إجراءات مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء بعض الممارسات الدولية

إعداد:

د/ سارة محمد حسين أبو حجاب

مدرس التربية المقارنة والإدارة التربوية

كلية التربية– جامعة بورسعيد

ملخص البحث:

قدم التقرير الدولي لمعهد الذكاء الرقمي DQ لعام ٢٠٢٠–الذي يقيِّم مؤشر أمان الطفل على الإنترنت في العالم– **الشواهد** على ارتفاع مستويات المخاطر السيبرانية لأطفال مصر؛ فقد احتلت مصر المرتبة ٧ على مستوى الدول في مستوى المخاطر السيبرانية من أصل ٣٠ دولة مشاركة بمجموع نقاط ٧٩ في مقابل المتوسط العالمي ٥٠ نقطة؛ مما يشير إلى أن هناك ضرورة حتمية لإدارة تلك المخاطر السيبرانية.

وبالنظر إلى "إلزامية" المدرسة الابتدائية في غالبية الدول، صارت المدرسة خياراً ممتازاً لإدارة المخاطر السيبرانية؛ فالتأثير الاجتماعي للإنترنت –خاصة بالنسبة للقصر– وانتهاكات حقوق الطفل هي قضية تهم المجتمع بشكل كبير، وهذا هو الدور الاجتماعي للمدرسة.

ومن هنا تهدف هذه الدراسة إلى تعرف المخاطر السيبرانية التي يتعرض لها تلاميذ المدارس الابتدائية وتحديدها باستقراء آراء أولياء أمور تلاميذ المدارس الابتدائية من خلال الدراسة الاستطلاعية، وكذا تقديم نظرة عامة على مجموعة مختارة من الممارسات الدولية التي يتم من خلالها إدارة المخاطر السيبرانية ذات التأثير السلبي على التربية والمجتمع والثقافة، فضلاً عن اقتراح العديد من الإجراءات في إطار إجراءات مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر.

ولتحقيق ذلك استخدمت الدراسة المنهج الوصفي التحليلي بأسلوب دراسة الحالة في محافظة بورسعيد؛ لمناسبته لموضوع الدراسة. وأعدت الباحثة استبانة استقصت فيها آراء عينة من مديري المدارس الابتدائية بمحافظة بورسعيد؛ للتعرف على واقع إدارة

المخاطر السيبرانية في المدارس الابتدائية بمحافظة بورسعيد، وخلصت الدراسة إلى إجراءاتٍ مقترحةٍ لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء بعض الممارسات الدولية.

الكلمات المفتاحية: إدارة المخاطر السيبرانية- الاستمالة- التنمر السيبراني- مشاهدة عناصر غير لائقة- إدمان الانترنت.

Proposed Procedures for Managing Primary School Cyber Risks in Egypt in Light of some International Practices.

Abstract:

The International Report of the Institute of Digital Intelligence (DQ) - which assesses the child cyber security around the world - provided evidence in 2020 of the high levels of cyber risks for Egyptian children; as Egypt has ranked the 7th regarding cyber risks out of 30 participating countries, with a total of 79 points, compared to the global average of 50 points. This indicates that there is an imperative to manage those cyber risks.

Considering that elementry school is compulsory in most countries, it becomes an excellent option for managing cyber risks; the social impact of the internet and violations towards children's rights - especially for minors - is an issue of great concern to society, and this is the social role of the school.

Hence, this study aims to identify the cyber risks that primary school students are exposed to and define them by extrapolating the opinions of parents of primary school pupils, as well as providing an overview of a selection of some International Practices through which cyber risks that have a negative impact on education, society and culture are managed. Besides, providing several procedures within the framework of proposed Procedures for managing primary school cyber risks in Egypt.

To achieve this, the study used the descriptive analytical approach in the design of a case study in Port Said Governorate, for being appropriate to the subject of the study. The researcher prepared a Questionnaire form in which she surveyed the opinions of a sample of primary school principals in Port Said governorate to identify the reality of cyber risk management in primary schools in Port Said Governorate. The study concluded with proposed Procedures for managing primary school cyber risks in Egypt in light of some International Practices.

Keywords: cyber risk management, cyber grooming, cyber bullying, viewing inappropriate content, internet addiction.

إجراءات مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء بعض الممارسات الدولية

إعداد:

د/ سارة محمد حسين أبو حجاب

مدرس التربية المقارنة والإدارة التربوية

كلية التربية– جامعة بورسعيد

المحور الأول: الإطار العام للدراسة.

تعمل التقنيات السيبرانية الحالية للقرن الحادي والعشرين على إعادة تشكيل التوزيع العالمي للسلطة والعدالة والمسؤولية؛ فأصبح يُنظر الآن إلى شركات مثل فيسبوك وجوجل وأبل وأمازون ومايكروسوفت على أنها تتمتع بمستويات من النفوذ السياسي العالمي التي يمكن مقارنتها بالدول والأمم (Vallor, & Rewak, 2018, 3)

وقد أحدث الإنترنت ثورة في العالم الحديث، فهو أعظم تجربة في تاريخ البشرية بما يتيح من ثروة المعرفة البشرية بضغطة زر مع فوائدٍ لا تعد ولا تحصى من هذا المورد (Cybersecurity Tech Accord, 2020, 3)؛ فحوَّل الدقائق والثواني إلى نانو ثانية، ومَكَّنَ أي شخص، في أي وقتٍ وفي أي مكان تقريبًا من التواصل والتعاون والمشاركة (Suppo, 2013, 2)

ووفقًا لـ DataReportal، في يناير ٢٠٢١ يستخدم الإنترنت ما يقرب من ٤.٦٦ مليار شخص(وتحديداً ٥٩.٩٪) –أي أكثر من نصف سكان العالم البالغ عددهم ٧.٨٣ مليار نسمة– بزيادة قدرها ٣١٦ مليون (٧.٣ %) عن العام الماضي (٢٠٢٠). (Kemp, 2021, 8–9)كما أنَّ نِصْف مستخدمي الإنترنت في القارة الأفريقية هم دون سن ٢٠عامًا (Widiputera, Satria, Perdana, & Zamjani, 2021, 2) فأحدث الانترنت ثورة في حياة الأطفال وتزايَدَ استخدامهم له في جميع أنحاء العالم؛ فهم يشكلون ثلث مستخدمي الإنترنت على مستوى العالم؛ أي واحد من كل ثلاثة مستخدمين للإنترنت عالمياً يقل عمره عن ١٨ عامًا، ويتزايد الآن استخدام أطفال المدارس الابتدائية الأصغر سنًا –دون سن التاسعة– للأجهزة المتصلة بالإنترنت، وعلى وجه الخصوص

الأجهزة اللوحية والهواتف الذكية Smartphones التي تعمل باللمس (Unicef, 2017, 1). بل أظهرت دراسة في المملكة المتحدة أن ٧٥ % من الأطفال الذين تتراوح أعمارهم بين ٨-١١ عاماً يستخدمون أكثر من جهاز إلكتروني في ذات الوقت. (Unicef, 2016, 7)

ونتيجة لتلك الزيادة المستمرة في الاعتماد على الإنترنت، ظهر الأمن الرقمي وإدارة مخاطره كواحدٍ من القضايا الحاسمة التي تواجه مدارس القرن الحادي والعشرين فلا تقل أهمية موضوعات السلامة والأمن والأخلاق عبر الإنترنت عن القراءة والكتابة والرياضيات(Saluja, Bansal, & Saluja, 2012, 4)، ويتزايد الاعتراف بأنه على الرغم من جميع فوائد الإنترنت الاجتماعية والاقتصادية – التي لا يمكن إنكارها – إلا أنه ينتج عنه العديد من المخاطر والتهديدات ذات الأثر الضار على القيم التربوية الأساسية في أي مجتمع مثل المساواة واحترام حقوق الإنسان والديمقراطية، بالإضافة إلى الآثار السلبية التي يُحدثها الإنترنت على الأخلاق والعلاقات الاجتماعية والتماسك الاجتماعي، ومخاطر تنمية الأطفال وحمايتهم بسبب التعرض لمعلومات وسلوكيات غير أخلاقية. (Quaglio & Millar, 2020, 3, 5, 22)

علاوة على الآثار الضارة على المستوى الأكاديمي للتلاميذ؛ حيث أصدرت المؤسسة الوطنية للصحة نتائج تشير إلى أن الأطفال والشباب الذين يقضون أكثر من ساعتين يوميًا على الشاشات يحققون درجات أقل في اختبارات اللغة والتفكير؛ كما أظهرت التجربة أن الأطفال والشباب الذين يلعبون على الانترنت بشكل مفرط يتدهور أداؤهم الأكاديمي(Dubicka & Theodosiou, 27)

ولاحَظَت دولٌ مثل المملكة المتحدة، الولايات المتحدة وكندا وأستراليا ونيوزيلندا استمرار تهديدات السلامة السيبرانية لديها، واستجابةً لذلك، خصصت جزءًا من ميزانيتها للتوعية والتثقيف حول هذه الظاهرة (Paraiso, 2019, 32) علاوةً على القيام بإنشاء مفوضية أوروبا والولايات المتحدة الأمريكية التي تهدف إلى توحيد الجهود حول العالم لمكافحة جرائم (الجنس عبر الإنترنت ضد الأطفال) بشكلٍ فعال، وحاليا يتم تمثيل ٥٤ دولة حول العالم لتشمل جميع أعضاء الاتحاد الأوروبي، والولايات المتحدة الأمريكية وأستراليا.(De Barros & Lazarek, 2018, 256)

وتشير الدراسات الحديثة مثل دراسة (Jemeljanenko, 2019, 10) إلى أن تشجيع التطبيق العملي لتقنيات إدارة المخاطر السيبرانية في إدارة التعليم أمر بالغ الأهمية، كما تشير الدراسات إلى أن التعليم السيبراني يحتاج إلزام من خلال إضفاء الطابع المؤسسي على مختلف شرائح المستخدمين، وأفضل قناة لذلك هي أن تتم من خلال المدارس(Saluja, Bansal & Saluja, 2012, 2) ؛ حيث أن من الوظائف الأساسية لنظام التعليم إنتاج مواطنون أكفاء ومسؤولون.(Schubart, 2021, 12)

وفي هذا السياق؛ فقد أكدت العديد من الدراسات على دور المدرسة كأحد الوسائط التربوية بالمجتمع في إدارة المخاطر السيبرانية لدى منتسبيها؛ فأشارت دراسة (Saluja, Bansal & Saluja, 2012, 2-3) إلى أن الاعتماد على المدارس يضمن تغطية أوسع ليصل إلى عدد أكبر من الأطفال؛ نظرًا لأن الجميع يذهبون إلى المدرسة، كما أشارت دراسة (De Barros & Lazarek, 2018, 255) إلى أن المدرسة هي القناة الأفضل للوصول إلى غالبية الأطفال، بغض النظر عن العمر، الدخل أو الخلفية، كما أشارت دراسة (Kritzinger, Bada, & Nurse, 2017, 2) إلى أن المدرسة خياراً ممتازاً كواحدة من أفضل الأماكن التي يتم توفيرها للتدريب على التوعية بالمخاطر السيبرانية. ولما كانت المدرسة مركز اتصال مجموعة كاملة من قيم وتطلعات المجتمع بل وتحدد القيم التي تتجاوز المجتمع، ولما كان النظام المدرسي لديه التزام أخلاقي وقانوني لخلق بيئة آمنة للتلاميذ والمعلمين والموظفين؛ كان لابد أن تتحمل المدرسة مسؤولية تعليم التلاميذ حدود السلوك المقبول اجتماعياً وتتأكد من أن المتعلمين لديهم الوعي والمعرفة والمهارات اللازمة فيما يتعلق بأمان الإنترنت، وتأسيسا على ذلك يحق للمدارس وضع قيود على أي شكل من أشكال تعبيرات التلاميذ وانتهاك حقوق التلاميذ الآخرين(White, 2013, 36 -39) فتقع مسؤولية تعليم هذا النوع من التعليم في المواطنة الرقمية على عاتق المدارس(Payne, 2016, 12) وعليها ضمان الإجراءات اللازمة لتعزيز الوقاية من مخاطر الاضطرابات والتسلط عبر الإنترنت.(Lopez-Fernandez & Kuss, 2020, 13)

تأسيساً على ما سبق، يجلب التقدم التكنولوجي العديد من الفوائد، ولكن يمكن أن تأتي في أعقابه مخاطرٌ كبيرة؛ فقد تشكل هذه الأجهزة الرقمية تحديات محتملة لتلاميذ

المدارس على النحو التالي: (Richardson, Lemoine, Stephens, & Waller, 2020, 26) (Dubicka & Theodosiou, 2020, 10, 19, 26)

١-قد يطغى الوقت المستغرق في تعامل التلاميذ مع التكنولوجيا الرقمية على أنشطة أخرى أكثر أهمية فتضيع فرصاً لممارسة مهارات الاتصال والمهارات الحركية والشخصية والنوم. ٢- قد يتم عرض محتوى غير مناسب بما في ذلك المحتوى العنيف أو الدموي، والتعرض للصور الجنسية أو التعرض لخطاب يحض على الكراهية. ٣- التعرض للتنمر عبر الإنترنت.٤-مخاطر الاستغلال بما في ذلك الاستغلال الجنسي.٥- يمكن إنفاق الأموال بسرعة وسهولة عبر الإنترنت، على سبيل المثال في شراء الألعاب، المقامرة عبر الإنترنت وعلى منتجات مثل الوصفات الطبية والعقاقير المحظورة.٦- تؤثر التكنولوجيا الرقمية على الوزن والمزاج وأفكار الانتحار وإيذاء النفس وصورة الجسم.٧- الاكتئاب، القلق وحالات النمو مثل اضطراب فرط الحركة ونقص الانتباه، ولا تزال الأبحاث تفتقر إلى دراسة التفاعل الديناميكي للمدة والمحتوى، ولكن الأدلة الأولية تشير إلى السلبية الجسدية والعقلية.

وعلى الصعيد التربوي؛ وفقاً لدراسة مسحية أجراها مكتب الأمم المتحدة عام ٢٠١٢ شملت الدول الأعضاء في منظمة الأمم المتحدة -وعددها ١٩٣ دولة- وُجد أن ١١٤ دولة لديها برامج وطنية للأمن السيبراني، وأن ٤٧ دولة أناطت تلك المهمة لمؤسسات مدنية منها المدارس والجامعات؛ فعلى سبيل المثال قامت الولايات المتحدة بإنشاء معهد مهني لاستقطاب البرامج القصيرة المختصة بالأمن السيبراني بحضور أكثر من ألف ومئتين مشاركاً عالمياً ما بين تلاميذ ومعلمين لدورات مدتها من يوم إلى خمسة أيام، واتخذت العديد من الدول الآسيوية إجراءات مماثلة لتفعيل دور المؤسسات التربوية ودور المعلم في مجال الأمن السيبراني ومنها: اليابان وسنغافورة وماليزيا والهند وبنجلاديش. (حريري والمنتشري، ٢٠٢٠، ٩٧)

وأطلقت الحكومة الأمريكية المبادرة الوطنية للتربية السيبرانية؛ بهدف إعداد قوى عاملة في مجال الأمن السيبراني، (المنتشري، ٢٠٢٠، ٤٥٩) وقد أوصت وزارة التعليم بولاية كونيتيكت بالولايات المتحدة الأمريكية بتشجيع جميع المدارس والمقاطعات على تناول مواضيع إدارة المخاطر السيبرانية ودعم المواطنة الرقمية (NetSafe, 2010,

(15وتم تضمين الأمان عبر الإنترنت كموضوع محدد في المنهج الدراسي لـ ٢٣ نظامًا تعليميًا عبر أوروبا، وأطلق الاتحاد الأوروبي مجموعة أدوات لتطوير الأمان عبر الانترنت وبناء المعرفة بشأن استخدام الإنترنت، (De Barros & Lazarek, 2018, 252) وفي دراسة استقصائية دولية ثبت فعالية دمج التثقيف التوعوي في هذا الصدد من خلال تضمينه في المناهج؛ حيث تم إجراء تحليل لتعزيز تعليم الوعي الجنسي لأطفال المدارس الابتدائية، وتبيَّن أهمية المشاركة المتكاملة لأطراف متعددة مثل المعلمين، الآباء ووسائل الإعلام لجعل الأطفال أكثر وعياً. (Spiering, 2018, 22)

مشكلة الدراسة:

في ظل ما يمر به العالم المعاصر من تخبط قيمي وتدني للمعايير الإيجابية في السلوك، والتباين في الوعي بمفهوم الحرية، وتفشي نزعات سوء استخدام الانترنت (الزهراني، ٢٠١٩، ٣٩٨)، وما صاحب تلك التحديات من انفجار معرفي واجتياح الثورة الصناعية الرابعة للاتصالات الرقمية (الذكاء الاصطناعي وانترنت الأشياء) (حريري والمنتشري، ٢٠٢٠، ٩٩)، وما أفرزته هذه الأخيرة من تطبيقات رقمية وأجهزة مختلفة سهلت سرعة عمليات التواصل مع أفراد مجهولين قد يشكلون خطراً عليهم فكراً وسلوكاً، وفي ظل تعذر مراقبة الأجيال وما قد يطلعون عليه من مواقع مشبوهة خطيرة، أو يبنون أفكار وسلوكيات تخالف تعاليم الدين وقيمه التربوية وأخلاقه وتتعارض مع الثوابت الوطنية.

وعليه كان لا بد من التوجه لإدارة المخاطر السيبرانية، ولاسيما أن الدراسات العلمية والإحصاءات تشير إلى تزايد عدد مستخدمي الانترنت في مصر؛ فوفقا لإحصائيات (يناير – مارس ٢٠٢١) تزايد عدد مستخدمي الانترنت في مصر عبر الهاتف المحمول إلى ٥٥.٩٨ مليون مشترك، أما مستخدمو مودم USB فيبلغون ٣.٣٠ مليون مستخدم، ومشتركو ADSL يبلغون ٩.٢٦ مليون مشترك، وبلغ استخدام الإنترنت من المنزل ٧٠.٥٪ في المناطق الحضرية، مقابل ٥١.٢٪ في المناطق الريفية. (MCIT, 2021, 1-11)

فضلاً عن تزايد معدل استخدام الأطفال لهذه الأجهزة في مصر والذي قد يصل إلى ثماني ساعات يومياً؛ –بمعنى التأثير عليهم أكثر من نصف ساعات الاستيقاظ–؛

تلك الأوقات الطويلة والاستخدام غير الرشيد للتكنولوجيا في ظل قصور إدارة المخاطر السيبرانية في المدارس يؤدي إلى إشكاليات سلوكية خطيرة؛ أضحت تتحدى المربين القائمين على التربية والتعليم.(الزهراني، ٢٠١٩، ٣٩٨)

وعلى الرغم من اهتمام وزارة التربية والتعليم المصرية بالتحول نحو التعليم الإلكتروني في المدارس وخاصةً في ظل جائحة كورونا (هلل، ٢٠٢١، ٦٧٥) علاوة على التوجه نحو أتمتة Automation نظام التعليم والامتحانات بدءاً من العام الدراسي٢٠١٨/٢٠١٩ في إحدى مراحلها كخطوة أولية للتعميم من خلال الاستعانة بأجهزة التابلت (خليل، ٢٠٢٠، ٥٤)؛ إلا أنه –على حد علم الباحثة– لم يتزامن ذلك التوجه مع تشكيل لجان لإدارة المخاطر السيبرانية في مدارس مصر لتقوم بتحديد مخاطرها السيبرانية أو تحليلها وبيان أسبابها ووضع ضوابط وقائية للتصدي لها أو تقييم المخاطر أو تخفيفها ومعالجتها أو تتبع تلك المخاطر وتحديث أساليب إدارتها.

وللتأكد من مشكلة الدراسة تم إجراء دراسة استطلاعية أسئلتها مفتوحة –لتسمح بالتعبير الحرّ– على عينة عشوائية من مديري المدارس الابتدائية في محافظة بورسعيد عددهم ٢٥ مديراً للفصل الدراسي الثاني للعام الدراسي ٢٠٢٠– ٢٠٢١ ملحق (١)، وفي ضوء تحليل استجابات المفحوصين توصلت الدراسة لمجموعة من النتائج على النحو التالي:

فبالنسبة للسؤال الأول كيف تشارك المدرسة الابتدائية في إدارة المخاطر السيبرانية ؟ فقد أسفرت استجابات المفحوصين عن مجموعة من جوانب الخلل في إدارة المخاطر السيبرانية بالمدارس الابتدائية على النحو التالي:

– هناك نقص واضح في السياسات والممارسات والإجراءات المتعلقة بإدارة المخاطر السيبرانية تحقيقاً للسلامة السيبرانية بسبب قلة توجيهات الوزارة نحو تحسين أمان الإنترنت داخل المدارس، وبالتالي؛ ضعف الالتزام التنظيمي للمدارس بإدارة المخاطر السيبرانية؛ حيث أن مجرد وجود الرغبة دون سياسات وإجراءات مدروسة لا يكفي لخلق ثقافة مناهضة للمخاطر السيبرانية في المدرسة.

–قلة مساهمة المدارس حاليًا بشكل كبير في إنشاء ثقافة أمان الإنترنت وتنميتها بين المتعلمين في المدارس على الرغم من أن هؤلاء الأطفال لديهم القليل جدًا من التعليم

المتعلق بالسلوك الصحيح في الفضاء السيبراني داخل المدارس، ولا يبلغون عن المخاطر السيبرانية أو حوادث التسلط عبر الإنترنت التي تواجههم؛ مما يترك المتعلمين عرضة للخطر والتهديدات السيبرانية؛ وأرجعها البعض إلى مواجهة المدرسة مشاكل في العثور على المعلومات ذات العلاقة من جهات علمية.

أما عن السؤال الثاني كيف يشارك المعلمون في إدارة المخاطر السيبرانية ؟ فقد أسفرت استجابات المفحوصين عن مجموعة من جوانب الخلل في أدوار المعلمين تجاه إدارة المخاطر السيبرانية بالمدارس الابتدائية؛ فوفقًا للمفحوصين من مديري المدارس:

– معظم المعلمين لديهم معرفة وخبرة محدودة بموضوع المخاطر السيبرانية والسلامة على الإنترنت، بالإضافة إلى أنهم لم يتلقَّوْا تدريبًا محددًا خلال تعليمهم الجامعي.

–أما عن قيام المعلمين بالتثقيف التوعوي عبر محو الأمية الرقمية؛ فغالبًا ما يكون أطفال المدارس أكثر خبرة رقمية من مدرسيهم بشأن الفضاء الإلكتروني، ومع ذلك لا يزالون بحاجة إلى إرشادات لتعليمهم كيفية استخدام مهاراتهم في مكان آمن.

– غالبًا ما لا يكون لدى المعلمين أدنى فكرة عما يفعله الأطفال في الفضاء الإلكتروني خارج المدرسة والمخاطر التي يواجهونها.

– قليلاً ما يعطي المعلمون التلاميذَ الإرشاداتِ) الحاسمة) للإنترنت حول كيفية البقاء بأمان أثناء التصفح.

–أما ما يتم تدريسه من تعليم السلامة عبر الإنترنت من خلال الكتب المدرسية يكون بشكل نظري بحت ولا يوفر للطالب أي خبرة عملية، كما لا يؤدي إلى تعرض كافٍ، علاوة على أنه غير مرتبط بالناحية الاجتماعية، وقد لا يغطي التهديدات الحديثة عبر الإنترنت مثل الخصوصية على الشبكات الاجتماعية والتسلط عبر الإنترنت والأخلاقيات الإلكترونية.

أما عن السؤال الثالث هل هناك ضرورة لإدارة المخاطر السيبرانية في المدارس الابتدائية؟ فقد أسفرت استجابات المفحوصين عن موافقة جميع أفراد العينة بنسبة ١٠٠٪؛ وقد أرجعوا ذلك إلى التأثير السلبي لتلك المخاطر على النسق التربوي والأكاديمي لتلاميذ المدارس الابتدائية.

كما أسفرت بعض استجابات المفحوصين على أنه لا يوجد لديهم فكرة تماماً عن بعض مفاهيم المخاطر السيبرانية والأمن السيبراني، علاوة على أن درجة تأهيل وتدريب منسوبي مؤسسات التعليم الابتدائي على مواجهة المخاطر منخفضة، وإن كان لديهم الاستعدادات العالية للتعلم والمشاركة.

كما حرصت الباحثة على إجراء دراسة استطلاعية أخرى بعض أسئلتها مفتوحة موجهة لعدد ٤٦٢ وليَ أمر لتلاميذ المدارس الابتدائية في محافظة بورسعيد للفصل الدراسي الثاني للعام الدراسي ٢٠٢٠- ٢٠٢١ ملحق (٢)؛ وتركت لهم حرية التعبير المطلق وتداعي الأفكار؛ لبيان المخاطر السيبرانية التي تواجه أبنائهم، والتي يمكن للمدارس الابتدائية أن يكون لها رور رئيس في إدارة تلك المخاطر، وبناء على تحليل استجابات المفحوصين أمكن الحصر المبدئي للمخاطر السيبرانية –التي تثير استياء وقلق أولياء الأمور– فيما يلي: التنمر الإلكتروني ومشاهدة عناصر غير لائقة وتعرض أبنائهم لمحاولات استمالة وإدمان الانترنت. وأعرب ١٩.٧٪ من عينة الدراسة أنهم قد أوقفوا أبناءهم تماما من الدخول على الانترنت؛ مما يدل على تعرض الأبناء لمخاطر سيبرانية كبيرة ومعرفة الآباء بذلك، وصرح ٥٣.٥ % من أفراد العينة أنهم بدءوا بالفعل بفرض بعض القيود على استخدام أبنائهم للانترنت، وأعرب ٢٦.٢٪ من أنهم يعانون صعوبة فرض قواعد على أبنائهم بعد سنوات الاستخدام، وأكد ٠.٦٪ أنهم يتيحون الانترنت بلا قيود.

إذاً جاءت نتائج الدراسات الاستطلاعية لتؤكد أهمية هذا المجال والحاجة لدراسته والاستفادة من الجهود البحثية لتفعيله بمدارس التعليم الابتدائي، كما أفادت جوانب قصور في إدارة المخاطر السيبرانية؛ واستناداً إلى ما سبق وفي ظل ذلك الاهتمام الدُوَلِي بإدارة المخاطر السيبرانية وبالاعتماد على الكثير من التقارير والتوصيات الأخيرة، وأيضًا من خلال الفحص الدقيق لأحدث البيانات؛ فإن الدراسة الحالية توفر تقييمًا مدروسًا لإيجاد الحلول العاجلة اللازمة للتخفيف من المخاطر السيبرانية الحالية، وتسعى إلى وضع إجراءات مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء الممارسات الدولية ذات الصلة في هذا المجال؛ بما يسهم في دعم قدرة هذه

المدارس في تحقيق أهدافها المنشودة، وتخفيف حدة المخاطر المتوقع حدوثها بها، وعليه تكون أسئلة الدراسة على النحو التالي:

أسئلة الدراسة:

- ما المخاطر السيبرانية التي تهدد الأمن التربوي والأكاديمي لتلاميذ المدارس الابتدائية؟
- ما الإطار الفكري لإدارة المخاطر السيبرانية في المدارس الابتدائية؟
- ما الممارسات الدولية لإدارة المخاطر السيبرانية في المدارس الابتدائية؟
- ما الواقع الميداني لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر بصفة عامة وفي بورسعيد بصفة خاصة؟
- ما الإجراءات المقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء الممارسات الدولية؟

أهداف الدراسة:

تهدف الدراسة إلى تعرف واقع إدارة المخاطر السيبرانية في المدارس الابتدائية بمصر، وكذا تقديم نظرة عامة على مجموعة مختارة من الممارسات الدولية التي يتم من خلالها إدارة المخاطر السيبرانية ذات التأثير السلبي على التربية والمجتمع والثقافة من خلال المدارس الابتدائية، فضلاً عن توفير العديد من الإجراءات في إطار إجراءات مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء تلك الممارسات الدولية.

أهمية الدراسة:

تتمثل أهمية الدراسة الحالية في الآتي:

أ-الأهمية النظرية:

-تأتي هذه الدراسة استجابةً للتوجهات العالمية في تعزيز ورفع درجة الوعي بإدارة المخاطر السيبرانية تحقيقاً للأمن السيبراني لدى تلاميذ المدارس الابتدائية ومن ثم تحقيق أهداف التعليم الابتدائي والحفاظ على سمعة مؤسساته وتميزها.

-كما قد تساعد هذه الدراسة مدارس التعليم الابتدائي في الحد من المخاطر السيبرانية والتي يمكن أن تُعَرَّض تلاميذ المدارس الابتدائية لكثير من الخسائر التربوية الكبيرة التي قد يصعب معالجة آثارها.

– تُبرز هذه الدراسة واقع إدارة المخاطر السيبرانية بمدارس التعليم الابتدائي؛ لذا يمكن أن تساعد نتائج هذه الدراسة في الحصول على فهم أفضل لكيفية إدارة المخاطر السيبرانية في المدارس الابتدائية بمصر.

