيجية الامن السيبراني العراقي ، مستشارية الامن الوطني امانة سر اللجنة الفنية العليا لامن الاتصالات والمعلومات ، ٢٠١٧، ٢٠١٧، ص٤.

[١٥] Nick Heard and others , Data Science for Cyber-Security , World Scientific , London , 2018 , p3 .

الرابعة واحراز تقدم تقني كبير يسهم في تحقيق ازدهار الدولة وتقدمها في الوقت الذي يجب على الدول ان تعي مخاطر هذا التطور والانفتاح على الفضاء العالمي الالكتروني وتكون قادرة على حماية امن مجتمعها وسلامته . وايجاد السياسات والتشريعات التي تعمل على تعزيز امنها السيبراني وتطويره والدخول في مجال التنافس مع غيرها من الدول والتي اصبحت قائمة على المساهمة في الابداع والابتكار ، وترجمة ذلك عن طريق تطبيقات تستطيع من تحقيق الاستخواذ على الاسواق الاقتصادية ضمن العالم الجديد . وتظل اهداف الاستراتيجية العليا للامن السيبراني مقترنه بالسياسات والقدرات الدفاع السيبرابي ، وتحقيق المرونه السيبرانية ، والحد من جرائم الالكترونية ، ودعم الصناعة في مجال الامن السيبراني ، وتامين البنية التحتية للمعلومات المهمة .[١٦] فالوجود الاقتصادي للبلد اصبح يعتمد اليوم بشكل كبير جداً على الفضاء الالكتروني ، والذي بدوره جعل هذا الاقتصاد منفتح على فاعلين ودول اخرى ، منها ما قد يحمل نوايا طيبة او لا ، وهو ما يفرض على البلدان تطوير بنى تحتية معلوماتية[١٧] قادرة على حماية المجالات المهمة في البلد كالامن والاقتصاد والمجتمع من جرائم خطيرة وحديثة من نوعها اوجدت تحدٍ لمواجهتها والتي قللت معها من قدرة الدولة على السيطرة عليها ، خاصة وانها قد تتم من قبل اشخاص ودول عديدة كالحالة مع : [١٨]

١- العمليات التي تستهدف المعلومات المهمة في مؤسسات الدولة .
٢- اساءة استخدام شبكة المعلومات الانترنيت ومواقع التواصل لنشر الشاعات والاخبار المضللة التي قد تضر امن وسلامة الدولة .
٣- جرائم الاحتيال وكذلك انتحال الشخصية .
٤- جرائم الابتزاز التي تمارس خصوصاً على طبقة الشباب .
٥- التدخل في الاجهزة الرقمية وانظمة الكمبيوتر .
٦- التخريب الاقتصادي من خلال منع المواطنين من الوصول الى الخدمات الحكومية وغير الحكومية .
٧- الوصول الى معلومات حساسة لمؤسسات الدولة الامنية والخدمية .
٨- الارهاب الالكتروني .
٩- سرقة الاصول الفكرية .
١٠- غسيل الاموال .

ان نقطة انطلاق استراتيجية الامن السيبراني تبدأ مع العمل على تطوير سياسة وطنية لرفع الوعي حول قضايا الامن السيبراني وكيف التعامل مع اي خلل او خرق يتعرض له امن

[١٦] عادل عبد الصادق ، مصدر سبق ذكره ، ص١٦ وما بعدها .

[١٧] Tim Stevens , Cyber Security and Political of Time , Cambridge University Press , London , 2016 , p4-7.

[١٨] استراتيجية الامن السيبراني العراقي ، مصدر سبق ذكره ، ص ٣ .

المعلومات الشخصية للافراد والمؤسسات والابلاغ عنه ، بهدف تقليص المخاصر والتهديدات السيبرانية ، وكذلك يتضمن عمل الدول على المشاركة في الجهود الدولية والاقليمية لتشجيع الوقاية الوطنية والتحضير والاستجابة والتعافي من الحوادث السيبرانية .[١٩] كالحالة مع الجهود الدولية التي تسعى الى دعم الجهود الدولية الرامية لمنع الجهات الفاعلة من غير الدول من اقتناء او صناعة او نقل تحويل او استخدام تقنيات الكترونية ذو استخدامات متعددة قد تستخدم كادوات للهجمات الالكترونية وكذلك العمل على اعتماد وتنفيذ قواينن لحظر استخدام او تطوير او اقتناء الاسلحة الالكترونية .[٢٠]

