الأمن السيبراني والمواطنة الرقمية

Cybersecurity and Digital Citizenship

د. عبير بنت محمد بن ربيع عاتي -الأستاذ المشارك بجامعة الامام محمد بن سعود الإسلامية

Email: abeer221910@gmail.com

ملخص الدراسة:

تُقدم هذه الدراسة استكشافًا نظريًا شاملاً للعلاقة المتكاملة بين الأمن السيبراني والمواطنة الرقمية، وذلك بالاعتماد على الأدبيات والدراسات السابقة حيث تتعقب الدراسة التطور التاريخي لكلا المفهومين وتؤكد على الاعتماد المتبادل المتزايد بينهما في عصر الاتصال الرقمي في كل مكان. وتتناقش الدراسة كيف خلق الأمن السيبراني بيئة آمنة تسهل المواطنة الرقمية النشطة والمسؤولة إلى جانب مناقشة كيف يمكن للمواطنة الرقمية أن تعزز الأمن السيبراني من خلال ممارسات متعلمة ويقظة. كما تركز الدراسة على سياق المملكة العربية السعودية والتي تعمل بنشاط على تطوير أجندتها للتحول الرقمي. علاوة على ذلك، تسلط الدراسة الضوء على الاتجاهات المستقبلية للعلاقة ما بين الأمن السيبراني والمواطنة الرقمية وتقدم توصيات بشأن السياسات لمختلف أصحاب المصلحة. في المحصلة، تؤكد هذه الدراسة على العلاقة التكافلية المتنامية بين الأمن السيبراني والمواطنة الرقمية وتدعو إلى الالتزام الجماعي بالأمن والشمولية والمسؤولية في عالمنا الرقمي.

الكلمات المفتاحية: الأمن السيبراني، المواطنة الرقمية، التطور التاريخي، المملكة العربية السعودية.

Abstract:

This research provides a comprehensive theoretical exploration of the integral relationship between cybersecurity and digital citizenship. Drawing from a wealth of literature, the study traces the historical evolution of both concepts and underscores their increasing interdependence in an era of ubiquitous digital connectivity. It examines how cybersecurity creates a secure environment that facilitates active and responsible digital citizenship, while also discussing how digital citizenship can enhance cybersecurity through educated and vigilant practices. The research further elucidates the specific context of Saudi Arabia, a nation actively advancing its digital transformation agenda. Moreover, the study highlights future trends shaping cybersecurity and digital citizenship and offers policy recommendations for various stakeholders. Through its examination, this research underscores the growing symbiotic relationship between cybersecurity and digital citizenship and advocates for a collective commitment to security, inclusivity, and responsibility in our digital world

Keywords: Cybersecurity, Digital Citizenship, Historical Evolution, Saudi Arabia, Future Trends, Policy Recommendations

المقدمة:

شهد بداية القرن الحادي والعشرين تسارعًا غير مسبوق في الثورة الرقمية، مما أدى إلى نشوء عالم مترابط بشكل معقد حيث تتداخل العوالم المادية والافتراضية بشكل متزايد (Buchanan, 2016) وأدى هذا التقدم السريع إلى ولادة مفهومين أساسيين ومترابطين، وهما الأمن السيبراني والمواطنة الرقمية. يلخص الأمن السيبراني، كما حدده (Singer and Friedman 2014)، الممارسات والتدابير المنفذة لحماية الشبكات

الرقمية من الوصول غير المصرح به أو الهجمات الإلكترونية. وبالتالي، فقد برزت كقضية ذات أهمية كبيرة للأفراد والمنظمات والدول على حد سواء.

ويكتسب مفهوم المواطنة الرقمية، الذي يحدد معايير السلوك المناسب والمسؤول فيما يتعلق باستخدام التكنولوجيا (Ribble, 2015)، زخمًا باعتباره كفاءة حيوية في العصر الرقمي المعاصر. تسعى الدراسة الحالية إلى الشروع في فحص شامل لهذه المفاهيم المعقدة والمترابطة. الهدف الأساسي من هذا المسعى العلمي هو تجميع فهم شامل للأمن السيبراني والمواطنة الرقمية بناءً على مجموعة الأدبيات الحالية ووجهات النظر النظرية. علاوة على ذلك، تهدف هذه الدراسة إلى استكشاف العلاقة المعقدة بين هاتين الظاهرتين وكيف تشكل إحداهما الأخرى وتأثيرها.

كما تهدف هذه الدراسة إلى توضيح كيف يعزز الأمن السيبراني المواطنة الرقمية الفعالة والعكس صحيح، وبالتالي توفير فهم شامل للتبادلية بينهما. كما تحاول استقراء الاتجاهات المستقبلية من هذه الملاحظات ووضع توصيات فيما يتعلق بالسياسات واتجاهات البحث المستقبلي في هذا المجال. وتعتبر أهمية هذه الدراسة متعددة وذات قيمة هائلة لمجموعة متنوعة من الأسباب أهمها توفير توليفة شاملة للمعرفة حول الأمن السيبراني والمواطنة الرقمية وهما القوتان الأساسيتان اللتان تشكلان المشهد الرقمي المعاصر. كما ستكون هذه الدراسة بمثابة ضوء إرشادي للسياسات والممارسات التي تهدف إلى زيادة السلامة الرقمية وتعزيز السلوك المسؤول على الإنترنت (Dede, 2014).

وفي السياق ذاته، من خلال صياغة فهم نظري للتفاعل بين الأمن السيبراني والمواطنة الرقمية، من المتوقع أن تثري الدراسة الخطاب الأكاديمي في هذه المجالات، وملء الفراغ في منظور شامل غالبًا ما يكون مفقودًا في البحث الحالي. أخيرًا، تحمل الرؤى المتولدة من هذه الدراسة القدرة على تشكيل المناهج التعليمية وبرامج التدريب التنظيمي والسياسات الوطنية. يمكن أن يساهم ذلك في زيادة الوعي وتعزيز ثقافة رقمية أكثر أمانًا ومسؤولية. في المحصلة، الهدف الرئيسي لهذه الدراسة هو صياغة فهم نظري قوي للعلاقة بين الأمن السيبراني والمواطنة الرقمية، وبالتالي توفير رؤى مهمة يمكن أن تشكل السياسات المستقبلية، وتوجهات البحث، وتوجه الممارسات في المشهد الرقمي.

خلفية الدراسة:

أحدث العصر الرقمي تحولًا زلزاليًا في طريقة عمل المجتمعات وتواصلها ونموها، لا سيما مع الوجود المتزايد لتكنولوجيا المعلومات والاتصالات في كل مكان مما أدى إلى تزايد المخاطر المتصلة بالأمن السيبراني.

يتمثل الأمن السيبراني في جوهره في حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية (Scarfone et al., 2008).

وقد ولد هذا المفهوم نتيجة ظهور وانتشار التقنيات الرقمية إلى تشكل تهديدات ونقاط ضعف في بعض الأنظمة المحوسبة. تصاعد التحدي المتمثل في الحفاظ على بيئة إلكترونية آمنة على مر السنين، مما استلزم فهمًا شاملاً لتطور المفهوم وتفسيراته الحديثة والعديد من التهديدات الموجودة في المشهد الرقمي. علاوة على ذلك، أدى التطور المتزايد للتهديدات السيبرانية إلى تطوير استراتيجيات تكنولوجية وتنظيمية معقدة للوقاية والتخفيف (Singer & Friedman, 2014).