–قد تكون الدراسة الحالية إضافة جديدة للبحوث التربوية والدراسات العربية النادرة في هذا المجال؛ فالدراسات التي تتناول إدارة المخاطر في التعليم ماتزال تحظى باهتمام ضئيل للغاية من قبل الباحثين، علاوة على أن البحوث المتعلقة بموضوع إدارة المخاطر السيبرانية في التعليم نادرة للغاية، ويمكن أن تعتبر هذه الدراسة تعويضاً للنقص الملحوظ في تبني ونشر ثقافة إدارة المخاطر السيبرانية بالمدارس الابتدائية.

–قد تكون الدراسة الحالية نواة لأبحاث مستقبلية تتبنى اتجاهات أكثر حداثة.

ب–الأهمية التطبيقية:

يمكن إيجاز الأهمية التطبيقية للدراسة في النقاط التالية:

–توجيه اهتمام القائمين على برامج (إعداد المعلم) في كليات التربية والأكاديمية المهنية للمعلمين على أهمية إدراج مفاهيم إدارة المخاطر السيبرانية ضمن تلك البرامج.

–قد تقدم نتائج الدراسة بعض الخطوط الإرشادية لواضعي السياسات التعليمية؛ إذ تؤدي إلى إعادة النظر في طبيعة أدوار ومهام المدير في عصر المعلوماتية، واتخاذ ما يلزم لإعداد وتأهيل المدير لمواجهة الثورة المعلوماتية المعاصرة.

–العمل على توجيه اهتمام الباحثين التربويين لتناول موضوع المخاطر السيبرانية، والذي لم يحظ بالاهتمام الكافي من قبل التربويين على الرغم من أهميته في عصر المعلوماتية.

–البحث في المخاطر سيوفر نظرة ثاقبة لمساعدة قادة المستقبل بمؤسسات التعليم على التخطيط لقراراتهم.

–تكمن أهمية البحث في أنه يتفق مع الرؤى العالمية الحديثة التي أصبحت تهتم باستشراف المخاطر واستباقها وتجنب وقوعها حتى لا تتفاقم فتضطر للتعامل مع أزمات يصعب إدارتها.

منهج الدراسة، وأدواتها:

طبقاً لطبيعة الدراسة الحالية فقد استخدمت الباحثة ما يلي:

المنهج الوصفي؛ وذلك لمناسبة هذا المنهج للدراسات التربوية فهو يفيد في تجميع المعلومات المطلوبة (لوفيل ولوسون، ١٩٨١، ٣)، كما أنه يتميز بكونه يهتم باستقصاء الأسباب التي تساعد الباحثة على فهم مشكلة الدراسة الحالية، فهو لا يقتصر على جمع البيانات، بل يتضمن قدراً من التفسير، وتحديد العلاقات والبيانات واستخراج الاستنتاجات ذات الدلالة بالنسبة لمشكلة الدراسة ومدى الحاجة لإحداث تغييرات جزئية أو أساسية فيه. (عبيدات، ٢٠٠٠، ٦٣) وعليه؛ فقد اعتمدت الدراسة هذا المنهج؛ حيث يقتضي تحليل الأدبيات الخاصة بإدارة المخاطر السيبرانية التي تهدد الأمن التربوي والأكاديمي لتلاميذ المدارس الابتدائية، واستقصاء مبررات التوجه الدولي لإدارتها، وكذا تحليل الممارسات الدولية لإدارة المخاطر السيبرانية في المدارس الابتدائية.

وتستخدم الدراسة من أساليب المنهج الوصفي ما يلي:

-أسلوب دراسة الحالة Case Study:

دراسة الحالة هي استفسار يحقق في ظاهرة معاصرة بعمق وضمن سياقها الواقعي(Payne, 2016, 8) ؛ فهو أحد الأساليب العلمية في دراسة إدارة المنظمات التعليمية، يهتم بالتحليل العميق للمشكلات بعد تقصي المعلومات عنها وتحليل وتقييم حقائقها، واستنباط الحلول المحتملة، ومن ثم اختيار الحل الأرجح لها والتخطيط لتنفيذه. (القريوتي، وزويلف ، ١٩٩٣، ١٠٨-١١٠) وعليه؛ فقد تناولت الباحثة المدارس الابتدائية بمحافظة بورسعيد فأحد مكامن قوة هذا الأسلوب هو تقريب الدارس من الواقع بشكل يعينهم على التفكير المنطقي والتحليل الناقد؛ مما يؤمل معه أن يؤدي ذلك إلى تطوير مداركهم؛ للوقوف على واقع إدارة المخاطر السيبرانية في المدارس الابتدائية بمحافظة بورسعيد.

أدوات الدراسة:

استخدمت الباحثة في هذه الدراسة الأدوات التالية:

-الاستبانة:

استخدمت الباحثة الاستبانة باعتبارها الوسيلة التي يمكن من خلالها الحصول على البيانات الخاصة بالدراسة، على النحو التالي:

– أعدت الباحثة استبانة استقصت فيه آراء عينة من مديري المدارس الابتدائية بمحافظة بورسعيد؛ للتعرف على واقع إدارة المخاطر السيبرانية في المدارس الابتدائية بمحافظة بورسعيد؛ تناولت فيه الباحثة مجموعة من العمليات والإجراءات التي استخلصتها من الدراسة النظرية، وقد تم تطبيقها على عينة عشوائية بلغت (٧٨) مديراً.

حدود الدراسة:

اقتصرت الدراسة الحالية على الحدود التالية:

أ–الحدود الموضوعية:

–اقتصرت الدراسة الحالية على إدارة (المخاطر السيبرانية) التي تقابل الأمن السيبراني cyber– safety وتشمل أربعة مخاطر سيبرانية هي: إدمان الانترنت، مشاهدة عناصر غير لائقة، التنمر الإلكتروني، الاستمالة؛ لكي يتوافق مع الدور التربوي لمؤسسات التعليم، وليس الأمن السيبراني cyber– security والذي يعني السلامة من قرصنة أجهزة الحاسوب في المدرسة؛ لسرقة بيانات المدرسة أو وصول التلاميذ إلى شبكات المدارس لتغيير درجاتهم أوحذفها؛ حيث أنه لا يتوافق مع طبيعة ودرجة الاستخدام التكنولوجي في المدارس المصرية.

–تبنت الباحثة خمس عمليات لإدارة المخاطر التزمت بها في إطارها النظري والميداني وإجراءاتها المقترحة، وهي: تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، الاستجابة للمخاطر، وتتبع المخاطر وتحديث إدارتها.

–واقتصرت الدراسة على المدارس (الابتدائية) الحكومية في محافظة بورسعيد بنوعيها عربي ولغات؛ لأهمية تلك المرحلة في الإعداد والتكوين بما يؤهلها أن تكون قاعدة قوية للمراحل الأعلى؛ وتوصية الدراسات عامة وبشكل خاص دراستيّ(Spiering, 2018) و(Saluja, Bansal, & Saluja, 2012) بأهمية التعرض المبكر للتوعية بالمخاطر والتهديدات السيبرانية بطريقة منظمة في التعلم التأسيسي للتلاميذ بالمدرسة الابتدائية؛ لتكون أهدافها الرئيسة غرس السلوك والأخلاق السيبرانية الصحيحة في التلاميذ؛ لتسهم في ضمان عادات صحية للاستخدام السيبراني بين جيل الألفية؛ فتم اختيار أطفال المدارس الابتدائية، الذين تتراوح أعمارهم بين ٧ و ١٢ عامًا لأن هذه هي الفئة العمرية التي يكون للأطفال الصغار عمومًا تجربتهم الأولى في الفضاء السيبراني، ففي دراسة

استقصائية دولية ثبت أن دمج التثقيف التوعوي لتعزيز الوعي الجنسي لأطفال المدارس الابتدائية من خلال تضمينه في المناهج كان فعالاً ، وهذا يتوافق مع توصية مجلس الأمن السيبراني لعام ٢٠١٥ بضرورة حصول الأطفال في التعليم الابتدائي على شهادة الكفاءة الرقمية؛ لتدعم الأطفال بالمهارات التي تمكنهم من التصرف بأمان في المجال الرقمي (Spiering, 2018, 22, 25)؛ وقد أشارت دراسة (مرعي، ٢٠١٣، ١٣٨) أن الطفل في المراحل العمرية المبكرة أكثر عرضة للتأثر بما يشاهده؛ حيث أن خياله أكثر خصوبة فيمزج الواقع بالخيال ويتشكل سلوكه على هذا الأساس، والمدارس هي القناة الأفضل لتعليم الأطفال ومحو الأمية الرقمية الحرجة لديهم لتعظيم الفرص وتقليل المخاطر.(Šimandl, 2015, 52)

ب–الحدود الزمنية:

تم تطبيق الدراسة الميدانية خلال الفصل الدراسي الثاني من العام الدراسي ٢٠٢١/٢٠٢٢.

ج–الحدود المكانية:

–انطلقت الدراسة الحالية من محافظة بورسعيد؛ وذلك لكونها محل معيشة الباحثة، وما يصاحب ذلك من المعايشة للوضع الحالي ورؤية أوجه القصور والمخاطر التي يتعرض لها طلاب المدارس، ولمس المشكلة وما يستلزمها من تطبيق نظم لإدارة تلك المخاطر السيبرانية بمدارسها.

مصطلحات الدراسة:

تعِّرف الدراسة المصطلحات المتعلقة على النحو التالي:

أ–المخاطر السيبرانية:

المخاطر (إجرائياً): مزيج مركب من احتمال تحقق الحدث ونتائجه، تؤدي للانحراف عن تحقيق الأهداف؛ وقد ينتج عنها أزمة لو لم يتم التصدي لها.

السيبراني: تشير المقاربة الإيتيمولوجية لكلمة "cyber" إلى أنها لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم ."governor" ، ومنذ أوائل العقد الأول من القرن الحادي والعشرين لم

يستخدم مصطلح سيبراني إلا للتعبير عن المصطلحات الأمنية كالجريمة السيبرانية.(Kurbalija, 2016, 14)

المخاطر السيبرانية (إجرائياً): تقابل الأمن السيبراني Cyber safety؛ ويقصد بها مخاطر تهدد الأمن التربوي والأكاديمي لتلاميذ المدارس الابتدائية؛ تنتج عن خلل في التزام التلاميذ بمعايير السلوك المناسب والمسئول عند استخدام التكنولوجيا الموصلة بالانترنت؛ فيما يتعلق بحماية ذاتهم وهويتهم ومعلوماتهم الشخصية، وتمييز المواقف الخطرة؛ بما يؤثر سلباً على تحقيق أهداف المدارس الابتدائية، وبما يطال في الأخير قيم المجتمع وأخلاقه.

مثل: إدمان التلاميذ لاستخدام الانترنت كالألعاب الإلكترونية، ومشاهدة عناصر غير لائقة، والتعرض للاستمالة عبر الانترنت من الغرباء ذوي الأغراض السيئة، والتنمر الإلكتروني.

ب–إدارة المخاطر السيبرانية في المدارس الابتدائية (إجرائياً): هي العمليات والأنشطة المنسقة التي تهدف إلى مساعدة المدارس الابتدائية على اتخاذ الإجراءات المسئولة بشأن جميع **المخاطر السيبرانية** بها؛ –تلك التي يتعرض لها تلاميذها نتيجة ضعف التزامهم بمعايير السلوك المسئول عند استخدام التكنولوجيا الموصلة بالانترت– فيتم معالجتها بالوقاية الاستباقية أو التخفيف من آثارها وبسبل الإدارة العلمية الأخرى.

ج–الممارسات الدولية (إجرائياً): ما تمارسه الدول، وما توصلت إليه المنظمات الدولية المتعلقة كاليونيسيف من إجراءات توجيهية وممارسات جيدة وإجراءات تمهيدية تساعد المدارس الابتدائية على إدارة المخاطر السيبرانية بها.

الدراسات السابقة:

من خلال استقراء الدراسات والبحوث لم تجد الباحثة أي دراسة تتناول إدارة المخاطر السيبرانية بشكل مباشر، وتم التعرف على عدة دراسات مرتبطة يمكن أن تستفيد منها الدراسة الحالية، وفيما يلي عرض موجز –من الأقدم للأحدث– لبعض هذه الدراسات العربية والأجنبية:

١-دراسة (أبو بكر، ٢٠١٧) بعنوان: تصور مقترح لمواجهة إدمان الألعاب الإلكترونية في المرحلة الابتدائية بالمملكة العربية السعودية في ضوء خبرتيّ كل من الولايات المتحدة الأمريكية وكوريا الجنوبية.

هدفت هذه الدراسة إلى وضع تصور مقترح لمواجهة ظاهرة إدمان الألعاب الإلكترونية في المرحلة الابتدائية بالمملكة العربية السعودية على ضوء خبرتيّ الولايات المتحدة الأمريكية وكوريا الجنوبية، وقد تم تطبيق استبانة موجهة لأولياء الأمور، والثانية لتلاميذ المرحلة الابتدائية في مدينة بريدة بمنطقة القصيم بالمملكة العربية السعودية؛ لمعرفة واقع إدمان هذه الألعاب الإلكترونية، وقد اختارت الباحثة عينة مكونة من ٢٠٠ تلميذ وتلميذة من المرحلة الابتدائية من مدينة بريدة ، وعدد ٢٠٠ من أولياء الأمور وتم الحصول على ٣٣ استبانة تم الإجابة عليها، وقد توصلت الدراسة إلى توصياتٍ أبرزها: العمل على تضافر الجهود لإبراز مكانة اللعب كوسيط تربوي بما يتوافق مع معايير الجودة العالمية، وتبني رؤية تربوية تواكب التطورات العلمية الحديثة في مجال اللعب، وألعاب الأطفال الإلكترونية، وتستشرف التطورات المستقبلية مع الحفاظ على الهوية الثقافية والاجتماعية للمجتمع السعودي، وطرح مبادرات مجتمعية لمعاونة المربين على فهم الألعاب المتاحة في الأسواق وتوظيفها بشكل إيجابي.

٢-دراسة (De Barros, M. J. Z., & Lazarek, H., 2018) بعنوان: نموذج أمان إلكتروني للمدارس في موزمبيق.

استهدفت الدراسة اقتراح نموذج أمان إلكتروني للمدارس الابتدائية والثانوية في موزمبيق لمعالجة الفجوة بين فرص ومخاطر الانترنت، وتعزيز ثقافة السلامة على الإنترنت بين الأطفال والشباب، واستخدمت الدراسة المنهج الوصفي بتحليل مبادرات السلامة الإلكترونية؛ استجابة للنقص الحالي في هذه المبادرات، وتوصلت الدراسة في نتائجها إلى نموذج يهدف إلى زيادة الوعي بالسلامة الإلكترونية وتعزيزه، وتنمية المهارات والمعرفة ومساعدة جيل شباب موزمبيق لتعزيز وغرس ثقافة الأمن السيبراني، ويتكون النموذج من بعض العناصر مثل دور الحكومة، التعاون الدولي، وموضوعات السلامة السيبرانية.

٣-دراسة (Spiering, M. A. 2018) بعنوان: تحسين السلامة على الإنترنت: تعليم الوعي في المدارس الابتدائية الهولندية.

استهدفت الدراسة التحقق من التحسينات التي يمكن إجراؤها لتعزيز تعليم الوعي بالسلامة على الإنترنت. واستخدمت المنهج الوصفي، واستخدمت طرق جمع البيانات التالية: دراسات الحالة والمقابلات والمسح. وكشف البحث في نتائجه أنه كلما زاد وصول الأطفال إلى الانترنت زادت فرص المخاطرة التي يواجهونها، وعند التركيز على الأطفال في سن المدرسة الابتدائية الهولندية: وجدت الدراسة أن ٣٦.١٪ من عينة الدراسة يمتلكون جهاز كمبيوتر شخصي خاص بهم، ٧،٧٪ لديهم إنترنت محمول، ١٤،٨٪ لديهم كمبيوتر ألعاب (غالبًا متصل بالإنترنت)، أيضا ٧١.٧٪ من الأطفال يمكنهم الوصول إلى الإنترنت دون إشراف الوالدين مما يشكل فرصًا ومخاطر إضافية. ومن العوامل التي ينبغي أخذها في الاعتبار الساعات التي يتم قضاؤها في الفضاء السيبراني: كما أشارت نتائج الدراسة أنه بالنسبة للأطفال من سن ٨ إلى ١٠ سنوات يكون عدد الساعات في المتوسط حوالي ساعة واحدة يوميًا، وتتضاعف للأطفال من سن ١٠ إلى ١٢ عامًا ويستمر في الارتفاع مع تقدم الأطفال في السن.

٤-دراسة (Zulkifli, Z., Molok, N. N. A., Abd Rahim, N. H., & Talib, S, 2020) بعنوان: التوعية بالأمن السيبراني بين تلاميذ المدارس الثانوية في ماليزيا.

تستهدف هذه الدراسة استكشاف مستوى فهم الأمن السيبراني والوعي بين تلاميذ المدارس الثانوية ومعلميهم وكذلك والديهم في ماليزيا، واستخدمت الدراسة المنهج الوصفي، وتم تصميم مجموعة استبيانات، تظهر النتائج أن معظم المستجيبين على دراية بالتهديدات السيبرانية ومخاطر التواجد في الفضاء السيبراني، لكن القليل منهم يتخذ إجراءات أمنية وقت الاتصال بالإنترنت، وأكدت الدراسة أنه إذا تم تجاهل المساحات غير المحدودة وغير المقيدة للانترنت لجميع مستويات الأعمار سيخلق المزيد من الجرائم السيبرانية الجديدة وغير المتوقعة بالإضافة إلى زيادة الموجودة، وأوصت الدراسة بالتعرض المبكر للفهم والتوعية بالمخاطر والتهديدات الأمنية، وأكدت أنها تسهم في ضمان عادات صحية للإنترنت بين جيل الألفية وبيئتهم في ماليزيا.

٥-دراسة (Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. 2020) بعنوان: التخطيط للأمن السيبراني في المدارس: العامل البشري.

تهدف الدراسة إلى التحقيق في التخفيف من مخاطر الأمن السيبراني بالمدرسة، واستخدمت الدراسة المنج الوصفي، وتوصلت الدراسة في نتائجها إلى أن مستخدمي الكمبيوتر غير المتعلمين في المدارس هم الحلقة الأضعف التي يستهدفها مجرمو الإنترنت باستخدام الهندسة الاجتماعية social engineering حيث يستخدم قراصنة الكمبيوتر تقنيات خادعة للتلاعب عمدًا بالأهداف البشرية، وتستخدم في المقام الأول لحث الضحايا على الكشف عن البيانات السرية؛ فيرسل المجرمون بريدًا إلكترونيًا يُزعم أنه من شخص أو منظمة أو شخص شرعي؛ ليُطلب من المستلم النقر فوق ارتباط وإدخال معلومات حساسة؛ ثم يختطف المجرم الإلكتروني هذا الحساب لسرقة ما يمكنهم، بالإضافة إلى أن هناك تقارير عن وصول التلاميذ إلى شبكات المدارس لتغيير درجاتهم أوحذفها.

تعقيب عام على الدراسات السابقة:

من خلال استقراء الدراسات العربية والأجنبية يمكن الخروج بعدد من المؤشرات التي قد تمثل نقطة انطلاق مهمة للبحث الراهن؛ وعليه يمكن إجمالها على النحو التالي:

- كلما زاد وصول الأطفال إلى الانترنت زادت فرص المخاطرة التي يواجهونها. (Spiering, M. A. 2018)

- إذا تم تجاهل المساحات غير المحدودة وغير المقيدة للانترنت لجميع مستويات الأعمار سيخلق المزيد من الجرائم السيبرانية الجديدة وغير المتوقعة. (Zulkifli, Z., Molok, N. N. A., Abd Rahim, N. H., & Talib, S, 2020)

- أهمية التركيز على ضرورة معالجة الفجوة بين الفرص والمخاطر السيبرانية، وتعزيز ثقافة السلامة على الإنترنت بين الأطفال، بل بتحويل تلك المخاطر إلى فرص تعلم لصالح الطفل (أبو بكر، ٢٠١٧) De Barros, M. J. Z., & Lazarek, H., (2018)؛ فقد أوصت دراسة (أبو بكر، ٢٠١٧) بتوظيف الألعاب الإلكترونية كفرصة للتعلم بشكل إيجابي كوسيط تربوي بما يتوافق مع معايير الجودة العالمية.

-أهمية التعرض المبكر للفهم والتوعية بالمخاطر والتهديدات السيبرانية بطريقة منظمة؛ بدمج هذا التعليم في التعلم التأسيسي للتلاميذ في المدرسة الابتدائية؛ لتكون أهدافها الرئيسية غرس السلوك والأخلاق السيبرانية الصحيحة في التلاميذ؛ لتسهم في ضمان عادات صحية للإنترنت بين جيل الألفية.(Spiering, M. A. 2018)

-اتفاق الدراسات جميعها على مدى أهمية إدارة المخاطر السيبرانية في المدارس تحقيقاً للسلامة عبر الانترنت؛ إلا أن أيًّا من تلك الدراسات لم يتعرض لآليات إدارة المخاطر السيبرانية، كما لم تتناول أيٌّ من الدراسات الممارسات الدولية في هذا الصدد.

واستفادت الدراسة الحالية أيضاً من دراسة (Saluja, S. Bansal, D. & Saluja, S., 2012) في إدراك أهمية توعية التلاميذ بما هو قانوني وما هو ليس كذلك، وإعلامهم بتداعيات أفعالهم، ووقوفهم على دراسات الحالة لأمثلة سابقة أدت الأخلاق السيبرانية إلى إلحاق الضرر على الطالب، كما أكدت على أهمية الحفاظ على تحديث المناهج الدراسية بشكل منتظم بناءً على التعليقات الواردة وعلى أساس دوري مع تغير التهديدات وتعليم السلامة عبر الإنترنت تتطور المتطلبات مع مرور الوقت، كما ساعدت دراسة (Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. 2020) الباحثة على تمييز الأمن السيبراني cyber- safety الذي هو مجال اهتمام الدراسة بالأمن السيبراني cyber- security والذي يعني قرصنة أجهزة الحاسوب في المدرسة باستخدام الهندسة الاجتماعية social engineering من خلال استهداف مستخدمي الكمبيوتر غير المتعلمين؛ لسرقة بيانات المدرسة أو وصول التلاميذ إلى شبكات المدارس لتغيير درجاتهم أوحذفها.

وبصفة عامة قد أفادت الدراسات السابقة -على تنوعها واختلاف نتائجها- الدراسة الحالية في التأكيد على أهمية الدراسة الحالية، وفي الاستدلال على جوانب التركيز العالمي في إدارة المخاطر السيبرانية في المدارس الابتدائية، وتحديد وعرض مشكلة الدراسة الحالية، وتشكيل الإطار النظري، والإلمام بالمنهجية المستخدمة، وتختلف الدراسة الحالية عن الدراسات المعروضة في هدفها العام؛ فالدراسة الحالية بصدد التوصل لإجراءاتٍ مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء بعض الممارسات الدولية.

وعليه تسير الدراسة وفق المحاور التالية:

المحور الأول: الإطار العام للدراسة ويتضمن تحديد المشكلة والأهداف والمنهجية وتحديد المصطلحات والدراسات السابقة والتعقيب عليها.

المحور الثاني: الإطار النظري ويتضمن المخاطر السيبرانية التي تهدد الأمن التربوي والأكاديمي لتلاميذ المدارس الابتدائية مع توضيح الإطار الفكري لإدارة المخاطر السيبرانية في المدارس الابتدائية.

المحور الثالث: ويتضمن الممارسات الدولية لإدارة المخاطر السيبرانية في المدارس الابتدائية.

المحور الرابع: ويتضمن الواقع الميداني لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر بشكل عام وبورسعيد بشكل خاص.

المحور الخامس: ويتضمن الإجراءات المقترحة التي يمكن اتباعها لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء الممارسات الدولية.

شكل (١) التقسيمات الفرعية للإطار النظري.

المحور الثاني: الأسس النظرية لإدارة المخاطر السيبرانية في المدارس الابتدائية.

يستخدم هذا الجزء لتكوين نظرة ثاقبة عن طبيعة المخاطر السيبرانية التي يتعرض لها تلاميذ المدارس الابتدائية، وإدارة مخاطرها، ومراجعة الأدبيات التي تحقق في الوضع الحالي فيما يتعلق بنضج أمان الإنترنت داخل البيئات المدرسية.

أما عن مسؤولية مدارس التعليم قبل الجامعي عن إدارة المخاطر السيبرانية؛ فمنذ ظهور الفضاء الإلكتروني، زاد عدد مستخدمي الانترنت بشكل كبير إلى أن وصل عددهم ٤.٦٦ مليار مستخدم حول العالم، (وتحديداً ٥٩.٩٪) –أي أكثر من نصف سكان العالم البالغ عددهم ٧.٨٣ مليار نسمة– بزيادة قدرها ٣١٦ مليون (٧.٣٪) عن العام الماضي (٢٠٢٠). (Kemp, 2021, 8-9) فبينما ينظر الأطفال والكبار إلى العديد من الأنشطة عبر الانترنت بعبارات إيجابية، إلا أن تلك الفرص عبر الإنترنت – في حد ذاتها– محفوفة بالمخاطر؛ على سبيل المثال: إضافة أشخاص جدد إلى جهات اتصال الطفل، قد تكون طريقة رائعة لتكوين صداقات جديدة ، ولكن يمكنها أيضًا أن تجعل الأطفال على اتصال مع غرباء يحتمل أن يكونوا مسيئين. (Livingstone, Davidson, Bryce, Batool, Haughton & Nandi, 2017, 15).

فانفتح مستخدمو الإنترنت على المخاطر المتعلقة به، في وقتٍ يتم فيه استخدام الإنترنت على نطاق واسع كأداة تعليمية في المدارس، ومع ذلك كان ذلك الاستخدام مصحوبًا بفهم ضعيف للقضايا الأخلاقية، ونقص في الوعي، وقلة وجود سياسات تجعله يتماشى مع الأهداف التربوية العالمية، (Payne, 2016, 6) كما أن هذه المخاطر الأخلاقية تهدد وظائف مهمة للمدارس كضمان سلامة التلاميذ وتقديم تعليم عالي الجودة.(Schubart, 2021, 7)؛ فمتعلمو المدارس (الأطفال) من جميع الأعمار هم مستخدمو التكنولوجيا الأكثر عرضة للمخاطر السيبرانية؛ فغالبًا ما يُنظر إلى المتعلمين في المدارس على أنهم أهداف سهلة ومعرضة لمخاطر استغلال مجرمي الإنترنت.(Kritzinger, 2020, 2– 3)

وبالنظر إلى أن المدرسة إلزامية في غالبية الدول، صارت المدرسة خياراً ممتازاً كواحدة من أفضل الأماكن التي يتم توفيرها للتدريب على التوعية السيبرانية. (Kritzinger, Bada & Nurse, 2017, 2)

ومن هنا كان لا بد أن تضع المدارس الوطنية في الاعتبار أنه بزيادة وصول التلاميذ إلى الأجهزة المحمولة قد تزداد فرص التسلط عبر الإنترنت (Nye, 2014, 39)، وكان لابد للمدرسة من إدارة تلك المخاطر؛ فالتأثير الاجتماعي للإنترنت –وخاصة بالنسبة للقصر– هي قضية تهم المجتمع بشكل كبير، وهذا هو الدور الاجتماعي للمدرسة. (Lim, 2012, 2)

ولما كانت المدرسة مركز اتصال مجموعة كاملة من قيم وتطلعات المجتمع بل وتحدد القيم التي تتجاوز المجتمع، ولما كان النظام المدرسي لديه التزام أخلاقي وقانوني لخلق بيئة آمنة للتلاميذ والمعلمين والموظفين؛ كان لابد أن تتحمل المدرسة مسؤولية تعليم التلاميذ حدود السلوك المقبول اجتماعياً بهذا الصدد؛ لذا يحق للمدارس وضع قيود على أي شكل من أشكال تعبيرات التلاميذ وانتهاك حقوق التلاميذ الآخرين (White, 2013, 36, 39) فتقع مسؤولية تعليم هذا النوع من تعليم الشخصية في المواطنة الرقمية على عاتق المدارس (Payne, 2016, 12) وعليها ضمان الإجراءات اللازمة لتعزيز الوقاية من مخاطر الاضطرابات والتسلط عبر الإنترنت.(Lopez–Fernandez & Kuss, 2020, 13) ليتأتى دور قادة التعليم في التأكد من أن جميع التلاميذ لديهم

معلمين مهرة يستخدمون التكنولوجيا بنشاط لتلبية احتياجات تعلمهم، وضمان وصول جميع التلاميذ إلى التكنولوجيا بما تمثله من فرص تعلم حقيقية وجذابة، وأن يمثلوا نموذجا للمواطنة الرقمية من خلال التقييم النقدي للموارد عبر الإنترنت، والانخراط في الخطاب المدني عبر الإنترنت واستخدام الأدوات الرقمية للمساهمة في التغيير الاجتماعي الإيجابي، وتنمية السلوك المسؤول عبر الإنترنت، بما في ذلك السلوك الآمن والأخلاقي والقانوني عند استخدام التكنولوجيا.(Schubart, 2021, 6).

أولاً: إدارة المخاطر السيبرانية (المفهوم ، العمليات، التصنيفات).

