الامن السيبراني في العراق: قراءة في تأثيره على صنع السياسة العامة وتعزيز الأمن الوطني

م.م. بنين سعد صافي
الجامعة المستنصرية/ كلية العلوم السياسية
baneensaad@uomustansiriyah.edu.iq

الملخص

يتناول هذا البحث موضوع الأمن السيبراني في العراق من خلال قراءة تحليلية لمدى تأثيره في عملية صنع السياسة العامة وانعكاسه على تعزيز الأمن الوطني . وينطلق البحث من فرضية مفادها أن تصاعد التهديدات السيبرانية وتحول الفضاء الرقمي إلى مجال حيوي لإدارة شؤون الدولة قد جعلا من الأمن السيبراني عاملاً محدداً في إعادة ترتيب أولويات الأجندة الحكومية وصياغة السياسات العامة.

اعتمد البحث على المنهج الوصفي التحليلي ومدخل تحليل النظم، إلى جانب الاستفادة من مقاربات الحوكمة الرقمية ونظرية الأمننة، لتفسير كيفية إدراج قضايا الأمن السيبراني ضمن الإطار الاستراتيجي للدولة .وقد خلص إلى أن الأمن السيبراني في العراق يشهد تطوراً تدريجياً على مستوى الإدراك المؤسسي والتشريعي، إلا أنه ما يزال يواجه تحديات تتعلق بتعدد الجهات المعنية، وضعف التنسيق المؤسسي، ووجود فراغات قانونية، فضلاً عن محدودية الوعي المجتمعي والثقافة الرقمية.

كما أظهر البحث أن إدماج الأمن السيبراني في التخطيط الوطني يسهم في حماية البنى التحتية الحيوية، وصون العملية الانتخابية، وتعزيز السيادة الرقمية، مما يجعله أحد المرتكزات الأساسية للأمن الوطني المعاصر .ويوصي البحث بضرورة بناء استراتيجية وطنية متكاملة للأمن السيبراني، وتطوير القدرات البشرية والتقنية، وتعزيز الشراكة بين القطاعين العام والخاص، والاستفادة من التجارب الدولية

المقارنة بما يتلاءم مع خصوصية البيئة العراقية.

الكلمات المفتاحية :

الأمن السيبراني، السياسة العامة، الأمن الوطني، السيادة الرقمية، الحوكمة الرقمية، الجرائم الإلكترونية، البنية التحتية الحيوية، العراق.

تأريخ الاستلام 2026/9/18 تأريخ قبول النشر 2026/9/21

Cybersecurity in Iraq: An Analysis of its Impact on Public Policy Making and National Security Enhancement

Assistant Lecturer Baneen Saad Safi
Al-Mustansiriya University/College of Political Science
baneensaad@uomustansiriyah.edu.iq

Abstract

This research examines cybersecurity in Iraq through an analytical perspective that explores its impact on public policy-making and its role in strengthening national security. The study is based on the assumption that the growing scale of cyber threats and the increasing reliance on digital infrastructure have positioned cybersecurity as a strategic priority within the governmental agenda, directly influencing policy formulation and national planning processes.

The research adopts a descriptive-analytical approach, drawing on systems analysis, digital governance perspectives, and securitization theory to interpret how cybersecurity issues are integrated into Iraq's public policy framework. The findings indicate that although Iraq has shown gradual progress in institutional awareness and regulatory efforts related to cybersecurity, significant challenges remain. These include institutional fragmentation, limited coordination among relevant authorities, legislative gaps, and insufficient public awareness and digital culture.

The study concludes that integrating cybersecurity into

national planning contributes to protecting critical infrastructure, safeguarding electoral processes and government data, and reinforcing digital sovereignty. Consequently, cybersecurity represents a fundamental pillar of contemporary national security. The research recommends the development of a comprehensive national cybersecurity strategy, the enhancement of human and technical capacities, stronger public–private partnerships, and the adoption of best practices from international experiences tailored to Iraq's specific context.

Keywords :
Cybersecurity, Public Policy, National Security, Digital Sovereignty, Digital Governance, Cybercrime, Critical Infrastructure, Iraq.

المقدمة:

شهد العالم المعاصر تحولاً جذرياً في مفهوم الأمن الوطني مع بروز "الفضاء السيبراني" كساحة جديدة للمنافسة والصراع، لم تعد تقتصر آثارها على الجوانب التقنية فحسب، بل امتدت لتؤثر بشكل مباشر في استقرار الدول وسيادتها. وفي الحالة العراقية، جاء التوسع المتسارع في تبني تطبيقات الحكومة الإلكترونية والرقمية في المؤسسات الحكومية والخدمية والمالية مصحوباً بتصاعد ملحوظ في التهديدات والجرائم السيبرانية؛ مما وضع صانع القرار السياسي أمام تحديات غير تقليدية.

بناءً على ذلك، لم يعد الأمن السيبراني مجرد خيار تقني ثانوي، بل تحول إلى ضرورة حتمية ومتغير حاسم يعيد تشكيل أولويات السياسة العامة للدولة. وتأتي هذه الدراسة لتسليط الضوء على هذه الديناميكية، من خلال قراءة تحليلية تفكك العلاقة التفاعلية بين متطلبات الأمن الرقمي وآليات صنع القرار والاستراتيجيات الوطنية في العراق.

أولاً: أهمية البحث

علمياً: سد الفجوة الأكاديمية بين علوم السياسة والدراسات السيبرانية في العراق عبر الربط النظري والتطبيقي.

عملياً: تقديم رؤية تشخيصية وحلول إجرائية لصنّاع القرار لحماية البنى التحتية الحيوية (الطاقة، المصارف، الانتخابات) وتحديث التشريعات.

ثانياً: إشكالية البحث

تتمحور حول: تحدي الموازنة بين تصاعد التهديدات الرقمية والحاجة للتحول الرقمي، في مقابل وجود فجوات تشريعية، وتشتت مؤسسي، ومحدودية في الوعي الأمني.

ثالثاً: فرضية البحث

يفترض البحث أن: تصاعد المخاطر السيبرانية يمثل متغيراً حاسماً يفرض على صانع القرار العراقي إعادة ترتيب أولويات الأجندة الحكومية وتبني سياسات استباقية تعزز الأمن القومي والسيادة الرقمية.

رابعاً: المناهج والمقاربات المستخدمة

المنهج الوصفي التحليلي: لتشخيص الواقع الرقمي والتشريعي في العراق.

مدخل تحليل النظم (David Easton): لتفسير تحويل التهديدات (مدخلات) إلى سياسات واستراتيجيات (مخرجات).

مقاربة الحوكمة الرقمية ونظرية الأمننة: لتفسير نقل الملف الرقمي إلى صلب قضايا الأمن القومي والشراكة مع القطاع الخاص

المبحث الاول : الإطار المفاهيمي والنظري للأمن السيبراني والسياسة العامة

يشكّل الإطار المفاهيمي لأي دراسة علمية الركيزة الأساسية التي تُبنى عليها التحليلات والاستنتاجات، إذ لا يمكن مقاربة موضوع معاصر ومعقّد كالأمن

السيبراني من دون تحديد مفاهيمه وضبط مصطلحاته وربطه بالسياق النظري الذي يفسّر علاقته بصنع السياسة العامة. وقد أصبح الأمن السيبراني أحد أبرز موضوعات الدراسات الأمنية الحديثة، بعد أن تحوّل الفضاء الرقمي إلى ساحة جديدة للصراع والتنافس بين الدول، وأضحى تأثيره يمتد إلى مختلف القطاعات الحيوية السياسية والاقتصادية والعسكرية والاجتماعية.