وبالتوازي مع تطور الأمن السيبراني، ظهر مفهوم المواطنة الرقمية كجانب رئيسي من جوانب العالم الرقمي والتي تشمل معايير السلوك المناسب والمسؤول فيما يتعلق باستخدام التكنولوجيا (Ribble, 2015) ويتجاوز هذا المفهوم مجرد الكفاءة التكنولوجية لتشمل فهم الحقوق والمسؤوليات الرقمية والسلوك الأخلاقي عبر الإنترنت والآثار الاجتماعية والثقافية المحتملة للتكنولوجيا الرقمية (Mossberger et al., 2007) وعليه، تتناول هذه الدراسة تطور هذا المفهوم وتفسيراته الحالية وأهميته في العالم المعاصر.

وأخيرا، تعمل المملكة العربية السعودية من خلال مبادرة رؤية 2030 الطموحة على تطوير أجندتها للتحول الرقمي بسرعة مما أدى إلى خطوات كبيرة في كل من الأمن السيبراني والمواطنة الرقمية (Alharbi, 2019) ومع ذلك، مع تطور هذه المفاهيم، من الضروري فهم كيفية تقاطعها وتفاعلها، وهذا ما تسعى إليه الدراسة الحالية.

منهجية الدراسة:

تعتمد الدراسة الحالية على مراجعة شاملة للأدبيات دون الحاجة إلى جمع البيانات الأولية، حيث يسمح هذا النهج بالفحص الشامل للأعمال العلمية الموجودة مسبقًا والتقارير المتعلقة بمجالات الأمن السيبراني والمواطنة الرقمية. ولضمان دقة هذه الدراسة، تم اتباع طريقة متعددة الخطوات تم إجراء بحث شامل عن الكلمات الرئيسية في العديد من قواعد البيانات ذات الترتيب العالي والتي تهتم بشكل قوي بمواضيع الأمن السيبراني والمواطنة الرقمية مثل Google Scholar و IEEE Xplore و JSTOR و SpringerLink و Taylor & Francis Online. تشمل الكلمات الرئيسية المستخدمة في البحث "الأمن السيبراني" و "المواطنة الرقمية" و "التطور التاريخي" و "المملكة العربية السعودية" و "الاتجاهات المستقبلية".

وبعد تحديد الدراسات ذات الصلة، تم مراجعتها وتقييمها بعناية من حيث صلتها بأهداف البحث، حيث تم تضمين المصادر التي تساهم بشكل مباشر في أهداف الدراسة فقط مع تفضيل الأعمال الحديثة وذات الاستشهادات العالية لضمان حسن توقيت البحث وأهميته.

الإطار النظري:

تطور وتعريف الأمن السيبراني:

يمكن إرجاع بداية مصطلح "الأمن السيبراني" إلى السنوات الأولى لتقنية الحوسبة والشبكات، حيث كان الأمن السيبراني في مرحلته الأولى مرتبطًا بشكل أساسي بحماية الأنظمة المادية والبنى التحتية. وخلال الستينيات والسبعينيات من القرن الماضي، عندما كانت أجهزة الكمبيوتر تُستخدم في الغالب للحسابات المعقدة ومعالجة البيانات في الإعدادات الأكاديمية والبحثية، كان التركيز الأساسي على الحفاظ على سلامة الأنظمة وضمان دقة البيانات (Landwehr, 2001) وقد أدى ظهور الإنترنت في أواخر الثمانينيات وتوسع الاتصال الرقمي في التسعينيات إلى تحول كبير في مشهد الأمن السيبراني خاصة مع بدء استخدام الإنترنت لأغراض تجارية وحكومية وشخصية مختلفة ليبدأ نطاق الأمن السيبراني في الاتساع مع التركيز ليس فقط على تكامل النظام ولكن أيضًا على خصوصية البيانات ومصادقة المستخدم (Denning & Denning, 2016).

وتطور الأمن السيبراني حديثاً إلى مفهوم شامل يشمل حماية أنظمة المعلومات والشبكات والبيانات من الهجمات الرقمية أو الوصول غير المصرح به بهدف ضمان السرية والنزاهة والتوافر والذي يشار إليه عادةً باسم ثالوث النزاهة والتوافر (Kuhn et al., 2010) وقد جعل التقدم التكنولوجي والاعتماد المتزايد على المنصات الرقمية لمختلف جوانب الحياة الأمن السيبراني مصدر قلق محوري على جميع المستويات، من المستخدمين الأفراد إلى الشركات الكبيرة وحتى الدول.

يشتمل الأمن السيبراني الحديث على ممارسات مختلفة مثل إدارة المخاطر والاستجابة للحوادث وتدريب توعية المستخدم ويستخدم مجموعة واسعة من الأدوات التكنولوجية مثل التشفير والجدران النارية وأنظمة كشف التسلل وبرامج مكافحة الفيروسات لحماية الأصول الرقمية (Kaplan et al., 2011) استلزم التطور المتزايد للتهديدات السيبرانية، بما في ذلك برامج الفدية وهجمات رفض الخدمة الموزعة (Distributed Denial-of-service) والتهديدات المستمرة المتقدمة (Advanced Persistent Threats)، تطوير استراتيجيات وتقنيات معقدة للأمن السيبراني (Sailio et al., 2020).

ومع ظهور إنترنت الأشياء (Internet of Things) والبيانات الضخمة والذكاء الاصطناعي والتعلم الآلي، يتعين على العاملين في مجال الأمن السيبراني التعامل مع التحديات ونقاط الضعف الجديدة، مما يجعله

مجالًا دائم التطور (Roman et al., 2013) وبالتالي، فإن الأمن السيبراني المعاصر هو مجال ديناميكي ومعقد يتطلب نهجًا متعدد الأوجه ومزج التكنولوجيا والعوامل البشرية والسياسة والقانون لإدارة المخاطر السيبرانية والتخفيف منها بشكل فعال.

مفهوم المواطنة الرقمية:

يمكن ربط نشأة مصطلح "المواطنة الرقمية" إلى حد كبير بانتشار التكنولوجيا الرقمية واستخدام الإنترنت الذي ميز أواخر القرن العشرين وأوائل القرن الحادي والعشرين. ويمكن تعريف المواطنة الرقمية ببساطة على أنها القدرة على المشاركة في المجتمع عبر الإنترنت بما يضن الوصول إلى التقنيات الرقمية والإنترنت والقدرة على استخدامها (Mossberger et al., 2007) ومع تطور شبكة الويب العالمية توفر الوصول إلى كميات غير مسبوقة من المعلومات وسبل الاتصال، وبالتالي بدأ المفهوم في النمو أكثر تعقيدًا. كما أدى تقديم Web 2.0، الذي يتميز بالاستخدام التفاعلي والتعاوني للإنترنت، إلى زيادة ارتباط المواطنة الرقمية بمحو الأمية الرقمية وشبكة الإنترنت والسلوك المسؤول عبر الإنترنت (Palfrey & Gasser, 2011)

وحديثاً، تم تعريف المواطنة الرقمية على أنها مجموعة واسعة من السلوكيات المسؤولة المتعلقة بالممارسات والسياسات والمعرفة التكنولوجية الحالية بما في ذلك فهم الثقافة والمجتمع والوعي العالمي المرتبط باستخدام التكنولوجيا والموارد (Ribble, 2015) ووسعت العناصر التسعة للمواطنة الرقمية التي اقترحها Ribble هذا المفهوم حيث بات يغطي جوانب مثل الوصول الرقمي والاتصالات الرقمية ومحو الأمية الرقمية والآداب الرقمية والقانون الرقمي والحقوق والمسؤوليات الرقمية والصحة الرقمية والعافية والأمن الرقمي.