تحظى إدارة المخاطر في المنظمات المعاصرة بشكل عام وفي المجال التربوي بشكل خاص بأهمية كبيرة في الوقت الحاضر، وتشكل توجهاً إدارياً جديداً؛ من أجل الاستفادة منها في توفير الحماية اللازمة للمنظمات وضمان استمرارها لأداء نشاطها بكفاءة عالية. (المخلفي، ٢٠١٩، ٢٠) كما تعد أنشطة الجرائم السيبرانية أكبر تحد سيواجهه المستخدمون الإلكترونيون في المستقبل، في عام ٢٠١٧، تأثر ٩٧٨ مليون مستخدم سلباً بجرائم الإنترنت؛ مما يستلزم أن يكون لكل دولة نهج شامل للتوعية بالسلامة الإلكترونية لضمان حصول جميع مستخدمي الإنترنت داخل بلدهم على الوعي والمعرفة والمهارات في الفضاء السيبراني(Kritzinger, 2020, 4)

أ–مفهوم المخاطر السيبرانية:

١– التعريفات النوعية الشاملة للمخاطر:

تعددت تعريفات المخاطر تبعاً لتنوع الخلفيات النظرية والإدارية للباحثين؛ وتعدد المعايير والأطراف الدولية الخاصة بالمخاطر، ويمكن أن نعرض ذلك فيما يلي:

– يعرّف المعيار الدولي لإدارة المخاطر (ISO 31000: 2018) المخاطر بأنها "تأثير عدم اليقين على الأهداف.(THE UNIVERSITY OF LEEDS, 2019, 1)

عرّف هوبكين الخطر على أنه حدث له القدرة على التأثير (تثبيط / إعاقة ، تعزيز أو سبب شك / عدم يقين) في المهمة، الإستراتيجية ، المشاريع ، العمليات الروتينية ، الأهداف ، العمليات الأساسية وتحقيق توقعات أصحاب المصلحة، ويقدّر إطار عمل هوبكين أن التعلم عن طريق كل المعنيين هو حجر الزاوية لإدارة المخاطر والنمو التنظيمي.(Hopkin, 2012, 8)

يتم تعريف المخاطر على أنها احتمالية نشوء تأثير سلبي مقترن بقدر تأثيره، فتتكون إدارة المخاطر من تنفيذ مجموعة من التدابير والإجراءات والقرارات لتخفيف تلك المخاطر .(Bica, & Petruta, 2021, 2).

-تعني كلمة خطر في قاموس إكسفورد Risk إمكانية حدوث شيء غير مرغوب فيه في المستقبل.

وحسب معهد المدققين الداخليين الأمريكي فإن الخطر: ربط احتمال وقوع حدث بتأثيره على تحقيق الأهداف. (قارة عشرة وحبار، ٢٠٢٠، ٣٤٧)

-بحسب قاموس Webster المخاطر: إمكانية التعرض للخسارة.

- احتمال أو تهديد بحدوث ضرر أو إصابة أو أحداث سلبية ناتجة عن عوامل ضعف داخلية أو خارجية، والتي من الممكن أن يتم تجنبها من خلال إجراءات وقائية.

-حالة الخوف من تحقق ظاهرة أو موقف معين بالنظر لما قد يترتب عليه من نتائج ضارة.

(الحراحشة، ٢٠١٩، ١٠)

-احتمال وقوع حادث مؤسف أو خسارة أو إمكانية تحقيق عواقب سلبية غير مرغوب فيها من الحدث.(Aven, 2016, 4)

-الاقتراب من الهلاك، والإشراف على الهلاك، أو احتمالات التعرض للخسارة. (إبراهيم، ٢٠١٩، ٢٥٧)

-مشكلة واردة الحدوث، لو لم يتم التصدي لها سوف ينتج عنها أزمة. (إبراهيم، ٢٠١٩، ٢٦٤)

-موقف ينطوي على احتمال حدوث ضرر. (الخياط، ٢٠١٩، ٣٣٠)

- مزيج مركب من احتمال تحقق الحدث ونتائجه.

-الربط بين احتمال وقوع الحدث والآثار المترتبة على حدوثه.

-احتمالية وقوع حادث مستقبلاً قد يُحْدِث ضرراً.

-إمكانية حدوث انحراف في المستقبل بحيث تختلف النواتج المرغوب في تحقيقها عما هو متوقع.

-الآثار غير المواتية الناشئة عن أحداث مستقبلية متوقعة أو غير متوقعة. (العياشي، ٢٠١٦، ٢٢)

-الخطر: التغيير المجهول في القيمة المستقبلية للنظام، وتعرفه منظمة المعايير في أستراليا بأنه: فرصة حدوث شيء سيكون له تأثير على الأهداف.

-انحراف سلبي عن المتوقع.

ومن خصائصه: يكون نتيجة حادث غير متوقع، عدم التأكد، يكون في المستقبل ويُحْدِث تغييرا ما. (المدرع، ٢٠١٩، ٦٧)

- احتمال وقوع حادث مضاعفاً بالتأثير أو العواقب عند وقوعه، وهناك العديد من الخيارات للاختيار فيما يتعلق بمعالجة المخاطر:

-الاحتفاظ: قبول المخاطر كما هي، والتكاليف والجهود لا تفوق مكاسب المخاطر.

-تعديل المخاطر: تطبيق علاجات لتقليل المخاطر إلى مستوى مقبول.

-المشاركة: تحويل المخاطر إلى طرف آخر، مثل تأمين المخاطر (Spiering, 2018, 10)

٢- الفرق بين مصطلحات: سيبراني وإلكتروني ورقمي وافتراضي:

تستخدم البادئات e- / digital / virtual / cyber لوصف تكنولوجيا المعلومات والاتصالات؛ وتستخدم البادئة e في الجوانب التجارية، أما البادئة cyber فتستخدم في جوانب الجريمة والأمن، وتستخدم البادئة virtual للعملات الافتراضية مثل البيتكوين، وتستخدم البادئة digital من أجل التنمية فتُستخدم لوصف الدبلوماسية (الرقمية) في بريطانيا العظمى؛ ودليل على استخدامها في السياق التنموي: استخدام جان كلود يونكر، رئيس المفوضية الأوروبية، البادئة (digital) ١٠ مرات في خطابه الأول في البرلمان الأوروبي؛ حين قدم خطة السياسة لفترة ولاية مدتها خمس سنوات.

وتشير المقاربة الإيتيمولوجية لكلمة "cyber" إلى أنها لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم ."governor" من خلال كتاب عالِم الانترنت نوربرت وينر المسمى (علم التحكم الذاتي Cybernetics)، وفي عام ١٩٨٤ ابتكر ويليام جيبسون كلمة ("cyber"

الفضاء) في رواية الخيال العلمي نيورومانسر، وفي أواخر التسعينيات، أطلق لفظ سيبراني على كل ما يتعلق بالانترنت: المجتمع السيبراني، والقانون السيبراني، والجنس السيبراني، والجرائم السيبرانية، والثقافة السيبرانية حتى أوائل العقد الأول من القرن الحادي والعشرين؛ فاختفى الاستخدام الواسع للسيبراني بشكل تدريجي، ولم يستخدم منذ ذلك الحين إلا للتعبير عن المصطلحات الأمنية. وبذلك تم استخدام (سيبراني) لتسمية اتفاقية الجرائم السيبرانية لمجلس أوروبا لعام ٢٠٠١؛ وهي لا تزال المعاهدة الدولية الوحيدة في مجال أمن الإنترنت، فاليوم هناك استراتيجية الفضاء السيبراني للولايات المتحدة الأمريكية، وجدول أعمال الأمن السيبراني العالمي للاتحاد الدولي للاتصالات، وسياسة منظمة حلف الأطلسي (الناتو) بشأن الدفاع السيبراني، ومركز تميز الدفاع السيبراني الإستوني.(Kurbalija, 2016, 14)

٣- مفهوم المخاطر السيبرانية:

في البداية يتم أخذ منظور واسع للمخاطر التي يتعرض لها الأطفال في الفضاء السيبراني ثم تستكشف الدراسة التعريف الواسع للمخاطر السيبرانية، متبوعًا بتعريف أكثر تحديدًا بشكل إجرائي للمخاطر السيبرانية:

(أ) المخاطر السيبرانية: أي مخاطر تتعلق بالخسارة المالية أو الاضطراب أو الإضرار بسمعة منظمة بسبب شكل من أشكال فشل نظام تكنولوجيا المعلومات الخاص بها، تشمل مكونات المخاطر السيبرانية التهديدات الحالية ونقاط الضعف والقيم المعرضة للخطر (الأصول والسمعة والاستجابات)، أما الأمن السيبراني :القدرة على الحماية عند استخدام الفضاء الإلكتروني. (Moulton, 2021, 20)

وقد عرفت الهيئة الوطنية للأمن السيبراني عام ٢٠١٨ المخاطر السيبرانية بأنها: المخاطر التي تمس أصول المؤسسة وأفرادها وعملياتها والرؤية والرسالة والسمعة بسبب خلل في استخدام المعلومات أو بسبب الوصول غير المصرح لها بما يطال قيم المجتمع ودينه وأخلاقه والبنى التحتية. (حريري والمنتشري، ٢٠٢٠، ١٠٨)

(ب) التعاريف والمفاهيم المتطورة للأمن السيبراني وأمن المعلومات:

وفقًا لوزارة الدفاع الأمريكية United States Department of Defense (DoD)، فإن الفضاء الإلكتروني هو "شبكة متوافقة من البنى التحتية لتكنولوجيا

المعلومات، بما في ذلك الإنترنت وشبكات الاتصالات وأنظمة الكمبيوتر والمعالجات ووحدات التحكم المضمنة، والمحتوى الذي يتدفق عبر ومن خلال هذه المكونات، ويتم تقسيمها إلى ثلاث طبقات محددة: الشبكة المادية، الشبكة المنطقية، والطبقة الاجتماعية أو الشخصية الإلكترونية (Gioe, Goodman & Wanless, 2019, 5)

وهناك فئتان من الأمن السيبراني:

الفئة الأولى: الأمن السيبراني Cyber safety، والتي تركز على الأشخاص، وقدرة التلاميذ على البقاء آمنين عبر الإنترنت، وحماية هويتهم ومعلوماتهم الشخصية، بالإضافة إلى تعلم تمييز المواقف الخطرة والسلوكيات عبر الإنترنت، ومخاطرها هي محل الدراسة الحالية، ويعرف أيضاً بأنه الاستخدام الآمن والمسؤول لتقنيات المعلومات والاتصالات، بما في ذلك الحماية من التسويق والإعلان غير المرغوب فيه، وتعلم الجوانب السلوكية الإيجابية والسلبية لتكنولوجيا المعلومات والاتصالات، والحماية ضد الأفراد الذين يديرون مواقع ويب، أو يحاولون الاتصال بالأطفال عبر الإنترنت، أو ينظمون اجتماعات بدون إشراف مسئولي رعاية الأطفال.(Payne, 2016, 23-24)

والفئة الثانية: الأمن السيبرانيCyber Security: وهي الإجراءات المسؤولة المتعلقة بالحماية المادية للأجهزة والأنظمة والأشياء مثل الشبكات وأجهزة الكمبيوتر والتطبيقات السحابية والبيانات من الهجمات والقرصنة الإلكترونية، (Payne, 2016, 23-24) ، والتدابير المتخذة لحماية جهاز كمبيوتر أو الشبكة من الوصول غير المصرح به للحفاظ على سلامة المعلومات المخزنة (Richardson, Lemoine, Stephens, & Waller, 2020, 24) وكذا تأمين الأنظمة والبرامج (Vallor & Rewak, 2018, 4) ومثال عليها وقوع العديد من حالات الانتهاك السيبراني في الولايات المتحدة الأمريكية؛ حيث شهدت العديد من المدارس الأمريكية حالات قرصنة واستيلاء على المعلومات الشخصية لآلاف الطلبة والمعلمين والإداريين العاملين في تلك المدارس، ويمكن تعريف الأمن السيبراني بأنه:-جميع الأدوات والسياسات والضمانات الأمنية والمبادئ التوجيهية ومداخل إدارة المخاطر وأفضل الإجراءات والتقنيات التي يمكن استخدامها لتنظيم الأصول المعلوماتية للمستخدم في الفضاء السيبراني. (حريري

والمنتشري، ٢٠٢٠، ١١٠-١١٣) إذن يتعامل الأمان عبر الإنترنت محل الدراسة مع النوع الاجتماعي أكثر مما يتعلق بالقرصنة والملاحقين، والمحتالين عبر الإنترنت.

ويعرَّف الأمن السيبراني وفقاً للفئة الثانية على أنه" :الحفاظ على السرية والنزاهة والتوافر (CIA) للمعلومات في الفضاء السيبراني، كما يعرَّف بأنه " القدرة على حماية أو الدفاع عن استخدام الفضاء الإلكتروني من الهجمات عبر الإنترنت.(Payne, 2016, 23-24)

ومن أبرز تعريفات الأمن السيبراني أنه نشاط يؤَمِّن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانيات الحد من الخسائر والأضرار؛ فيتيح إعادة الوضع إلى ما كان عليه؛ بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة. (المنتشري، ٢٠٢٠، ٤٦٢) فتتضمن إدارة الهجمات السيبرانية عادةً (١) إزالة مصدر التهديد؛ (٢) معالجة نقاط الضعف في النظام؛ و(٣) تقليل التأثيرات من خلال تخفيف الضرر واستعادة الوظائف، ومع ذلك تستغرق هذه العمليات وقتًا وعمالة مكثفة، وغالبًا ما تحدث بعد حدوث اختراق(Richardson, Lemoine, Stephens, & Waller, 2020, 26)

ب- إدارة المخاطر السيبرانية.

إن إدارة المخاطر جزء أساسي من الإدارة الإستراتيجية لأي منظمة؛ تساعد على تحديد مجموعة من أنواع الأحداث المختلفة والنظر فيها وتأثيرها، وتعد المخاطر السيبرانية ومخاطر إدارة البيانات ومخاطر الخصوصية من المخاطر الآخذة في الظهور في العصر الحالي. (Jemeljanenko, 2019, 7-8) وبالتالي، عندما تتم إدارة هذه الأحداث بشكل غير فعال، يمكن أن تؤدي إلى عدم تحقيق للاستراتيجيات والأهداف التشغيلية للمؤسسة.(Sityata, Botha & Dubihlela, 2021, 2)

١- مفهوم إدارة المخاطر ، ونشأتها:

لمفهوم تقييمات المخاطر والمخاطر تاريخ طويل منذ أكثر من ٢٤٠٠ عاماً، فقد عرض الأثينيون قدراتهم على تقييم المخاطر قبل اتخاذ القرارات، ومع ذلك فإن تقييم وإدارة المخاطر -كمجال علمي حديث العهد- لا يزيد عمره عن ٣٠-٤٠ سنة Aven, (2016, 1) وتعود جذور المحاولات العلمية لقياس المخاطر إلى القرن السابع عشر

عندما اكتشف عالم الرياضيات باسكال نظرية الاحتمالات وهو يحاول حل لغز المقامرة، ثم قانون الأعداد الكبيرة الذي مكن من استخدام المعلومات المتوفرة عن الأمس لتوقع ما سيحدث بالغد، وكتاب فن التخمين لعالم الرياضيات جاكوب برلوني عام ١٧١٣، وأثبتت كتاباته ضرورة استخدام الماضي كمؤشر لاحتمالية وقوع أحداث مستقبلية، (قارة عشرة وحبار، ٢٠٢٠، ٣٤٧) كما أرجع البعض فكرة تحليل ودراسة المخاطر بعد الحريق الذي نشب في مركبة الفضاء الأمريكية أبولّو في مطلع العام ١٩٦٧ وأودى بحياة رواد الفضاء على متنه؛ فبعد هذه الحادثة تم تشكيل هيئة وظيفتها العمل على إيجاد معايير السلامة لرواد الفضاء؛ بحيث يكون نسبة الأمان في كل الرحلات ما فوق ٩٥٪. (النجار والفرا، ٢٠١٩، ٩)

وفي الآونة الأخيرة بدأ الاهتمام يتزايد بمجال إدارة المخاطر باستخدام مناهج ومفاهيم واستراتيجيات تسلم بأن تطوير أي مؤسسة يتوقف بقدر كبير على القدرة على استشراف المخاطر والتحسب لها، ووضع مجموعة من الإجراءات الاحترازية والعلاجية المناسبة لها، وهذا يفسر ما نلاحظه من الاهتمام الشديد بوضع استراتيجيات توقع المخاطر في النظم التعليمية والتنبؤ بالمشكلات المحتملة. (إبراهيم، ٢٠١٩، ٢٥٧)

أما مفهوم إدارة المخاطر فقد تطور بحيث انتقل من التركيز على الحوادث والكوارث ومعالجة آثارها إلى التنبؤ بها والحماية منها، ثم انتقل إلى ما هو أبعد من ذلك، وهو التعامل معها كفرص يمكن أن يكون منها نتائج إيجابية تُستغل لتحقيق مكاسب. (المدرع، ٢٠١٩، ٧٠) **ويمكن ملاحظة ذلك من التعريفات التالية لإدارة المخاطر:**

-عملية تقييم للمخاطر، وتطوير إستراتيجيات لإدارتها.

-العمليات التي تتضمن أسلوب للتحكم ومعالجة بالمخاطر بعد تحليلها وتحديدها سواء كانت مخاطر من داخل أو خارج المنظمة، سواء تواجه الأفراد والمؤسسات والدولة، في محاولة لتجاوز الخسارة المترتبة على حدوث المخاطر في أدنى حدودها، والاستفادة من الإيجابيات في الأمد البعيد. (المدرع، ٢٠١٩، ٦٩)

-خطوة استباقية ومقاربة منهجية للتحكم في المخاطر من خلال التعرف على تلك الأخطار وتحليلها وتفسيرها لمحاولة التقليل من آثارها أو منع حدوثها.

-النشاط الإداري الذي يهدف إلى التحكم بالمخاطر وتخفيضها إلى مستويات مقبولة. (المخلفي، ٢٠١٩، ٢١-٢٣)

-عملية تحديد وتقييم ومراقبة التهديدات التي تتعرض لها المؤسسة وتنال من رصيدها السوقي بين المنافسين وتؤثر على رأس مالها.

-عملية لتحديد المخاطر وتقييمها للتعرف على مدى شدتها وأثرها على المشروع، ووضع الاستراتيجية المناسبة لتقليل الخسائر الناجمة عنها. (الخياط، ٢٠١٩،٣٣٠، ٣٣٥)

-الوسائل المنظمة لتحديد وقياس المخاطر مع تطوير واختيار وإدارة الخيارات الملائمة للتعامل معها.

-توقع أحداث مستقبلية تؤدي إلى تأثيرات غير ملائمة. (العياشي، ٢٠١٦، ٢٤)

-مجموعة من الإجراءات التي تهدف لحماية الأفراد والأصول(قارة عشرة وحبار، ٢٠٢٠، ٣٤٧)

-التوصل إلى وسائل متجددة للتحكم في الخطر، والحد من تكرار وقوع حوادثه، والتقليل من حجم الخسائر التي تترتب على ذلك، مما يترتب عليه تخفيض درجة الخطر، عن طريق تقدير ناجح لتحقق الظاهرة مقدماً، ثم اتخاذ الوسائل التي تفي بمجابهة الخسائر المتوقعة منها.

-عملية ديناميكية منظمة مستمرة تهدف للحد من وقوع المخاطر والتعامل معها بأكبر قدر من الفعالية الكفاءة بما يضمن تحقيق الأهداف المنشودة. (الحراحشة، ٢٠١٩، ١٠)

-مدخل علمي للتعامل مع المخاطر بتحديد الخسائر المحتملة، وتقسيم وتطبيق الإجراءات التي تقلل حصول الخسارة أو تأثير الخسارة.

-عملية اختيار نظامية لطرائق ذات تكلفة فعالة من أجل التقليل من أثر تهديد معين على المنظمة، وهي عملية قياس وتقييم المخاطر، وتطوير إستراتيجيات لإدارة تبعاتها. (الريح، ٢٠١٩، ٤٤)

-الطريقة التي تم بها إدارة الأثر الضار للمخاطر وتحقيق الفرص المحتملة منها.

- نهج مؤسسي موضوعي موجه نحو تحديد أفضل الطرق للتحكم بالتهديدات التي تواجه أمان المؤسسة. (النجار والفرا، ٢٠١٩، ١٩)

ويمكن إجمال التعريفات الأولية لإدارة المخاطر في الجدول التالي:

جدول (١) تعريفات إدارة المخاطر وفقا للمؤسسات المتخصصة.

المصدر: (Hopkin, 2018, 37)

المنظمة	تعريف إدارة المخاطر
دليل ISO 73 BS 31100	أنشطة منسقة لتوجيه ومراقبة المنظمة فيما يتعلق بالمخاطر.
معهد إدارة المخاطر (IRM)	العملية التي تهدف إلى مساعدة المنظمات على فهم، وتقييم واتخاذ إجراءات بشأن جميع المخاطر؛ بهدف زيادة احتمالية النجاح وتقليل احتمال الفشل.
HM Treasury	جميع العمليات المتضمنة تحديد وتقييم والحكم على المخاطر، وتحديد الملكية، واتخاذ الإجراءات اللازمة للتخفيف أو توقعها وتقديم المراقبة والمراجعة.
كلية لندن للاقتصاد	اختيار تلك المخاطر التي يجب أن تتخذها المؤسسة وتلك التي ينبغي تجنبها أو التخفيف من حدتها، يليها العمل لتجنب أو تقليل المخاطر.
معهد استمرارية الأعمال	الثقافة والعمليات والهياكل التي يتم وضعها لإدارة الفرص المحتملة والتأثيرات السلبية بشكل فعال.

وقد استرعى مجال إدارة المخاطر انتباه قيادات المنظمات الصناعية والاقتصادية وكان لها السبق في ذلك، حيث انتهجته كثير منها في أواخر الثمانينيات من القرن الماضي خصوصاً بعد الإخفاقات والخسائر الكبيرة التي حدثت، وكان على إثرها إقرار كثير من الإجراءات للتخفيف أو نقل أو معالجة آثار هذه المخاطر، ثم أعقبه إصدار إرشادات لإدارة المخاطر من بعض المعاهد والهيئات في المجال، ثم كانت المطالبة للمنظمات بتقديم تقارير حول كيفية تحديد المخاطر بها وتحملها وإدارتها والمساءلة حولها، حتى نشأ مفهوم إدارة المخاطر، وأصبح هناك قناعة بأهمية إدارة المخاطر، وأنها ليست طبقة بيروقراطية جديدة، وأصبحت متكاملة مع جميع عمليات التخطيط والإدارة؛ لتتخطى إدارة المخاطر مخاطر المجالات المالية بالمنظمات؛ لتشمل

جميع المنظمات ومجالات ومستويات العمل فيها، وبذلك ترتبط إدارة المخاطر في المنظمات بالحوكمة المؤسسية والأهداف الإستراتيجية والتشغيلية؛ حيث اعتبرت أفضل ممارسة إدارية لجميع المؤسسات الحكومية والخاصة منها.(المدرع، ٢٠١٩، ٥٦- ٥٧)

وقد تم تشكيل بعض المنظمات لتطوير أطر إدارة المخاطر، ولتوفير نهج موحد لإدارة المخاطر؛ فأصبح هناك العديد من أطر إدارة المخاطر (ERM)، مثل لجنة الرعاية المنظمات المعروفة باسم إطار COSO ERM (Compliance Risk Management) المتكامل، والمنظمة الدولية للتوحيد القياسي المعروفة باسم إطار إدارة المخاطر ISO 31000 والعمليات(Sityata, Botha & Dubihlela, 2021, 3)

٢- أنواع المخاطر، وتصنيفات المخاطر السيبرانية:

وقد قسم (النجار والفرا، ٢٠١٩، ١٩) مخاطر المؤسسات التعليمية إلى مخاطر أكاديمية -أخلاقية- متعلقة بالطلبة- متعلقة بالأمن- تراجع السمعة. ومن مخاطر الموارد البشرية مخاطر التعامل والامتثال والثقة والمخاطر الفكرية والأخلاقية والسلوكية، وتصنف المخاطر أيضاً لمخاطر التوافر العددي والنوعي والخطر الاجتماعي. (المدرع، ٢٠١٩، ٦٨)

وقد حظي الانترنت بإقبال كبير من جانب المواطنين؛ ففي دراسة أجرتها شبكة America On Line عن أفضل طرق التواصل مع الغير من خلال سؤال العملاء المربوطين بالشبكة سؤال "إنك ستُنفى إلى جزيزة وأمامك خيار واحد للاتصال مع العالم ما طريقة الاتصال المفضلة لديك؟" أوضح ٦٨٪ اختيار الانترنت، ٢٣٪ الهاتف، ٨٪ التلفزيون. (العصيمي، ٢٠٠٤، ١١٥)

وعلى الرغم من أن الأبحاث قد أشارت إلى أن استخدام الكمبيوتر في المنزل كان مفيدًا بشكل واضح على مستويات التحصيل الأكاديمي للأطفال في القراءة والرياضيات، وارتبط إيجابياً بنمو القدرات اللفظية لهم، ويمكن أن يغطي وقت الشاشة مجموعة واسعة من الأنشطة من قراءة الروايات على قارئ إلكتروني أو إجراء بحث لمشروع مدرسي، أو لعب الألعاب بشكل تعاوني مع الآخرين في جميع أنحاء العالم، ويُمَكِّنُهم أيضاً من الحصول على المعلومات؛ والتعبير عن الإبداع وتطوير وتعزيز العلاقات؛ وتحسين نتائج التعليم؛ فيوفر فرصاً لا مثيل لها للأطفال؛ للتعلم والإبداع والتواصل الاجتماعي

(Psotka, 2013, 76)، علاوة على أن استخدام الأدوات الذكية تؤدي إلى تطوير الدماغ الأيسر للأطفال(Munawar & Nisfah, 2020, 65) ولكن أوضحت الدراسات الحديثة أن هناك زيادة في الطرق التي يمكن أن يتعرض بها الأفراد للمخاطر الناتجة من الاستخدام غير المناسب للتقنيات. (Swanton, Blaszczynski, Forlini, Starcevic & Gainsbury, 2021, 5)

يمكن تقسيم تلك المخاطر إلى ثلاث فئات رئيسة كما في جدول (٢) ؛ تعرضها الدراسة فيما يلي:

جدول (٢): تصنيفات المخاطر وفقاً لمسح منظمة EU للأطفال عبر الانترنت

Source: (Hasebrink, Görzig, Haddon, Kalmus & Livingstone. 2011, 26-27)

تصنيف المخاطر	التعريف	أمثلة
مخاطر المحتوى	استقبال الأطفال لمحتوى ضار	العنف، الكراهية، المحتوى الإباحي.
مخاطر الاتصال	مشاركة الأطفال في أنشطة خاصة	الاستمالة، سوء استخدام بيانات شخصية، بالبالغين عبر الانترنت أو نماذج أخرى من الاستغلال الجنسي.
مخاطر السلوك	مقترف جريمة أو ضحية في تبادل نظير إلى نظير.	التنمر، الرسائل الجنسية، توليد محتوى ضار

(أ) مخاطر المحتوى: عندما يتلقى التلميذ محتوى قد يكون غير مناسب أو غير قانوني يشمل هذا قرصنة المحتوى أو اللغة العدوانية والسلوك، وتشمل على سبيل المثال لا الحصر: التعرض لمواد غير لائقة أو ضارة عبر الإنترنت، مثل محتوى المقامرة أو المواد الإباحية، سواء تدافع عن المثلية الجنسية Homosexuality أو تروج لجنس المحارم Incest واستهواء الأطفال Pedophilia والبهيمية Bestiality واشتهاء جنس الموتى Necrophilia، أو محتوى العنف مثل السادية وهي استعذاب إحداث الألم بالآخر والماسوشية أو المازوكية وهي استعذاب تلقي الألم للوصول للمتعة، وكذا إيذاء الذات

الرقمي والتعرض لمحتوى يحرض على القلق أو السلوك الضار مثل الانتحار وإيذاء النفس واضطرابات تناول الطعام. (مرعي، ٢٠١٣، ١٥٤) وقد لخص باندورا في نظريته عن الإدراك الاجتماعي (التعلم الاجتماعي) أن مشاهدي الإعلام يكتسبون الاتجاهات وردود الأفعال والسلوكيات من النماذج التي يقدمها الإعلام، وأشار إلى أن هناك طرق متعلقة بتقليد النماذج التي تقدمها وسائل الإعلام–كنماذج العنف مثلاً– أبرزها:

١–التعلم عن طريق الملاحظة Observational Learning

يكسب نماذج سلوك من خلال المشاهدة؛ فجميعاً قد نعرف كيف نطلق النار باستخدام البندقية على الرغم من أن العديد منا لم يقم بذلك فعلياً.