وفي الحالة العراقية، تبرز أهمية هذا الإطار المفاهيمي بسبب التحول الرقمي المتسارع الذي تشهده مؤسسات الدولة، مقابل تصاعد التهديدات السيبرانية العابرة للحدود. ومن هنا، يهدف هذا المبحث إلى تأصيل المفاهيم الأساسية المرتبطة بالأمن السيبراني وأمن المعلومات، وبيان التطور النظري لهما، تمهيداً لتحليل تأثيرهما في عملية صنع السياسة العامة وتعزيز الأمن الوطني.

المطلب الأول : تعريف الأمن السيبراني وأمن المعلومات

يمثل تحديد المفاهيم خطوة منهجية ضرورية لتفادي الخلط الاصطلاحي بين الأمن السيبراني وأمن المعلومات، إذ كثيراً ما يُستخدم المصطلحان بوصفهما مترادفين، رغم وجود تمايز نسبي بينهما من حيث النطاق والوظيفة. فالأمن السيبراني يرتبط بحماية الفضاء الإلكتروني بكل مكوناته التقنية والبشرية، في حين يركّز أمن المعلومات على حماية البيانات ذاتها من الوصول غير المصرح به أو الاستخدام أو التعديل أو الإتلاف.

وعليه، فإن فهم هذا التمييز يسهم في بناء تصور أدقّ لطبيعة التهديدات المعاصرة، ويساعد في صياغة سياسات عامة أكثر شمولاً واستجابة للتحديات الرقمية التي تواجه الدولة العراقية في بيئة دولية تتسم بالتشابك والتعقيد.

المحور الأول: تعريف الأمن السيبراني وأمن المعلومات

أولاً: تعريف الأمن السيبراني

يُعرَّف الأمن السيبراني بأنه مجموعة الإجراءات والتدابير التقنية والتنظيمية والقانونية التي تهدف إلى حماية الأنظمة الحاسوبية والشبكات والبرمجيات والبيانات من الهجمات الرقمية أو الاختراق أو التخريب أو التجسس. ويشمل ذلك حماية البنية التحتية الحيوية الرقمية وضمان استمرارية عملها، فضلاً عن الحفاظ على سرية المعلومات وسلامتها وتوافرها في البيئة الإلكترونية (الهيئة الوطنية للأمن السيبراني، 2018، 1) .

كما يُنظر إلى الأمن السيبراني بوصفه أحد مكونات الأمن الوطني المعاصر، إذ لم يعد مقتصراً على الجانب التقني فحسب، بل أصبح يرتبط مباشرة بحماية سيادة الدولة واستقرارها السياسي والاقتصادي، خاصة في ظل تصاعد الهجمات السيبرانية التي تستهدف المؤسسات الحكومية والقطاعات الحيوية مثل الطاقة والمصارف والاتصالات. ومن ثمّ، بات الأمن السيبراني يشكل بعداً استراتيجياً في منظومة الأمن الشامل للدول (الهاشمي، 2021، 44_47) .

ثانياً: تعريف أمن المعلومات

أما أمن المعلومات فيُقصد به حماية المعلومات بمختلف أشكالها (الرقمية أو الورقية) من التهديدات التي قد تؤدي إلى إفشائها أو تغييرها أو إتلافها، وذلك عبر تطبيق مجموعة من الضوابط التقنية والإدارية. ويرتكز أمن المعلومات على ثلاثة مبادئ أساسية تُعرف بمثلث الحماية (CIA Triad)، وهي: السرية (Confidentiality)، والسلامة أو التكامل (Integrity)، والتوافر (Availability) (العصيمي، 2024) .

ويُعدّ أمن المعلومات أوسع من حيث ارتباطه بحماية البيانات ذاتها بغض النظر عن الوسيط المستخدم، بينما يُعدّ الأمن السيبراني جزءاً منه يركز تحديداً على

البيئة الرقمية والشبكات الإلكترونية. ومع تطور التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية، أصبح التكامل بين أمن المعلومات والأمن السيبراني ضرورة لضمان حماية الموارد المعلوماتية للدولة وتعزيز قدرتها على مواجهة التهديدات الإلكترونية المعقدة (الشريف، 2020، 28)

المحور الثاني: الفرق بين الأمن السيبراني وأمن المعلومات

يُعدّ التمييز بين الأمن السيبراني وأمن المعلومات مسألة مفاهيمية ومنهجية مهمة في الدراسات الأمنية المعاصرة، إذ إن الخلط بين المصطلحين قد يؤدي إلى قصور في فهم طبيعة التهديدات الرقمية وصياغة السياسات العامة المناسبة لمواجهتها. وعلى الرغم من وجود تقاطع بين المفهومين، إلا أن لكل منهما نطاقاً ووظيفة وأدوات مختلفة نسبياً (عتوم، 2023، 116).

أولاً: من حيث نطاق الحماية

يركّز أمن المعلومات على حماية المعلومات ذاتها، سواء كانت مخزنة إلكترونياً أو محفوظة ورقياً أو متداولة شفهياً، ويشمل ذلك وضع ضوابط لضمان سريتها وسلامتها وتوافرها. فهو مفهوم شامل يتعامل مع البيانات كمورد استراتيجي يجب حمايته بغض النظر عن الوسيط الذي يحتويه.

أما الأمن السيبراني فينصرف إلى حماية الفضاء الإلكتروني بما يتضمنه من شبكات وأنظمة وأجهزة وبرمجيات وبنى تحتية رقمية، أي أنه يركّز على البيئة التقنية التي تُدار من خلالها المعلومات. وعليه فإن الأمن السيبراني يُعدّ جزءاً من الإطار الأوسع لأمن المعلومات، لكنه يتميز بتركيزه على مواجهة الهجمات الإلكترونية والاختراقات الرقمية التي تتم عبر الشبكات (الهاشمي، 2021، 32).

ثانياً: من حيث طبيعة التهديدات

تتمثل التهديدات التي يعالجها أمن المعلومات في السرقة أو الإفشاء غير المشروع أو الإتلاف أو التلاعب بالبيانات، سواء كان مصدرها بشرياً داخلياً (موظفون) أو

خارجياً. وهو بذلك يتعامل مع المخاطر الإدارية والتنظيمية إضافة إلى المخاطر التقنية.

في المقابل، يركّز الأمن السيبراني على التهديدات ذات الطابع الإلكتروني مثل الهجمات السيبرانية، البرمجيات الخبيثة، هجمات حجب الخدمة، الاختراقات المنظمة، والحروب السيبرانية بين الدول. وبالتالي فإن طبيعته أكثر ارتباطاً بالبيئة الرقمية المتصلة بالإنترنت وبالتطور التكنولوجي المتسارع (الشريف، 2020، 35).

ثالثاً: من حيث الأدوات والآليات

يعتمد أمن المعلومات على سياسات الحوكمة، وإدارة المخاطر، وضوابط الوصول، والتشفير، والتدقيق الداخلي، والتوعية المؤسسية، إضافة إلى الإجراءات القانونية والتنظيمية.

أما الأمن السيبراني فيعتمد بدرجة أكبر على أنظمة الحماية التقنية المتقدمة مثل الجدران النارية، وأنظمة كشف التسلل، وتحليل البرمجيات الضارة، ومراكز الاستجابة للحوادث السيبرانية، إلى جانب التعاون الدولي في تبادل المعلومات الاستخبارية الرقمية.

ومن ثمّ يمكن القول إن العلاقة بين المفهومين علاقة تكامل لا تعارض؛ إذ يشكل أمن المعلومات الإطار الشامل لحماية البيانات، بينما يمثل الأمن السيبراني البعد التقني–الاستراتيجي لحماية الفضاء الرقمي الذي يحتوي تلك البيانات.