وفي عصر تُجرى فيه غالبية أنشطتنا المهنية والتعليمية والشخصية عبر الإنترنت، لا يمكن التقلي من أهمية المواطنة الرقمية، حيث بات من الضروري أن يمتلك المستخدمون ليس فقط المهارات اللازمة لاستخدام التكنولوجيا بشكل فعال ولكن أيضًا للقيام بذلك بطريقة آمنة وأخلاقية ومسؤولة. إنها تشكل الطريقة التي يتفاعل بها الأفراد عبر الإنترنت وكيف يدركون وينشرون ويقيمون المعلومات (Ohler, 2011)

في المحصلة، يعد فهم وتعزيز المواطنة الرقمية أمرًا أساسيًا لضمان بيئة رقمية محترمة وتعاونية. وبالنسبة للمعلمين وأولياء الأمور وصانعي السياسات، يعد تعزيز ممارسات المواطنة الرقمية الجيدة بين الشباب أمرًا بالغ الأهمية لتمكينهم من التنقل في العالم الرقمي بأمان ومسؤولية والمشاركة في المجتمع الرقمي بفعالية، وتسخير الإمكانات الكاملة للتقنيات الرقمية للتعلم والابتكار.

الفجوة البحثية:

في حين أن مجموعة الأدبيات المتوفرة حول الأمن السيبراني والمواطنة الرقمية شاملة في اتساعها وعمقها، إلا أن هناك ثغرة ملحوظة فيما يتعلق بسياق المملكة العربية السعودية. بالإضافة إلى ذلك، تدرس الأدبيات الحالية هذه المفاهيم إلى حد كبير بمعزل عن غيرها، مع ندرة الأبحاث التي تركز على التفاعل فيما بينها.

أولاً، تكشف مراجعة سريعة للأدبيات عن غياب الدراسات التي تركز على الخصائص الثقافية للمواطنة الرقمية والأمن السيبراني في المملكة العربية السعودية. ويجدر الإشارة هنا إلى أن الممارسات الرقمية مدمجة في السياقات الثقافية والمجتمعية وتؤثر وتتأثر بالأعراف والعادات والسلوكيات المحلية. في حين أن هناك مؤلفات كبيرة حول ممارسات الأمن السيبراني والمواطنة الرقمية العالمية والغربية، إلا أنها قد لا تنطبق بالكامل على سياق المملكة العربية السعودية نظرًا لمشهدها الثقافي والاجتماعي والتكنولوجي الفريد (Al-Rahmi et al., 2015) ويشير الافتقار إلى الدراسات الخاصة بالسياق إلى وجود فجوة بحثية كبيرة يجب معالجتها. علاوة على ذلك، كانت دراسات الأمن السيبراني في المملكة العربية السعودية ذات طبيعة تقنية في الغالب، مع التركيز على أنظمة المعلومات والبنية التحتية (Alrubaiq & Alharbi, 2021)في حين أن مثل هذا البحث مهم بلا شك، إلا أن هناك حاجة لتوسيع نطاق التركيز ليشمل الجوانب الاجتماعية والثقافية، مثل مواقف المستخدم وسلوكياته ووعيه، التي تؤثر بشدة على فعالية الأمن السيبراني. على هذا النحو، فإن اتباع نهج أكثر شمولية يتضمن جوانب من المواطنة الرقمية يمكن أن يوفر رؤى لا تقدر بثمن.

ثانيًا، على الرغم من الصلة الواضحة بين الأمن السيبراني والمواطنة الرقمية، فقد أجريت أبحاث محدودة حول العلاقة المتبادلة بينهما، حيث ركزت معظم الدراسات إما على الأمن السيبراني أو المواطنة الرقمية، مع القليل منها فقط لاستكشاف العلاقة بين الاثنين (Jones & Mitchell, 2016)يعد فهم هذا التفاعل أمرًا بالغ الأهمية لأنه لديه القدرة على توجيه السياسات والممارسات بطريقة أكثر شمولية وتكاملاً.

في المحصلة، توضح المراجعة الدقيقة للأدبيات المتاحة عن فجوتين رئيسيتين: الافتقار إلى البحث حول الأمن السيبراني والمواطنة الرقمية في سياق المملكة العربية السعودية والاستكشاف المحدود للعلاقة المتبادلة بين هذين المفهومين.

النظريات ذات الصلة بالأمن السيبراني:

نظرية الردع:

تم تطبيق نظرية الردع، التي تم تصورها مبدئيًا في مجال الحرب النووية خلال حقبة الحرب الباردة، في مجال الأمن السيبراني في السنوات الأخيرة (Libicki, 2009)تفترض هذه النظرية أنه يمكن منع الهجمات الإلكترونية من خلال توعية المهاجمين المحتملين بالعواقب الوخيمة التي قد يواجهونها، وبالتالي ردعهم عن الشروع في مثل هذه الإجراءات. وتؤكد نظرية الردع على أهمية تحديد عواقب التهديدات السيبرانية والإبلاغ عنها بوضوح، والتي يمكن أن تتراوح من العقوبات القانونية إلى الإجراءات الإلكترونية الانتقامية. في حين أن تطبيق نظرية الردع في الأمن السيبراني كان موضوعًا للنقاش بسبب تحديات عزو الهجمات الإلكترونية وإنفاذ العواقب، إلا أنها تظل إطاراً نظرياً مؤثراً.

نظرية النشاط الروتيني:

وجدت نظرية النشاط الروتيني المستخدمة بشكل أساسي في علم الإجرام تطبيقها أيضًا في أبحاث الأمن السيبراني. اقترحت النظرية في الأصل من قبل كوهين وفلسون (1979)، وتقترح النظرية أن الجريمة من المحتمل أن تحدث إذا تم استيفاء ثلاثة شروط: الجاني الدافع والهدف المناسب وغياب وصي قادر. وعند تطبيق هذه الشروط على الأمن السيبراني، يُترجم ذلك إلى مهاجم إلكتروني محتمل وأنظمة أو بيانات رقمية ضعيفة وغياب تدابير الأمن السيبراني الفعالة (Cohen & Felson, 1979)وبمعنى أدق، تسلط هذه النظرية الضوء على الحاجة إلى ممارسات قوية للأمن السيبراني لتعمل كـ "حراس مؤهلين" وأهمية تقليل نقاط ضعف النظام.

النظرية الاجتماعية والتقنية:

تقترح النظرية الاجتماعية والتقنية أنه لا يمكن فصل التكنولوجيا واستخدامها عن السياق الاجتماعي الذي توجد فيه .(Baxter & Sommerville, 2011) وتؤكد أن كلا من العوامل الاجتماعية والتقنية تسهم في أمن نظم المعلومات. هذا المنظور مهم بشكل خاص في عصر الأنظمة الرقمية المعقدة والمتشابكة، حيث تلعب العوامل البشرية دورًا حاسمًا في الأمن السيبراني. وعلى هذا النحو، لا يتعلق الأمن السيبراني بتأمين الأنظمة فحسب، بل يتعلق أيضًا بإدارة سلوكيات وممارسات المستخدمين والتي غالبًا ما تشكل الحلقة الأضعف في الدفاع السيبراني. وبالتالي، تؤكد هذه النظرية على أهمية دمج تعليم المستخدم وتوعيته في استراتيجيات الأمن السيبراني.