٢–التأثيرات غير المانعة Disinhibitory إذا صاحب العنف المقدم عبر وسائل الإعلام مكافأة ما قد يزيد من احتمال تقليد السلوك(حجازي، ٢٠١٨، ٣٦)

(ب) مخاطر الاتصال: قد يكون هذا الاتصال غير مرغوب فيه أو غير مناسب، مثل الاستمالة أو الاتصال الجنسي غير المرغوب فيه – مشاركة معلومات بشكل عشوائي بشكل يتجاهل ما إذا كانت المعلومات المقدمة حقيقية أم خلاف ذلك (Rahman, Malaysia, Sairi, Zizi, & Khalid, 2020, 378) بالإضافة إلى إساءة استخدام اللغة عند التواصل السيبراني في مهامهم فأصبحت اللغة والاختصارات والأخطاء الإملائية وباءً. (Payne, 2016, 3)

وقد أجريت دراسة عام ٢٠١١ مع أطفال تتراوح أعمارهم بين ستة وتسع سنوات، وجدت أن أكثر من نصف (وتحديداً ٦٤٪) من أطفال المملكة المتحدة، ٥٥٪ من الإسبان الأطفال ٤٦٪ من الأطفال الألمان ٣٨٪ من الأطفال الإيطاليون و٣٧٪ من الأطفال الفرنسيين هـَمَّ باستخدام وظائف الشبكة الاجتماعية (Holloway, Green & Livingstone, 2013, 12) وهو ما يخالف القانون وَأَدْعَى إلى الوقوع في مخاطر الاتصال.

(ج) مخاطر السلوك: – يكون فيها الطفل كمشارك نشط – ويبالغ في إظهار المعلومات الشخصية أو يقوم بالتنمر على شخص آخر أو سرقة الهوية عبر الإنترنت، أو إدمان

الاستخدام، ويُعد إيذاء الذات الرقمي شكلاً من أشكال العدوان على الذات بحيث يتضمن نشر ملاحظات مؤذية ومسيئة أحيانًا عن الذات. (مرعي، ٢٠١٣، ١٥٤)

وبمراجعة الأدبيات التي تحقق في الوضع الحالي فيما يتعلق بنضج أمان الإنترنت داخل البيئات المدرسية تبين أنه: لا يوجد دليل تقييم متفق عليه عالميًا لتعليم الأمن السيبراني للتلاميذ، ولا يزال الأمن السيبراني راسخًا في مهنة تكنولوجيا المعلومات – ومنفصلاً بشكل كبير عن نظام التعليم – ولا يمتلك المحترفون الأمنيون ولا التربويون فهماً جيداً للمهارات المهمة المطلوب نقلها إلى الأطفال الصغار (Malecki, 2018, 5) بالإضافة إلى أنه من المستحيل مراعاة كل المخاطر المحتملة التي قد تنشأ على الإنترنت (AVA ,2020, 10)

٢- عمليات إدارة المخاطر.

يمكن تحديد الممارسات الدولية لإدارة المخاطر وفقا للدراسات فيما يلي:

عادة ما يتم تقديم إدارة المخاطر كعملية وتتكون المراحل مما يلي: تحديد المخاطر وتحليل المخاطر وتقييم المخاطر والاستجابة للمخاطر والمراقبة ومراجعة المخاطر. (Klucka, Gruenbichler, & Ristvej, 2021, 2)

فتتضمن إدارة المخاطر تطبيق طريقة منطقية ومنهجية لتحديد المخاطر وتحليلها وتقييمها ومعالجتها ومراقبتها بطريقة تمكن المنظمات من تقليل الخسائر وتعظيم المكاسب، ويمكن تطبيق إدارة المخاطر على العديد من المستويات في المنظمة؛ فيمكن تطبيقها في المستوى الاستراتيجي والمستويات التشغيلية.(Authority, 2002, 21)

ويعد إنشاء مسار لإدارة المخاطر الناشئة والاستجابة بسرعة وفعالية أمرًا بالغ الأهمية لضمان استجابة مبسطة وضمان التخفيف من أي خطر محتمل قدر الإمكان (AVA ,2020, 10)؛ وتنفيذ استراتيجيات الاستجابة وعمليات الإدارة بشكل استباقي (Sityata, Botha & Dubihlela, 2021, 4) **وتسير عمليات إدارة المخاطر وفقاً للخطوات التالية:**

(أ) تحديد المخاطر:

تحدد المؤسسة المخاطر المحتملة التي قد تؤثر سلبا على عملية ما أو مشروع معين تقوم به، كما يجب تحديد بيئة الأعمال والعوامل المساهمة التي يمكن أن تسبب

حدوث المخاطر والأسباب الجذرية للمخاطر، ووصف المخاطر وفهم الهدف من المخاطر والتهديدات التي تواجه المؤسسة. وجدير بالذكر أنه يتم دعم التقييم الاستباقي من خلال البيانات ذات الصلة والاتجاهات والأحداث الجارية. (Pest Management Regulatory Agency Health Canada, 2021, 31)

ويمكن تحديد المخاطر من مجموعة من المصادر بما في ذلك ، على سبيل المثال لا الحصر:

(١) تبادل الأفكار باستخدام أفراد عمليات ذوي خبرة ؛(٢) تطوير سيناريوهات المخاطر.(٣) برامج تحليل البيانات؛(٤) استقصاءات السلامة ومراجعات السلامة في مراقبة العمليات ؛(٥) بيان التحقيقات في الحوادث؛(٦) العوامل التنظيمية، مثل سياسات الشركة للتوظيف والتدريب، والمكافآت وتخصيص الموارد؛ (٧) عوامل البيئة التشغيلية، مثل الضوضاء والاهتزازات المحيطة، درجة الحرارة والإضاءة ومعدات الحماية (٨) العوامل البشرية، مثل الحالات الطبية، وقيود الأداء البشري، وواجهة الإنسان والآلة. (٩) عوامل الامتثال التنظيمي، مثل انطباق اللوائح واعتماد المعدات والأفراد والإجراءات. (Authority, 2002, 23)

كما تشمل أدوات تحديد المخاطر المحتملة: قوائم المراجعة، والدراسات الاستقصائية، وعمليات التفتيش الشخصية، وآراء الخبراء التي تعتمد على وعي الخبير وإدراكه لمدى حجم الخطر، وطريقة تداول الأفكار؛ بمعنى عمل توليفة مما سبق للوصول إلى أفضل النتائج، ومن وسائل تحديد المخاطر أيضاً العصف الذهني–SWOT– استبيانات المخاطر– ورش العمل – تحليل المخاطر– تقييم المخاطر– سياسات علاج المخاطر– مراقبة ومتابعة الخطر". (النجار والفرا، ٢٠١٩، ٢٤، ٢٦).

(ب) تحليل المخاطر:

تعد تحليل المخاطر الخطوة التالية في عملية إدارة المخاطر، ولكن يمكن أن تكون أيضًا الخطوة الأولى إذا كانت هناك مخاطر تم تحديدها بوسائل أخرى غير تقييم المخاطر، أما الغرض الأساسي من تحليل المخاطر فهو التقييم، فبمجرد تحديد أنواع محددة من المخاطر، تحدد المؤسسة تصنيفها وأولوياتها وضوابطها ومستويات الخطر وبعد ذلك احتمالات حدوثها وكذلك عواقبها، والهدف من تحليل تلك المخاطر زيادة فهم

كل حالة محددة من المخاطر، وكيف يمكن أن تؤثر على الأهداف الإستراتيجية للمؤسسة. (Authority, 2002, 27)

ومن أساليب تحليل المخاطر وفهمها بشكل أفضل بعض التطبيقات مثل: شبكات بايزيBayesian networks وأشجار الخطأ fault trees ونظرية القيمة القصوىextreme value كما توجد طرق أخرى لتحليل البيانات (Klucka, Gruenbichler, & Ristvej, 2021, 2)

ويمكن توضيح الخطوات الخمس لعملية تحليل المخاطر فيما يلي: (Authority, 2002, 21) (الخياط، ٢٠١٩، ٣٣٦-٣٣٧) (ناصف، ٢٠١٢، ٦٣-٦٧) (THE UNIVERSITY OF LEEDS, 2019, 14)

(١) وصف واضح للمخاطر:

يجب أن يكون هناك بيانًا موجزًا يصف ماهية المخاطر، وكيف يمكن أن تؤثر على تحقيق الأهداف، ويجب أن يتفق فريق مراجعة المخاطر على نطاق المخاطر ثم وصف سيناريو المخاطرة، مما يوضح للمجموعة ما يبدو عليه حدث الخطر المحتمل.

(٢) أسباب المخاطر:

وتعني "لماذا يحدث هذا الخطر؟" بصرف النظر عن الأسباب المباشرة للمخاطر، نحتاج أيضًا إلى فهم جيد للأسباب الأساسية الجذرية والمحركات الرئيسة؛ من أجل تقليل احتمالية المخاطر بشكل فعال.

(٣) الضوابط الوقائية:

بمجرد أن نفهم الأسباب الجذرية، نحتاج إلى الاتفاق على الضوابط الموجودة بالفعل والتي تساعد على تقليل احتمالية حدوث هذه الأسباب أو الدوافع، وتحديد الضوابط الإضافية التي يمكننا وضعها لتقليل الاحتمالية بشكل أكبر؟؛ فالمنظمات التي تتبع استراتيجية استباقية لإدارة مخاطر السلامة تعتقد أنه يمكنها التقليل من مخاطر الحوادث من خلال تحديد نقاط الضعف، واتخاذ الإجراءات اللازمة للحد من العواقب السلبية للمخاطر الناشئة.

(٤) عواقب المخاطر:

وتعني ماذا سيكون الأثر إذا تحققت هذه المخاطر؟ فإن تحديد هذه العواقب المحتملة مقدمًا يساعد في وضع خطط للطوارئ في حال حدث خطر.

(٥) الضوابط المخففة:

– ما الضوابط التي يجب تطبيقها، والتي من شأنها أن تساعد في تقليل تأثير العواقب؟

– ما الضوابط الإضافية التي يمكن وضعها لتقليل التأثير بشكل أكبر؟

(ج) تقييم المخاطر:

يتم بعد ذلك تقييم المخاطر بشكل أكبر بعد تحديد احتمالية حدوثها بشكل عام، ويمكن للمؤسسة بعد ذلك اتخاذ قرارات بشأن ما إذا كانت المخاطر مقبولة، وما إذا كانت المؤسسة مستعدة لإدارتها.

يتضمن تقييم المخاطر مقارنة مستوى الخطر الموجود أثناء عملية التحليل مقابل أوزان المخاطر المحددة مسبقًا، ويُستخدم تقييم المخاطر لاتخاذ قرارات تجاه الأخطار ذات الأهمية للمؤسسة، ومدى قبولها أو معالجتها؛ ويتم تقييم المخاطر لتحديد أشدها خطورة، وذلك عن طريق جدولتها ثم البدء بمعالجة أشد المخاطر؛ يليها الأقل منها شدة، وهكذا حتى تنتهي قائمة المخاطر، مع تحديد احتمال وتأثير كل خطر على حدة ثم تأثيرها إجمالاً؛ لذا تعد مصفوفة تقييم المخاطر Risk matrix –والتي يشار إليها أحيانًا بخريطة المخاطر– أداة مفيدة لمساعدة الفرق في ضمان دراسة المخاطر بعمق ووضع تدابير التخفيض المضمنة في سياسات وإجراءات الحماية عبر الإنترنت". (AVA, 2020, 8)

فتوضح مصفوفة المخاطر العلاقة بين احتمالية حدوث المخاطر وتأثير الحدث كما يتضح من شكل (٢)، وهي الوسيلة الأكثر شيوعًا، ويمكن استخدامها أيضًا للإشارة إلى آليات التحكم في المخاطر المحتملة التي يمكن تطبيقها، كما يمكن أيضًا استخدامها لتسجيل المستويات المتأصلة والحالية (أو المتبقية) والمستهدفة من الخطر (Hopkin, 2018: 45–46, 152).

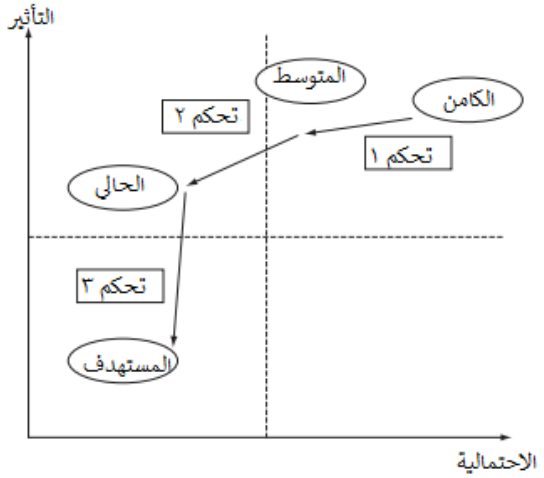
شكل (٢) مصفوفة إدارة المخاطر

المصدر :(Hopkin, 2018, 45-46, 152)

وتوجد عملية تقييم المخاطر ضمن إطار عمل إدارة المخاطر(RMF) لتؤكد على: المحافظة على الوعي بالوضع الحالي بشكل مستمر من خلال عمليات المراقبة المعززة، كذلك توفير تقييم المعلومات الأساسية المتعلقة بالمخاطر لكبار القادة تسهيلاً لاتخاذ القرارات بشأن تخفيف أو قبول المخاطر المتعلقة بنظم المعلومات للعمليات التنظيمية والأفراد والمنظمات الخارجية، وجدير بالذكر أن تقييمات المخاطر ليست مجرد أنشطة لمرة واحدة توفر معلومات دائمة ونهائية لصانعي القرار -لاستغلالها في توجيه وإبلاغ الاستجابات للمخاطر-؛ وإنما تستخدمها المنظمات على أساس مستمر طوال دورة حياة تطوير النظام وعبر جميع المستويات في التسلسل الهرمي، ويتضمن تقييم المخاطر: التهديد والضعف، كما يحلل ويأخذ في الاعتبار عوامل التخفيف المعمول بها، والغرض من عنصر تقييم المخاطر هو تحديد: (١) التهديدات الموجهة للمنظمات (أي العمليات أو الأصول أو الأفراد) أو التهديدات الموجهة من خلال منظمات ضد منظمات أخرى؛ (٢) نقاط الضعف داخل وخارج المنظمات؛ (٣) الضرر(أي التأثير المعاكس) الذي قد يحدث في ضوء احتمالية حدوث التهديدات؛ و (٤) احتمال وقوع الضرر. (Centers for Medicare & Medicaid Services Information Security and Privacy Group, 2021, 9, 16) ويأخذ التقييم النوعي للمخاطر في الاعتبار العوامل التالية: - مصدر / الخطر -مسار العمل، هدف / المستقبل & (Bica, Petruta, 2021, 3).

يقوم الممارس بتحليل المخاطر لتحديد احتمالية أن تؤدي أحداث التهديد والظروف المعرضة للخطر إلى تأثيرات ضارة على أصل النظام، وبالمثل يقوم الممارس بتحليل قيمة التأثير وحساب مخاطر التعرض باستخدام المنهجية المحددة في استراتيجية مخاطر المؤسسة (على سبيل المثال، مثل ([احتمالية المخاطرة] × [تأثير المخاطر].) يتم تسجيل نتائج هذه التحليلات في عمود "التقييم الحالي، ومن تلك الأساليب أيضاً تحليل شجرة الأحداث؛ فيعد تحليل شجرة الأحداث (ETA) أسلوبًا بيانيًا يساعد الممارسين على تقييم تأثير سيناريو معين؛ لذا فإن تحليل السبب الجذري (التفكير في الأحداث السابقة التي أدت بالفعل إلى حدث ما) يساعد في النظر إلى العواقب المحتملة للأحداث المستقبلية، كما يساعد على توثيق تسلسل النتائج التي يمكن أن تنشأ بعد بدء حدث تهديد، وبينما يعتبر حكم الخبراء ذا قيمة في تقدير عوامل الخطر، إلا أن هناك طريقة واحدة لتقليل الذاتية هو استكمال هذا الحكم باستخدام نماذج المحاكاة مثل مونت كارلو (Quinn, Ivy, Barrett, Feldman, Witte, & Gardner, 2021, 21, 52-53).

وهناك ثلاثة مستويات للمخاطر مهمة في مصفوفة المخاطر المستوى الكامن وهو مستوى الخطر الذي قد يكون موجودًا إذا لم تكن هناك ضوابط في المكان، والمستوى الحالي وهو المستوى الذي توجد عنده المخاطر في وقت تقييم المخاطر، عندما يكون عنصر التحكم ١ و ٢ في مكانهما الصحيح، وغالبًا ما يشار إلى هذا على أنه المستوى المتبقي من المخاطر، وتكمن مشكلة وصف المستوى الحالي على أنه المستوى المتبقي – وتوحي بأن مستوى المخاطرة ثابت وأن المنظمة لا تستطيع اتخاذ المزيد من التخفيف من المخاطر؛ فيعطي استخدام عبارة "المستوى الحالي" إحساسًا ديناميكيًا أكثر لعملية إدارة المخاطر، ومع ذلك، فإن المديرين يركزون على المستوى المستهدف الذي سيقلل من تأثير المخاطر؛ بحيث يكون مستوى الخطر المستهدف هو ضمن الربع السفلي الأيسر من خريطة المخاطر، أو منطقة التقبل / الراحة كما في شكل (Hopkin, 2018, 169).(٣)



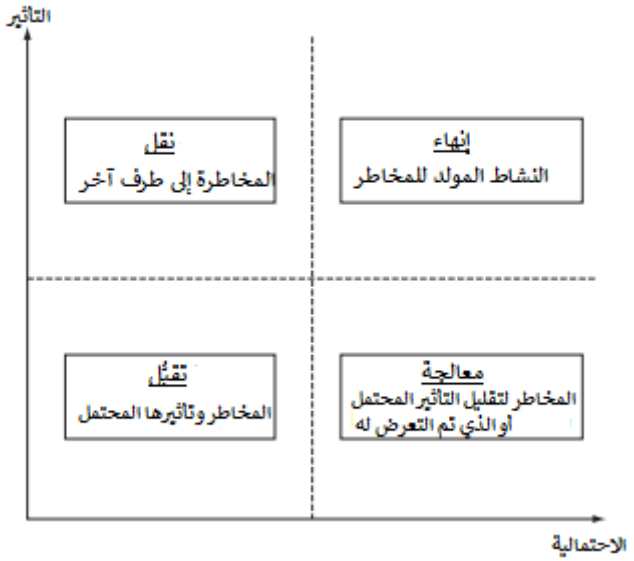
شكل (٣) مستويات المخاطر في المصفوفة

المصدر: .(Hopkin, 2018, 169)

(د) الاستجابة للمخاطر:

تتضمن الاستجابة للمخاطر تحديد مجموعة الخيارات لمعالجة المخاطر وتقييمها وإعداد خطط معالجة المخاطر وتنفيذها، وتشمل تلك الخيارات تجنب المخاطر، وتقليل احتمالية الحدوث، وتقليل العواقب، ونقل المخاطر، والاحتفاظ بالمخاطر.

وتشمل خيارات الاستجابة للمخاطر كل من: **التسامح** (وهي مناسبة فقط عندما يكون من الممكن قبولها حين تكون الخسارة أو الضرر قد حدث / **الاحتفاظ** ، **والمعالجة** / **التقليل** Corrective /(treat) ، **والنقل**Directive /(transfer) (وتستند إلى إعطاء توجيهات للناس حول كيفية التأكد من عدم حدوث خسائر، لكنها تعتمد على الأشخاص الذين يتبعون أنظمة عمل آمنة راسخة)، **والإنهاء** Preventive /(terminate) / **والتجنب** (من خلال تنفيذ الضوابط الوقائية المناسبة)، وُتنتقد الاستجابة للمخاطر على أنها قيادة تصحيحية حتى الآن أكثر من كونها وقائية (Maphorisa, 2021, 5, 17)



شكل (٤) إستراتيجيات الاستجابة للمخاطر

المصدر: (Maphorisa, 2021, 5, 17)

خلال هذه الخطوة تقوم المؤسسة بتقييم المخاطر الأعلى تصنيفاً، والتعامل معها بإيجابية، ووضع خطة لتخفيفها باستخدام ضوابط محددة للمخاطر، وتشمل هذه الخطط عمليات تخفيف المخاطر وتكتيكات الوقاية من المخاطر، وخطط الطوارئ في حالة ظهور المخاطر.(Buganová, & Šimíčková, 2019, 987)

(هـ) مراقبة المخاطر:

وهي جزء من خطة التخفيف تقوم على متابعة كل المخاطر من رصد وتتبع الجديدة منها والحالية بشكل مستمر، بالإضافة إلى مراجعة عملية إدارة المخاطر الشاملة وتحديثها وفقاً للمواقف المختلفة والمتغيرة.

وتتم مراجعة المخاطر على أساس ربع سنوي – وتحديد المخاطر الجديدة والتغييرات القائمة، وتحديث سجل المخاطر ، وتقييم الإجراءات التي يتخذها أصحاب المخاطر لإدارة المخاطر وتصحيح الأداء غير اللائق.

الغرض من مكون مراقبة المخاطر هو: (١) تحديد الفعالية المستمرة للاستجابات للمخاطر (بما يتفق مع إطار المخاطر التنظيمية)؛ (2) تحديد التغييرات

التي تؤثر على المخاطر والبيئات التي تعمل فيها الأنظمة ؛ و(3) التحقق من تنفيذ استجابات المخاطر المخطط لها، واستيفاء التشريعات والتوجيهات واللوائح والسياسات والمعايير والمبادئ التوجيهية. (Centers for Medicare & Medicaid Services Information Security and Privacy Group, 2021, 18)

ووفقا لدراسة (قارة عشرة وحبار، ٢٠٢٠، ٣٤٧) فتتضمن عمليات إدارة المخاطر: التحديد–القياس–المعالجة–التنفيذ. أما وفق دراسة (النجار والفرا، ٢٠١٩، ٢٤، ٢٦) فتشمل عمليات إدارة المخاطر: التعرف على المخاطر وتحديد مقدار آثارها المحتملة، ووضع الخطط المناسبة لما يمكن القيام به لتجنب هذه المخاطر أو لكبحها أو السيطرة عليها وضبطها للتخفيف من آثارها، إن لم يكن القضاء على مصدرها، ووفقا لدراسة (إبراهيم، ٢٠١٩، ٢٨٠) فإن إطار إدارة المخاطر يتمثل في: تحديد السياق–تحديد المخاطر–تحليل الخطر–أثر الخطر–درجة الاحتمال–تقدير مستوى الخطر–تقييم المخاطر–قبول المخاطر–معالجة المخاطر. ووفقا لدراسة (المدرع، ٢٠١٩، ٦٥) تتضمن المنهجية ٥ مراحل لإدارة مخاطر الموارد البشرية هي الإعداد، التحليل، التخطيط، التنظيم، التحكم. وتتحدد عمليات إدارة المخاطر فيما يلي: تأطير المخاطر –تقييم المخاطرة –الاستجابة للمخاطر– مراقبة المخاطر (Centers for Medicare & Medicaid Services Information Security and Privacy Group, 2021, 16)

إلا أن الأساس العلمي لتقييم المخاطر وإدارة المخاطر لا يزال مشوشاً إلى حد ما في بعض القضايا، بمعنى أن يعتمد كل من العمل النظري والممارسة على وجهات النظر والمبادئ(Aven, 2016, 10)

ويتعين على المنظمة تعيين مدير سلامة يكون مسؤولاً عن:

(أ) إسداء المشورة للمسؤولين والمديرين التنفيذيين بشأن إدارة السلامة القضايا؛ (ب) إدارة تنفيذ نظام إدارة السلامة بما في ذلك:

(١) إجراء أو تسهيل تحديد المخاطر وتحليل مخاطر السلامة؛ (٢) مراقبة مخاطر السلامة والإجراءات التصحيحية وتقييم النتائج؛ (٣) تقديم تقارير دورية عن أداء سلامة المنظمة؛ (٤) الاحتفاظ بالسجلات والوثائق المتعلقة بالسلامة؛ (٥) تخطيط وتسهيل

تدريب الأفراد المتعلق بالسلامة؛ (٦) مراقبة مخاوف السلامة وملاحظة التأثير على عمليات المنظمة؛ والتنسيق والتواصل مع الهيئات المختلفة في القضايا المتعلقة بالسلامة.(Authority, 2002, 11)

كما يجب على مجموعة عمل السلامة أن تشمل في مجالها الوظيفي ما يلي: (أ) الإشراف على أداء السلامة التشغيلية؛ (ب) التأكد من أنشطة إدارة مخاطر السلامة، مثل تحديد المخاطر، وإجراء تقييم المخاطر والتخفيف ؛(ج) تقييم تأثير التغييرات التشغيلية أو التكنولوجيات الجديدة على السلامة ؛(د) تنسيق وتنفيذ ضوابط مخاطر السلامة والإجراءات التصحيحية في الوقت المناسب؛ (هـ) استعراض فعالية ضوابط مخاطر السلامة والإجراءات التصحيحية؛ (و) تنسيق أنشطة تعزيز السلامة لزيادة الوعي بأمور السلامة.(Authority, 2002, 12)

٤-معوقات إدارة المخاطر بالمدرسة:

من العوامل التي تعوق عمل إدارة المخاطر بالمدرسة وتؤثر على سلامتها ما يلي (ناصف، ٢٠١٢، ٦٩):

(أ) أن يتم ترتيب المخاطر حسب الأولوية بشكل غير مناسب مما يؤدي إلى ضياع الوقت في التعامل معها.

(ب) التقدير الخاطئ للخسائر المترتبة على المخاطر التي تواجه المدرسة.

(ج) عدم وجود خطط للتخفيف من حدة المخاطر التي تم تحديدها، ثم وصف كيفية التعامل معها، تحديد متى وكيف سيتم تجنب أو تقليص آثارها عندما تصبح إدارة المخاطر مسئولية قانونيةعلى المدرسة.

(د) القصور في تدريب القيادات المدرسية على إدارة المخاطر: ويتضح ذلك من افتقار البرنامج التدريبي للترقية لوظيفة مدير مدرسة لموضوعات محددة تتعلق مباشرة بإدارة المخاطر أو إدارة الأزمات في حين أن دولة كماليزيا تركز برامجها التدريبية لمديري المدارس على بعض الموضوعات المرتبطة بإدارة المخاطر مثل تحليل الظواهر والمشكلات المدرسية والسلوكية باستخدام المنهج العلمي، وفنيات إدارة الأزمات المدرسية، والإطار القانوني لعمل مدير المدرسة، وكذلك

الأمر في الولايات المتحدة الأمريكية يتم تدريب المديرين على حل المشكلات المدرسية وتعزيز السلوكيات الأخلاقية للمعلمين.

ثانياً: دواعي الحاجة إلى إدارة المخاطر السيبرانية في المدارس الابتدائية.

من الأمور التي تدفع الدولة وتربويها إلى إدارة المخاطر السيبرانية:

أ-حماية حقوق الطفل ضد الإساءة السيبرانية.

فالإساءة الرقمية هي شكل جديد من أشكال إساءة معاملة الأطفال، وتُعَرَّف منظمة الصحة العالمية "إساءة معاملة الأطفال" أو "سوء المعاملة": بأنه جميع أشكال الإساءة الجسدية و/ أو سوء المعاملة العاطفية، والاعتداء الجنسي، والإهمال أو المعاملة بإهمال، والاستغلال التجاري أو غيره مما ينتج عنه -فعلاً أو محتملاً- الإضرار بصحة الطفل أو بقائه أو نموه أو كرامته. وتقوم مبادئ اتفاقية حقوق الطفل على أن حماية الطفل ومصالحه لها الأولوية، ويجب أن يكون الاعتبار الأساسي في صنع القرار: احترام حقوق الأطفال، بما في ذلك الحق في الحماية والترفيه الآمن، والمشاركة والوصول إلى المعلومات والخصوصية، واحترام القيم الدينية والأخلاقية، والحفاظ على سرية البيانات الشخصية الحساسة، فلا يمكن الوصول إلى المعلومات ومشاركتها ومعالجتها إلا عند الضرورة الصارمة.(Taibah, Khalifa & Alshebaiki, 2020, 3)

وغالبًا ما يكون المتعلمون أصغر من أن يفهموا مخاطر التكنولوجيا (Cilliers & Chinyamurindi, 2020, 28)؛ وتشير المادة الأولى من اتفاقية حقوق الطفل إلى أن مصطلح "الطفل" يطلق على أي شخص يقل عمره عن ١٨ عامًا (Livingstone, Lievens & Carr, 2020, 12) وتحدث المراهقة عادة بين سن ١٣ و ١٩ سنة (Lewis, 2020, 37) وتعرف اليونيسف ووكالات الأمم المتحدة الأخرى "المراهقة" على أنها العمر من ١٠-١٩، كما تعرّف وكالات الأمم المتحدة "الشباب" على أن أعمارهم تتراوح بين ١٥ و٢٤ عامًا. (Unicef, 2016, 5-6).

ومن حقوق الأطفال الحق في الحماية، بما في ذلك الحماية ضد التعسف أو التدخل غير القانوني في خصوصية الأطفال، والاعتداءات غير القانونية على شرفهم وسمعتهم، وتقر المادة ١٦ من اللائحة العامة الخاصة بحماية البيانات(GDPR) صراحةً بأن الأطفال بحاجة إلى حماية أكثر من البالغين، كما أوضحت الحيثية ٣٨ من اللائحة

العامة الخاصة بحماية البيانات، أن الأطفال يستحقون حماية خاصة لأنهم قد يكونون أقل وعياً بهذه المخاطر والعواقب والضمانات وحقوقهم فيما يتعلق بمعالجة البيانات الشخصية خاصة عبر الإنترنت بموجب المادة ٦ (١) (أ) من اللائحة العامة الخاصة بحماية البيانات (GDPR)، واستحدثت المادة ٨ من تلك اللائحة ضرورة موافقة الوالدين قبل تقديم خدمات مجتمع المعلومات بشكل مباشر للأطفال أقل من ١٦ عامًا (ما لم يتم تطبيق حد أدنى للسن القومي بين ١٣ و ١٦ عامًا)، ونظرًا لهذه المخاطر عبر الإنترنت والمخاوف العامة، كانت هناك نداءات متزايدة من صانعي السياسات والأكاديميين لتغيير حقوق الأطفال، ولا سيما حماية الحقوق– وفقًا لاتفاقية الأمم المتحدة لحقوق الطفل–؛ لتلبية الاحتياجات الرقمية للعمر من بينها الحقوق في الإتاحة والمشاركة. (Macenaite & Kosta, 2017, 147–148)

ب– التصدي لتهديدات النسق الخلقي والأكاديمي والرفاه المجتمعي.