وبذلك يتضح أن إدراك هذا التمييز يسهم في صياغة سياسات عامة أكثر دقة وفعالية، خاصة في الدول التي تسعى إلى بناء منظومة وطنية متكاملة للأمن السيبراني ضمن إطار أوسع لحماية معلوماتها وتعزيز أمنها الوطني.

المحور الثالث: تطور مفهوم الأمن السيبراني في الدراسات الاستراتيجية المعاصرة

شهد مفهوم الأمن السيبراني تحولات جوهرية في الأدبيات الاستراتيجية المعاصرة، إذ انتقل من كونه مفهوماً تقنياً محدود النطاق إلى مفهوم استراتيجي يرتبط بالأمن القومي والسيادة الوطنية وإدارة الصراعات الدولية. ويعكس هذا التطور التحولات البنيوية في طبيعة النظام الدولي، وتزايد الاعتماد على التكنولوجيا الرقمية، وظهور الفضاء السيبراني كساحة جديدة للتنافس بين الفاعلين الدوليين وغير الدوليين.

أولاً: المرحلة التقنية – الأمن السيبراني بوصفه حماية للأنظمة

في بدايات ظهوره خلال تسعينيات القرن العشرين، ارتبط مفهوم الأمن السيبراني بحماية أنظمة الحاسوب والشبكات من الاختراقات التقنية والفيروسات. وكانت المقاربة السائدة ذات طابع تقني–إجرائي تركز على أدوات الحماية مثل التشفير والجدران النارية وأنظمة كشف التسلل، دون النظر إليه كبعد من أبعاد الأمن القومي.

وقد انحصرت المعالجة آنذاك في إطار أمن المعلومات وإدارة المخاطر التقنية داخل المؤسسات، ولم يكن يُنظر إلى الفضاء الإلكتروني باعتباره مجالاً للصراع الاستراتيجي بين الدول (الهاشمي، 2021، 18).

ثانياً: المرحلة الأمنية – الأمن السيبراني كتهديد للأمن القومي

مع مطلع الألفية الثالثة، خاصة بعد تصاعد الهجمات الإلكترونية الكبرى واستهداف البنى التحتية الحيوية في عدد من الدول، بدأ مفهوم الأمن السيبراني يتخذ بعداً أمنياً–استراتيجياً. فقد أظهرت الهجمات السيبرانية قدرتها على تعطيل منشآت الطاقة، والأنظمة المصرفية، والمرافق الحكومية، مما دفع الدول إلى إدراج الأمن السيبراني ضمن استراتيجيات الأمن القومي.

وفي هذه المرحلة، توسعت الدراسات الاستراتيجية لتتناول مفاهيم مثل "الحرب السيبرانية" و"الردع الرقمي" و"التهديدات الهجينة"، وأصبح الفضاء السيبراني يُعدّ المجال الخامس للصراع بعد البر والبحر والجو والفضاء الخارجي. كما برزت أهمية إنشاء قيادات عسكرية مختصة بالأمن السيبراني في العديد من الدول (الشريف، 2020، 52) .

ثالثاً: المرحلة الاستراتيجية الشاملة – الأمن السيبراني كأداة قوة وطنية

في المرحلة المعاصرة، تطور مفهوم الأمن السيبراني ليصبح جزءاً من مفهوم القوة الشاملة للدولة، إذ لم يعد مقتصراً على الحماية والدفاع، بل امتد ليشمل القدرة على التأثير الرقمي، وإدارة الفضاء المعلوماتي، وحماية السيادة الرقمية، وتعزيز المكانة الدولية.

وأصبحت الدراسات الاستراتيجية تنظر إلى الأمن السيبراني من منظور الحوكمة الرقمية، والتنافس الجيوسياسي، والاقتصاد الرقمي، وربطته بمفاهيم مثل الأمن الإنساني، والأمن الاقتصادي، والاستقرار السياسي. كما برز اتجاه يُعرف بـ"أمننة الفضاء السيبراني"، حيث يتم التعامل مع التهديدات الرقمية بوصفها تهديدات وجودية تستوجب إجراءات استثنائية ضمن سياسات الدولة (عبد الحميد، 2022، 87) .

يتضح من هذا العرض أن مفهوم الأمن السيبراني مرّ بثلاث مراحل رئيسة: مرحلة تقنية ركزت على حماية الأنظمة، ومرحلة أمنية ربطته بالأمن القومي، ومرحلة استراتيجية شاملة جعلته أحد مكونات القوة الوطنية وأداة في إدارة التنافس الدولي. ويعكس هذا التطور التحولات العميقة في طبيعة التهديدات المعاصرة، الأمر الذي يفرض على الدول — ومنها العراق — إعادة صياغة سياساتها العامة بما ينسجم مع هذا الفهم الاستراتيجي المتكامل للأمن السيبراني.

المطلب الثاني: مفهوم السياسة العامة وعلاقتها بالأمن الوطني

تُعدّ السياسة العامة الأداة الرئيسة التي تُترجم من خلالها الدولة رؤيتها وأهدافها إلى قرارات وبرامج عملية تستجيب لحاجات المجتمع وتحديات البيئة الداخلية والخارجية. وفي ظل التحولات المتسارعة التي يشهدها النظام الدولي، لم يعد مفهوم الأمن الوطني مقتصراً على البعد العسكري التقليدي، بل اتسع ليشمل أبعاداً سياسية واقتصادية واجتماعية وتقنية، ومن بينها البعد السيبراني. ومن ثمّ أصبحت العلاقة بين السياسة العامة والأمن الوطني علاقة عضوية، إذ تُصاغ السياسات العامة في ضوء متطلبات الحفاظ على الاستقرار وحماية المصالح العليا للدولة.

ويُظهر هذا الترابط أن عملية صنع السياسة العامة لا تنفصل عن الاعتبارات الأمنية، بل تتأثر بها في تحديد الأولويات وتخصيص الموارد واختيار البدائل المناسبة. فكلما تعاظمت التهديدات، سواء كانت تقليدية أو رقمية، ازدادت الحاجة إلى سياسات عامة رشيدة قادرة على تحقيق التوازن بين التنمية والحماية، وبين الانفتاح والسيادة. وعليه، فإن فهم مفهوم السياسة العامة ومراحل صنعها يمثل مدخلاً ضرورياً لتحليل كيفية إدماج قضايا الأمن الوطني، بما فيها الأمن السيبراني، ضمن الأجندة الحكومية (العيساوي، 2019، 41).

المحور الأول: تعريف السياسة العامة ومراحل صنعها

أولاً: تعريف السياسة العامة

تُعرَّف السياسة العامة بأنها مجموعة القرارات والإجراءات والتوجهات التي تعتمدها السلطات الرسمية في الدولة لمعالجة قضية عامة أو إشباع حاجة مجتمعية معينة. وهي تعبّر عن اختيار من بين بدائل متعددة في ضوء اعتبارات سياسية واقتصادية واجتماعية وأمنية، وتصدر عادة عن المؤسسات الدستورية المختصة مثل السلطة التنفيذية أو التشريعية.

ويذهب عدد من الباحثين إلى أن السياسة العامة لا تقتصر على القرارات المعلنة فحسب، بل تشمل أيضاً ما تمتنع الدولة عن فعله، إذ إن الامتناع ذاته يُعدّ موقفاً سياسياً يعكس توجهاً معيناً. ومن هذا المنظور، تُفهم السياسة العامة بوصفها عملية ديناميكية مستمرة تتداخل فيها المصالح والقيم والضغوط المؤسسية ضمن بيئة داخلية وخارجية متغيرة (الطائي، 2020، 34).