نظريات قابلة للتطبيق على المواطنة الرقمية:

البناء الاجتماعي للتكنولوجيا:

تقترح نظرية البناء الاجتماعي للتكنولوجيا (Social Construction of Technology) أن التكنولوجيا لا تتطور بشكل مستقل ولكنها تتشكل من قبل المجتمع الذي يتم تطويره واستخدامه فيه (Pinch & Bijker, 1984) وفي سياق المواطنة الرقمية، توجه النظرية بأن الطريقة التي يتصرف بها الأشخاص عبر الإنترنت ليست مجرد نتيجة للحتمية التكنولوجية ولكنها أيضًا انعكاس للمعايير والقيم

والتأثيرات المجتمعية، كما توضح النظرية أن فهم هذه البنى الاجتماعية هو المفتاح لتعزيز المواطنة الرقمية المسؤولة. على سبيل المثال، كيف تتفاوض المجتمعات وتفسر السلوك المقبول أو غير المقبول عبر الإنترنت هو بناء اجتماعي يؤثر بشكل مباشر على المواطنة الرقمية.

نظرية الممثل والشبكة

نظرية الممثل والشبكة (Actor-Network Theory)هي نظرية اجتماعية أخرى مؤثرة تطبق على دراسة المواطنة الرقمية، وهي تقترح أن الظواهر الاجتماعية، بما في ذلك المواطنة الرقمية، هي نتيجة التفاعلات بين الكيانات البشرية وغير البشرية داخل الشبكة. بمعنى آخر، تشكل كل من الأدوات التكنولوجية (الجهات الفاعلة غير البشرية) والمستخدمين (الفاعلين البشريين) طبيعة المواطنة الرقمية. على سبيل المثال، تتيح منصات الوسائط الاجتماعية (الجهات الفاعلة غير البشرية) للمستخدمين الفرصة للمشاركة والتعليق والرد (أفعال الفاعل البشري) والتي بدورها يمكن أن تؤثر على مفاهيم المواطنة الرقمية (Bennett & Segerberg, 2012).

نظرية المواطنة الرقمية:

كمنظور نظري ناشئ، تركز نظرية المواطنة الرقمية بشكل خاص على حقوق ومسؤوليات وسلوكيات الأفراد في العالم الرقمي (Ribble, 2015) وتفترض هذه النظرية أن المواطنين الرقميين لا يجب أن يكون لديهم فقط القدرة على استخدام التقنيات الرقمية ولكن أيضًا القدرة على القيام بذلك بشكل مسؤول وأخلاقي وآمن. وتشمل هذه النظرية عدة جوانب مثل محو الأمية الرقمية والآداب الرقمية والقانون الرقمي والأمن الرقمي مما يشير إلى الطبيعة المعقدة والمتعددة الأوجه للمواطنة الرقمية. وبالتالي، تعمل هذه النظرية كإطار شامل لفهم وتعزيز المواطنة الرقمية الفعالة.

التحليل والمناقشة:

الأمن السيبراني: التحدي والتهديدات:

تعتبر التهديدات السيبرانية بمثابة فضاء سريع التطور يتميز بمجموعة متزايدة من الأنشطة الخبيثة المصممة لتقويض سرية نظم المعلومات أو تكاملها أو توفرها (Choo, 2011)وتختلف أنواع التهديدات اختلافًا كبيرًا من حيث التعقيد، من محاولات القرصنة الفردية إلى الهجمات الإلكترونية المنسقة التي ترعاها الدولة. وأحد أبرز أشكال التهديد الشائعة هو البرامج الضارة، والتي تشمل الفيروسات والديدان وأحصنة طروادة، المصممة لاختراق الأنظمة وإتلافها أو سرقة البيانات. وانتشرت برامج الفدية، وهي نوع من البرامج الضارة التي تشفر بيانات المستخدم وتطلب فدية لإصدارها، بشكل خاص في السنوات الأخيرة، مما تسبب في اضطرابات وخسائر مالية كبيرة (Gazet, 2010).

كما أصبحت هجمات التصيد الاحتيالي التي تنطوي على خداع المستلمين للكشف عن معلومات حساسة من خلال رسائل البريد الإلكتروني أو مواقع الويب المخادعة أكثر تعقيدًا. بالإضافة إلى ذلك، فإن هجمات رفض الخدمة الموزعة (DDoS)، التي تفرط في تحميل شبكة أو نظام لتعطيل خدماتها، تشكل تهديدات كبيرة لتوافر الخدمات الرقمية. علاوة على ذلك، فإن التهديدات المستمرة المتقدمة (Advanced Persistent Threats)، المرتبطة عادةً بالأنشطة التي ترعاها بعض الدول، هي هجمات مستهدفة طويلة المدى تسعى إلى التسلل إلى شبكة خلسة غالبًا لأغراض التجسس (Cavelty, 2010).

وأبرزت العديد من الهجمات الإلكترونية البارزة في السنوات الأخيرة الآثار واسعة النطاق لفشل الأمن السيبراني. على سبيل المثال، تسبب هجوم WannaCry ransomware لعام 2017، والذي أثر على مئات الآلاف من أجهزة الكمبيوتر في 150 دولة، في حدوث اضطرابات كبيرة في مختلف القطاعات، وأثر بشكل ملحوظ على الخدمة الصحية الوطنية في المملكة المتحدة، والتي تشكل جزءً هاماً من المواطنة الرقمية، مما قد يؤثر على توجه المواطنين للخدمات الرقمية. كما أدى هجوم DDoS في عام 2016 إلى تعطيل العديد من

مواقع الويب الشهيرة، بما في ذلك Twitter وNetflix وReddit، مما يؤكد احتمالية تأثير مثل هذه الهجمات بشكل كبير على الاقتصاد الرقمي والحياة اليومية (Perlroth, 2016)وأظهر اختراق Sony Pictures 2014، المنسوب إلى كوريا الشمالية، قدرة الجهات الفاعلة التي ترعاها الدولة على تنفيذ هجمات ضارة لدوافع سياسية (Ismail, 2017).

وفي الختام، تسلط هذه الهجمات الضوء على الآثار الملموسة للتهديدات السيبرانية، والتي يمكن أن تشمل الاضطرابات التشغيلية والخسائر المالية والإضرار بالسمعة وحتى التوترات الجيوسياسية المحتملة. كما أنها تؤكد على الحاجة الملحة لاتخاذ تدابير قوية للأمن السيبراني في جميع قطاعات المجتمع، مما يعزز أهمية تركيز هذا البحث على الأمن السيبراني في سياق المواطنة الرقمية.

استراتيجيات الوقاية:

مع استمرار تطور التهديدات الإلكترونية، يجب أن تتطور أيضًا الاستراتيجيات التي تستخدمها المنظمات للتخفيف من حدتها. وبالنظر إلى النهج الذي اقترحه (Heikka et al 2006)، يتعين تطوير نهج دفاعي متعدد الطبقات يشار إليه باسم "الدفاع في العمق"، وهو أمر حيوي لتعزيز المواطنة الرقمية حيث يستلزم هذا النهج تنفيذ تدابير أمنية متعددة لحماية طبقات مختلفة من نظام معلومات المنظمة، مما يضمن أن فشل عنصر تحكم واحد لا يؤدي إلى حل وسط على مستوى النظام.

أحد المكونات الرئيسية لهذا النهج هو نشر حلول تكنولوجية قوية، مثل جدران الحماية وأنظمة كشف التسلل وبرامج مكافحة الفيروسات وتقنيات التشفير للحماية من مجموعة واسعة من التهديدات. ومع ذلك، يتزايد الاعتراف بأن التدابير التقنية وحدها غير كافية، فوفقًا لدراسة أجراها Albrechtsen and Hovden (2010)، فإن الأمن السيبراني ليس مجرد مشكلة تقنية بل هو قضية بشرية أيضًا، مما يستلزم إدراج استراتيجيات تهدف إلى معالجة العامل البشري في الأمن السيبراني.