من الصعب الجدال في حقيقة أن الإنترنت قد أحدث ثورة في صناعة المواد الإباحية Lucrative وتوسيع نطاق وصول الأطفال والمراهقين إلى تلك المواد Hornor, (2020, 191) ويبدو أن ذلك الغزو الإباحي نتيجة إفرازات العولمة، وزيادة والمضامين السلبية التي تدعو إلى استباحة الرذائل وطمس العقائد إلى حد تنامي ثقافة الغريزة وإعلاء قيمة الجسد المقترن بالمتعة والجنس؛ فمن أخطر ماذكر حول الآثار السلبية للعولمة شيوع الرذيلة وسهولة ارتكابها، بتعويد الناس على الوسائل المحرمة والدعاية لها، وإن الأمر لا يتوقف عند ترويج الثقافة الغربية، بل يمتد إلى إقحام وتغلغل أفكار مغلوطة؛ فقد أدركت إسرائيل حقيقة أن فكرة الاحتلال العسكري الآن باتت أمراً عقيماً وغير مُجْدٍ، خاصةً بعد أن خسرت كثيراً من الأرواح والأموال؛ فالاحتلال اليوم ليس معناه أن تشهر سلاحك في وجه الآخر وتخضعه لإرادتك، وإنما أن تأسر من حولك بأدوات مثل الانبهار بالتكنولوجيا وثقافة الآخر، وصولاً لأخطرها وهو فقد الهوية والتخلي عن القيم المتوارثة والتقاليد العريقة.

فالانترنت ينتمي إلى ما يُعرَف بوسائط الإنفوميديا أو النيوميديا؛ والتي تنتمي بدورها لحزمة القوة الناعمة أو الـ Soft Power التي كانت مفتاح انتصار الولايات المتحدة الأمريكية والغرب على الاتحاد السوفيتي السابق والكتلة الشرقية خلال الحرب

الباردة؛ حيث كانت الوسيلة الأساسية للقفز على الستار الحديدي الذي أقامه ستالين حول الاتحاد السوفيتي والدول الشيوعية، ونقل قيم الحياة الغربية إلى شعوب هذه البلدان، حتى جاء التصدع من داخل هذه الدول، وليس من خارجها. (شفيق، ٢٠١٤، ٩)

إذن فإن التقنيات ليست محايدة أخلاقياً، لأنها تعكس القيم التي نلتزم بها والتي توجه توزيعنا واستخدامنا لها؛ فتمامًا كما لم نسلم طفل مجموعة من مفاتيح السيارة مع عدم وجود تعليمات حول كيفية القيادة، لا ينبغي أن نرسل الأطفال إلى عالم الانترنت بدون فهم قوي لكيفية أن تكون آمنًا عبر الإنترنت، أنه أمر حرج للأمن القومي والاقتصادي، وهي مسؤولية مشتركة للآباء والمعلمين. (Payne, 2016, 21)

ومن هنا كان هناك إجماع دولي متزايد على أن الأخلاق لها أهمية متزايدة في التعليم في المجالات التقنية؛ فاليوم أكبر منظمة مهنية تقنية في العالم IEEE (المعهد الهندسي للكهرباء والإلكترونيات) بالولايات المتحدة الأمريكية، خصصت قسما كاملا لأخلاقيات التكنولوجيا؛ فيعمل IEEE فقط على معايير أخلاقية جديدة في المجالات الناشئة مثل الذكاء الاصطناعي، الروبوتات وإدارة البيانات ,Vallor & Rewak) (3-2 ,2018 ويمكن عرض بعض الآثار السلبية السلوكية والاجتماعية للمخاطر السيبرانية فيما يلي.

جدول (٣) أهم الآثار السلبية السلوكية والاجتماعية للمخاطر السيبرانية.

المخاطر السيبرانية	الآثار السلبية
إدمان الانترنت	– هناك أدلة تشير إلى أن النمو المعرفي للأطفال يمكن أن يتضرر بفترات طويلة من استخدام الإنترنت، بما في ذلك تطوير مهارات الذاكرة، ومدى الانتباه، وقدرات التفكير النقدي، واكتساب اللغة والقراءة والتعلم، ويكون لديه استدعاء أقل للمعلومات (Quaglio & Millar, 2020, 5) – ثبت الارتباط المباشر بين المشاركة المفرطة في الألعاب عبر الإنترنت والعجز البنيوي في منطقة الدماغ، وفي إحدى الدراسات أيد أكثر من ٨٥٪ من المعلمين عبارة "اليوم تخلق التقنيات الرقمية جيلًا يسهل تشتت انتباهه" (Dubicka & Theodosiou, 2020, 27,

المخاطر السيبرانية	الآثار السلبية
	(37-38. وقد أشار الاستطلاع الذي أجري على العديد من المدارس الأمريكية التي تسمح بدخول أجهزة متعددة إلى الفصل الدراسي: أن أكثر الأمور إلحاحًا بين المعلمين كان الإلهاء، والذي تجاوز قضايا الخصوصية والأمان(Lester, 2018, 9) - وفقًا لتحليل المحتوى الذي أجرته منظمة معلومات الألعاب الأوروبية: 89٪ من الألعاب على الانترنت تحتوي على عناصر عنف ودم -بشكل صريح- بما يؤدي لزيادة العدوانية بل قد يقلل من الشعور بالضمير(Charmaraman, Riche, & Göldag, 2020, 120) (Moreno,2020, 3 كما يؤدي اللعب المفرط إلى انخفاض الدافع للتعلم، وتؤثر سلبًا على الصحة البدنية والعقلية، (Tsai, Wang & Weng, 2020, 14) وتشير دراسات التصوير بالرنين المغناطيسي إلى تغييرات هيكلية في القشرة الأمامية للمخ مرتبطة بخلل وظيفي لدى مدمن الإنترنت(Dresp, 2020, 3) -الاعتلال المشترك هو القاعدة وعادة ما يشمل الاكتئاب الاجتماعي، واضطراب القلق، والرهاب الاجتماعي، والوسواس القهري، واضطراب فرط الحركة ونقص الانتباه، والعداء، واضطرابات تعاطي المخدرات. (Lopez-Fernandez & Kuss, 2020, 14) -هناك ألعاب ذات عناصر شبيهة بالمقامرة والتي يمكن أن تجعل لعب القمار أمرًا طبيعيًا بالنسبة للأطفال بالإضافة إلى تكاليف الإنفاق داخل اللعبة.(UNICEF, 2020, 11) . -يؤثر على الدماغ الأيمن فيجعلها متخلفة وهي المرتبطة بالتركيز وتخزين الذاكرة وتنظيم العاطفة، كما يؤدي لامتصاص إشعاع الموجات الكهرومغناطيسية، والإضرار بسرعة نمو دماغ الأطفال. (Munawar & Nisfah, 2020, 65- 67) -التعرض (غير المنضبط وغير المحدود) للتكنولوجيا بين الأطفال

المخاطر السيبرانية	الآثار السلبية
	الصغار يؤدي إلى العديد من المخاطر الفسيولوجية والصحية المتعلقة بالرؤية، وكذلك المخاطر العقلية والنفسية والسلوكية مثل الانعزال، والإدمان. (Tosun & Mihci, 2020, 2)
التنمر الإلكتروني	-تشمل العواقب المرتبطة بالإيذاء السيبراني تدني احترام الذات وزيادة مستويات الاكتئاب لدى الضحايا، وكذلك ضعف الأداء الأكاديمي، والتسرب من المدرسة، والعنف الجسدي والانتحار (Mark, 2014, 25) كما تشمل عواقب التنمر عبر الإنترنت على المتعلم: المشاكل الأكاديمية، والعنف المدرسي، والسلوك المنحرف (Cilliers & Chinyamurindi, 2020, 30)
-مشاهدة الأطفال للمواد الإباحية (Spiering, 2018, 14) (مرعي، ٢٠١٣، ٢١، ١٤٧، ١٨٧،، ٢٠٣، ٢٠٤، ٢١٠، ٢١١)	-إيقاظ الرغبة الجنسية مبكراً Awaking Sexual Passions وزيادة النشاط الجنسي عن طريق التفاصيل المرئية للممارسة الجنسية؛ فَتُقْصِي قيم الحياء، وتشكل صدمة شعورية للطفل في بداية رؤيتها سرعان ما يعتاد عليها من كثرة التعرض، الأمر الذي يدفعه إلى محاولة تجربتها في الواقع! مما يسهم في زيادة جرائم التحرش الجنسي أو زنا المحارم، خاصة في ظل غياب الرقابة الأسرية. -غرس الفكر الجنسي المتجرد من الفطرة والشريعة، وتوسيع مساحة الغرائز في حياته. -التغير الفسيولوجي وما يتبعه من زيادة معدلات ضربات القلب والآثار السلوكية behavioral effects التي ترتبط بإجراء معين بعد التعرض لوسيلة إعلامية. -يصبح الطفل مهووساً أسيراً لها، مدفوعاً بشكل لاإرادي نحوها، مصاباً بوابل من الأمراض النفسية والاجتماعية التي تصعب مقاومتها. -ينجرف الفرد نحو إشباع ملذاته دون وضع أي قيود على سلوكه. -تُحْدِث له نوع من التصادم الذي لايكون في مصلحته أو مصلحة الوطن؛ حيث يفرز شخصاً غير قادر على الإبداع أو الإنتاج منساقاً

المخاطر السيبرانية	الآثار السلبية
	وراء ما تروجه دول الغرب من إرواء الغرائز الجنسية؛ فيتجرد من هويته الدينية والأخلاقية ويهدد مستقبل مجتمعه وأمته العربية. -تشكيل اتجاهات سلبية فيما يتعلق بالعلاقات الحميمية Intimate Relationships؛ فالأشخاص الذين يتعرضون لمثل هذه المحتويات قد يعتقدون بأن ما يشاهدونه طبيعي وملائم للتطبيق في الحياة اليومية. -تكوين صورة ذهنية عن الأنثى في عقول مشاهديها؛ بحيث تتحول من كائن يحترمه ويتعايش معه إلى مجرد رمز جنسي. - ارتفاع معدلات التحرش بين شريحة المراهقين، وزيادة معدل الجرائم الجنسية.
الاستمالة	-يمكن أن تؤدي الاستمالة إلى حالات بغاء القصر وخطر الاتجار بالأطفال (Widiputera, Satria, Perdana , Zamjani & 2021, 3)؛ حيث يُنظر إلى استغلال الأطفال في المواد الإباحية على أنها مشكلة واسعة الانتشار ومتفاقمة في مجتمع العصر الحديث، إذ أن المواد الإباحية المشارك بها أطفال هي صناعة مربحة بمليارات الدولارات، حيث يتراوح إجمالي أرباحها من ١ إلى ٥ مليارات دولار سنويًا (Sitarz, Rogers, Bentley, and Jackson, 2014, 64-65)

وفي الأخير تفضي كل تلك المخاطر إلى سلوكيات لاتربوية تضعف البنية الاجتماعية داخل المجتمع وهي أمر حرج للأمن القومي والاقتصادي.

ج-الدواعي المتعلقة بمستجدات العصر.

١-الرقمنة والتوسع في استخدام الانترنت.

مما هو جدير بالملاحظة أنه في عام ١٩٧٠، بدأ الطفل الأمريكي العادي مشاهدة التلفاز بانتظام في سن ٤ سنوات، ولكن اليوم يبدأ الأطفال في التفاعل-باستخدام الوسائط الرقمية- في سن ٤ أشهر؛ ونتيجة لذلك يدرس الباحثون بشكل متزايد سياقات وعواقب أنشطة تلك الوسائط الرقمية الخاصة (Hornor, 2020, 191) ومن أسباب

انتشار الاستخدام انشغال الأبوين واستخدامهما له كجليسة أطفال أو "والد بديل" 'surrogate parent'؛ بغية تمكين الأبوين من القيام بالأعمال المنزلية، بل وجدت الدراسة أن الآباء قد أعطَوْا أطفالهم الهواتف الذكية كأداة لوقف بكائهم، وأظهرت الدراسة أن إدمان الأطفال على الأجهزة يأتي من عادات تساهل الوالدين؛ فلا يطلب الآباء من أبنائهم الالتزام والمسؤولية.(Munawar & Nisfah, 2020, 67-68))
(Livingstone, Mascheroni, Dreier, Chaudron, & Lagae, 2015, 9)

وقد أجرت مؤسسة Common Sense Media أبحاثاً -وهي مؤسسة مستقلة غير ربحية تعمل مع الآباء والمعلمين – أظهرت نتائجها أن الأطفال ينفقون أكثر وقتهم مع الوسائط الرقمية والأنشطة ذات الصلة أكثر مما يفعلون مع أسرهم أو في المدرسة. (Payne, 2016, 1)

وتمثل الزيادات الأخيرة لاستخدام الأطفال الأصغر سناً اتجاهاً عالمياً -خاصة في البلدان المتقدمة-؛ ففي **كوريا الجنوبية** (الدولة ذات أعلى سرعة انتشار للإنترنت في العالم) يستخدم فيها ٩٣٪ من الأطفال بسن ٣-٩ سنوات الإنترنت بمتوسط ٨-٩ ساعات أسبوعيًا، وفي **هولندا:** ٧٨٪ من الأطفال الصغار الهولنديين متصلون بالفعل بالإنترنت، وفي **الولايات المتحدة الأمريكية** يتصل بالإنترنت يوميًا ٧٠٪ من الأطفال في سن الثامنة، وفي **أستراليا** يتصل بالانترنت ٧٩٪ من الأطفال الذين تتراوح أعمارهم بين ٥-٨ سنوات(Holloway, Green & Livingstone, 2013, 8)

وقد كان أثر استخدام التكنولوجيا الشخصية (PTU) على الشباب في الولايات المتحدة "سريعًا وصعبًا"؛ حيث بلغ معدل انتشار الإنترنت ٩٢٪ ؛ مما يخلق عددًا كبيرًا من الشباب المعرض لخطر الوقوع ضحايا لجرائم الإنترنت(Dresp, 2020, 2) (Lewis, 2020, 14) كما أن في أستراليا، يتصل بالإنترنت أكثر من ٩٥٪ ممن تتراوح أعمارهم بين ٨ و ١٧ عامًا، و ٨١٪ من الأطفال في سن ما قبل المدرسة الذين تتراوح أعمارهم بين ٢-٥ سنوات، لذا أصبح هناك اهتمام متزايد بالأمان على الانترنت. (Australian Centre to Counter Child Exploitation, 2020, 7)

٢-أزمة كورونا وقضاء وقت أطول على الانترنت.

تسببت جائحة COVID-19 في ظهور أكبر اضطراب في أنظمة التعليم بالتاريخ، فأثرت على ما يقرب من ١.٦ مليار متعلم في أكثر من ١٩٠ دولة جميعها قام بإغلاق المدارس، كما أثرت على ٩٤ % من عدد التلاميذ في العالم، لدرجة لم تعلن فيها ١٠٠ دولة عن موعد لإعادة فتح المدارس عبر العالم، بالإضافة إلى إغلاق المدارس؛ وقد تم تأجيل الامتحانات؛ في عدد قليل، أو إلغاؤها؛ وفي حالاتٍ أخرى لديهم تم استبدالها بالتقييمات المستمرة أو طرق بديلة، مثل الاختبار عبر الإنترنت للامتحانات النهائية، والتقييم المستمر المبتكر، وتَمَثَّلَ التأثير العالمي لـ COVID-19 في أن الشباب يقضون وقتًا أطول في المنزل- والمزيد من الوقت على الإنترنت، وتشير التقديرات إلى أن أنشطة التعلم عن بعد في البلدان ذات الدخل المرتفع تغطي حوالي ٨٠-٨٥ %، بينما ينخفض هذا إلى أقل من ٥٠ % في بلدان الدخل المنخفض، ويمكن أن يُعزى هذا النقص -إلى حد كبير -إلى الفجوة الرقمية للمحرومين من الوصول المحدود إلى الخدمات المنزلية الأساسية مثل الكهرباء، ونقص البنية التحتية التكنولوجية؛ والمستويات المنخفضة من الأمية الرقمية بين التلاميذ وأولياء الأمور والمعلمين (De Giusti, 2020, 2, 3, 12, 14) ومن ثم دعا قادة الحكومة -جميع المواطنين للقيام بدورهم لوقف انتشار الفيروس ومنع الوفيات غير الضرورية(Buchholz, DeHart & Moorman, 2020, 11)، ونظرًا لمتطلبات التباعد التي تمليها جائحة كوفيد -١٩؛ تمت عمليات إغلاق غير مسبوقة للمدارس عام ٢٠٢٠ -على حد وصف تقرير الأمم المتحدة- وتحويل التعليم إلى ساحة الإنترنت؛ ليصبح التعلم عن بعد إلزاميًا على مستوى العالم (Shersad & Salam, 2020, 348) وأثر الفيروس سلبا على جميع قطاعات الصحة والتعليم والاقتصاد والسياسة والاجتماع. (Hassan, 2021, 236) كما كشفت جائحة COVID-19 عن أوجه عدم مساواة كانت أقل وضوحًا في سياق التعلم وجهًا لوجه، خاصة فيما يتعلق بالوصول إلى الأجهزة الرقمية الضرورية(Buchholz, DeHart & Moorman, 2020, 15)

د-الدواعي المتعلقة بطبيعة الاستخدام.

يبدأ الأطفال في استخدام الإنترنت في سن مبكرة جدًا من العمر، مما يجعل من الضروري أن يبدأ تعليم الأمان عبر الإنترنت في الطفولة المبكرة، بالإضافة إلى أن

التلاميذ لا يستخدمون الإنترنت كمستهلكين فقط ولكنهم يساهمون أيضًا في قاعدة بياناته الواسعة من المدونات والصور ومقاطع الفيديو باستمرار، (Saluja, Bansal & Saluja 2012, 1-3) وكثيرًا ما يستخدم التلاميذ التقنيات التعليمية للأنشطة خارج المهمة مما يؤدي إلى انخفاض في الأداء التعليمي.(Schubart, 2021, 2)

ووفقا للإحصاءات العالمية الحديثة فإن مستخدمي الإنترنت يقضون في المتوسط ٦ ساعات و ٤٣ دقيقة يوميًا على الانترنت، وهذا يعني أن ٤٠٪ من وقت الاستيقاظ اليومي يستخدم للوصول إلى الإنترنت. (Widiputera, Satria, Perdana, Zamjani & 2021, 1) بل تحول الكثير من الناس منذ عام ٢٠٠٧ وبشكل تلقائي إلى مراسلين جماهريين؛ فنمو الإعلام الاجتماعي من وسائل التواصل الاجتماعي والمدونات سمح بالعودة الهائلة لمصطلح "صحافة المواطن" أو " وسائل إعلام النحن" باستخدام أجهزة الإعلام الشخصية المتواجدة في كل وقت وكل مكان. (شفيق، ٢٠١٤، ٦٦)

كما أنه قد يصعب على الآباء التعامل مع الأجهزة الإلكترونية والرقمية، وذلك لعدة أسباب: أولاً، إنها أكثر تعقيدًا من الناحية التكنولوجية، ثانيًا، تفرض ابتكارات السوق على الآباء ضرورة الاستمرار في تحديث وتكييف عاداتهم؛ فقد يكون الآباء أنفسهم أقل دراية ببعض الأجهزة أو الخدمات الرقمية المستحدثة باستمرار، ثالثًا، نظرًا لأن الأجهزة الرقمية أصبحت أكثر تخصيصًا وقابلية للحمل، أصبحت الاستراتيجيات التقليدية للاستخدام المشترك للوسائط أو الإشراف عليها أقل فاعلية. (Livingstone, Mascheroni, Dreier, Chaudron, & Lagae, 2015, 7)

والناس أنفسهم ليس لديهم مجموعة صارمة من الأخلاق حول ما هو صواب أو خطأ في سلوكهم عبر الإنترنت، وفي الواقع غالبًا ما يشعرون بأنهم مجهولون، وبالتالي يمكنهم الابتعاد عن مدونة الأخلاق المعتادة(Muir, 2010, 7, 17)، ويقوم بعض التلاميذ بالنشر والتصرف بشكل غير لائق عبر الإنترنت؛ معتقدين أنهم مجهولون تمامًا للآخرين (Payne, 2016, 14) الأمر الذي يؤدي إلى ظهور ما يسمى بالتهديدات الأخلاقية Moral Panics؛ وكذا الانهيار الأخلاقي Breakdown of morals ؛ حيث أحدثت شبكة الانترنت ثورة مروعة في النشر؛ فأصبح النشر العاري في متناول

عموم الأفراد وليس فقط الأناس العريقين في صناعة المواد الإباحية مما جعلها تصنف بأنها خطر يهدد قيم ومصالح المجتمع (مرعي، ٢٠١٣، ٢٠٣،١٥٦)

هـ–الدواعي المتعلقة بطبيعة شبكة الانترنت.

إن الانترنت متاح ٢٤ ساعة في اليوم، ٧ أيام في الأسبوع؛ فيمكن أن تقع مخاطر التنمر الإلكتروني –على سبيل المثال– في جميع أوقات اليوم، مع احتمال جمهور أكبر؛ حيث يقوم الأشخاص بإعادة توجيه المحتوى بنقرة واحدة (Department for Education, 2017, 8)، وبالتالي يقد تتعرض الضحية للسخرية والإحراج ليس أمام قلة من زملائها بل أمام العالم بأسره (Muir, 2010, 28).

وبعد أن كان باب البيت الأمامي في وقتٍ ما يقف حاجزاً أمام المجرمين؛ أما الآن، فوسائل التواصل الاجتماعي تسمح لهم بمتابعة ضحاياهم في منازلهم. بالإضافة إلى أن المعلومات عبر الإنترنت دائمة: فالمعلومات تبقى على الإنترنت إلى الأبد، وتبين المعلومات للغرباء الضعف العاطفي للشخص من خلال بصمته الرقمية، علاوة على أنه في عالم الانترنت لا أحد مسؤول؛ لا يمكن للحكومات السيطرة على الحدود عبر الإنترنت؛ لذلك فإن الإنترنت هي منطقة مثالية لمجرمي الإنترنت الذين يعرفون كيف يظلون مجهولين(Muir, 2010, 6, 14) ويضع هؤلاء الأطفال معلوماتهم الشخصية وصورهم في الأماكن العامة دون أن تدرك تلك الفئة أنها تعرض نفسها للخطر، وقد ذكر الأمن البريطاني وشركة حماية البيانات Sophos أنها أجرت تحقيقًا أظهر أن ٤٦٪ من مستخدمي Facebook كانوا على استعداد تام لمصادقة الغرباء وبالتالي تسليم المعلومات الشخصية عن طيب خاطر.(Saluja, Bansal & Saluja, 2012, 2)

فضلاً عن أن الفضاء السيبراني ليس له قوانين أو تشريعات ملزمة تنظم التفاعل بين المستخدمين، وليس له حدود جغرافية فلا يقتصر الفضاء الإلكتروني على بلد أو قارة واحدة، بل هو عبارة عن شبكة تمتد عالميًا (أكثر من ٢٠٠ دولة) وتضم حوالي ٤.٥ مليار من المستخدمين، كما أن إخفاء الهوية داخل الفضاء السيبراني يسمح للمجرمين بالاختباء وراء الافتقار إلى الحدود والتشريعات داخل الفضاء السيبراني (Kritzinger, 2020b, 16–17)

بالإضافة إلى طبيعتها الجاذبة، ويؤيد ذلك إفادة إحدى الدراسات أن أكثر من نصف الأطفال والشباب من مستخدمي وسائل التواصل الاجتماعي كانوا قد أمْضَوْا وقتًا على الإنترنت أطول مما كانوا يقصدون. (Dubicka & Theodosiou, 2020, 8, 23)

ثالثاً: المخاطر السيبرانية التي يتعرض لها تلاميذ المدارس الابتدائية.

جدول (٤) المخاطر حسب الفئة العمرية:(Muir, 2010, 10-11)

الصف	المخاطر
من الصفوف ١-٤	▪ التعثر في مواقع غير مناسبة. ▪ مشاركة كلمات المرور. ▪ تكوين صداقات مع شخص غريب عبر الإنترنت. ▪ الاستجابة للحيل الإعلانية في ألعاب الأطفال/ المواقع الاجتماعية.
من الصف ٥-٨	▪ التنمر السيبراني . ▪ نشر صور غير لائقة لأنفسهم. ▪ إرسال الرسائل النصية الساخنة في الألعاب عبر الإنترنت. ▪ كشف المعلومات الشخصية على الشبكات الاجتماعية. ▪ التعرض للمفترسين الجنسيين (الاستمالة).
من الصف ٩-١٢	▪ نشر معلومات / صور يمكن أن تضر. ▪ كشف نقاط الضعف العاطفية للغرباء مع الأطفال الأكبر سنًا.

تمثل الزيادات الأخيرة لاستخدام الأطفال الأصغر سناً اتجاهاً عالمياً، وخاصة في البلدان المتقدمة؛ ففي السويد: يستخدم ٧٠٪ من الأطفال الذين تتراوح أعمارهم بين ٣ و٤ سنوات الإنترنت، وفي هولندا: ٧٨٪ من الأطفال الصغار الهولنديين وأطفال ما قبل المدرسة متصلون بالفعل بالإنترنت. وفي كوريا الجنوبية (الدولة ذات أعلى سرعة انتشار للإنترنت في العالم) يستخدم فيها ٩٣٪ من الأطفال بسن ٣-٩ سنوات الإنترنت بمتوسط ٨-٩ ساعات أسبوعيًا، وفي الولايات المتحدة يتصل بالإنترنت يوميًا ٢٥ ٪ من الأطفال بعمر ٣ سنوات، وترتفع إلى حوالي ٥٠٪ بحلول سن الخامسة، و٧٠٪ بحلول سن الثامنة، وفي أستراليا، ٧٩٪ من الأطفال الذين تتراوح أعمارهم بين ٥-٨ سنوات على الإنترنت في المنزل بهم(Holloway, Green & Livingstone, 2013, 8)

ويتعرض تلاميذ المدارس للعديد من المخاطر عبر الانترنت كما في جدول (٢)، وقد صنفت تلك المخاطر إلى مخاطر محتوى ومخاطر سلوك ومخاطر اتصال، كما صُنِّفَت حسب المرحلة الصفية كما في جدول (٤) .وستتناول الدراسة من كل صنفٍ خطراً على الأقل بمزيد من التركيز:

أ-إدمان الانترنت.

تعتبر وسيلة اللعب أداة قوية يمكن استخدامها لتعزيز قدرة الأطفال على مواجهة التحديات بشكل أفضل؛ إنها في الغالب وسيلة التفاعل المفضلة لديهم وتسمح لهم بمعالجة التجارب بشكل هزلي، (Weis, 2020, 2) فقد جمعت الألعاب الإلكترونية بين الصوت والصورة والموسيقى والمؤثرات الصوتية والمحاكاة للواقع (حجازي، ٢٠١٨، ٣).