ثانياً: مراحل صنع السياسة العامة

تمر عملية صنع السياسة العامة بعدة مراحل مترابطة تشكل ما يُعرف بدورة السياسة العامة، ويمكن إجمالها فيما يأتي:

1. مرحلة تحديد المشكلة ووضعها على جدول الأعمال:

تبدأ العملية بتشخيص قضية عامة تستدعي التدخل الحكومي، ثم إدراجها ضمن أولويات صانع القرار، متأثرةً بعوامل مثل الرأي العام، وضغط النخب، والتهديدات الأمنية.

2. مرحلة صياغة البدائل:

يجري في هذه المرحلة اقتراح مجموعة من الحلول والخيارات لمعالجة المشكلة، مع دراسة تكاليف كل بديل ومنافعه وانعكاساته المحتملة.

3. مرحلة اتخاذ القرار:

يتم اختيار البديل الأنسب وفقاً لمعايير سياسية وقانونية واقتصادية وأمنية، ويُصدر القرار بصيغة رسمية من الجهة المختصة.

4. مرحلة التنفيذ:

تُحوَّل القرارات إلى برامج وإجراءات عملية عبر الأجهزة الإدارية المختصة، ويُعدّ حسن التنفيذ عاملاً حاسماً في نجاح السياسة.

5. مرحلة التقييم والمراجعة:

يتم قياس نتائج السياسة العامة ومدى تحقيقها للأهداف المرسومة، وقد يؤدي ذلك إلى تعديلها أو إعادة صياغتها بما يتلاءم مع المتغيرات المستجدة.

وتتسم هذه المراحل بالتداخل والتفاعل المستمر، إذ قد تعود السياسة إلى مرحلة سابقة نتيجة تغير الظروف أو ظهور تهديدات جديدة، وهو ما يبرز أهمية المرونة في إدارة الشأن العام، خاصة عندما يتعلق الأمر بقضايا ذات صلة مباشرة بالأمن الوطني (العيساوي، 2019، 68).

المحور الثاني: الفاعلون في عملية صنع السياسة العامة

تتسم عملية صنع السياسة العامة بطابعها التفاعلي، إذ لا تقتصر على جهة واحدة، بل تشارك فيها مجموعة من الفاعلين الرسميين وغير الرسميين الذين يتباين تأثيرهم تبعاً لطبيعة النظام السياسي وبنية الدولة. ويؤدي فهم هؤلاء الفاعلين إلى إدراك ديناميات اتخاذ القرار وكيفية توجيه السياسات، خاصة في القضايا ذات الصلة بالأمن الوطني والأمن السيبراني.

أولاً: الفاعلون الرسميون

يشمل الفاعلون الرسميون المؤسسات الدستورية التي تمتلك سلطة قانونية في صياغة واعتماد السياسات العامة، وفي مقدمتها السلطة التنفيذية التي تضطلع بالدور المركزي في اقتراح السياسات وتنفيذها، والسلطة التشريعية التي تمارس دور الإقرار والرقابة، فضلاً عن السلطة القضائية التي تضمن مشروعية القرارات وتفسيرها. كما تلعب الأجهزة البيروقراطية دوراً فنياً وإدارياً مهماً في إعداد الدراسات وصياغة البدائل وتنفيذ البرامج.

وتتفاوت درجة تأثير هذه المؤسسات بحسب طبيعة النظام السياسي، غير أن السلطة التنفيذية غالباً ما تكون الفاعل الأبرز في القضايا المرتبطة بالأمن الوطني، نظراً لارتباطها المباشر بإدارة الملفات الأمنية والدفاعية (الطائي، 2020، 92).

ثانياً: الفاعلون غير الرسميين

إلى جانب المؤسسات الرسمية، تؤثر أطراف غير حكومية في عملية صنع السياسة العامة، مثل الأحزاب السياسية، وجماعات الضغط، ومنظمات المجتمع المدني، ووسائل الإعلام، ومراكز البحوث والدراسات. وتعمل هذه الجهات على توجيه الرأي العام، وتقديم المقترحات، وممارسة الضغط على صانع القرار لتبني سياسات معينة (الطائي، 2014، 115).

كما برز في العصر الرقمي فاعلون جدد يتمثلون في الشركات التكنولوجية الكبرى، وشبكات التواصل الاجتماعي، وخبراء الأمن السيبراني، الذين أصبح لهم تأثير مباشر في تشكيل الأجندة الحكومية، لا سيما في القضايا المرتبطة بالتحول الرقمي وحماية الفضاء الإلكتروني (العيساوي، 2019، 124).

ثالثاً: التفاعل بين الفاعلين

لا تعمل هذه الأطراف بمعزل عن بعضها، بل تتداخل أدوارها ضمن شبكة معقدة من المصالح والتوازنات. وقد يؤدي اختلاف الرؤى بين الفاعلين إلى صراعات أو مساومات تؤثر في مضمون السياسة العامة. وفي القضايا الأمنية، يميل ميزان التأثير غالباً لصالح المؤسسات التنفيذية والأمنية، بحكم امتلاكها المعلومات والقدرة على إدارة المخاطر، مما ينعكس على طبيعة القرارات المتخذة (الطائي، 2020، 138).

المحور الثالث: الأمن الوطني كمحدد رئيس في توجيه السياسات العامة

يُعدّ الأمن الوطني أحد أهم المحددات التي تؤثر في صياغة السياسات العامة وتوجيهها، إذ يمثل الإطار الذي تُقاس في ضوئه أولويات الدولة وقراراتها الاستراتيجية. وقد تطور مفهوم الأمن الوطني ليشمل أبعاداً متعددة، فلم يعد مقتصراً على حماية الحدود والدفاع العسكري، بل امتد ليشمل الأمن السياسي والاقتصادي والاجتماعي والثقافي والتقني.

أولاً: تطور مفهوم الأمن الوطني

كان المفهوم التقليدي للأمن الوطني يركّز على مواجهة التهديدات العسكرية الخارجية، إلا أن التحولات الدولية المعاصرة أدت إلى توسيع نطاقه ليشمل تهديدات غير تقليدية مثل الإرهاب، والأزمات الاقتصادية، والجريمة المنظمة، والهجمات السيبرانية. ونتيجة لذلك، أصبح الأمن الوطني مفهوماً شاملاً يتداخل مع مختلف القطاعات العامة (عبد الحميد، 2022، 45).

ثانياً: تأثير الأمن الوطني في ترتيب الأولويات السياسية

عندما تُدرج قضية ما ضمن إطار الأمن الوطني، فإنها تحظى بأولوية متقدمة على جدول أعمال الحكومة، وتُخصص لها موارد أكبر، وتُتخذ بشأنها قرارات أكثر حسماً. ومن هنا يظهر تأثير الأمن الوطني في توجيه السياسات الاقتصادية والتقنية والتعليمية والإعلامية، بما يخدم هدف حماية استقرار الدولة وسيادتها (العتيبي، 2016، 78).

وفي سياق الأمن السيبراني، يؤدي تصنيفه كقضية أمن وطني إلى تبني استراتيجيات وطنية شاملة، وتعزيز التشريعات، وبناء قدرات بشرية وتقنية قادرة على مواجهة التهديدات الرقمية المتصاعدة (الهاشمي، 2021، 112).

ثالثاً: الأمن الوطني بين متطلبات الحماية ومتطلبات التنمية

يُشكّل التوازن بين الأمن والتنمية تحدياً رئيساً في عملية صنع السياسة العامة، إذ قد يؤدي التركيز المفرط على الاعتبارات الأمنية إلى تقييد الحريات أو تقليص الموارد المخصصة للتنمية. لذلك تسعى الدول الحديثة إلى تبني مقاربة شاملة تحقق الأمن دون الإخلال بمتطلبات التنمية المستدامة.