ويمكن أن تشمل تلك الإستراتيجيات تنفيذ برامج وطنية شاملة لتدريب وتثقيف المواطنين حول التهديدات المحتملة والممارسات الآمنة عبر الإنترنت وإنشاء سياسات أمن إلكتروني واضحة وقابلة للتنفيذ وتعزيز ثقافة الوعي بالأمن السيبراني داخل المنظمة (Furnell & Clarke, 2012).

وفي المملكة العربية السعودية وعلى المستوى الوطني، تلعب الحكومة السعودية دورًا حاسمًا في تشكيل مشهد الأمن السيبراني من خلال السياسات واللوائح التي أطلقتها وتطورها من حين لآخر. وأحد هذه الأساليب هو تطوير استراتيجيات الأمن السيبراني الوطنية، والتي تحدد رؤية المملكة وأهدافها ونهجها لتعزيز الأمن السيبراني والحفاظ عليه. وتشتمل هذه الاستراتيجيات مجموعة من التدابير بما في ذلك إنشاء وكالات مخصصة للأمن السيبراني والاستثمار في البحث والتطوير في مجال الأمن السيبراني والشراكات بين القطاعين العام والخاص وجهود التعاون الدولي.

وعلى الصعيد الدولي، تعمل قوانين حماية البيانات مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي على حماية خصوصية بيانات الأفراد وتفرض متطلبات صارمة على المؤسسات للتعامل مع هذه البيانات وحمايتها (Voigt et al., 2017) كما قدمت العديد من الحكومات تشريعات تستهدف جرائم الإنترنت على وجه التحديد مثل قانون الاحتيال وإساءة استخدام الكمبيوتر في الولايات المتحدة والذي يجرم مختلف أشكال الأنشطة الإلكترونية الضارة.

في جوهرها، تعد كل من الاستراتيجيات التنظيمية والسياسات واللوائح الحكومية المحلية والدولية مكونات حاسمة لنهج شامل للأمن السيبراني، مما يساهم في ضمان استراتيجية متعددة الطبقات ومتعددة الأوجه لمكافحة تطور التهديد السيبراني والمواطنة الرقمية.

جهود المملكة العربية السعودية في مواجهة التهديدات السيبرانية

تحرص المملكة العربية السعودية على تعزيز المواجهة ضد التهديدات السيبرانية حيث يلعب تطور التكنولوجيا دورًا مهمًا في تشكيل استراتيجيات الأمن السيبراني. وفي السنوات الأخيرة، ظهرت العديد من الابتكارات التكنولوجية لمعالجة المشهد المعقد بشكل متزايد للتهديدات السيبرانية، ولكل منها تطبيقات محتملة في إطار الأمن الرقمي في المملكة العربية السعودية.

وبرز التعلم الآلي والذكاء الاصطناعي كأداتين مؤثرتين في مجال الأمن السيبراني، حيث يقدمان طرقًا جديدة لتوقع التهديدات الإلكترونية وتحديدها والتخفيف من حدتها (Buczak & Guven, 2015)يمكن لهذه التقنيات معالجة كميات هائلة من البيانات بسرعة لا مثيل لها وتطبيق التحليلات التنبؤية للتعرف على أنماط النشاط الضار. تسمح هذه القدرة باستجابات أكثر استباقية وفعالية للتهديدات السيبرانية، وهو أمر بالغ الأهمية لدولة رقمية بشكل متزايد مثل المملكة العربية السعودية (Shaukat et al., 2020).

علاوة على ذلك، يعد تطبيق تقنية Blockchain في الأمن السيبراني حلاً مشجعا لتعزيز سلامة البيانات وسريتها. فمن خلال إنشاء دفاتر أستاذ رقمية للمعاملات لا مركزية وواضحة للعبث، يمكن لتقنية Blockchain منع التلاعب بالبيانات وتعزيز إمكانية تتبع الأنشطة الإلكترونية. تجعل هذه السمات احتمالًا صعبًا للمهاجمين للتعامل مع البيانات، وهو أمر بالغ الأهمية لحماية الأصول الرقمية في الاقتصاد الرقمي المزدهر في المملكة العربية السعودية (Khezr et al., 2019).

في السياق ذاته، يقدم التشفير الكمومي نموذجًا جديدًا للاتصال الآمن، حيث يسمح توزيع المفاتيح الكمومية، وهي ميزة بارزة في التشفير الكمومي، لطرفين بتبادل مفتاح سري يستخدم لتشفير وفك تشفير الرسائل. وهذا التوفير الأمني القابل للإثبات، المستند إلى مبادئ ميكانيكا الكم، هو أداة هائلة في تأمين البنية التحتية للاتصالات السعودية.

علاوة على ذلك، فإن ظهور خدمات الأمن السحابية مثل Security as a Service (SECaaS) يقدم مسارًا فعالاً من حيث التكلفة للمنظمات للوصول إلى أحدث أدوات وخدمات الأمان، وبالتالي تعزيز مرونتها ضد التهديدات السيبرانية. ويمثل ظهور SECaaS خطوة مهمة في رحلة المملكة العربية السعودية نحو الرقمنة، وتأمين بصمتها الرقمية (Almorsy et al., 2016).

في الختام، يمكن لتوظيف المملكة العربية السعودية لهذه الابتكارات التكنولوجية الديناميكية للأمن السيبراني مساعدتها في مواجهة التهديدات الناشئة. ونظرًا لأن هذه التقنيات تحقق تقدمًا كبيرًا، فإنها تقدم أيضًا نقاط ضعف محتملة مما يؤكد ضرورة استمرار البحث والتطوير في مجال الأمن السيبراني، لا سيما في السياق السعودي حيث يتقدم التحول الرقمي بسرعة.

المواطنة الرقمية في السياق السعودي:

أدى صعود العصر الرقمي إلى ظهور نموذج جديد في التفاعل المجتمعي، حيث كان مفهوم المواطنة الرقمية في طليعة هذا التطور، لا سيما في بلد يتحول إلى رقمنة سريعًا مثل المملكة العربية السعودية. ومن المعروف أن المواطنون الرقميون، الذين يُعرَّفون على أنهم أفراد يستخدمون الإنترنت بانتظام وفعالية، يتحملون حقوقًا ومسؤوليات محددة. يتضمن تصور Ribble (2015) لحقوق المواطنة الرقمية حرية الوصول إلى المعلومات ومشاركتها، والحق في الخصوصية، والحق في التعبير عن الآراء عبر الإنترنت، وهو ما باتت تحرص عليه المملكة العربية السعودية.

كما أن هذه الحقوق مصحوبة بمسؤوليات تتطلب الالتزام بالمعايير الأخلاقية أثناء التفاعلات عبر الإنترنت، واحترام الحقوق الرقمية والخصوصية للآخرين، واستخدام الموارد الرقمية بشكل مسؤول. وتعتبر هذه المسؤوليات، التي تم توضيحها من خلال العناصر التسعة للمواطنة الرقمية لـ Ribble (2015)، وثيقة الصلة بشكل خاص بالسياق السعودي، وذلك بالنظر إلى التزام الدولة بتعزيز ثقافة رقمية أخلاقية. وتشمل

العناصر التسعة – كما ذكرنا سابقاً – الوصول الرقمي والتجارة الرقمية والاتصالات الرقمية ومحو الأمية الرقمية والآداب الرقمية والقانون الرقمي والحقوق والمسؤوليات الرقمية والصحة والعافية الرقمية والأمن الرقمي.