بينما يجذب العالم الرقمي الأطفال من خلال وسائل الترفيه الخاصة به وفرص التعليم، إلا أن الحقيقة أن هذا العالم الرقمي لا يزال هيكلًا تجاريًا للغاية؛ فمخططات الاستغلال الاقتصادي في الليبرالية الجديدة لا تهتم إذا كانت المواد مناسبة للبالغين أو للأطفال؛ علاوة على أنها تقوم بتقديم إعلانات مخصصة لحث الأطفال على شراء أو محاولة الفوز بعناصر داخل التطبيق للتقدم في الألعاب التي يلعبونها؛ ولذلك الاستغلال تأثير سلبي كبير على الأطفال، بما في ذلك انتهاك حقوقهم في النمو والخصوصية وحرية الفكر والحماية ضد الاستغلال الاقتصادي لأوائل القرن الحادي والعشرين، Tosun (& Mihci, 2020, 4) وتم توثيق دور تقنية الإقناع فيما يتعلق بالاستخدام القهري، ويظهر-على سبيل المثال- في الإشعارات التي تفيد بأنه تم "الإعجاب" بمنشور ما أو بتغريدة. (Dubicka & Theodosiou, 2020, 21)

تم تشخيص اضطراب إدمان الإنترنت (IAD) مؤخراً، ويسمى أحيانًا أخرى الإنترنت الباثولوجي / الإشكالي، اضطراب الألعاب عبر الإنترنت (IGD)على أنه اضطراب عقلي في الإصدار الخامس (DSM-5) للدليل الإحصائي للاضطرابات العقلية في عام ٢٠١٣ (Dresp, 2020, 2) وعام ٢٠١٨، قررت منظمة الصحة العالمية إدراج اضطراب الألعاب في التصنيف الدولي للأمراض - المراجعة الحادية عشرة للأمراض (ICD-11) (Faltýnková, Blinka, (World Health Organisation (WHO), 2018). Ševˇcíková, & Husarova, 2020, 1)

أدى هذا الإدراج إلى أن نبهت وسائل الإعلام لديها الجمهور العام فيما يتعلق بمشاكل الإدمان الناشئة على الإنترنت، وتم التركيز عليها في المناطق الأمريكية والأوروبية وأستراليا وبلدان آسيا، ولكن حققت الإجراءات الوقائية التي اتخذت نجاحا محدودا (Lopez-Fernandez & Kuss, 2020, 2)

وقد اعترفت الصين بإدمان الإنترنت باعتباره اضطرابًا رسميًا عام ٢٠٠٨، وبالمثل، عام ٢٠٠٢ افتتحت حكومة كوريا الجنوبية أول مركز استشاري في العالم للوقاية من إدمان الإنترنت، ومنذ ذلك الحين طُوِّرت مشاريع واسعة النطاق لمعالجة الإفراط في استخدام التكنولوجيا، وتشير التقارير إلى أن ١٢٪ من آباء الأطفال بعمر ثلاث سنوات، و ١٩٪ من الآباء بين سن الخامسة والسابعة، ٣٣٪ من الآباء من سن ٨ إلى ١١ عامًا و ٤١٪ من الآباء من ١٢ إلى ١٥ عامًا يجدون صعوبة في التحكم في وقت الشاشة، ويتعرض الشباب -بشكل خاص- للاستخدام القهري لأنهم أقل قدرة على التنظيم الذاتي ويميلون إلى الحصول على مكافآت فورية؛ ويساعد على ذلك تصميم التطبيقات بنظام (الاستخدام الممتد) بخصائص الإخطارات من خلال (الطنين، والأصوات، والاهتزازات)؛ لقراءة (عدد الإعجابات، إعادة التغريد، الأصدقاء)؛ فتجذب انتباههم للمشاركة في التطبيق. (Dubicka & Theodosiou, 2020, 23, 35-36) بالإضافة إلى أن المؤثرات الصوتية والضوئية للألعاب الرقمية والمكافآت والترويج والصور الواقعية والممتعة والتحدي يمَكّن من إشباع حس الإنجاز في عقول الأطفال وتحقيق الترفيه (Tsai, Wang & Weng, 2020, 14) كما تمثل الألعاب ذريعة للهروب من هذه الحياة والدخول إلى منطقة نشاط مؤقت ذات ميول فريدة خاصة.(Göldag, 2020, 118)

أما مصطلح مدمن الإنترنت فيعني شخص يستخدم الإنترنت بشكل مفرط "لغرض واحد" مثل الألعاب أو المواد الإباحية (Lim, 2012, 11) ووصلت نسبة إدمان الألعاب في (جنوب كوريا) لدى الأطفال الذين تتراوح أعمارهم بين ١٣ و ١٦ عامًا ٥٠٪ (Göldag, 2020, 125)

عرّف DSM-5 (الدليل التشخيصي والإحصائي للاضطرابات النفسية) اضطراب الألعاب عبر الإنترنتIGD بأنه "الاستخدام المتكرر للألعاب القائمة على

الإنترنت في غضون عام، ويكون غالبًا استخداماً تفاعلياً مع لاعبين آخرين، وبما يؤدي إلى مشكلات كبيرة في الأداء (Dubicka & Theodosiou, 2020, 62) وقد حددت الدراسات الأكاديمية مقدار الاستخدام المؤذي أو المكثف للإنترنت بواقع ٤ ساعات يوميًا أو ٣٠ ساعة أسبوعياً (King, Delfabbro, Doh, Wu, Kuss, Pallesen, Mentzoni, Carragher, & Sakuma, 2018, 234) ويجب استيفاء المؤشرات التالية للتأكيد بأن شخصاً ما مدمنٌ للألعاب:

١- الانشغال أو الهوس بألعاب الإنترنت٢-أعراض الانسحاب عند عدم ممارسة ألعاب الإنترنت٣- التسامح أي تراكم التراخي بما يلزم قضاء المزيد من الوقت في ممارسة الألعاب٤- الانتكاس: وتعني محاولة الشخص إيقاف أو منع ممارسة ألعاب الإنترنت ولكنه فشل في ذلك٥- فقد الشخص الاهتمام بأنشطة الحياة الأخرى، مثل الهوايات٦- استمرار الشخص في الإفراط في استخدام ألعاب الإنترنت حتى مع العلم لمدى تأثيرها على حياة الشخص٧- كذب الشخص على الآخرين حول مقدار الوقت الذي يقضيه في اللعب ٨-استخدام الشخص ألعاب الإنترنت لتعديل المزاج وكطريقة للتخلص من القلق أو الذنب (للهروب)٩-خسارة الشخص فرصة أو علاقة أو وظيفة بسبب الإنترنت. (Ünübol, Koç, Sayar, Stavropoulos, Kircaburun & Griffiths, 2020, 3)

أما عن العواقب فهناك أدلة تشير إلى أن النمو المعرفي للأطفال يمكن أن يتضرر بفترات طويلة من استخدام الإنترنت، بما في ذلك تطوير مهارات الذاكرة، ومدى الانتباه، وقدرات التفكير النقدي، واكتساب اللغة والقراءة والتعلم، وتشير الدراسات إلى أن الإنسان يكون لديه استدعاء أقل للمعلومات عند اعتماده على استخدام محتوى الإنترنت فيبذل جهوداً أقل لتخزين المعلومات في الذاكرة؛ حيث يمكن للمرء بدلاً من ذلك حفظ مكان استرداد المعلومات فقط، إذا علم المرء أن المعلومات لن تكون متاحة -كما في الوضع العادي- فإن المرء يبذل المزيد من الجهد في ترميزه ويتولد لديه استدعاء أفضل للمعلومات.(Quaglio & Millar, 2020, 5, 17)

على الرغم من وجود أدلة على أن الألعاب الرقمية قد يكون لها تأثيرات إيجابية منها تطوير القدرة على تعزيز المهارات البصرية والريادة لاكتساب المهارات،

وتستخدم في سياق إعادة التأهيل على سبيل المثال، للأطفال الذين يخضعون للعلاج الكيميائي، وللأطفال الذين يعانون من ضمور العضلات وللأطفال المصابين بالتوحد (Dubicka & Theodosiou, 2020, 37-38)، كما تتطلب الألعابُ مستخدمينَ يتمتعون بمهارات عالية في اللغة الإنجليزية، من أجل فهم إعدادات اللعبة وإجراءاتها، هذا سوف تشجع بشكل غير مباشر على تطوير القراءة والكتابة ومهارات التحدث باللغة الإنجليزية (Rahman, Malaysia, Sairi, Zizi, & Khalid, 2020, 379)

فعلى الرغم من أن استخدام الأدوات الذكية يؤدي إلى تطوير الدماغ الأيسر، إلا أن ذلك يؤثر سلباً على الدماغ الأيمن فيجعلها متخلفة -وهي المرتبطة بالتركيز وتخزين الذاكرة وتنظيم العاطفة-، كما أظهرت البيانات أن البالغين يمتصون ٢٥٪ من إشعاع الموجات الكهرومغناطيسية، بينما الأطفال بعمر ١٢ سنة يمتصون ٥٠٪ من الإشعاع، والأطفال بعمر ٥ سنوات يمتصون ٧٥٪ من الإشعاع؛ بما يشكل خطورة عالية، وقد يؤدي العنف أو المواد الإباحية إلى الإضرار بسرعة بنمو دماغ الأطفال (Munawar & Nisfah, 2020, 65- 67) ، وأظهرت الدراسات أن التعرض (غير المنضبط وغير المحدود) للتكنولوجيا بين الأطفال الصغار يؤدي إلى العديد من المخاطر الفسيولوجية والصحية المتعلقة بالرؤية أو الموقف، وكذلك المخاطر العقلية والنفسية والسلوكية مثل الانعزال والإدمان، (Tosun & Mihci, 2020, 2) بالإضافة إلى ضعف الإبداع والمهارات الاجتماعية الأقل تطورًا بسبب نقص الممارسة في الواقع. (Spiering, 2018, 13) كما أنه ثبت الارتباط المباشر بين المشاركة المفرطة في الألعاب عبر الإنترنت والعجز البنيوي في منطقة الدماغ. (Dubicka & Theodosiou, 2020, 37-38)

ب-التنمر الإلكتروني.

يعد التسلط عبر الإنترنت مشكلة عالمية، واحد من كل ستة آباء في جميع أنحاء العالم يبلغون عن إنجاب طفل تعرض للتنمر السيبراني (Wilbon, 2020, 2) من خلال المضايقات الخبيثة المتعمدة والمستمرة أو التشهير بالمعلومات عن عمد باستخدام الإنترنت(White, 2013, 1, 16) ويُعرَّف التنمر الإلكتروني على أنه أي سلوك يتم إجراؤه من خلال الوسائط الإلكترونية أو الرقمية من قبل الأفراد أو المجموعات ينقل بشكل متكرر رسائل عدائية أو عدوانية؛ تهدف إلى إلحاق الأذى أو عدم الراحة

للآخرين، فيتميز التنمر عبر الإنترنت بِسِمتين: تكرار الفعل ونية إلحاق الأذى بالضحية(Cilliers & Chinyamurindi, 2020, 28)

وفي أحد الأبحاث مع ما يقرب من ٢٠٠٠ طالباً من تلاميذ المدارس المتوسطة الذين تم اختيارهم عشوائيًا في منطقة تعليمية رئيسة في الولايات المتحدة الأمريكية كانوا ضحايا للإنترنت، من بين هؤلاء التلاميذ البالغ عددهم ٢٠٠٠ طالب، أفاد ٢٠٪ منهم أنهم يفكرون بجدية في الانتحار و ١٩٪ حاولوا الانتحار –بعد تعرضهم للتنمر السيبراني– ؛ لذا أصدر كونغرس الولايات المتحدة قانونًا يجعل من الإزعاج أو الإساءة أو التهديد أو مضايقة شخص آخر عبر الإنترنت جريمة فيدرالية White, 2013, 7, (54)، وتكمن خطورته في أنه قد يُحْدِث انتهاك كرامة الطفل، و/ أو يجعلهم يشعرون بالخوف أو الإهانة أو الإذلال و/ أو يخلق بيئة معادية أو مسيئة، من خلال إبداء تعليقات بذيئة، والإدلاء بملاحظات جنسية حول الملابس والمظهر. (Department for Education, 2014, 93)

فالتنمر الإلكتروني "هو تنمر يستخدم التكنولوجيا الإلكترونية كوسيلة لإيذاء الآخرين"؛ يستخدم تقنيات خدمة الإنترنت مثل البريد الإلكتروني أو مجموعات مناقشة غرفة الدردشة أو المراسلة الفورية أو صفحات الويب أو الرسائل القصيرة (الرسائل النصية)؛ بقصد إيذاء شخص كتخويف المتلقي أو التحكم فيه أو التلاعب به أو إذلاله. (Department of Education and Children's Services, 2009, 18)

يُعَرَّف التنمر إلى حد كبير من خلال تأثير السلوك على المتلقي؛ فيمكن النظر إلى التنمر في المقام الأول من منظور العدوان، أو عنف طويل الأمد، جسديًا أو نفسيًا، يمارسه فرد أو مجموعة، وموجه ضد فرد غير قادر على الدفاع عن نفسه في الوضع الفعلي (ENISA, 2012, 8) ووجب على المدارس أن تبذلَ جهوداً استباقية لمكافحة التسلط عبر الإنترنت، ولكن جهوداً تتجاوز نطاق الدورات التدريبية؛ فقد يكون للتسلط عبر الإنترنت نتائج مميتة، وقد وجدت دراسة (Nye, 2014, 41, 50) أنه بمجرد تعرض مجموعة من التلاميذ للتنمر، تأثر نجاحهم الأكاديمي باستمرار؛ حيث تسمح التكنولوجيا الجديدة للضحايا بالهجوم في أي وقت وفي أي مكان، كما أدى استخدام المتنمرين عبر الإنترنت لإخفاء الهوية إلى صعوبة إدارتها داخل نظام المدرسة

(Yancey, 2017, 26)؛ فالفرق الرئيس بين التنمر في ساحة المدرسة والتسلط عبر الإنترنت هو أن التنمر عبر الانترنت يحدث ٢٤ ساعة في اليوم، ٧ أيام في الأسبوع، ويمكن أن يعَرِّض الضحية للسخرية والإحراج ليس أمام قلة من زملائه بل أمام العالم بأسره (Muir, 2010, 28).

ج–مشاهدة عناصر غير لائقة.

فبالإضافة إلى مشاهدة الأطفال مدوّني فيديو وشخصيات على YouTube ومقاطع فيديو مضحكة. (Rahman, Malaysia, Sairi, Zizi, & Khalid, 2020, 378) بشكل مبالغ فيه ومبتذل، قد يتعرض لمخاطر المحتوى.

وتُعرِّف اليونيسف "مخاطر المحتوى" على أنها مواقف "يتعرض فيها الطفل لمحتوى غير مرحب به وغير مناسب، يمكن أن يشمل ذلك المحتوى الجنسي والإباحي والصور العنيفة، بعض أشكال الإعلان، المواد العنصرية أو التمييزية أو خطاب الكراهية؛ ومواقع الويب التي تدعو إلى سلوكيات غير صحية أو خطيرة، مثل إيذاء النفس والانتحار وفقدان الشهية والانضمام لجماعات مشبوهة. (UNICEF, 2017, 21).

فالأطفال عرضة للفكر المتطرف، ويحدث التأثير من خلال العديد من الطرق المختلفة (مثل وسائل التواصل الاجتماعي أو الإنترنت)؛ فالتطرف هو المعارضة الصوتية أو النشطة لقيمنا الأساسية، بما في ذلك الديمقراطية وسيادة القانون والحرية الفردية والاحترام المتبادل والتسامح مع الأديان والمعتقدات المختلفة؛ يتضمن هذا أيضًا الدعوة إلى مقتل عناصر من القوات المسلحة؛ أما الإرهاب هو عمل يعرض للخطر أو يتسبب في عنف خطير لشخص أو مجموعة يتسبب في أضرار جسيمة للممتلكات؛ أو عنف يتدخل بشكل خطير أو يعطل النظام الإلكتروني. (Department for Education, 2014, 90)

ويمكن تعريف المواد الإباحية بأنها الصور أو مقاطع الفيديو المقلدة التي تظهر فيها الأعضاء التناسلية و/ أو الأشخاص يمارسون الجنس بهدف إثارة المستهلك جنسيا وتشتمل على بعض السلوكيات العدوانية بما في ذلك الاختناق، والضرب، والركل، واستخدام الأسلحة، والجلد والاختناق والعض، والمعضلة أن المواد الإباحية على الإنترنت متاحة ومتوفرة ٢٤ ساعة في اليوم، ٧ أيام في الأسبوع من أي مكان متصل بالإنترنت،

وفي دراسة أمريكية على ما يقرب من ١٠٠٠ مراهق ذكرت أن ٦٦٪ من الذكور و ٣٩٪ من الإناث شاهدوا المواد الإباحية على الإنترنت(Hornor, 2020, 192)

ومن الأضرار الشائعة للمشاهدة: ممارسة الجنس والاتصال غير المرغوب فيه، وزيادة النشاط الجنسي بسبب مخاطر المحتوى الجنسي عبر الإنترنت (Spiering, 2018, 14) ورأى مسئولون جنائيون أن استهلاك المواد الإباحية من أكثر السمات المشتركة بين مرتكبي جرائم القتل والاغتصاب (مرعي، ٢٠١٣، ٢١٠)

وقد وجدت دراسة أجرتها شركة سيمانتيك لأمن الكمبيوتر أن أكثر الموضوعات شيوعاً والتي يبحث عنها الأطفال والمراهقون على الانترنت من خلال استخدامهم لموقع يوتيوب هي كلمتا جنس وصور فاضحة واللتين احتلتا المركزين الرابع والسادس على التوالي، كما تزيد عدد المواقع الإباحية بشكل كبير؛ فخلال ٥ سنوات زادت بمعدل ١٨٠٠٪ حيث وصل عددها ٢٦٠ مليون صفحة عام ٢٠٠٣، وأن كل ثلاثة من عشرة في البلدان العربية يتصفحون هذه المواقع، كما كشف موقع ياهو تقريراً إحصائياً حول أكثر من ٢٠٠ مصطلح يبحث عنها بالموقع ذاته، وأفاد بأن ١٨٤ مصطلحاً كان جنسياً، واعترف ٨٦٪ من الجناة بأنهم يكثرون من استخدام هذه المحتويات. (مرعي، ٢٠١٣، ١٦٨، ١٨٣، ٢١٣)

وأثبتت المباحث الفيدرالية اقتران ٨٠٪ من حالات جرائم الاغتصاب بالعثور على مواد إباحية وجنسية في منزل الجاني؛ فقد قام دارل بوب الضابط في شرطة متشغان بأمريكا بدراسة ٣٨٠٠٠ حالة اغتصاب فوجد أن نسبة ٤١٪ من مقترفي تلك الجرائم كان قد عرض نفسه قبل أو خلال ارتكاب جريمته إلى مواد إباحية، ويدعم هذا الموقف الباحث ديفيد سكات الذي وجد أن ٥٠ من المغتصبين قد عرضوا أنفسهم لمواد خليعة لتهيئة وتنشيط أنفسهم جنسياً قبل المباشرة بجريمتهم، ورجال الاستخبارات الأمريكية وجدوا أن ٨٠ من حالات جرائم الاغتصاب يتم العثور على مواد إباحية إما في موطن الجريمة أو في منزل الجاني. ويبدو أن العامل الاقتصادي هو الحافز الأول لانتشار تجارة الإباحية؛ فقد قدر معهد فورستر للأبحاث العوائد السنوية التي جنتها المواقع التي تتعامل مع الصور الفاضحة في عام ١٩٩٨ بمبلغ ٨٠٠ مليون دولار بينما تجاوزت مبلغ البليون دولار عام ٢٠٠٠. (العصيمي، ٢٠٠٤، ١١١-١١٢)

لذا تقسم الاتجاهات العالمية المعاصرة في إدارة مخاطر مشاهدة القُصَّر لعناصر غير لائقة لاتجاهين: أولهما الاتجاه التقييدي والذي تقوم فيه الحكومات بمنع الوصول إلى المحتويات غير المرغوبة أو غير المناسبة، وفرض ضوابط وقوانين للحد من مخاطرها، وهذا الاتجاه مأخوذ به في كل من الصين والسعودية وسنغافورة والإمارات العربية المتحدة وفيتنام. وفي هذا الصدد صنف (Warf, 2011) رقابة الدول على الانترنت في إطار إدارة المخاطر السيبرانية على النحو التالي:

– أسوأ رقابة للإنترنت مع أمثلة: الصين وبورما وكوريا / ميانمار وفيتنام وإيران.

– رقابة صارمة على الإنترنت مع أمثلة: روسيا، بيلاروسيا، باكستان، وكازاخستان دول العالم العربي مثل المملكة العربية السعودية والأردن والبحرين، إلخ.

أما الاتجاه الآخر فاتجاه تمكيني في إدارة المخاطر السيبرانية Enabling Trends وفيه تُبْنَى السياسات الحكومية على تشجيع التنظيم الذاتي لشبكة الانترنت، والاستخدام الطوعي للمستخدمين لتكنولوجيا الترشيح/الحجب Filtering / Blocking Technologies وانتهج هذا المدخل بريطانيا وكندا وفرنسا واليابان ونيوزيلندا وأستراليا وعدد كبير من دول أوروبا الغربية، وفي هذا الصدد يصنف (Warf, 2011, 7) رقابة الدول على استخدام الانترنت على النحو التالي:

***رقابة معتدلة للإنترنت** مع أمثلة: تايلاند، ماليزيا، سنغافورة، روسيا، إندونيسيا، الهند وآسيا الوسطى والإمارات العربية المتحدة وجنوب أفريقيا وأمريكا اللاتينية، وتسمى تكتيكات الرقابة "الناعمة ولاسيما الرقابة الذاتية وتشجيع مزودو خدمات الإنترنت لمراقبة مستخدميهم.

***مراقبات الإنترنت الخفيفة** مع أمثلة: بعض دول أمريكا اللاتينية، وجنوب وشرق أوروبا.

***الإنترنت غير الخاضع للرقابة** مع أمثلة من أوروبا الغربية وشمال أوروبا والولايات المتحدة الأمريكية) وأشكالًا أخرى من الرقابة الضمنية لم يتم ملاحظتها، فيفضِّل الكثيرون ترك السيطرة في أيدي الوالدين فقط، بينما يدعم الآخرون السياسات الحكومية التي تتطلب تصفية واسعة النطاق.

د–الاستمالة.

يتعرض الصغار لسوء المعاملة من خلال التكنولوجيا أثناء استكشافهم بشكل مستقل للإنترنت بلا حدود أو مراقبة، وبحسب إحصاءات الشرطة الملكية الماليزية (PDRM)، ما يقرب من ٨٠ ٪ من حالات الاغتصاب المبلغ عنها في البلاد على مدى العامين الماضيين أشركت الصداقات في الواقع الافتراضي، ومعظم الضحايا دون سن ١٨ (Rahman, Malaysia, Sairi, Zizi, & Khalid, 2020, 378) وتتم الاستمالة بصور مختلفة منها: الاستمالة من خلال الدردشة عبر الإنترنت أو داخل اللعبة.(UNICEF, 2020, 11)

وفقًا لمسح أجراه (Clarke & Crowther, 2015, 5) في ١١ مدرسة ابتدائية تَبَيَّنَ أن أكثر من ربع تلاميذ المدارس الابتدائية تواصلوا مع أشخاص لا يعرفونهم عند استخدام وسائل التواصل الاجتماعي.

وتعرَّف الاستمالة في إتفاقية لانزاروت –وهي أول صك قانوني دولي– بأنها "الاستدراج المقصود للأطفال من مشتهي الأطفال؛ لممارسة الجنس، أو للحصول على صور أو مقاطع فيديو جنسية لهم، ويمكن أن تشمل هذه الجرائم البث المباشر، ومن إستراتيجياته تعريض الطفل تدريجيًا لمواد جنسية صريحة لتقليل المقاومة أو الموانع المتعلقة بالجنس (الاعتداء الجنسي) وتعليم الأطفال ما يريدونه منهم بالضبط، وتهدئتهم بأن هذا النشاط الجنسي ممتع لا خوف منه، قد لا يؤدي ذلك بالضرورة إلى لقاء شخصيًا، قد تظل العلاقة على الإنترنت ومع ذلك تسبب ضررا جسيما للطفل (Council of Europe Project Combating violence against children in Ukraine, 2020, 2) وبالتالي فالاستمالة تقوم عبر إقامة علاقة اجتماعية مع الطفل، وأحيانًا الأسرة؛ بهدف الاعتداء الجنسي على الأطفال؛ ولتجنيدهم في لقاءات جنسية عبر الإنترنت أو خارجها (Finkelhor, Walsh, Jones, Mitchell & Collier, 2020, 3) أما "مشتهو الأطفال" 'paedophiles'فَهُم (أولئك الذين توجههم الجنسي الوحيد يكون تجاه الأطفال قبل سن البلوغ) ويسيئوا للطفل. (Australian Centre to Counter Child Exploitation, 2020, 54)

وفي مارس ٢٠٢٠، في خضم الكورونا أبلغ اليوروبول عن زيادات كبيرة في تنزيل OSEC–المواد الإباحية المشارك فيها أطفال– في إسبانيا وزيادة محاولات للوصول إلى

تلك مواقع في الدنمارك وقد سجل مفوض السلامة الإلكترونية – وهو الجهة التنظيمية المستقلة الوطنية الأسترالية للإنترنت– أنه تم الإبلاغ في مكتبه عن زيادة بنسبة ٨٦٪ في إساءة استخدام الصور على الثلاثة أسابيع السابقة ٩ أبريل ٢٠٢٠، وفي يوليو ٢٠٢٠ لاحظت مؤسسات حقوق الإنسان وهيئة الأمم المتحدة زيادة عدد التقارير المتعلقة بالإساءة للأطفال خلال فترة تدابير الطوارئ الخاصة بـCOVID-19 ، بما في ذلك طرق جديدة للاستغلال والاعتداء الجنسي الأطفال، مثل البث المباشر للاعتداء الجنسي على الأطفال؛ ولأن OSEC هي جريمة عالمية تخضع للعرض والطلب، يمكن أن يؤدي الطلب المتزايد في CSEM بسهولة إلى الزيادات في الجرائم الجنسية الجديدة ضد الأطفال لتلبية هذا الطلب في أطفال جنسيين جدد. (IJM's Center to End Online Sexual Exploitation of Children, 2020, 3-4)

***مراحل الاستمالة:**

تم تمييز سلوك الاستمالة من دراسة المستميلين في السجن لعدة سنوات، ويمكن أن يساعد التعرف على سلوكيات هؤلاء في تجنب الوقوع ضحية، ويمكن عرض تلك المراحل فيما يلي:

المرحلة١: انتقاء أو استهداف ضحية محتملة؛ يبحث جميع أنواع الجناة عن الأطفال المحتاجين عاطفيا أو أولئك المنعزلين بطريقة ما بسبب مشاكل في المدرسة أو المنزل. (NetSafe, 2010, 17)ويستخدم المجرم Digital footprint البصمة الرقمية للطفل لتحديد الضحية؛ وهي آثار يتركها نشاط شخص ما في بيئة رقمية ويمكن تحليل هذه الآثار. (Department of Education and Children's Services, 2009, 18) مستغلين أن التلاميذ يقومون –بشكل يومي– بإنشاء بصمة رقمية، قد يستخدمها الأشخاص ضدهم (Payne, 2016, 39).

المرحلة ٢: بناء الثقة، فيقومون بإقامة العلاقات التي تسهل جرائمهم؛ من خلال عمل وقيعة بين الأطفال وأولياء أمورهم، والخداع حول الهوية والدوافع الجنسية، مستخدماً الإطراء والاهتمام المودة واللطف وحتى الهدايا وعروض المغامرة والتعليم الجنسي أو الرومانسي والخداع والرشوة مع التركيز على الثقة والسرية (Lewis, 2020, 10) فالمراهقون لديهم فضول مشروع حول العلاقات والجنس لذا يفضل تناولها في التربية

الجنسية الشاملة والعلاقات. (Finkelhor, Walsh, Jones, Mitchell & Collier, 2020, 4)

المرحلة٣: تلبية احتياجات الأطفال ومقدمي الرعاية فتظهر الهدايا والاهتمام الإضافي والعاطفة؛ لذا يُنصح أولياء الأمور بالانتباه لأي شخص بالغ حصل على مكانة بارزة في حياة الطفل أو يبدو الآن أنه بطل في نظر الطفل، المرحلة ٤: عزل الطفل تكوين الأوقات والمواقف التي يكون فيها البالغ والطفل بمفردهما دون إثارة شكوك الوالدين ودون إشرافهم مثل الرحلات الخاصة، ومجالسة الأطفال، والتدريب في الدروس الخصوصية. (Georgia, Elizabeth & Leah. 2020, 12-14) المرحلة ٥: الانخراط في النشاط الجنسي إزالة حساسية الطفل بشكل طبيعي لمقاومة الاتصال الجنسي، يمكن أن يحدث هذا من خلال عرض المواد الإباحية والرسوم الجنسية والنكات لجعل الضحية المحتملة تشعر بالراحة الكافية لتكون قريبة من الجاني وحدها. (ENISA, 2012, 8) المرحلة ٦: المحافظة على السرية ومنع الأطفال من التحدث والحصول على المساعدة، ما يقرب من ٤٢٪ من جميع البالغين الذين اعترفوا بالتعرض للتحرش وهم أطفال لم يخبروا أحداً عن الإساءة. (Georgia, Elizabeth & Leah. 2020, 12-14)

بالإضافة إلى ما سبق يعمد المستميل إلى أن يجعل الضحية تشعر بحبه لها، مما يجعل الطفل يحب المستميل -في المقابل؛ جعل الضحية تشعر بالذنب: فيقول للطفل لقد جعلتني أتصرف بهذه الطريقة، كنت تريد ذلك، وهلم جرا، هذا التكتيك يجعل الضحية خائفة من الإبلاغ عن السلوك للآخرين لأن الضحية تشعر بالمسؤولية عن الوضع، ومن العلامات التي يمكن من خلالها اكتشاف أن الشخص يتم ملاحقته بواسطة المستميل ما يلي:-ينسحب الشخص- أو يتلقى مكالمات في أوقات غريبة من اليوم أو يتلقى هدايا من أشخاص لا يعرفهم ولي الأمر، فضلاً عن أن الطالب يبدأ في عزل نفسه عن الأصدقاء والعائلة. (Muir, 2010, 18-19) ومن المهم أن يتلقى الأطفال المساعدة المناسبة في الوقت المناسب لمواجهة المخاطر ومنع تصاعد المشكلات. (Department for Education, 2014, 15)

إذن تناول هذا المحور الأساس الفكري لإدارة المخاطر السيبرانية، ودواعي الحاجة إليها، علاوة على تصنيف المخاطر السيبرانية التي يتعرض لها تلاميذ المدارس الابتدائية؛ واتضح من خلال هذا العرض مدى أهمية إدارة المخاطر السيبرانية والتي تمثل أساساً لحماية النسق القيمي والخلقي للمجتمع مما قد تخلفه تلك المخاطر السيبرانية لدى تلاميذ تلك المدارس، الأمر الذي يتطلب ضرورة البحث عن بعضٍ مما تمارسه الدول، وما توصلت إليه المنظمات الدولية المتعلقة كاليونيسيف من إجراءاتٍ توجيهية وممارسات جيدة وإجراءات تمهيدية تساعد المدارس الابتدائية على إدارة المخاطر السيبرانية بها؛ وهذا ما سيتناوله المحور التالي.