وعليه، فإن إدماج مفهوم الأمن الوطني — بما فيه الأمن السيبراني — ضمن السياسات العامة ينبغي أن يتم وفق رؤية استراتيجية متوازنة تضمن حماية الدولة ومصالحها، وفي الوقت نفسه تعزز الاستقرار السياسي والاقتصادي والاجتماعي.

المطلب الثالث: المقاربات النظرية المفسِّرة للعلاقة بين الأمن السيبراني والسياسة العامة

يقتضي تحليل العلاقة بين الأمن السيبراني والسياسة العامة الاستناد إلى أطر نظرية تساعد في تفسير كيفية إدراج القضايا الرقمية ضمن أولويات الدولة، وكيفية تفاعل المؤسسات معها بوصفها تهديدات أو فرصاً. فالقضية لا تتعلق فقط بالبعد التقني، بل ترتبط بكيفية إدراك صانع القرار للتهديد، وآليات الاستجابة المؤسسية، وطبيعة الخطاب السياسي المصاحب له. ومن هنا تبرز أهمية توظيف عدد من المقاربات النظرية التي تفسر ديناميات التفاعل بين الأمن السيبراني وعملية صنع السياسة العامة.

المحور الأول: مدخل تحليل النظم

يُعدّ مدخل تحليل النظم من أبرز المداخل المستخدمة في دراسة السياسة العامة، إذ ينظر إلى النظام السياسي بوصفه منظومة تتكون من مدخلات وعمليات تحويل ومخرجات وتغذية راجعة. ووفق هذا المدخل، تمثل المطالب والضغوط المجتمعية والتهديدات الخارجية "مدخلات" تدخل إلى النظام السياسي، ليتم تحويلها عبر مؤسسات الدولة إلى قرارات وسياسات عامة، ثم تُقاس نتائجها من خلال التغذية الراجعة (Easton،1965).

وفي سياق الأمن السيبراني، تُعدّ الهجمات الإلكترونية، أو تزايد الجرائم المعلوماتية، أو الضغوط الدولية لتأمين الفضاء الرقمي، بمثابة مدخلات تدفع النظام السياسي إلى صياغة استراتيجيات وتشريعات خاصة بالأمن السيبراني. وتُظهر هذه المقاربة كيف يؤثر حجم التهديد السيبراني في شكل الاستجابة السياسية، وكيف يمكن للتغذية الراجعة (كتقييم الأداء أو حدوث اختراقات جديدة) أن تؤدي إلى تعديل السياسة العامة أو تطويرها (الهيئة الوطنية للأمن السيبراني، 2023، 19) .

ويتميز هذا المدخل بقدرته على تفسير التفاعل المستمر بين البيئة الداخلية والخارجية للنظام السياسي، مما يجعله مناسباً لتحليل قضايا عابرة للحدود مثل الأمن السيبراني (العيساوي، 2019، 55).

المحور الثاني: مدخل الحوكمة الرقمية

يستند مدخل الحوكمة الرقمية إلى فكرة أن إدارة الشأن العام في العصر الحديث لم تعد حكراً على الدولة، بل أصبحت عملية تشاركية تتداخل فيها مؤسسات القطاع الخاص، ومنظمات المجتمع المدني، والشركات التكنولوجية، فضلاً عن الفاعلين الدوليين. ويُبرز هذا المدخل أهمية التنسيق والتكامل بين مختلف الأطراف لضمان إدارة فعالة للفضاء الرقمي.

في إطار الأمن السيبراني، تؤكد الحوكمة الرقمية على ضرورة بناء شراكات بين الحكومة وشركات الاتصالات ومزودي الخدمات الرقمية ومراكز البحث العلمي، بما يضمن تبادل المعلومات والاستجابة السريعة للتهديدات. كما تسلط الضوء على أهمية التشريعات المرنة التي توازن بين حماية الأمن الوطني وضمان حقوق الأفراد في الخصوصية وحرية التعبير.

ويُظهر هذا المدخل أن نجاح السياسة العامة في مجال الأمن السيبراني يعتمد على مستوى التنسيق المؤسسي والقدرة على إدارة المخاطر الرقمية ضمن إطار تشاركي متعدد المستويات (عبد الحميد، 2022، 114).

المحور الثالث: نظرية الأمننة (Securitization Theory)

تُعدّ نظرية الأمننة من المقاربات الحديثة في الدراسات الأمنية، وترتبط بمدرسة كوبنهاغن، إذ تفترض أن القضايا لا تصبح تهديدات أمنية بطبيعتها، بل يتم "أمننتها" عبر خطاب سياسي يصوّرها بوصفها تهديداً وجودياً يستوجب اتخاذ إجراءات استثنائية. ووفق هذه النظرية، فإن عملية الأمننة تتطلب وجود فاعل مؤثر

يطرح القضية كتهديد، وجمهور يتقبل هذا الطرح، وإجراءات تتجاوز السياسة العادية.

وفي سياق الأمن السيبراني، يمكن ملاحظة كيف يتم تقديم الهجمات الإلكترونية أو الاختراقات بوصفها تهديداً للأمن الوطني، مما يبرر سنّ تشريعات خاصة، أو إنشاء مؤسسات جديدة، أو توسيع صلاحيات الأجهزة الأمنية. وتُفسر هذه النظرية سبب إدراج الأمن السيبراني أحياناً ضمن أعلى أولويات الدولة، حتى وإن كانت آثاره غير مرئية مادياً كالحروب التقليدية.

وتُظهر نظرية الأمننة أن إدماج الأمن السيبراني في السياسة العامة لا يعتمد فقط على حجم التهديد الفعلي، بل أيضاً على طبيعة الخطاب السياسي ومدى قبول المجتمع بإضفاء الطابع الأمني على الفضاء الرقمي (عبد الحميد، 2022، 91).

تُبرز هذه المقاربات الثلاث — تحليل النظم، والحوكمة الرقمية، ونظرية الأمننة — أبعاداً مختلفة للعلاقة بين الأمن السيبراني والسياسة العامة؛ فالأولى تفسر التفاعل المؤسسي، والثانية تؤكد البعد التشاركي والإداري، والثالثة تكشف دور الخطاب السياسي في تحويل القضية الرقمية إلى أولوية أمنية.

ومن خلال التكامل بين هذه الأطر النظرية، يمكن بناء فهم أعمق لكيفية توجيه السياسات العامة في مواجهة التحديات السيبرانية المعاصرة.

المبحث الثاني: واقع الأمن السيبراني في العراق والتحديات المؤسسية والتشريعية

يشهد العراق تحولاً رقمياً متدرجاً في مختلف مؤسسات الدولة، رافقه توسع في استخدام التقنيات الحديثة والاعتماد على الشبكات الإلكترونية في إدارة الخدمات والبيانات. غير أن هذا التحول لم يكن بمعزل عن تحديات أمنية متصاعدة، تمثلت في تنامي الجرائم الإلكترونية، وازدياد الهجمات السيبرانية، وظهور ثغرات تنظيمية وتشريعية تتطلب معالجة شاملة. وعليه، يهدف هذا المبحث إلى تحليل الإطار

المؤسسي والقانوني للأمن السيبراني في العراق، واستعراض أبرز التهديدات والتحديات التي تواجهه.

المطلب الأول: الإطار المؤسسي للأمن السيبراني في العراق

المحور الأول: دور الجهات الحكومية المختصة

تتولى عدة جهات رسمية مسؤوليات متداخلة في مجال الأمن السيبراني في العراق، من أبرزها:

1 – هيئة الإعلام والاتصالات:

تضطلع بدور تنظيمي ورقابي في قطاع الاتصالات والإنترنت، وتعمل على وضع الضوابط الفنية لحماية الشبكات، وتنظيم عمل مزودي الخدمة، ومراقبة الالتزام بالمعايير التقنية والأمنية.