ويلعب التعليم دورًا أساسيًا في تعزيز المواطنة الرقمية، وذلك في المقام الأول من خلال تزويد المتعلمين بالمهارات والمعرفة اللازمة للتنقل في العالم الرقمي بشكل أخلاقي ومسؤول. هذا الدور مهم بشكل خاص في المملكة العربية السعودية، حيث يمثل التحول الرقمي أولوية وطنية (رؤية السعودية 2030). تعمل المدارس والجامعات كمنصات مهمة لتعليم المواطنة الرقمية، حيث يشجع دمج المواطنة الرقمية في المناهج المتعلمين على التفكير بشكل نقدي في سلوكهم عبر الإنترنت والآثار الأخلاقية الأوسع لاستخدام التكنولوجيا الرقمية (Choi et al., 2017)

وللمواطنة الرقمية لها آثار مجتمعية كبيرة يمكنها إضفاء الطابع الديمقراطي على الوصول إلى المعلومات، وتعزيز الإدماج الاجتماعي من خلال ضمان وصول جميع المواطنين بغض النظر عن وضعهم الاجتماعي والاقتصادي إلى الموارد الرقمية والمشاركة في المجتمعات عبر الإنترنت. وتتماشى هذه الديمقراطية مع أهداف رؤية السعودية 2030، والتي تؤكد على الوصول الرقمي الشامل كوسيلة لتعزيز مجتمع نابض بالحياة (رؤية السعودية 2030). علاوة على ذلك، يمكن أن يساهم تعزيز السلوك الأخلاقي عبر الإنترنت من خلال المواطنة الرقمية في تفاعلات محترمة ومتناغمة عبر الإنترنت وتحسين الجودة الشاملة للبيئة الرقمية (Ribble, 2015)

وتظهر العديد من دراسات الحالة التنفيذ الناجح لمبادئ المواطنة الرقمية، فعلى سبيل المثال، يُظهر نظام التعليم في سنغافورة المعروف بتكنولوجيا المعلومات والاتصالات المتكاملة كيف يمكن لرعاية المواطنة الرقمية منذ سن مبكرة أن تؤدي إلى مجتمع رقمي أكثر شمولاً واحترامًا .(Patiño et al., 2023) وبالمثل، أدت برامج تعليم المواطنة الرقمية الواسعة النطاق في فنلندا إلى إلمام عدد كبير من السكان بالتعليم الرقمي .(Johannes et al., 2017) هذه الأمثلة، على الرغم من أنها خارج السياق السعودي، تقدم دروسًا قيمة لرحلة التحول الرقمي في المملكة العربية السعودية، لا سيما في إنشاء مواطنين رقميين مدركين أخلاقياً.

في المحصلة، يعد مفهوم المواطنة الرقمية مكونًا حاسمًا في المجتمع الرقمي اليوم وله آثار كبيرة على تفاعلات الأفراد عبر الإنترنت والصحة العامة للبيئة الرقمية. في بلد يتحول إلى رقمنة سريعًا مثل المملكة العربية السعودية، يعد فهم واحترام حقوق ومسؤوليات المواطنة الرقمية أمرًا أساسيًا للمساهمة في عالم رقمي أكثر أخلاقية وشمولية واحترامًا.

العلاقة المتبادلة بين الأمن السيبراني والمواطنة الرقمية:

ينبع الترابط العميق بين الأمن السيبراني والمواطنة الرقمية من الأسس المشتركة بينهما في المشهد الرقمي. يتصارع كلا المجالين مع التحدي المتمثل في تحقيق توازن بين الاستفادة من فوائد التقنيات الرقمية وتخفيف مخاطرها المحتملة. يركز الأمن السيبراني على حماية سلامة الأنظمة والبيانات الرقمية وتوافرها وسريتها، وبناء الأساس الآمن الذي تحدث عليه التفاعلات الرقمية. أما المواطنة الرقمية، من ناحية أخرى، تتعلق بالمعايير والسلوكيات التي تحدد المشاركة المسؤولة والأخلاقية في المجتمع الرقمي. وبالتالي، فإن فعالية ممارسات المواطنة الرقمية مرتبطة بطبيعتها بتدابير الأمن السيبراني المعمول بها، والعكس صحيح.

ومن منظور أكثر دقة، يمكن اعتبار الأمن السيبراني شرطًا أساسيًا للمواطنة الرقمية الفعالة، حيث يحتاج المواطنون الرقميون إلى الثقة في أمان الأنظمة الرقمية التي يستخدمونها لأغراض الاتصال والمعلومات والمعاملات. وبدون تدابير فعالة للأمن السيبراني، يمكن للمخاطر المرتبطة بالمشاركة الرقمية ردع المستخدمين وبالتالي تقويض مُثُل المواطنة الرقمية.

على الجانب الآخر، تلعب المواطنة الرقمية دورًا مهمًا في تشكيل ممارسات الأمن السيبراني، حيث يمكن أن تؤثر مواقف وسلوكيات ومهارات المواطنين الرقميين بشكل كبير على أمن البيئات الرقمية. فعلى سبيل المثال، يمكن أن تؤدي الممارسة الواسعة النطاق لاستخدام كلمة مرور قوية أو الوعي بخداع التصيد الاحتيالي أو تجنب الشبكات غير الآمنة إلى تعزيز الأمن السيبراني بشكل كبير على مستوى المجتمع أو المجتمع (Spremić & Šimunic, 2018). وغالبًا ما يكون المواطنون الرقميون المسؤولون هم في الأساس خط الدفاع الأول ضد التهديدات الإلكترونية.

علاوة على ذلك، يوجد تعزيز متبادل بين مجالات الأمن السيبراني والمواطنة الرقمية. كما يؤكد Mossberger وآخرون (2007)، فإن تعزيز بيئة رقمية أكثر أمانًا يعزز مشاركة رقمية أكبر وبالتالي مواطنة رقمية أكثر حيوية. في الوقت نفسه، يمكن أن يؤدي تعزيز السلوكيات الرقمية المسؤولة والمستنيرة إلى ممارسات أمن إلكتروني شخصية وجماعية أفضل.

وختاماً، الأمن السيبراني والمواطنة الرقمية ليسا مجرد مفهومين مرتبطين ببعضهما البعض ولكنهما متشابكان بشكل لا ينفصم ويتفاعلان بشكل ديناميكي ويشكلان بعضهم البعض، ويشتركون في بناء المشهد الطبيعي لمجتمعنا الرقمي.

الأمن السيبراني كوسيلة مسهلة لتطوير المواطنة الرقمية:

يلعب الأمن السيبراني دوراً محورياً في الانتقال للمواطنة الرقمية، حيث يكمن أحد الجوانب الحاسمة لهذا الدور في تعزيز بيئة رقمية آمنة تشجع المشاركة النشطة في الأنشطة الرقمية. وحيث يشارك المواطنون الرقميون عبر الإنترنت من تبادل المعلومات إلى التجارة الإلكترونية والشبكات الاجتماعية، تتطلب هذه المشاركة النشطة بيئة إلكترونية آمنة وخالية من التهديدات، بالإضافة إلى إطار وقائي يحمي من الانتهاكات المحتملة. يمكن لتدابير الأمن السيبراني، مثل بروتوكولات التشفير القوية والمنصات الآمنة عبر الإنترنت وأنظمة الحماية من البرامج الضارة الفعالة، أن توفر هذه البيئة الآمنة، وبالتالي تمكين وتشجيع الأفراد على أداء أدوارهم كمواطنين رقميين نشطين .(Von Solms & Van Niekerk, 2013).