المحور الثالث: بعض الممارسات الدولية في مجال إدارة المخاطر السيبرانية في المدارس الابتدائية، ومتطلبات إدارتها على المستوى المركزي.

إن الإمكانية الهائلة للشبكة السيبرانية بما تشمله من تعدد أدواتها ووسائلها، دفعت بعض الدول نحو الاهتمام بفرض ضوابط قانونية للحد من المضامين التي تشكل خطورة على القاصرين من تلاميذ المدارس، بينما سعى آخرون إلى تحفيز أسلوب التنظيم الذاتي سواء للمستخدمين أنفسهم من التلاميذ أو المزودين لخدمة الانترنت ليحقق هدف الاختيار السليم للمحتوى القائم على الانتقاء وإعمال العقل، وهناك من الدول من لجأ إلى الجمع بين الأسلوبين السابقين، كما وجه البعض اهتمامه نحو دور الأسرة ومنظمات المجتمع التربوي والمدني في حماية التلاميذ –خاصة– وأفراد المجتمع –عامة– من الاستخدام السلبي للشبكة السيبرانية، وتفعيل الضوابط الأخلاقية النابعة من الأديان والعادات والتقاليد الخاصة بكل مجتمع. وانطلاقا من التعريف الإجرائي لإدارة المخاطر السيبرانية في المدارس الابتدائية بالدراسة على أنه **العمليات والأنشطة المنسقة التي تهدف إلى مساعدة المدارس الابتدائية على اتخاذ الإجراءات بشأن جميع المخاطر السيبرانية بها؛ وتوافقاً مع نمط الإدارة التعليمية في مصر القائم على مركزية التخطيط ولامركزية التنفيذ،** أمكن استخلاص بعض الممارسات التي اتبعتها الدول لإدارة المخاطر السيبرانية بها والتي قد تتوافق مع الشأن المصري على النحو التالي:

أولاً–تحديد المخاطر السيبرانية:

وهي الخطوة الأهم؛ فالإدارة السليمة للمخاطر تتطلب تحديدَ تلك المخاطر وأولويات المواجهة بشكلٍ فعال، **وقد حرصت العديد من الدول على تحديد مخاطرها السيبرانية على المستوى المركزي وتوجيه المدارس** إليها تمهيدا لاتخاذ إجراءات إدارتها، ونذكر من تلك الأساليب:

أ-اتخاذ نسب بعض الظواهر المرتبطة مؤشراً لتحديد المخاطر السيبرانية:

حددت إنجلترا وكوريا الجنوبية والولايات المتحدة الأمريكية مخاطرها السيبرانية في الاستخدام المفرط، وزادت عليها الولايات المتحدة والصين والسعودية وصول الأطفال لمحتوى فاحش، وأضافت السعودية سوء معاملة الأطفال عبر الانترنت وسنعرض آليات التحديد فيما يلي:

وجدت إنجلترا أنه قد تضاعف لديها إيذاء النفس ثلاث مرات تقريبًا خلال السنوات العشر الماضية، وفي المتوسط يموت بالانتحار كل أسبوع أكثر من أربعة أطفال في سن المدرسة؛ وثبت أن ٢٣٪ من حالات الانتحار في إنجلترا بين الأشخاص الذين تقل أعمارهم عن ٢٥ عامًا **كان مرتبطا باستخدام الإنترنت**، بالإضافة إلى أن إنجلترا لديها أحد أعلى معدلات السِّمنة لدى الأطفال نتيجة الاستخدام المفرط للانترنت؛ مما دفع حكومة المملكة المتحدة إلى نشر الكتاب الأبيض بشأن أضرار الإنترنت، والورقة الخضراء الحكومية حول أمان الإنترنت (Dubicka & Theodosiou, 2020, 6, 9, 25,31, 69)

وفي الولايات المتحدة الأمريكية تكشف المنحنيات عن اتجاه ينذر بالخطر نحو زيادة حادة لمعدلات الانتحار -بشكل خاص- للأعمار من ١٥ إلى ٣٤ -بين عامي ٢٠٠٨ و٢٠١٦ في الوقت الذي يبلغ فيه معدل انتشار الإنترنت ٩٢٪ (Dresp, 2020, 3)؛ لذا وضعت الولايات المتحدة الأمريكية تشريعاتٍ واستراتيجيات لتطوير تعليم الأمن السيبراني؛ فتم إنشاء المبادرة الوطنية لتعليم الأمن السيبراني (NICE) لتحسين وضع الأمن السيبراني على المدى الطويل للولايات المتحدة الأمريكية.(Spiering, 2018, 2)

وقد حددت أيضاً الولايات المتحدة الأمريكية مخاطرها في: مخاطر وصول الأطفال لمحتوى فاحش أو ضار؛ فيستخدم أطفال الولايات المتحدة الأمريكية العالم الرقمي بكثافة كبيرة؛ فيقضون ما يصل إلى ثماني ساعات يوميًا عبر الإنترنت وفقًا

لبعض التقديرات، في حين لا يتلقى المعلمون تدريبًا مناسبًا في موضوعات الأمان عبر الإنترنت، هذا بالإضافة إلى أن المدارس لم تَعتَمِد بَعْدُ نهجًا كجزء من التعليم الابتدائي(Saluja, Bansal, & Saluja, 2012, 4)، ويؤكد ذلك ما أشارت إليه دراسة (Malecki, 2018, 5) من أنَّ وزارة التعليم الأمريكية" (ED) لا تفرض مناهج معينة أو خطط دروس في هذا الصدد؛ لذا سَنَّ الكونجرس عام ٢٠١٩ قانون حماية الأطفال على الإنترنت (CIPA) لمنع الأطفال من الوصول إلى محتوى فاحش أو ضار عبر الإنترنت، لذا يُطلب من المدارس المشاركة في البرنامج المدعوم من الحكومة أن يكون لديها سياسة أمان الإنترنت، وتلبي معظم المدارس هذا المطلب من خلال تطبيقات تصفية الإنترنت وقواعد سلوك التلاميذ، وتحدد معظم المناطق التعليمية سياسة السلامة الخاصة بها وتطالب الآباء، جنبًا إلى جنب مع تلاميذهم، لقراءة سياسة الاستخدام المقبول (AUP) والتوقيع عليها (Schubart, 2021, 2–3).

وقد حددت بعض الدول مخاطرها السيبرانية بناء على مؤشر قدر الاستخدام فكوريا الجنوبية قد حددت أولى مخاطرها السيبرانية في إدمان الألعاب؛ فاعتبرت قضية إدمان الإنترنت قضية مثيرة للقلق في كوريا، وكان هذا الموضوع مجال بحث مكثف بين المجتمع الأكاديمي في البلاد. (Lim, 2012, 10) حيث تعد كوريا هي الرائدة عالميا في مجال تكنولوجيا المعلومات فأكثر من ٧٥٪ من الكوريين لديهم هواتف محمولة، ويستخدم ثلثا الكوريين الذين تقل أعمارهم عن ٣٠ عامًا الأجهزة اللاسلكية للوصول إلى الإنترنت، ويقدر متصلو الإنترنت بنحو ٨٥ % من الكوريين الجنوبيين؛ لذا فإن إدارة المخاطر السيبرانية تعد بؤرة اهتمام حكومة كوريا الجنوبية؛ فتعتبر أول دولة دشنت قوانين محددة بشأن تنظيم ورقابة شبكة الانترنت. (مرعي، ٢٠١٣، ٢٩٨) ويرجع تاريخ أول قانون مخصص للأمن السيبراني في كوريا الجنوبية إلى عام ١٩٩٥ بشكل يعلي من تعزيز المعلوماتية ويجعل أمن المعلومات مسؤولية الحكومة، أما عام ١٩٩٦ فتم إنشاء مركز أمن المعلومات الكوري (وكالة KISA) باعتباها واحدة من أولى خطوات البلاد في مجال الأمن السيبراني، وفي عام ٢٠١١، أعلنت جمهورية كوريا"(ROK) الخطة الرئيسة للأمن السيبراني الوطني للرد على الهجمات الإلكترونية، وفي مارس ٢٠١٥، أعلنت جمهورية كوريا تعيين مستشار رئاسي جديد مخصص لمسائل الأمن السيبراني،

وتسعى جمهورية كوريا إلى رفع مستوى الوعي العام حول الأمن السيبراني، ومشاركة أفضل الممارسات، فأطلقت لجنة الاتصالات الكورية في أكتوبر ٢٠١٣ حملة Internet Safety Keeper التي جندت سفراء المشاهير للتحدث في التلفزيون والراديو عن حماية البيانات الشخصية، واستُكملت هذه المبادرة بعمل لافتات وإعلانات على قطارات الأنفاق والحافلات، وفي مراكز التسوق وقاعات الألعاب كجزءٍ من هذا الجهد العام (Lewis, Porrúa, Catalina & Díaz, 2016, 36–37, 39)

كما حددت الصين مخاطرها السيبرانية في محتوى المقامرة أو المواد الإباحية أو العنف أو أي محتوى يعتبر انتهاكًا للقانون، (Taibah, Khalifa & Alshebaiki, 2020, 5) وأرجعت سبب اعتبار تلك مخاطراً؛ أن تلك المضامين بمثابةِ إضعافٍ للأخلاق الاجتماعية وانتهاكٍ للقوانين (King, Delfabbro, Doh, Wu, Kuss, Pallesen, Mentzoni, Carragher, & Sakuma, 2018, 245–246) كما حددت أيضاً إدمان الانترنت وخاصة الألعاب الالكترونية كمخاطر عاجلة لديها. (Lim, 2012, 11)

أما السعودية فحددت المخاطر السيبرانية في مشاهدة الأطفال لمواد البالغين الإباحية على الإنترنت، والمحتوى"غير الأخلاقي"، بما في ذلك قضايا المثليين والسحاقيات (Fourie, Bothma& Bitso, 2013, 13, 18)؛ علاوة على تحديد أولويات مخاطرها في مخاطر الإساءة الرقمية (إساءة معاملة الأطفال عبر الانترنت)(Alqahtani, 2017, 2–3, 50).

تأسيسا على ما سبق حددت إنجلترا والولايات المتحدة الأمريكية مخاطرها السيبرانية وفقا للدراسات العلمية من خلال ربطهما بزيادة معدل إيذاء النفس والانتحار، كما حددت كوريا الجنوبية والصين وماليزيا مخاطرها السيبرانية بناء على النسب والإحصائيات الوطنية لاستخدام الانترنت.

ب- إيلاء مهمة تحديد المخاطر السيبرانية للآباء مع توفير سبل المساعدة:

فقد أعلنت ماليزيا عن عزمها عدم تنفيذ برنامج تصفية وترشيح وطني لديها – مثلها في ذلك مثل إسرائيل- (Lee, & Liu, 2012, 125–126) وكل ما ركزت

ماليزيا على القيام به إصدار كتاب إرشادي يساعد الآباء على تحديد التهديدات السيبرانية. (Thah, Kaur & Ling, 2019, 29, 38).

كما سعت الحكومة الأسترالية إلى سلامة سكانها عند دخولهم للفضاء السيبراني بأقل قدر ممكن من المخاطر؛ فأنشأت الحكومة لديها موقعًا تفاعليًا مثيرًا للاهتمام يحتوي على إرشادات للآباء ومقاطع فيديو ومقالات حول كيفية مساعدة الأطفال في الأمان على الإنترنت؛ بشكل يعطي معلومات قيّمة حول أدوات الرقابة الأبوية المتاحة ويعلمها للآباء، ويعطي تلميحات حول التطبيقات التي قد يستخدمها أطفالهم، والمخاطر المرتبطة بها، وكذلك يشرح للآباء الدور الذي يجب أن يلعبوه حسب عمر الأطفال، وحرصت الحكومة على أن تكون المواد المقدمة للوالدين بسيطة ومختصرة (كملخص لشروحات) وقابلة للطباعة مُحدِّدةً إجراءات الإبلاغ عن تهديدات السلامة السيبرانية بكفاءة (Paraiso, 2019, 32).

ج- مطابقة الوضع الحالي لاستخدام أطفال المدارس للانترنت بمؤشرات الاستخدام الصحي للانترنت :

ويمكن عرض مستويات الاستخدام الصحي للانترنت وفقا للمنظمات الدولية والأبحاث العالمية فيما يلي:

١-مستويات الاستخدام الصحي للانترنت.

توصي الأكاديميةُ الأمريكية لطب الأطفال الآباءَ والأطباء بالعمل معًا لتطوير خطة استخدام عائلية تأخذ في الاعتبار المستوى التنموي للطفل؛ وأَوْصت منظمة الصحة العالمية (WHO) بأنه لا ينبغي توفير أي وقت أمام الشاشة للأطفال أقل من عام واحد (World Health Organisation, 2019)، أما عن سن بدء مشاركة الطفل لعمل حساب على وسائل التواصل الاجتماعي فيجب الالتزام بالتقييد للسن الرسمي عند بلوغ 13 عامًا، وفي أيرلندا أوصت الدكتورة ماري أيكن الأكاديمية في كلية دبلن الجامعية بأنه يجب ألا يكون للأطفال دون سن ١٤ عامًا أي هاتف ذكي، (Dubicka & Theodosiou, 2020, 26, 67, 70)

ما أوصت منظمة الصحة العالمية بضورة وضع حد أقصى أمام الشاشة للأطفال الذين تتراوح أعمارهم بين (٢-٤) أعوام ليكون ساعة واحدة يوميا؛ ويجب خلالها

على البالغين من أفراد الأسرة مشاهدة الشاشات مع الأطفال لتمكينهم من فهم ما يشاهدون(World Health Organisation, 2019). وقد ذكرت الأكاديمية الأمريكية لطب الأطفال أن الأبناء من (سنة ونصف- سنين) عرضة للتعلم والاحتفاظ بالمحتوى الموجود في البيئات الرقمية بشكل أفضل طالما أنهم يتفاعلون مع المحتوى جنبًا إلى جنب مع والديهم أثناء مشاهدتهم ومناقشته معًا(Tosun & Mihci. 2020, 2)

ويجب على المدارس أن توجه الوالدين إلى النظر في الجودة وليس فقط كم الوقت الذي يقضيه على الإنترنت؛ فكلما زاد مشاركة الأطفال عبر الإنترنت، زاد احتمال أن يواجهوا المحتوى الذي يجدونه مزعجاً، وقد وجدت دراسة حديثة طُبِّقت على الأطفال الإيطاليين أن ١٣٪ من الأطفال الذين تتراوح أعمارهم بين ٩ و ١٧ عامًا كانوا "منزعجين" من شيءٍ رأوه عبر الإنترنت في العام الماضي. (Blum-Ross, Donoso, Dinh, Mascheroni, O'Neill, Riesmeyer, & Stoilova, 2018, 34)

وقد يكون من المفيد للوالدين التفاوض على أوقات خالية من الشاشة من اليوم مثل أوقات الوجبات؛ فنصحت الكلية الملكية لطب الأطفال وصحتهم (The Royal RCPCH (College of Paediatrics and Child Health بعدم استخدام الأطفال للشاشات قبل وقت النوم بساعة (Dubicka & Theodosiou, 2020, 8, 21, 65) .

٢- وقت الاستخدام اليومي والأسبوعي.

أوصت إدارات الصحة بالدول الشرقية والغربية بأنه يجب الاعتدال في استخدام أنشطة ألعاب الإنترنت لمدة لا تزيد عن عدد معين من الساعات في اليوم Certain Number، على أساس رأي الأكاديمية الأمريكية لطب الأطفال السابق ذكره، وقد حددت الدراسات الأكاديمية مقدار الاستخدام المؤذي أو المكثف للإنترنت بواقع ٤ ساعات يوميًا أو ٣٠ ساعة أسبوعياً (King, Delfabbro, Doh, Wu, Kuss, Pallesen, Mentzoni, Carragher, & Sakuma, 2018, 234)؛ لذا يجب على المعلمين وأولياء الأمور تنظيم ومحاولة التحكم في الاستخدام اليومي لأطفالهم لمدة لا تزيد عن ساعة واحدة لمدة ٥ مرات في الأسبوع، ويمكن بديلاً عن ذلك أن تُزيد الأسرة من

الأنشطة العائلية في الهواء الطلق؛ لتقليل فرص استخدام الانترنت. (Tsai, Wang & Weng, 2020, 14)

ثانياً: تحليل المخاطر (أسبابها والضوابط الوقائية وعواقب المخاطر)

وهي من أهم خطوات إدارة المخاطر، لذا حرصت العديد من الدول على تحليل مخاطرها السيبرانية بناء على تحديد أسباب تلك المخاطر ووضع ظوابطاً وقائية استباقية لإدارتها، فهناك عدد من ممارسات الضوابط الوقائية التي حددتها الدول؛ نحددها فيما يلي:

أ-وضع بروتوكول لانضباط المدارس محدد فيه عواقب المخاطر السيبرانية:

وتشير دراسة (Jemeljanenko, 2019, 8) أن من أسباب المخاطر التي يتعرض لها قطاع التعليم على الصعيد العالمي، هي: نقص الأطر القانونية المحددة بوضوح. وهي بمثابة أداة وقائية استباقية لحماية التلاميذ من مخاطر التكنولوجيا؛ حيث تحتوي وثيقة سياسة الاستخدام المسؤول على ثلاث فئات من القيم الأساسية: الاحترام والتعليم والحماية (REP) لتعليم التلاميذ القواعد الصحيحة، والسلوك الآمن في البيئات الرقمية. (Hassan, 2021, 236) فمن الضروري أن يتم تعليم الشباب التهديدات السيبرانية المحيطة بهم، ومعرفة ما هو قانوني وما هو ليس كذلك، بل يجب أن يكون الجميع على دراية بتداعيات أفعالهم؛ ففي القرن الحادي والعشرين، لا تقل موضوعات السلامة والأمن والأخلاق عبر الإنترنت أهميةً عن موضوعات القراءة والكتابة والرياضيات.(Saluja, Bansal, & Saluja, 2012, 4-5)

لذا كانت من أفضل جهود مكافحة المخاطر السيبرانية إنفاذ سياسات المدرسة، حيث أنه يجب أن يكون لدى المدارس بروتوكول يوجه الإدارة عند التعامل مع الحوادث السيبرانية؛ ففي جنوب إفريقيا، تم نشر الإطار الوطني للمدارس الآمنة عام ٢٠١٥ لمساعدة المدارس على فهم التهديدات الأمنية العامة والاستجابة لها (Cilliers, & Chinyamurindi, 2020, 32, 37)

وفي هذه الممارسة بالرغم من أن المدرسة تحترم حقوق التلاميذ في الخصوصية، إلا أنها تحتفظ بالحق في مراقبة واعتراض الاتصالات الإلكترونية كما في كينيا؛ فوفقًا لأحكام قانون المعلومات والاتصالات (قانون إساءة استخدام الكمبيوتر

والجرائم الإلكترونية) الكيني لعام ٢٠١٨ على الطالب المشتبه في استخدامه جهازًا إلكترونيًا بالمخالفة لهذه الشروط أن يخضع لإجراءات تأديبية لسوء السلوك، بموجب قانون المدرسة؛ وفي حالة صدور حكم بالإدانة، قد يفقد الطالب الحق في حمل جهاز إلكتروني للمدرسة بالإضافة إلى أي لوم آخر؛ تنطبق هذه القواعد على استخدام أي جهاز إلكتروني مملوك للمدرسة و/ أو جهاز إلكتروني موجود في مبنى المدرسة، أو أي جهاز إلكتروني قيد الاستخدام سواء كان الجهاز مرتبطاً بمزود خدمة المدرسة على حساب المدرسة أم لا(Crawford International School, 2018, 4-5).

وفي مدرسة صني فيو بكاليفورنيا تحرص المدرسة على التحقيق في الحوادث، والإنذار بالتعليق إلى الطرد حسب خطورة الحادث، وتطبيق مصفوفة الانضباط بالمنطقة لتحديد العواقب حسب الاقتضاء؛ فيتبع تعليم كاليفورنيا ممارسة التأديب التدريجي في المدارس(Nye, 2014, 68)؛ وقد تكون تلك خطوة متميزة للتخفيف من المخاطر.

ولمدير المدارس الأسترالية السلطة بموجب اللائحة وفقًا لقانون التعليم لعام ١٩٧٢ لتعليق أو استبعاد أي طالب من الحضور في المدرسة إذا كان الطالب المسجل يتصرف عبر الإنترنت بطريقة تهدد رفاهية طفل أو طالب آخر أو ولي أمر أو عضو في المجتمع المدرسي، -حتى لو حدث هذا خارج الموقع و/ أو خارج ساعات المدرسة-، ثم يتم توجيههم ودعم وإدارة سلوكهم؛ وجدير بالذكر أن السياسات والإجراءات الحاكمة لتلك المخاطر تُرَاجع كل سنتين على الأقل. (Department for Education and Child Development, 2009, 8, 12, 17)

ب- دمج المواطنة الرقمية في المناهج الدراسية.

خلال الفترة الكلاسيكية من اليونان القديمة، أعلن الفيلسوف سقراط (٤٦٩ قبل الميلاد-399 قبل الميلاد) قوله: "أنا مواطن، لست من أثينا أو اليونان، ولكن من العالم"؛ أشارت كلماته إلى وعي ذاتي بالمواطنة يتجاوز العلاقة بينه وبين آخرين في المنطقة التي كان يعيش فيها، مع علمه بعلاقته بـ"العالم" كما كان يعرفه؛ Suppo, (2013, 2) فتشير المواطنة إلى "مجموعة العلاقات بين الحقوق والواجبات والمشاركة في الحياة المدنية.(Soares & Lopes, 2020, 3)

أما المواطنة الرقمية فهي فهم القضايا الإنسانية والثقافية والمجتمعية المتعلقة بالتكنولوجيا، وممارسة السلوك القانوني والأخلاقي، والمواطنة الرقمية ليست قائمة مهام أو "منهجًا راكدًا" يتم استخدامه حتى حقبة التبني التالية، إنها طريقة حياة دائمة التغير تُمَكّن التلاميذ من أن يكونوا مستخدمين فعالين ومسؤولين؛ فالمواطنة الرقمية هي تَعَلُّم احترام حقوق الآخرين والاستخدام المسؤول والأخلاقي للإنترنت، والمواطنة الرقمية معايير السلوك المناسب والمسؤول فيما يتعلق باستخدام التكنولوجيا (Payne, 2016, ii, 5, 12, 15) ويطلق عليها أيضاً المواطنة الرقمية العالمية، المواطنة الرقمية الراديكالية؛ وتتبادر إلى الذهن ثلاث ركائز أساسية عند محاولة تعريف المواطنة الرقمية: الانتماء، المشاركة والحماية. (Fernández-Prados, Lozano-Díaz & Ainz-Galende, 2021, 1-2) والأمل هو أن المجتمع الرقمي -الذي نحن جميعًا جزء منه- يقف معًا ويحدد ما هو أخلاقيًا واجتماعيًا وما هو مقبول أخلاقيًا وما هو غير مقبول (Suppo, 2013, 2)

وفي دراسة كمية شبه تجريبية أجريت عام ٢٠١٠ حول فعالية منهج المواطنة الرقمية على السلوكيات غير الملائمة لتلاميذ المرحلة الثانوية في مدرسة حضرية، تم تقسيمهم إلى مجموعتين: مجموعة واحدة تتلقى دروس المواطنة الرقمية (المعالجة)، والبعض الآخر ليس لديه معالجة؛ فأظهرت النتائج مكاسب رائعة للمجموعة التي تم تدريس المنهج لها؛ خاصةً في جوانب الآداب الرقمية والحقوق الرقمية والمسؤوليات(Payne, 2016, 33)

ويمثل الأمان عبر الإنترنت أولوية في مناهج التربية الجنسية والتربية الصحية في المدراس، ويقدم قائمة بموارد للأمان على الإنترنت؛ فتتضمن العديد من المدارس "مواد اختيارية إلزامية" مثل فئة الصحة التي تعلم التلاميذ بشكل أساسي المحافظة على أجسامهم، بالإضافة إلى المساعدة في شرح وإدارة المراهقة؛ وبالتالي يمكن لمنهج الأمن السيبراني المحدد جيدًا أن يخدم غرضًا مشابهًا لتحضير الأطفال بشكل عملي للمواقف التي قد يتعرضون لها على الإنترنت؛ فيتعلمون موضوعات مثل ما يجب فعله إذا طلب شخص غريب الاجتماع وجهًا لوجه، هذه الفئة من الدروس بعيدة عن الجوانب الأكثر تقنية في الأمن السيبراني(Malecki, 2018, 12) ووصل الاهتمام بذلك أنه في التعليم

العالي، أطلقت كلية تكنولوجيا المعلومات الإستونية برنامجاً جديداً في هندسة **الأمن السيبراني** منذ عام ٢٠٠٩، وأطلقت برنامج ماجستير في الطب الشرعي الرقمي، لتبدأ برامجها في سن الدراسة الابتدائية والمتوسطة والثانوية ولتحتوي مناهجها على وحدات الأمن السيبراني.(Lewis, Porrúa, Catalina & Díaz, 2016, 15)

وقد تم تضمين السلامة الإلكترونية في المناهج المدرسية للعديد من الدول المتقدمة، مثل الولايات المتحدة المملكة وأستراليا والولايات المتحدة الأمريكية ونيوزيلندا وكندا، أما في إفريقيا فتم تضمين السلامة السيبرانية في مناهج كل من تونس ورواندا، وبدأت موريشيوس عملية تثقيف المتعلمين حول الأمان عبر الإنترنت (Cilliers, & Chinyamurindi, 2020, 32)

ولكن ينبغي الاهتمام بالكيفية التي يتم بها تناول تلك المناهج؛ ففي الهند، لا تؤتي تلك المناهج نتائجها المتوقعة؛ حيث يتم تدريس تعليم السلامة عبر الإنترنت CBSEللتلاميذ في عمر ١١-١٢ عام من خلال الكتب المدرسية؛ بشكل نظري بحت، فلا توفر للطالب أي خبرة عملية؛ وبالتالي لا تؤدي إلى تعرض كافٍ ولا ترتبط بالتلاميذ، ولا تغطي التهديدات الحديثة عبر الإنترنت مثل الخصوصية على الشبكات الاجتماعية والتسلط عبر الإنترنت والأخلاقيات الإلكترونية (Saluja, Bansal, & Saluja, 2012, 3)

أما على المستوى التطبيقي فتفرض العديد من الولايات في أمريكا مناهج التسلط عبر الإنترنت (Muir, 2010, 28)، وثمة مبادرة أطلقتها وزارة الخارجية الهولندية عام ٢٠١٤ لتحديد مناهج القرن الحادي والعشرين (المذكورة باسم مهارات القرن الحادي والعشرين ومحو الأمية الرقمية) تحتوي على إحدى عشرة مهارة ضرورية ليتم تعليمها للأطفال في التعليم الابتدائي والثانوي، تم تخصيص أربع من هذه المهارات لمحو الأمية الرقمية هم: التفكير الحاسوبي، المهارات الأساسية لتكنولوجيا المعلومات والاتصالات، ومحو الأمية الإعلامية، ومهارات المعلومات (Spiering, 2018, 26)

أما اسكتلندا فقد نشرت حكومتها في نوفمبر ٢٠١٣ إرشادات حول تطوير سياسات تعزيز الاستخدام الآمن والمسؤول لتكنولوجيا الهاتف المحمول في المدارس، والتي تروج للاستخدام الآمن والمسؤول لتكنولوجيا الهاتف المحمول في المدارس، وفي

عام ٢٠١٤ نشرت الحكومة الاسكتلندية توجيهات بشأن تعليم سلوك العلاقات والصحة الجنسية والأبوة (RSHP) relationships, sexual health and parenthood في المدارس، وكانت بمثابة إرشادات للمعلمين حول كيفية تدريس RSHP، يعرض الحقائق في إطار القيم السليمة والوعي بقوانين السلوك الجنسي، وقد تطور اتجاه اسكتلندا إلى الأمان عبر الانترنت على النحو التالي: في سبتمبر ٢٠١٦ نشرت الحكومة الاسكتلندية تعزيز التعلم والتدريس من خلال استخدام التكنولوجيا الرقمية: استراتيجيات التعلم والتعليم الرقمي في اسكتلندا؛ تهدف الإستراتيجية إلى تهيئة الظروف لتحسين استخدام التكنولوجيا في المدارس، أما في ٢٠١٧ أصبح التركيز أقوى على محو الأمية الرقمية، والذي يتضمن أمان الإنترنت والمرونة الإلكترونية؛ لذا تدعم اسكتلندا توجيه المناهج، والذي يركز بشكل خاص على محو الأمية الرقمية، ويسلط الضوء على التقييم الذاتي الفعال كنقطة انطلاق لتحسين المدرسة ويتم دعمهم من قبل خبراء الصناعة (Education Scotland, 2017, 7, 16)

وقد حددت (NetSafe, 2010, 11) خطوات فعالة للمساعدة في عملية كتابة مناهج المواطنة الرقمية في ولاية كونيتيكت الأمريكية هي: تحديد الموظفين والتلاميذ وأولياء الأمور للعمل في لجنة كتابة المناهج (ويعد صوت الوالدين ضروريًا لمراجعة ومن المهم أيضاً استخدام المبادئ التوجيهية لمناهج المواطنة الرقمية التي وضعتها المدارس الأخرى، وإنشاء أسئلة أساسية لتوجيه عمل كتابة المناهج، مثل كيف يمكننا (أي فريق العمل والتلاميذ وأولياء الأمور والمجتمع) استخدام التكنولوجيا لتكون فعالة كيف ندير المعلومات والأدوات لاستخدامها بأمان وفعالية وقانونية؟ مع ضرورة التخطيط لعملية مراجعة منهج المواطنة الرقمية كل عامين، والحرص على تماشي الأنشطة الحالية مع الاتجاهات الرقمية .