2 – وزارة الداخلية العراقية:

تتولى عبر مديرياتها المختصة، ولا سيما أقسام مكافحة جرائم المعلوماتية، متابعة الجرائم الإلكترونية والتحقيق فيها، إضافة إلى تنفيذ الإجراءات القانونية بحق المتورطين في الاختراقات والابتزاز الرقمي.

3 – جهاز الأمن الوطني العراقي:

يضطلع بمهام استخبارية تتعلق برصد التهديدات السيبرانية ذات البعد الأمني أو الإرهابي، ومتابعة الأنشطة الرقمية التي قد تمس استقرار الدولة أو أمنها الوطني.

ويُلاحظ أن هذه الجهات تعمل ضمن إطار مؤسسي متعدد المستويات، إلا أن طبيعة التهديدات السيبرانية العابرة للقطاعات تفرض الحاجة إلى تنسيق أعلى وتكامل أوضح في الأدوار (الهاشمي، 2021، 135).

المحور الثاني: التنسيق بين المؤسسات الأمنية والتقنية

يمثل التنسيق المؤسسي أحد التحديات الجوهرية في إدارة ملف الأمن السيبراني في العراق، نظراً لتعدد الجهات المعنية وتداخل صلاحياتها. فالتعامل مع الهجمات

الرقمية يتطلب استجابة سريعة وتبادلاً فورياً للمعلومات بين الأجهزة الأمنية والهيئات التقنية ومزودي الخدمة.

غير أن غياب مركز وطني موحد لإدارة الحوادث السيبرانية أو استراتيجية وطنية شاملة لفترة طويلة أدى إلى تشتت الجهود، وضعف التكامل في إدارة المخاطر الرقمية. ومن ثمّ، فإن تعزيز آليات التنسيق وتحديد الأدوار بوضوح يُعدّ شرطاً أساسياً لبناء منظومة سيبرانية فعالة (عبد الحميد، 2022، 121).

المحور الثالث: البنية التحتية الرقمية في العراق

شهد العراق توسعاً ملحوظاً في شبكات الاتصالات وخدمات الإنترنت خلال السنوات الأخيرة، إلا أن البنية التحتية الرقمية ما زالت تواجه تحديات تتعلق بضعف الحماية التقنية، وتقادم بعض الأنظمة، والاعتماد على تجهيزات مستوردة دون وجود منظومة وطنية متكاملة للأمن السيبراني.

كما أن التحول نحو الحكومة الإلكترونية والخدمات المصرفية الرقمية زاد من حجم البيانات المتداولة إلكترونياً، مما يضاعف الحاجة إلى أنظمة حماية متطورة. وعليه، فإن تطوير البنية التحتية الرقمية يمثل ركيزة أساسية لتعزيز الأمن السيبراني الوطني (الطائي، 2020، 158).

المطلب الثاني: الإطار القانوني والتنظيمي

المحور الأول: القوانين والتشريعات ذات الصلة بالأمن السيبراني

يعتمد العراق في معالجة الجرائم الإلكترونية على مزيج من النصوص القانونية المتفرقة، مثل قانون العقوبات وقانون الاتصالات، التي تتضمن مواد يمكن تطبيقها على بعض الأفعال المرتبطة بالجرائم المعلوماتية. إلا أن هذه النصوص لم تُصغَ أصلاً لمواجهة التهديدات السيبرانية الحديثة، مما يحدّ من فعاليتها في بعض الحالات.

ويعكس هذا الواقع الحاجة إلى إطار قانوني متخصص يواكب التطورات التقنية ويحدد الجرائم والعقوبات بشكل دقيق، مع ضمان حماية الحقوق والحريات الأساسية (الهاشمي، 2021، 142).

المحور الثاني: مشروع قانون الجرائم المعلوماتية

شهد العراق نقاشاً واسعاً حول مشروع قانون الجرائم المعلوماتية، الذي يهدف إلى تنظيم الفضاء الرقمي وتجريم الأفعال الضارة بالنظام العام أو الأمن الوطني عبر الوسائل الإلكترونية. وقد أثار المشروع جدلاً مجتمعياً يتعلق بمدى توازنه بين متطلبات الأمن وحماية حرية التعبير.

ويعكس هذا الجدل حساسية العلاقة بين الأمن السيبراني والحقوق المدنية، مما يفرض صياغة تشريعات دقيقة تحقق الردع القانوني دون المساس بالمبادئ الدستورية (عبد الحميد، 2022، 98).

المحور الثالث: التحديات التشريعية والفراغ القانوني

تتمثل أبرز التحديات في بطء تحديث التشريعات مقارنة بسرعة تطور التكنولوجيا، إضافة إلى غياب تعريفات قانونية دقيقة لبعض الجرائم السيبرانية، وصعوبة إثباتها أمام القضاء. كما يبرز تحدي التعاون الدولي في ظل الطبيعة العابرة للحدود للجرائم الإلكترونية.

ومن ثمّ، فإن سدّ الفراغ القانوني يتطلب تحديثاً تشريعياً مستمراً، وبناء قدرات قضائية متخصصة في التعامل مع الأدلة الرقمية (الطائي، 2020، 165).

المطلب الثالث: التحديات والتهديدات السيبرانية

المحور الأول: الجرائم الإلكترونية والاختراقات

تشمل الجرائم الإلكترونية في العراق حالات الابتزاز عبر وسائل التواصل الاجتماعي، والاحتيال المالي، واختراق الحسابات الشخصية والمؤسساتية. وقد أدى

الانتشار الواسع للإنترنت إلى زيادة هذه الظواهر، في ظل محدودية الوعي الأمني لدى بعض المستخدمين (الهاشمي، 2021، 151).

المحور الثاني: الهجمات على البنى التحتية الحيوية

تُعدّ البنى التحتية الحيوية مثل قطاعات الطاقة والمصارف والاتصالات أهدافاً محتملة للهجمات السيبرانية، لما تمثله من أهمية استراتيجية. وأي اختراق لهذه القطاعات قد يؤدي إلى تعطيل الخدمات العامة وإرباك الاستقرار الاقتصادي (عبد الحميد، 2023، 105).

المحور الثالث: التهديدات المرتبطة بالأمن الاقتصادي والسياسي

قد تُستخدم الهجمات السيبرانية كأداة للتأثير في الأسواق المالية أو إثارة الفوضى السياسية عبر نشر الأخبار المضللة أو استهداف المؤسسات الحكومية. وهو ما يجعل الأمن السيبراني مرتبطاً مباشرة بحماية الاستقرار السياسي والاقتصادي للدولة (الطائي، 2020، 172).

المحور الرابع: ضعف الوعي المجتمعي والثقافة الرقمية

يُعدّ ضعف الثقافة الرقمية لدى شريحة من المستخدمين عاملاً مفاقماً للمخاطر السيبرانية، إذ يؤدي إلى سهولة الوقوع ضحية لعمليات الاحتيال أو الاختراق. ومن ثمّ، فإن تعزيز التوعية المجتمعية، وإدراج مفاهيم الأمن الرقمي في المناهج التعليمية، يُمثلان خطوة أساسية في بناء منظومة وطنية متكاملة للأمن السيبراني.

المبحث الثالث :تأثير الأمن السيبراني على صنع السياسة العامة وتعزيز الأمن الوطني في العراق

يمثل الأمن السيبراني اليوم أحد المحاور الاستراتيجية المؤثرة في توجيه السياسات العامة للدول، لاسيما في ظل التحول الرقمي المتسارع وتنامي التهديدات الإلكترونية العابرة للحدود .وفي الحالة العراقية، باتت القضايا السيبرانية تفرض نفسها على جدول الأعمال الحكومي، نظراً لارتباطها المباشر بحماية مؤسسات

الدولة واستقرارها السياسي والاقتصادي .وعليه، يتناول هذا المبحث أثر الأمن السيبراني في إعادة تشكيل أولويات السياسة العامة، ودوره في تعزيز الأمن الوطني، إضافة إلى استشراف آفاق تطوير هذا المجال مستقبلاً.