ومن الامور المعروفة في العلاقات الدولية ان القوة واشكالها في حال تغير مستمر والتاثير الناتج عنها يخضع لذات الامر ، فمن القوة الصلبة بشقيها العسكري والاقتصادي وتزايد الاهتمام بالقوة الصلبة بوصفها التعبير الاوحد لها ، الى بروز شكل جديد من اشكال القوة [٢١]والمتمثل بالقوة الناعمة وقدرت الدول على الجذب والاقناع ، ومع ظهور ثورة المعلومات ظهر شكل جديد من من اشكال القوة وهو القوة السيبرانية Cyber Power والتي اصبح لها تاثير كبير على صعيد المحلي والدولي ، فقد ادى ظهور هكذا ادت الى توزيع وانتشار القوة بين عدد كبير من الفاعلين وهو ما جعل موضوع قدرة الدولة على السيطرة على مواردها وممتلكاتها وبناها التحتيتة في حالة من عدم الاستقرار ومنح الفاعلين الاصغر القدرة على التحكم في القوة الصلبة والقوة الناعمة عبر الفضاء السيبراني وهو ما يعني تغير في شكل العلاقات الدولية وهو ما اثر على الامن القومي للدول وتاثير الفضاء الالكتروني على قوة الدولة والسيادة والحكومة الالكترونية . [٢٢]

ويتمثل هدف الامن السيبراني في قدرة الدولة على مواجهة التهديدات والتحديات التي فرضتها البيئة الدولية والقدرة كذلك على الاستجابة والتعافي من اي هجمات قد تتعرض لها الدولة فيما يخص المجال الالكتروني وبالتالي التحرر من الاضرار الناتجة عن تلك الهجمات كاتلاف او تعطيل الملعومات او بسبب اساءة استخدام تكنولوجيا المعلومات ونتيجة الاهمية المتزايدة للامن السيبراني في حياة الدول والافراد اصبح تعتبر على راس الاولويات المهمة للدول ، خاصة بعد ظهور مجال جديد للقوة والحروب خاصة بين الدول الكبرى وهي التنافس في الفضاء الالكتروني والحروب الالكترونية .

---

[١٩] علي زياد العلي ، مصدر سبق ذكره ، ص ٢٢٦ .

[٢٠] عادل عبد الصادق ، اسلحة القضاء الالكتروني في ضوء القانون الدولي الانسان ، المركز العربي لابحاث الفضاء الالكتروني ، ط٢ ، القاهرة ، ٢٠١٦ ، ص١٥٢.

[٢١] Riant Nugroho , Rethinking National Security Policy : Indonesia Case , Institute for Policy Reform, Pakistan , 2020 , p11 .

الخاتمة :

يُعدُّ الامن السيبراني احدى المقومات الاساسية لبناء امن الدول اليوم ، حيث ان التكنولوجيا والمعلومات اصبحت تشكل جزء كبيراً من مؤسسات الدولة وبناها التحتية ، فلم تعد الدولة تقتصر في قوتها على عناصر القوة الصلبة والناعمة او الذكية فقط بل اصبح جزء منها يذهب الى ما يعرف بالقوة السيبرانية التي تعتبر عن مدى قدرة الدولة على العمل في مجال نظم المعلومات والتكنولوجيا و حماية امنها المعلوماتي وضمان سلامة امنها ومجتمعها فيه ، فقد فتح الفضاء الالكتروني افاق لتحديات جديدة تواجهها الدولة ومخاطر غير تقليدية وجرائم قد تتم من قبل دول او اشخاص او عصابات منظمة متخصصة بهذا النوع من الجرائم ، وهو ما فرض على الدولة المزيد من الجهود لحماية هذا الجانب وكذلك المزيد من الموارد والامكانات والاستعداد لتكون مستعدة من الدخول في جانب التكنولوجيا والمعلومات والاستفادة من مزايا الثورة الصناعية الرابعة وتحقيق ميزة تنافسية مع غيرها من الدول ، فراحت الدول اليوم تتعامل وتتعاون مع غيرها من الدول عن طريق الفضاء الالكتروني الذي اصبح فيه نطاق المعلومات والامن الخاص بالدول مشترك ومنتشر في هذا المجال ، اضافة الى ان العديد من الدول انتقلت الى نمط الحكومة الالكترونية ، وهو ما يعني ان معلومات وبيانات المؤسسات وكذلك الخدمات المقدمة تتم عن طريق نظم المعلومات والاتصالات ، وهو ما جعل جرائم خطيرة وجديدة من نوعها تواجه الحكومات والتي لها تاثير كبير على الامن القومي للدول كالحالة مع سرقة المعلومات المهمة والحساسة او تغيرها ، ايقاف الخدمات المقدمة للمواطنين ، او الوصول الى معلومات متعلقة بامن الدولة ، وكذلك جرائم الاحتيال والنصب الالكتروني وانتحال الشخصية والابتزاز التي تمثل جرائم مهددة لامن وسلامة اي دولة ، وبالتالي فان وجود مستويات عالية من الامن السيبراني للدولة يعد اليوم ضرورة لحماية امنها وسلامتها ، طالما ان العالم اليوم يتجه الى ان تتم اغلب اعمال الدولة من خلال الفضاء الالكتروني والجانب المعلوماتي والتكنولوجي فان حماية هذه المعلومات يعد اساسي لضمان امنها واستقرارها ، والعكس صحيحاً أيضاً كل ما كانت الدولة ضعيفة في مستوى حماية امنها المعلوماتي فان هذا يعني تعرض تلك الدولة لجرائم خطيرة وتحديات تهدد امنها وسلامتها .