ويتعلق جانب مهم آخر من التفاعل بين الأمن السيبراني والمواطنة الرقمية بخصوصية البيانات. كما يعد الحق في الخصوصية مكونًا أساسيًا للمواطنة الرقمية، مما يؤكد الحاجة إلى تدابير فعالة للأمن السيبراني لدعم هذا الحق .(Ribble, 2015) وتشكل البيانات الشخصية العمود الفقري للعالم الرقمي، وحمايتها عنصر حاسم في الحفاظ على ثقة المستخدم. تضمن تدابير الأمن السيبراني مثل تشفير البيانات وقواعد البيانات الآمنة والضوابط الصارمة للوصول إلى البيانات خصوصية وأمن البيانات الشخصية، وبالتالي تعزيز الثقة في المنصات الرقمية. وتعتبر هذه الثقة جزء لا يتجزأ من المشاركة الفعالة والأخلاقية للأفراد كمواطنين رقميين (Livingstone, 2014).

دور المواطنة الرقمية في تعزيز الأمن السيبراني:

تلعب المواطنة الرقمية دوراً أساسياً في تعزيز جهود الأمن السيبراني من خلال تعزيز الوعي والممارسات الجيدة. يتضمن أحد المبادئ الأساسية للمواطنة الرقمية فهم وممارسة السلوكيات الآمنة عبر الإنترنت، بما في ذلك استخدام كلمات مرور قوية والتحديث المنتظم للبرامج والوعي بالتصيد الاحتيالي وأنواع التهديدات الإلكترونية الأخرى. ومن خلال التعليم الشامل في المواطنة الرقمية، يكون الأفراد مجهزين بشكل أفضل للتعرف على التهديدات المحتملة والتصرف بطرق تقلل من المخاطر، وبالتالي تعزيز إطار الأمن السيبراني الشامل.

كما تعزز المواطنة الرقمية اليقظة الجماعية ومراقبة الأقران كونهم مشاركين نشطين في العالم الرقمي، وبالتالي يمكن للمواطنين المساهمة بشكل جماعي في الأمن السيبراني من خلال الإبلاغ عن الأنشطة المشبوهة أو الانتهاكات التي يواجهونها. ويعزز هذا النوع من ضبط الأمن بواسطة الأقران الأمن السيبراني من خلال

إنشاء نهج مجتمعي لاكتشاف التهديدات والوقاية منها، وتعزيز بيئة رقمية أكثر أمانًا لجميع المشاركين (Livingstone & Third, 2017).

وفي السياق ذاته، لا يخلو التفاعل بين الأمن السيبراني والمواطنة الرقمية من التحديات، حيث يمكن أن تؤدي مشكلات مثل عدم المساواة الرقمية وافتقار بعض الأفراد إلى المهارات أو الموارد اللازمة للمشاركة بفعالية كمواطنين رقميين وفهم الأمن السيبراني، إلى تفاقم نقاط الضعف وتعريض هؤلاء الأفراد لمخاطر إلكترونية أكبر. بالإضافة إلى ذلك، تتطلب الطبيعة الديناميكية للتهديدات السيبرانية تحديثات مستمرة في المعرفة والمهارات، مما يشكل تحديات لكل من محترفي الأمن السيبراني والمواطنين الرقميين Von Solms (& Van Niekerk, 2013).

وتوفر هذه التحديات أيضًا فرصًا لتعزيز التآزر بين الأمن السيبراني والمواطنة الرقمية. فعلى سبيل المثال، لا يمكن لمعالجة عدم المساواة الرقمية من خلال السياسات الشاملة والبرامج التعليمية أن تعزز المواطنة الرقمية فحسب، بل تحسن أيضًا الأمن السيبراني العام من خلال تقليل الأهداف المعرضة للخطر. وبالمثل، فإن التعلم المستمر وتنمية المهارات استجابة للتهديدات المتطورة يمكن أن يعزز ثقافة اليقظة والسلوكيات الاستباقية، مما يفيد المواطنين الرقميين الأفراد والنظام البيئي السيبراني الأوسع (Ausawasowan et al., 2021).

الآفاق المستقبلية:

بالنظر إلى المستقبل، هنالك اتجاهات مختلفة لتشكيل المشهد المتطور للأمن السيبراني والمواطنة الرقمية، حيث تعمل زيادة الاتصال الرقمي التي تغذيها التطورات مثل إنترنت الأشياء وشبكات G5، على توسيع مساحة التهديد السيبراني، مما يستلزم تطوير المزيد من تدابير الأمن السيبراني المتطورة. بالإضافة إلى ذلك، يوفر انتشار الذكاء الاصطناعي وتقنيات التعلم الآلي كلاً من الفرص والتحديات، حيث يمكن استخدامها لتعزيز الأمن السيبراني ولكن أيضًا يمكن استغلالها من قبل الجهات الفاعلة الخبيثة. ومن ناحية أخرى، مع انتقال المزيد من الأنشطة والخدمات عبر الإنترنت، سيستمر دور ومسؤوليات المواطنين الرقميين في التطور، ويؤكد ذلك على ضرورة الاعتراف المتزايد بالحقوق الرقمية مثل الخصوصية وحرية التعبير فضلاً عن التوقعات المتزايدة للسلوكيات الأخلاقية عبر الإنترنت ومحو الأمية الرقمية.

واستجابة لهذه الاتجاهات، يجب اتخاذ تدابير استباقية لتعزيز الأمن السيبراني وتعزيز المواطنة الرقمية المسؤولة. ويشمل ذلك التحديث المستمر للبنية التحتية للأمن السيبراني والبروتوكولات لمواجهة التهديدات الناشئة، بالإضافة إلى تنفيذ برامج قوية للتثقيف والتوعية في مجال الأمن السيبراني لتزويد المواطنين الرقميين بالمهارات والمعرفة اللازمة. كما أن تعزيز ثقافة الأمن التي تعطي المنظمات والأفراد الأولوية للأمن السيبراني يمكن أن يساهم بشكل كبير في تعزيز الدفاعات السيبرانية الشاملة.

ومن منظور السياسات، يلعب العديد من أصحاب المصلحة، بما في ذلك الحكومات والمؤسسات التعليمية ومنظمات القطاع الخاص، أدوارًا حاسمة في تشكيل مستقبل الأمن السيبراني والمواطنة الرقمية. ويمكن للسياسات التي تعزز التعاون ومشاركة المعلومات بين هذه الكيانات أن تعزز الجهود الجماعية ضد التهديدات الإلكترونية. بالإضافة إلى ذلك، يجب أن تعطي السياسات الأولوية للشمولية الرقمية، مما يضمن حصول جميع الأفراد، بغض النظر عن وضعهم الاجتماعي والاقتصادي، على فرصة المشاركة في العالم الرقمي بأمان ومسؤولية.

وأخيرًا، مع استمرار انتشار التقنيات الرقمية في جميع جوانب الحياة، من الضروري دمج تعليم المواطنة الرقمية في كل من إعدادات التعلم الرسمية وغير الرسمية، وتمكين الأفراد من التنقل في العالم الرقمي بشكل أخلاقي وآمن.

الخاتمة:

قادت رحلة هذا البحث إلى استكشاف شامل للعلاقة المتكاملة بين الأمن السيبراني والمواطنة الرقمية. وبتتبع التطور التاريخي لكلا المفهومين، تم اكتشاف أنه بينما نشأت ككيانات متباينة، أصبحت مساراتها متشابكة بشكل متزايد في مواجهة الاتصال الرقمي المتزايد.