المطلب الأول :الأمن السيبراني كأولوية في الأجندة الحكومية

المحور الأول :إدراج الأمن السيبراني ضمن أولويات التخطيط الوطني

أدى التحول نحو الحكومة الإلكترونية وتوسيع استخدام الأنظمة الرقمية في العراق إلى إدراك متزايد لأهمية إدماج الأمن السيبراني ضمن خطط التنمية الوطنية .فمع توسع الخدمات الإلكترونية في القطاعات الحكومية والمصرفية والتعليمية، أصبحت حماية البيانات والبنى التحتية الرقمية ضرورة استراتيجية لا تقتصر على الجانب التقني فحسب، بل تمتد إلى صلب عملية التخطيط الوطني.

وقد انعكس ذلك في توجه الدولة نحو تعزيز الأطر التنظيمية، ودعم قدرات المؤسسات المعنية بالأمن الرقمي، وإدراج موضوع الأمن السيبراني ضمن الخطط الحكومية الرامية إلى تحديث الإدارة العامة .ويؤكد هذا التوجه أن الأمن السيبراني لم يعد قضية هامشية، بل أصبح جزءاً من منظومة التخطيط الاستراتيجي للدولة (الهاشمي،2020، 88).

المحور الثاني :تأثير التهديدات السيبرانية على إعادة ترتيب الأولويات السياسية

أسهمت الهجمات الإلكترونية وحوادث الاختراق في إعادة صياغة ترتيب الأولويات الحكومية، إذ دفعت صانع القرار إلى تخصيص موارد مالية وبشرية أكبر لحماية الفضاء الرقمي .فكلما تصاعدت التهديدات، تعززت القناعة بضرورة التعامل مع الأمن السيبراني بوصفه أولوية وطنية.

كما أن الطبيعة غير المرئية للهجمات السيبرانية لا تقلل من خطورتها، بل تجعلها أكثر تعقيداً، ما يدفع الحكومة إلى اعتماد سياسات وقائية واستباقية بدلاً من الاقتصار على المعالجة اللاحقة .ويُظهر ذلك كيف يمكن للتهديدات الرقمية أن

تؤثر مباشرة في توجهات السياسة العامة وتعيد تشكيلها (عبد الحميد، 2022، 84).

المطلب الثاني :دور الأمن السيبراني في تعزيز الأمن الوطني

المحور الأول :حماية البنى التحتية الحيوية (الطاقة، المصارف، الاتصالات)

تمثل قطاعات الطاقة والمصارف والاتصالات ركائز أساسية في بنية الدولة الحديثة، وأي اختراق لهذه القطاعات قد يؤدي إلى اضطراب واسع النطاق في الاقتصاد والخدمات العامة .ومن ثمّ، فإن تعزيز أنظمة الحماية السيبرانية لهذه المرافق يُعدّ جزءاً لا يتجزأ من استراتيجية الأمن الوطني.

وفي العراق، حيث يعتمد الاقتصاد بدرجة كبيرة على قطاع الطاقة، فإن تأمين الأنظمة الرقمية المرتبطة بالإنتاج والتوزيع يمثل أولوية استراتيجية، نظراً لما قد يترتب على تعطيلها من آثار اقتصادية واجتماعية خطيرة (الطائي، 2020، 178).

المحور الثاني :حماية العملية الانتخابية والبيانات الحكومية

تعدّ حماية البيانات الحكومية والأنظمة الانتخابية من أبرز أبعاد الأمن السيبراني المرتبطة مباشرة بشرعية النظام السياسي .فالتلاعب بالمعلومات أو استهداف قواعد البيانات قد يؤدي إلى تقويض الثقة بالمؤسسات العامة.

وعليه، فإن تعزيز الضوابط التقنية والتشريعية لحماية العملية الانتخابية يُعدّ ركيزة أساسية في صون الاستقرار السياسي، وضمان نزاهة العمليات الديمقراطية في الدولة (عبد الحميد،2022، 110)،

المحور الثالث :تعزيز السيادة الرقمية

يشير مفهوم السيادة الرقمية إلى قدرة الدولة على التحكم في بياناتها وبنيتها التحتية الرقمية، وحمايتها من التدخلات الخارجية .وفي ظل الاعتماد المتزايد على التكنولوجيا العالمية، أصبح تعزيز السيادة الرقمية جزءاً من الأمن الوطني.

ويقتضي ذلك تطوير تشريعات وطنية، وبناء مراكز بيانات محلية، وتعزيز القدرات التقنية بما يقلل من الاعتماد المفرط على الخارج، ويضمن حماية المصالح الوطنية في الفضاء السيبراني (الهاشمي، 2021، 160).

المطلب الثالث: آفاق تطوير السياسة العامة للأمن السيبراني في العراق

المحور الأول: بناء استراتيجية وطنية متكاملة للأمن السيبراني

يتطلب تطوير السياسة العامة في هذا المجال صياغة استراتيجية وطنية واضحة تحدد الأهداف، وتوزع الأدوار، وتضع آليات للتنسيق بين الجهات المعنية. كما ينبغي أن تتضمن هذه الاستراتيجية خططاً لإدارة المخاطر والاستجابة للحوادث السيبرانية.

المحور الثاني: تعزيز الشراكة بين القطاعين العام والخاص

نظراً لأن جزءاً كبيراً من البنية التحتية الرقمية مملوك للقطاع الخاص، فإن بناء شراكة فعالة بين الحكومة والشركات التكنولوجية يُعدّ أمراً حيوياً. ويسهم هذا التعاون في تبادل المعلومات وتعزيز القدرة على مواجهة التهديدات بصورة جماعية (عبد الحميد، 2022، 117).

المحور الثالث: تطوير القدرات البشرية والتقنية

يمثل العنصر البشري حجر الزاوية في منظومة الأمن السيبراني، إذ لا تكفي التقنيات المتطورة من دون كوادر مدرَّبة قادرة على إدارتها. ومن ثمّ، فإن إدراج تخصصات الأمن السيبراني في المناهج الأكاديمية، وتنظيم برامج تدريبية مستمرة، يُعدّ خطوة أساسية لتعزيز الجاهزية الوطنية (الطائي، 2020، 138).

المحور الرابع: الاستفادة من التجارب الدولية المقارنة

يمكن للعراق الاستفادة من التجارب الدولية في بناء استراتيجيات متكاملة للأمن السيبراني، خاصة في مجالات إنشاء مراكز وطنية للاستجابة للحوادث، وتحديث

التشريعات، وتعزيز التعاون الإقليمي والدولي. فالمقارنة توفر نماذج عملية تساعد في تطوير السياسات بما يتلاءم مع الخصوصية الوطنية.

يتضح أن الأمن السيبراني أصبح عاملاً مؤثراً في صياغة السياسة العامة في العراق، لما له من ارتباط وثيق بالأمن الوطني والسيادة الرقمية. ومن خلال إدراجه ضمن الأولويات الحكومية، وتعزيز الأطر المؤسسية والتشريعية، وبناء القدرات الوطنية، يمكن للعراق أن يطور سياسة عامة أكثر فاعلية في مواجهة التحديات السيبرانية المعاصرة.