الاستنتاجات :

١- ان امن المعلومات والبيانات اصبح ضرورة لاي دولة تسعى الى تحقيق الامن والاستقرار والازدهار لبلادها ، حيث ان وجود انظمة ومؤسسات متخصصة لحماية هذه المعلومات يعد من عناصر قوة الدولة الحديثة .

---

[٢٢] الموسوعة السياسية ، مصدر سبق ذكره .

٢- ان وجود الامن السيبراني يعني تحقيق النمو والتقدم على المستوى الاقتصادي ، حيث ان اقتصاد الدول اليوم تعتمد في جانب كبير منها على نظم المعلومات والتكنولوجيا وتتم في فضاء الكتروني تتشارك من خلاله عدد من الدول تلك العمليات الاقتصادية .

٣- ان الامن السيبراني اليوم يعكس في جزء كبير منه الامن القومي للدولة ومدى قدراتها على ضبط حدودها التقليدية (البرية والبحرية والجوية) وحدودها الافتراضية من خلال وجود امن المعلومات لديها .

٤- ان الضعف الحاصل في مجال الامن السيبراني و عدم جود الامكانات والاجهزة والمؤسسات المتخصصة في هذا المجال يعني دخول البلاد في سيل من الجرائم الالكترونية الخطيرة والتي تمس امن وسلامة البلاد والنظام القائم فيها .

٥- ان قدرة الدولة اليوم على تحقيق جانب متطور من الامن السيبراني يعني ذلك تحقيق الدولة ذات المستويات على الجانب الاقتصادي والسياسي والامني والدولي حيث ان الامن السيبراني يوفر الحماية والسلامة على الصعيد الداخلي للدولة ويمكنها لان تكون اكثر تعاوناً وتأثيراً على الصعيد الدولي .

المصادر :

١- استراتيجية الامن السيبراني العراقي ، مستشارية الامن الوطني امانة سر اللجنة الفنية العليا لامن الاتصالات والمعلومات ، ٢٠١٧.

٢- الامن السيبراني ، الموسوعة السياسية ، شبكة المعلومات الدولية (الانترنيت) ، تاريخ الاقتباس ، ٥-٥-٢٠٢٢ ، https://political-encyclopedia.org/dictionary/%D8%A7%D9%84%D8%A3%D9%85%D9%86%20%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A

٣- الجمهورية اللبنانية الهيئة المنظمة للاتصالات National Internet Safety Lebbanon ، الموقع الرسمي للهيئة ، شبكة المعلومات الدولية (الانترنيت) ، تاريخ الاقتباس ٢٥-٤-٢٠٢٢ ، http://www.tra.gov.lb/Cybersecurity-AR

٤- الضوابط الاساسية للامن السيبراني ، الهيئة الوطنية للامن السيبراني ، المملكة العربية السعودية ، ٢٠١٨ .

٥- عادل عبد الصادق ، اسلحة القضاء الالكتروني في ضوء القانون الدولي الانسان ، المركز العربي لابحاث الفضاء الالكتروني ، ط٢ ، القاهرة ، ٢٠١٦ .

٦- عادل عبد الصادق ، الاقتصاد الرقمي وتحديات السيادة السيبرانية ، المركز العربي لابحاث الفضاء الالكتروني ، القاهرة ، ٢٠٢٠.

٧- علي زياد العلي ، المرتكات النظرية في السياسة الدولية ، دار الفجر للنشر والتوزيع ، ط١ ، القاهرة ، ٢٠١٧.

٨-قاسم بشان التميمي ،الامن السيبراني واهميته في نشر الوعي المجتمعي ، معهد ابرار معاصر طهران ، شبكة المعلومات الدولية (الانترنيت) ، تاريخ الاقتباس ٢٨-٤-٢٠٢٢ ، https://tisri.org/ar/?id=mkl6y9sj

٩- Cisco ، ماهو الامن السيبراني ، الموقع الرسمي ل Cisco ، شبكة المعلومات الدولية (الانترنيت) ، تاريخ الاقتباس ٢٥-٤-٢٠٢٢ ، https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html

10- Greg Austin , Cyber Security in China : The next wave , Springer Briefs in Cyber Security , Australia , 2018 .

11- Joseph Steinberg , Cyber Security , Dummies , Canada , 2020 .

12- Kenneth Geers , Strategic Cyber Security , CCDCOE , USA , 2011 .

13- Nick Heard and others , Data Science for Cyber-Security , World Scientific , London , 2018 , p3 .

14- Riant Nugroho , Rethinking National Security Policy : Indonesia Case , Institute for Policy Reform, Pakistan , 2020 .

15- Tim Stevens , Cyber Security and Political of Time , Cambridge University Press , London , 2016 .