كما كشفت الدراسة عن الدور الكبير للأمن السيبراني كميسر للمواطنة الرقمية النشطة والآمنة، مما يوفر بيئة تزدهر فيها الثقة والمشاركة النشطة حيث تساهم المواطنة الرقمية في تعزيز الأمن السيبراني من خلال رعاية جمهور رقمي استباقي ومتعلم يساعد في اليقظة الجماعية والشرطة من الأقران. وفي سياق المملكة العربية السعودية، تحمل هذه العلاقات المتبادلة وزنًا خاصًا نظرًا للخطوات الكبيرة التي حققتها الدولة في التحول الرقمي والالتزام بتعزيز إطار قوي للأمن السيبراني.

ومن منظور السياسات، تشير النتائج إلى ضرورة مشاركة أصحاب المصلحة المتعددين، بما في ذلك الهيئات الحكومية والمؤسسات التعليمية ومؤسسات القطاع الخاص، في تشكيل مشهد الأمن السيبراني والمواطنة الرقمية في المملكة العربية السعودية. ويتعين على صانعي السياسات إعطاء الأولوية لتعزيز الشمولية الرقمية وتعزيز المبادرات التعليمية التي تهدف إلى تزويد جميع المواطنين بالمعرفة والمهارات الرقمية الأساسية في مجال الأمن السيبراني.

وبالنسبة للممارسة والتطبيق العملي، يتعين على المؤسسات والمراكز الاجتماعية أن تسعى جاهدة لخلق ثقافة تقدر الأمن السيبراني وتعطي الأولوية له مما يعزز أهمية اليقظة والالتزام بالسلوكيات الآمنة عبر الإنترنت.

وفيما يتعلق بالبحوث المستقبلية، توصي الدراسة الحالية بالقيام بالمزيد من الفحوصات التفصيلية لتأثير التقنيات الناشئة مثل الذكاء الاصطناعي وإنترنت الأشياء على الأمن السيبراني والمواطنة الرقمية وكذلك ودور العوامل الديموغرافية المختلفة في المواطنة الرقمية وفعالية مبادرات التوعية والتثقيف في مجال الأمن السيبراني في السياق السعودي.

في النهاية، تؤكد هذه الدراسة على العلاقة التكافلية المتزايدة بين الأمن السيبراني والمواطنة الرقمية. وفي عصر يتسم بتزايد الرقمنة، فإن مسؤوليتنا الجماعية هي ضمان تطور هذه العلاقة بطريقة تدعم الأمن والشمولية والمواطنة الرقمية المسؤولة. بينما نتنقل في هذا العصر الرقمي، فإن المفتاح هو أن نتذكر أنه بينما تتطور التكنولوجيا والتهديدات، يجب أن يظل التزامنا بإنشاء عالم رقمي آمن ومسؤول ثابتًا.

المراجع:

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432-445.

Alharbi, A. S. (2019, March). Challenges in digital transformation in Saudi Arabia obstacles in paradigm shift in Saudi Arabia. In 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1287-1291). IEEE.

Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

Al-Rahmi, W., Othman, M. S., & Yusuf, L. M. (2015). The role of social media for collaborative learning to improve academic performance of students and

researchers in Malaysian higher education. The International Review of Research in Open and Distributed Learning, 16(4).
Alrubaiq, A., & Alharbi, T. (2021). Developing a cybersecurity framework for e-government project in the Kingdom of Saudi Arabia. Journal of Cybersecurity and Privacy, 1(2), 302-318.
Ausawasowan, A., Adipat, S., Laksana, K., Busayanon, K., Pakapol, P., & Mahamarn, Y. (2021). Responsible Digital Citizenship: Safe and Respectful Online Community Life. Journal of Roi Kaensarn Academi, 6(7), 376-384.
Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. Interacting with computers, 23(1), 4-17.
Bennett, W. L., & Segerberg, A. (2012). The logic of connective action: Digital media and the personalization of contentious politics. Information, communication & society, 15(5), 739-768.
Buchanan, B. (2016). The cybersecurity dilemma: Hacking, trust, and fear between nations. Oxford University Press.
Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176.
Cavelty, M. D. (2010). Cyber-security. In The Routledge handbook of new security studies (pp. 154-162). Routledge.
Choi, M., Glassman, M., & Cristol, D. (2017). What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale. Computers & education, 107, 100-112.
Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & security, 30(8), 719-731.
Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American sociological review, 588-608.
Dede, C. (2014). The Role of Digital Technologies in Deeper Learning. Students at the Center: Deeper Learning Research Series. Jobs for the Future.
Denning, P. J., & Denning, D. E. (2016). Cybersecurity is harder than building bridges. American Scientist, 104(3), 154-157.
Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. computers & security, 31(8), 983-988.
Gazet, A. (2010). Comparative analysis of various ransomware virii. Journal in computer virology, 6, 77-90.

Heikka, J., Baskerville, R., & Siponen, M. (2006). A design theory for secure information systems design methods. Journal of the Association for Information Systems, 7(11), 31.
Ismail, M. (2017). Sony Pictures and the US Federal Government: A Case Study Analysis of the Sony Pictures Entertainment Hack Crisis Using Normal Accidents Theory.
Johannes, C., Morten, R., Niall, W., Anne, G., & Laurenz, L. (2017). Digital Education Policies in Europe and Beyond: Key Design Principles for More Effective Policies.
Jones, L. M., & Mitchell, K. J. (2016). Defining and measuring youth digital citizenship. New media & society, 18(9), 2063-2079.
Kaplan, J., Sharma, S., & Weinberg, A. (2011). Meeting the cybersecurity challenge. Digit. McKinsey.
Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9(9), 1736.
Kuhn, D. R., Coyne, E. J., & Weil, T. R. (2010). Adding attributes to role-based access control. Computer, 43(6), 79-81.
Landwehr, C. E. (2001). Computer security. International journal of information security, 1(1), 3-13.
Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND corporation.
Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. Communications, 39(3), 283-303.
Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. New media & society, 19(5), 657-670.
Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2007). Digital citizenship: The Internet, society, and participation. MIt Press.
Ohler, J. (2011). Digital citizenship means character education for the digital age. Kappa Delta Pi Record, 47(sup1), 25-27.
Palfrey, J., & Gasser, U. (2011). Born digital: Understanding the first generation of digital natives. ReadHowYouWant. com.
Patiño, A., Ramírez-Montoya, M. S., & Buenestado-Fernández, M. (2023). Active learning and education 4.0 for complex thinking training: analysis of two case studies in open education. Smart Learning Environments, 10(1), 8.
Perlroth, N. (2016). Hackers used new weapons to disrupt major websites across US. New York Times, 21.

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. Social studies of science, 14(3), 399-441.
Ribble, M. (2015). Digital citizenship in schools: Nine elements all students should know. International Society for technology in Education.
Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer networks, 57(10), 2266-2279.
Sailio, M., Latvala, O. M., & Szanto, A. (2020). Cyber threat actors for the factory of the future. Applied Sciences, 10(12), 4334.
Scarfone, K., Grance, T., & Masone, K. (2008). Computer security incident handling guide. NIST Special Publication, 800(61), 38.
Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), 2509.
Singer, P. W., & Friedman, A. (2014). Cybersecurity: What everyone needs to know. oup usa.
Spremić, M., & Šimunic, A. (2018, July). Cyber security challenges in digital economy. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 341-346). Hong Kong, China: International Association of Engineers.
Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). A Practical Guide, 1st Ed., Cham: Springer International Publishing, 10(3152676), 10-5555.
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.