الخاتمة والاستنتاجات

الخاتمة

أصبح الأمن السيبراني في العراق قضية استراتيجية ذات أبعاد متعددة، تتجاوز كونها مجرد حماية تقنية للأنظمة والمعلومات، لتشمل أبعاداً سياسية واقتصادية واجتماعية ترتبط مباشرة بالأمن الوطني واستقرار الدولة. وأظهر البحث أن إدماج الأمن السيبراني في صنع السياسة العامة لم يعد خياراً، بل ضرورة تفرضها طبيعة التهديدات الرقمية المتزايدة واعتماد الدولة على التكنولوجيا في إدارة شؤونها. كما بينت الدراسة أن التحديات المؤسسية والتشريعية، وغياب التنسيق الفعّال، وضعف الوعي الرقمي بين المواطنين، تمثل أبرز المعوقات أمام تعزيز قدرات الدولة في مواجهة المخاطر السيبرانية.

إلا أن الفرص متاحة لتعزيز الأمن السيبراني من خلال وضع استراتيجية وطنية متكاملة، وتطوير القدرات البشرية والتقنية، وتعزيز التعاون بين القطاعين العام والخاص، والاستفادة من التجارب الدولية المقارنة. وعليه، يمكن للأمن السيبراني أن يتحول من تحدٍ إلى أداة فعالة لتعزيز الاستقرار الوطني وحماية مصالح الدولة العليا، إذا ما تم تبنيه ضمن سياسات عامة متكاملة وممنهجة.

الاستنتاجات

1 – الأمن السيبراني عامل أساسي في صياغة السياسة العامة:

أصبح الأمن السيبراني مؤشراً رئيسياً لإعادة ترتيب أولويات الحكومة، حيث تؤثر التهديدات الرقمية في القرارات الاستراتيجية وتخصيص الموارد.

2 – الأمن الوطني مرتبط مباشرة بالأمن السيبراني:

حماية البنى التحتية الحيوية، وتأمين العملية الانتخابية، وصون البيانات الحكومية، وتعزيز السيادة الرقمية، كلها أبعاد تجعل الأمن السيبراني جزءاً لا يتجزأ من الأمن الوطني.

3 – التحديات المؤسسية والتنسيقية:

هناك تشتت في الأدوار بين الجهات الحكومية المختصة، ونقص في آليات التنسيق المؤسسي، مما يحد من فعالية الاستجابة للهجمات السيبرانية.

4 – الإطار القانوني بحاجة إلى تحديث:

الفراغ القانوني وضعف التشريعات المتخصصة في مواجهة الجرائم السيبرانية يمثلان عائقاً أمام تطبيق سياسات أمنية فعالة، مما يستدعي سنّ قوانين واضحة ومتوازنة.

5 – الوعي الرقمي والثقافة المجتمعية:

ضعف الثقافة الرقمية لدى المواطنين يسهل استهدافهم بالجرائم الإلكترونية، ومن ثمّ فإن نشر التوعية وبرامج التدريب يمثلان أولوية في تعزيز الأمن السيبراني.

6 – فرص التطوير:

بناء استراتيجية وطنية متكاملة، وتعزيز الشراكات بين القطاعين العام والخاص، وتطوير القدرات البشرية والتقنية، والاستفادة من التجارب الدولية، تمثل خطوات أساسية لرفع مستوى الأمن السيبراني في العراق.

المصادر

1 - الهيئة الوطنية للأمن السيبراني. (2018). تنظيم الهيئة الوطنية للأمن السيبراني. الرياض: الهيئة الوطنية للأمن السيبراني.
2 - الهاشمي، س. ع. (2021). الأمن السيبراني: المفهوم والتحديات المعاصرة. عمّان: دار أمجد للنشر والتوزيع.
3 - العصيمي، أ. (2024). ما هو مثلث الحماية CIA وماذا يقدم؟ المرسال. تم استرجاعه من https://www.almrsal.com/post/1399855
4 - الشريف، م. أ. (2020). أمن المعلومات وحماية البيانات في العصر الرقمي. القاهرة: دار الفكر العربي.
5 - عتوم، ب. (2023). ما الفرق بين أمن المعلومات والأمن السيبراني؟ إي عربي. تم الاسترجاع من https://e3arabi.com/التقنية/ماالفرقبينأمنالمعلوماتوالأمنالسيبرا
6 - عبد الحميد، ع. ر. (2022). الفضاء السيبراني وتحولات الأمن الدولي المعاصر. بيروت: المركز العربي للأبحاث ودراسة السياسات.
7 - العيساوي، م. م. (2019). مدخل إلى السياسة العامة وتحليلها. بغداد: دار الحكمة للطباعة والنشر.
8 - الطائي، ح. ك. (2020). تحليل السياسة العامة: مفاهيم ونماذج تطبيقية. عمّان: دار اليازوري العلمية للنشر والتوزيع.
9 - حسنين، س. (2012). صنع السياسة العامة. القاهرة: دار النهضة العربية.
10 - العتيبي، س. (2016). الأمن الوطني: المفهوم والأبعاد والاستراتيجيات. عمّان: دار الحامد للنشر والتوزيع.
11 - David Easton. (1965). A systems analysis of political life. New York: Wiley
12 -الهيئة الوطنية للأمن السيبراني. (2023). الاستراتيجية الوطنية للأمن السيبراني. الرياض: الهيئة الوطنية للأمن السيبراني.

References

1_ Abd al-Hamid, A. R. (2022). Cyberspace and transformations of contemporary international security [Al-Fadha' al-siberani wa tahawwulat al-amn al-dawli al-mu'asir]. Arab Center for Research and Policy Studies.

2_ Al-Issawi, M. M. (2019). Introduction to public policy and its analysis [Madkhal ila al-siyasah al-ammah wa tahli

Iha]. Dar Al-Hikmah for Printing and Publishing.

3_ Al-Hashimi, S. A. (2021). Cybersecurity: Concept and contemporary challenges [Al-amn al-siberani: Al-mafhum wa al-tahaddiyat al-mu'asira]. Dar Amjad for Publishing and Distribution.

4_ Al-Otaibi, S. (2016). National security: Concept, dimensions, and strategies [Al-amn al-watani: Al-mafhum wa al-ab'ad wa al-istratijiyyat]. Dar Al-Hamed for Publishing and Distribution.

5_ Al-Osaimi, A. (2024, May 15). What is the CIA triad and what does it provide? [Ma huwa muthallath al-himayah CIA wa madha yuqaddim?]. Almrsal. https://www.almrsal.com/post/1399855

6_ Al-Sharif, M. A. (2020). Information security and data protection in the digital age [Amn al-ma'lumat wa himayat al-bayanat fi al-asr al-raqami]. Dar Al-Fikr Al-Arabi.

7_ Al-Tai, H. K. (2020). Public policy analysis: Concepts and applied models [Tahlil al-siyasah al-ammah: Mafahim wa namadhij tatbiqiyyah]. Dar Al-Yazouri Scientific for Publishing and Distribution.

8_ Atoum, B. (2023, September 10). What is the difference between information security and cybersecurity? [Ma al-farq bayna amn al-ma'lumat wa al-amn al-siberani?]. e3arabi. https://e3arabi.com

9_**Easton, D.** (1965). *A systems analysis of political life*. Wiley.

10_ Hassanein, S. (2012). Public policymaking [Sun' al-siyasah al-ammah]. Dar Al-Nahda Al-Arabiyyah.

11_ National Cybersecurity Authority. (2018). Regulation of the National Cybersecurity Authority [Tandheem al-hay'ah al-wataniyyah lil-amn al-siberani]. National Cybersecurity Authority.

12_ National Cybersecurity Authority. (2023). National Cybersecurity Strategy [Al-istratijiyyah al-wataniyyah lil-amn al-siberani]. National Cybersecurity Authority.