أما عن تقييم محتوى مناهج المواطنة الرقمية فتتم من قِبَل أربعة هيئات تدريسية ممن يتفاعلون مع تلاميذ المرحلة الابتدائية على أساس منتظم يشمل هؤلاء الموظفون: (أ) معلم الصف الثالث، (ب) معلم الصف الرابع، (ج) أمين مكتبة المدرسة، (د) معلم التربية الخاصة؛ ليتم التقييم حول المعايير التالية: (أ) قيمة العرض التقديمي للغرض المقصود، (ب) ملاءمة المواد للمستويات العمرية، (ج) احتمالية أن يشارك التلاميذ

بنشاط، (د) الموضوعات التي ينبغي إضافتها أو حذفها–(MacArthur, 2009, 20 21)

ج– وضع ضوابط وقائية تقنية للمخاطر السيبرانية:

ومن أكثر الدول التي تمثل ذلك الاتجاه الصين؛ وقد وضعت تدابير متنوعة لتعزيز فرص الأطفال على الإنترنت مع تقليل المخاطر؛ ففرضت السلطات الصينية أنظمة رقابة أكثر شمولاً في العالم، بالإضافة إلى تصفية المحتوى باستخدام أجهزة التوجيه والخوادم. (Puddephatt, 2011, 13)، وتم تصدير تلك الأنظمة الرقابية المسماه (الدرع الذهبي) أو السد الأخضر إلى كوبا وإيران وبيلاروسيا (Warf, 2011, 9) وثمة احتمالية لوجود تطبيقات تشبه السد الأخضر يُطْلَب تثبيتها في إندونيسيا وفيتنام وهانوي كبرامج مراقبة لأجهزة الكمبيوتر في مقاهي الإنترنت والفنادق. (Hope, 2011, 21) أما في مدارس شيكاغو فتم تثبيت آليات تتبع، بحيث تطلق "صفارات إنذار تحذيرية عند وصول التلاميذ أو الموظفين إلى موقع غير مناسب (MacArthur, 2009, 14)

وفي صدد هذه الحملة الصينية لا يُحظر عليهم فقط حيازة أي شيء فاحش "obscene"ولكن أيضًا المحتوى الذي يعتبر "مبتذلاً كذلك."vulgar " ؛ وقد أعلنت الصين في إثْرِها أن من أكثر النتائج الإيجابية للحملة حظر ١٥٠٠٠ موقع إباحي وحذف مليون مشاركة فاحشة أو "مبتذلة"، وإزالة أكثر من ٨٥٠.٠٠٠ صورة فاحشة أو إباحية، وأكثر من ٣٠ رواية إباحية على الإنترنت، كما تم حظر ١٥ لعبة إباحية من الهواتف المحمولة ومعاقبتهم (Ning, 2011, 2,7–8,10,13)، علاوة على أنها أدت إلى التحقيق في٢١٩٧ قضية ومعاقبة ٤٩٦٥ مرتكباً لهذا النوع من الجنايات، منها السجن لفترات تتجاوز ٥ سنوات. (مرعي، ٢٠١٣، ٢٩٧)

وأصدرت وزارة الاتصالات وتكنولوجيا المعلومات توجيهًا في مايو ٢٠٠٩ اشترط أن يكون على كل جهاز كمبيوتر يتم بيعه في الدولة اعتبارًا من ١ يوليو ٢٠٠٩ وما بعده – برنامج ترشيح مثبت يعرف باسم Green Dam– Youth Escort بحيث يتم دمجه في تلك الأجهزة المباعة – وجدير بالذكر أن كلمة "أخضر" في اللغة الصينية تشير إلى السلامة والنظافة– (Yang, 2011, 102)، فأصدرت وزارة الصناعة

وتكنولوجيا المعلومات الصينية توجيهًا يطلب من مصنعي المعدات تضمين برنامج Green Damفي جميع أجهزة الكمبيوتر المباعة في الصين (Lee & Liu, 2012, 125) ويراقب هذا البرنامج سلوك الأفراد على الكمبيوتر عن طريق تثبيت مكونات في نظام التشغيل؛ فيعطي الحكومة سلطة مباشرة للتحكم في الوصول إلى المحتوى (بالإضافة إلى السماح بالتحكم عن بعد في الكمبيوتر الذي يقوم بتشغيل البرنامج (Puddephatt, 2011, 13)، فأدى هذا البرنامج العديد من الوظائف بما في ذلك حجب المحتوى الإباحي، وتصفية المواقع "غير المرغوب فيها" من خلال التعرف على صور العُري التي تحتوي على اللون الأصفر لبشرة الإنسان، بالإضافة إلى أهميته في الحد من ساعات الإنترنت، علاوة على تعتيم الشاشة كل ثلاث دقائق إذا كان يكتشف أن المستخدم يزور مواقع غير مشروعة (Ning, 2011, 11).

وفي هذا الإطار يمكن إجمالاً تركيز جهود الصين في هذا الصدد حول: حماية الطلبة القاصرين من المحتوى غير اللائق والبغيض؛ من خلال الحملات ومنع الوصول بالتصفية وتصميم قائمة بيضاء للتلاميذ.

أما المملكة العربية السعودية فتصنَّف الرقابة على الانترنت على مستوى العالم العربي كله بأنها أكثر حدة فيها؛ فشبكة الإنترنت بالكامل–مملوكة للدولة؛ ويجب على السعوديين أن يمروا من خلال خوادم تسيطر عليها الدولة إذا أرادوا الوصول إلى العالم الخارجي(Fourie, Bothma& Bitso, 2013, 13, 18)؛ فتعتمد السعودية في الجانب الأكبر لها على تقنيات الحظر، وفي عام ٢٠٠٤ تم حظر أكثر من ٤٠٠٠٠٠ صفحة ويب من قبل النظام السعودي، الجزء الأكبر منها تتعلق بمواد البالغين، ولكن تشمل أيضًا بعض الألعاب والمواقع الترفيهية والتسوق عبر الإنترنت. (Warf, 2011, 12)، ودعَّم قانون الجرائم الإلكترونية (٢٠٠٧)، وقانون حماية الطفل (٢٠١٤) بالسعودية حماية المستخدمين والأخلاقيات العامة والمصلحة العامة، وحماية الاقتصاد الوطني، وكان لتلك القوانين تأثيرٌ إيجابي على تقليل معدلات إساءة معاملة الأطفال، ومع ذلك، طالبت الدراسات بتطويرها لتغطية جميع جوانب الإساءة الرقمية؛ كحماية النمو النفسي للأطفال وصحتهم؛ فأنشأت حكومة المملكة العربية السعودية قانون

مكافحة الجريمة السيبرانية لمنع المجتمع من مثل هذه الجرائم وتحديد العقوبة عليها. (Alqahtani, 2017, 2-3, 50).

هذا وقد وضعت كوريا الجنوبية قيوداً استباقية على المواقع التكنولوجية، وأصبحت أول ولاية قضائية في العالم تطالب الأطفال والشباب بأن يكون لديهم تطبيقات لتصفية المحتوى مثبتة على هواتفهم (Dubicka & Theodosiou, 2020, 20, 70)

ثالثاً- تقييم المخاطر (احتمالها وتأثيرها ووضع خطط وتدابير التخفيف)

ويمكن توضيح ذلك من خلال العنصريين التاليين:

أ-تقييم تأثير المخاطر السيبرانية:

اعتبرت الصين مشاهدة أطفالها للمحتوى "المبتذل" قد يتسبب في ضرر جسيم للقُصَّر (Ning, 2011, 2,7-8,10,13) ، وأن لتلك المضامين تأثير سلبي قوي؛ فهي بمثابة إضعاف للأخلاق الاجتماعية social morals وانتهاك للقوانين. (King, Delfabbro, Doh, Wu, Kuss, Pallesen, Mentzoni, Carragher, & Sakuma, 2018, 245-246)؛ وبالتالي فقد قيمت تأثيرر تلك المخاطر السيبرانية.

ب-وضع الدولة خطة مبنية على تقييم الاحتمالية:

فاعتمدت ماليزيا في تحقيق الأمن السيبراني على الحوكمة الفعالة من وضع استراتيجية **وخطة** عمل لمعالجة هذه المسألة، والمشاركة في المنتديات وورش العمل والمؤتمرات ذات الصلة، وتبادل أفضل الممارسات؛ لأن ذلك من شأنه التمكين من معالجة هذه المشاكل السيبرانية.(Salamzada, Shukur & Bakar, 2015, 4-5)

وقد وضعت وزارة الأمن الداخلي في الولايات المتحدة الأمريكية **خطة** استهدفت تعزيز الوعي حول التهديدات السيبرانية عندما طلب أوباما مراجعة السياسة الفيدرالية للأمن السيبراني؛ فتم اعتماد برامج للتدريب على الأمن السيبراني في الحكومة الفيدرالية الأمريكية مثل مبادرة (توقف، فكر، تواصل) initiative "Stop.Think.Connect" في عام ٢٠٠٩ لتدريب الأطفال على الأمن السيبراني (Zepf & Arthur, 2013, 19)

وقد أوضحت الصين بالتفصيل **خطة** مدتها ١٤ شهرًا للحد من "الفُحش والمحتوى الإباحي "على الهواتف المحمولة، وأكدت السلطات الصينية أن الغرض الوحيد من الحملة هو توفير بيئة نظيفة وصحية للقصر، وشدد المسؤولون على أن الحملة

جاءت استجابة لدعوات متكررة من قبل الآباء لتنظيف الإنترنت، فقامت السلطات الصينية بإطلاق حملات تطهيرية (Ning, 2011, 2,7-8,10,13)

كما قدمت كوريا الجنوبية مبادرات حكومية واسعة واستراتيجية **خطط** طويلة المدى على جميع مستويات الوقاية؛ فقد طورت كوريا الجنوبية نظامًا منسقًا من ثماني وزارات والعديد من الكيانات الأخرى لمكافحة اضطراب الألعاب وتوفير بيئة صحية للأطفال على الإنترنت؛ لتتضافر جهود وزارات العلوم وتكنولوجيا المعلومات والاتصالات؛ فكانت حكومتها فريدة من نوعها لأنها في طليعة جهود الوقاية، على النقيض من الولايات المتحدة الأمريكية وأوروبا الغربية حيث أن منظمات الخدمات الخاصة والمنظمات غير الربحية هي الأساس في الوقاية؛ (King, Delfabbro, Doh, Wu, Kuss, Pallesen, Mentzoni, Carragher, & Sakuma, 2018, 242, 246)

رابعاً- الاستجابة للمخاطر:

وتتركز الممارسات الدولية الخاصة بالاستجابة للمخاطر السيبرانية في المدارس الابتدائية فيما يلي:

أ- الاستجابة للمخاطر السيبرانية من خلال حظر استخدام الطلاب للأجهزة اللوحية في المدارس:

فحديثاً فرضت المدارس في بريطانيا حظرًا صارمًا على الهواتف المحمولة لجميع التلاميذ لحين تصل أعمارهم إلى ١٦ عامًا؛ حيث يتم سحب الهواتف النقالة بعيدًا عنهم طوال اليوم الدراسي(Quaglio & Millar, 2020, 28) ، كما تم الموافقة من قبل على إدارة التفتيش على المدارس المستقلة (ISI) في المملكة المتحدة تحقيقاً للسلامة على الانترنت.(Department for Education, 2014, 25) ويبدو أن سبب اللجوء لذلك استخدام الانترنت المفرط لدى تلاميذهم وفقاً للدراسات العلمية؛ فنصف الأطفال في سن العاشرة بالمملكة المتحدة يمتلكون الآن هواتفهم الذكية، ويشاهد الكثير من الأطفال مقاطع الفيديو أكثر من مشاهدة البث التلفزيوني.(Ofcom, 2020, 2)

كذا اعتمدت المملكة المتحدة ممارسات السيطرة الخاصة بالوالدين التي تعزز الاختيار النشط؛ حيث تسأل العملاء في لحظة الشراء ما إذا كانوا يريدون الحصول على

ضوابط أبوية ليقدمونها لهم مجاناً، علاوة على تأسيس مجلس المملكة المتحدة لسلامة الأطفال على الإنترنت(UKCCIS) UK Council for Child Internet Safety تحقيقاً لأمان الإنترنت للأطفال ؛ وهي مجموعة مكونة من أكثر من ٢٠٠ منظمة تتألف من الحكومة والقانون والأكاديمية والصناعة والجمعيات الخيرية تعمل في شراكة للمساعدة في الحفاظ على الأطفال آمنين على الإنترنت. (De Barros & Lazarek, 2018, 252).

كما أدرجت حكومة المملكة المتحدة يومًا وطنيًا أكثر أمانًا في تقويمها يقام ذلك في ٩ تشرين فبراير فيُوَثَّق الإجراءات المتخذة خلال هذا اليوم من كل عام لتبادل الوعي حول هذه المسألة، وقدمت موقعا للويب يوفر محتوىً هادفاً مثل مقاطع الفيديو، والتي يصنعها الأطفال لتوعية أقرانهم، وصفحات الحقائق حول السلامة عبر الإنترنت التي يمكن أن تكون بمثابة نقطة انطلاق لمحادثةٍ بين الآباء والأطفال. (Paraiso, 2019, 37)

أما فرنسا فقد فرض مُشَرِّعُوها عام ٢٠١٨ حظراً على استخدام تلاميذ المدارس الفرنسيين الذين تتراوح أعمارهم بين ٣ و ١٥ عامًا للهواتف الذكية والأجهزة اللوحية أثناء التواجد في المدرسة، بما في ذلك أيضاً فترات الراحة ووقت الغداء، أما التلاميذ الذين يبلغون من العمر ١٥ عامًا فأكثر تتاح لمعلميهم الفرصة لاختيار ما إذا كانوا سيتبنون حظر الهاتف لتلاميذهم أم لا، كما فرضوا أيضا حظراً على فتح حساب Facebook للأطفال دون سن ١٦ من غير موافقة الوالدين. (Quaglio & Millar, 2020, 28).

ب-الاستجابة للمخاطر السيبرانية من خلال توفير المنصات البيضاء والمستشارين للطلاب:

وهذا ما يشار إليه بالمنصات "الآمنة" أو "الأكثر أمانًا" لبث المحتوى الخاص بالأطفال مثل YouTube Kids أو Disney Kids أو cBeebies أو MEO Kids أو Hopster أو Azoomee (Blum-Ross, Donoso, Dinh, Mascheroni, O'Neill, Riesmeyer, & Stoilova, 2018, 32)

وقد قدمت أستراليا منصة عبر الإنترنت لمساعدة المدارس الأسترالية والمجتمعات في تعزيز مسؤولية التلاميذ عبر الانترنت والمرونة؛ لبناء ثقافة مدرسية

إيجابية من خلال مكتب مفوض السلامة الإلكترونية للأطفال؛ وهي منصة أمان بكمية هائلة من المحاكاة للمعلومات والموارد، إلى جانب نظام شكاوى مكثف لمساعدة الأطفال والشباب الذين يتعرضون للتنمر عبر الإنترنت (De Barros & Lazarek, 2018, 253) فتم إنشاء مكاتب مفوض السلامة الرقمية على غرار المماثلة في نيوزيلندا، وتتمثل مهمته في الترويج للسلامة الرقمية من خلال تعزيز التربية الإيجابية حول المواطنة الرقمية بين الأطفال والشباب، ومن مهامها أيضاً أنه إذا لم يلتزم موقع التواصل الاجتماعي بامتثال المعايير الواردة في مدونة قواعد الممارسة، فيمكن للفرد أن يلجأ إلى مفوض السلامة الرقمية، الذي يمكنه توجيه موقع التواصل الاجتماعي للامتثال للمعايير الواردة في المدونة(SWGfL/UK Safer Internet Centre, 2017, 2, 13) .

علاوة على تصميم الصين لمنصة آمنة للقصر ذات قائمة بيضاء بمواقع الويب المحددة والمعتمدة الوصول إلى الإنترنت عبر الهاتف المحمول على الصعيد الوطني للقُصَّر (Ning, 2011, 37)

تمتعت جميع المدارس في ماليزيا –سواء كانت حضرية أو ريفية– بإمكانية وصول التلاميذ والمعلمين إلى بيئة Frog Virtual Learning (VLE) وقد خصصتها ماليزيا للتلاميذ بلا حدود داخل وخارج المدرسة أثناء وبعد ساعات الدوام المدرسي، ليمكِّن التلاميذ من التعلم عبر هذا النظام؛ وقد أدى ذلك إلى نظام الوصول المفتوح؛ حيث تُمكن تلك المنصة التلاميذ من أن يكونوا بمفردهم خلال دروس معمل الكمبيوتر وبعد ساعات الدوام المدرسي، كذا عينت المدارس في ماليزيا معلمين ومستشارين بحيث تكون مهمتهم تقديم المساعدة لتلاميذ المدارس عند الحاجة؛ فكل مدرسة لديها معلمين إرشاديين جاهزين لمساعدة التلاميذ وضمان رفاهيتهم. (Thah, Kaur & Ling, 2019, 29, 38).

ج–الاستجابة للمخاطر السيبرانية من خلال برامج التدخل المبكر في المدرسة ومعسكرات العلاج من إدمان الانترنت:

تم تطوير جهود مواجهة الإفراط في الاستخدام بدول شرق آسيا مثل كوريا والصين؛ فأقاما برامجاً تربوية نفسية تستمر من ٣ إلى ٦ أسابيع للأطفال في سن المدرسة؛ لتقديم المعلومات حول مخاطر الإفراط في استخدام الانترنت، وتقنيات ضبط النفس، ومهارات تحديد وإدارة الوقت، والأنشطة البديلة (King, Delfabbro, Doh,

Wu, Kuss, Pallesen, Mentzoni, Carragher, & Sakuma, 2018, 234) فأقامت الصين معسكرات لعلاج إدمان الانترنت تجبر الأطفال على الانخراط في الأنشطة البدنية، (Lim, 2012, 11

أما كوريا الجنوبية فيدير IAPC (Internet Addiction Prevention Center) مركز الوقاية من إدمان الانترنت: معسكرات تسعى إلى علاج مدمني الإنترنت من خلال حجب الوصول الكامل إلى أجهزة الكمبيوتر وجعلهم يشاركون في الهواء الطلق بدلا من المكوث أمام الأجهزة؛ فتهدف المعسكرات إلى تطوير ضبط النفس في المشاركين، وتعريفهم بالبدائل الصحية لاستخدام الإنترنت(Lim, 2012, 10) مثل اللغة والرسومات التي تجذب التلاميذ ذوي الفئة العمرية من المرحلة الابتدائية (MacArthur, 2009, 37)

د- مساهمة المدارس الابتدائية في بناء قدرات أولياء الأمور كمسئولي توعية لإدارة المخاطر السيبرانية:

بعض أنظمة المدارس قدمت دروسًا ليلية للآباء حول الأمان عبر الإنترنت (Lester, 2018, 80- 81)؛ وقد كشفت مراجعة حديثة أن الرابطة الأبوية القوية Paternal Bond يمكن أن تشكل وقاية من الألعاب التي تنطوي على مشاكل(Charmaraman, Riche, & Moreno, 2020, 3) وفي هولندا ساهم - بشكل ملحوظ- التواصل بين الآباء والأطفال ومتابعة استخدام الإنترنت في تقليل مخاطر الاستخدام القهري للإنترنت، مما يشير إلى أن التواصل كان أداة واعدة للآباء لتقليل مخاطر الاستخدام القهري لأبنائهم، (Dubicka & Theodosiou, 2020, 38) ويستخدم الآباء في هذا الصدد الانضباط الحازم -ويُطلق عليه نموذج الانضباط الجازم لكارتر Carter's Assertive Discipline Model وهو وسيلة للتوجيه بالطريقة الصحيحة والكلام السليم، لتعريفهم بشكل منطقي عواقب مفهومة وإعطاء تعليمات واضحة دون إعطاء أي عقوبة؛ ففي إطاره- جميع سلوكيات الأطفال تتم مراقبتها بطريقة حازمة ولكن غير مخيفة؛ فبدون سيطرة الوالدين سيفعل الأطفال ما يحلو لهم، مما قد يؤثر سلبًا على الأطفال، وقد أظهرت نتيجة دراسة (Munawar & Nisfah, 2020, 66) أن هناك ارتباط سلبي بين الانضباط الحازم وإدمان الأجهزة؛ بعبارة أخرى، كلما

زاد الانضباط الحازم للوالدين، انخفض إدمان الأطفال على الأدوات الذكية، والعكس صحيح؛ ويؤثر الانضباط الحازم على إدمان الأجهزة بنسبة ٨٣.٨٪ .

ودور المدارس مهم في التوجيه وإعلام الوالدين بشأن استخدام الأطفال للإنترنت في المنزل (Rahman, Malaysia, Sairi, Zizi, & Khalid, 2020, 378) فيمكن للمدارس إضافة روابط أو مواقع مقترحة أو ندوات عبر الإنترنت أو موارد مجانية موجهة للآباء في نشراتهم الإخبارية Newsletter بشكل مستمر لتجربتها؛ والنشرة الإخبارية للمدرسة هي أداة تسويق عبر البريد الإلكتروني وهي جزء من برنامج إدارة التلاميذ، تُعْلِم الرسائل الإخبارية أولياء الأمور بأي شيء وكل ما يتعلق بالمدرسة: الأنشطة المدرسية والسياسات والأخبار وتغييرات الجدول الزمني والتحديثات والأحداث والعروض وجوائز التلاميذ والأحداث المجتمعية (Lester, 2018, 80– 81)؛ **ومن المهم تدريبهم على الوساطة الأبوية التي تتخذ أشكال مختلفة؛ يمكن عرضها فيما يلي:**

١– الوساطة النشطة: بناء علاقة ثقة مفتوحة حول التكنولوجيا – الحفاظ على التواصل بشكل منفتح وداعم (Ofcom, 2016, 174) حتى يعرف طفلك أنه يمكنه القدوم إليك إذا حدث شيء ما خطأ؛ فيُعتبر التوسط النشط عن استخدام الأطفال للإنترنت (التحدث معهم) الاستراتيجية الأكثر شيوعًا التي يتبناها الآباء الأوروبيون الذين تتراوح أعمار أبنائهم بين (٩–١٦) عامًا من خلال المناقشات حول محتوى الوسائط. (Livingstone, Mascheroni, Dreier, Chaudron, & Lagae, 2015, 7–8)؛ فحتى لو كان الأب والطفل في المنزل معًا، فلا يمكن مراقبة أنشطة الطفل عبر الإنترنت كل ثانية من اليوم، وقد أثبتت الدراسات أنه مع الحظر، يصبح الأطفال خبراء في إيجاد طرق تلتف حول النظام، ولأن الإنترنت يتغير باستمرار، فإن آليات التصفية تصبح قديمة بسرعة، وعلى أي حال قد يتم حظر تعلم المواد القيِّمة عند تثبيت هذه الآليات.(MacArthur, 2009, 14)، لذا من المهم التحدث مع الأبناء حول مشكلات الأمان عبر الإنترنت؛ بما يساعد ذلك في تطوير تفكيرهم النقدي وقدرتهم على اتخاذ خيارات جيدة.(UNICEF, 2020, 3) فعلى الرغم من سياسة الاستخدام المقبول، وبرامج التصفية التجارية، والمراقبة الدقيقة من قبل المعلمين، يظل من المهم تثقيف التلاميذ من جميع الأعمار حول كيفية حماية سلامتهم الشخصية، وقد وضعت ISTE

معاييراً للتلاميذ والمدرسين والإداريين كي يؤسسون إحساسهم الخاص بالصواب والخطأ بالاحتكام إلى أخلاق مجتمعهم.(Schubart, 2021, 4, 6)

وقد نُقل عن كونفوشيوس قوله "إذا حكمت الناس لوجستيًا وتحكمت بهم عن طريق العقاب سوف يتجنبون الجريمة، لكن لن يكون لديهم إحساس شخصي بالعار؛ أما إذا كنت تحكمهم عن طريق الفضيلة والسيطرة عليهم بلياقة، سوف يكتسبون إحساسهم بالعار، وهكذا يصححون أنفسهم؛ لذا يجب أن يدرك اختصاصيو التوعية أن التلاميذ يحتاجون التوجيه في استيعاب العنصر المطلوب من السلوك الأخلاقي في هذا العصر المتقدم وإلا سيتعرضون للرفض الاجتماعي الذي يجلب العار(Payne, 2016, 31) وتكون تلك الوساطة من خلال الدعوة للمناقشة وحتى الدعوة لسرد القصص؛ حتى يتمكن الأطفال من تقديم الأفكار التي تدور في أذهانهم أو إبداعها. (Widiputera, Satria, Perdana , Zamjani & 2021, 38)

٢- الوساطة التقييدية: من خلال إرشادات وقيود السلامة بتوفير قواعد الاستخدام والقيود المفروضة على وقت الاستخدام وموقع الاستخدام والمحتوى الذي تم الوصول إليه.

٣- وساطة المشاهدة المشتركة: بمشاركة الطفل في المشاهدة واللعب معه عبر الإنترنت؛ يساعد هذا على فهم أفضل لما يفعلونه ولسبب استمتاعهم بتطبيق أو لعبة أو موقع ويب، أيضًا توفير فرصة رائعة لبدء محادثات حول الأمان عبر الإنترنت. (Hidayati, Afiatin & Susanti, 2019, 41) ويجب على الآباء إيجاد توازن بين كل من تعزيز الاستقلالية، وسلوك المراقبة عند استخدام الإنترنت؛ فتبعاً إلى الأدبيات الموجودة، يرتبط تقييد الاستقلالية فيما يتعلق باستخدام الإنترنت بنتائج سلبية وتظهر كعوامل خطر، بينما المراقبة الأبوية تعزز النمو النفسي الصحي والإيجابي. (Faltýnková, Blinka, Ševˇcíková, & Husarova, 2020, 2)

٤- وساطة بناء عادات جيدة تساعد الطفل على تنمية الذكاء الرقمي والاجتماعي والمهارات العاطفية – مثل الاحترام والتعاطف والتفكير النقدي وسلوك المسؤولية والمرونة – وممارسة كونه مواطنا صالحا عبر الإنترنت. (UNICEF, 2020, 3–11)

٥- الوساطة التقنية (استخدام عوامل التصفية، الرقابة الأبوية بما في ذلك عوامل تصفية المحتوى، /PIN رمز رقم التعريف الشخصي Personal identification number

كلمات المرور، والبحث الآمن) (Livingstone, Mascheroni, Dreier, Chaudron, & Lagae, 2015, 4)

وتتجه الدول لتوعية الآباء تمكيناً لهم من أن يكونوا أكثر مرونة سيبرانية؛ بإشراكهم في فهم المخاطر الناشئة والسلوك الإشكالي واختبار طرق تقليل الأضرار، والتثقيف حول المخاطر وإيصالها إلى أفراد الأسرة، ووضع إرشادات حول استخدام التقنيات الناشئة والمساعدة على الالتزام (Swanton, Blaszczynski, Forlini, Starcevic & Gainsbury, 2021, 2) وكذا فهم البرامج التي يمكن أن تساعدهم في إدارة استخدام التكنولوجيا الرقمية الخاصة بأبنائهم، على سبيل المثال، فهم التطبيقات التي تمكنهم من استخدام قيود الوقت وتطبيقات منع استخدام البرامج الضارة ومراجعة إعدادات الخصوصية (Dubicka & Theodosiou, 2020, 18, 20, 45) فيتم دعم تعليم الوالدين؛ بإعطائهم نصائح (عملية) للمراقبة والحفاظ على حوار مع أطفالهم حول إيجابيات وسلبيات التكنولوجيا والاستخدام المضلل للإنترنت، وتطوير خطة أمان عبر الانترنت–بما في ذلك برامج التصفية والحظر والمراقبة– لتقليل احتمالية التعرض للمواد الجنسية. (Hornor, 2020, 196)

كما يتم توعية الآباء باستخدام أدوات الرقابة الأبوية وهي برامج تتيح للمستخدمين– عادة الآباء– التحكم في بعض أو كل وظائف الكمبيوتر، هذه البرامج عادة محمية بكلمة مرور، يمكن لبعض أدوات التحكم تقييد الوصول إلى أنواع أو فئات معينة من مواقع الويب أو الخدمات عبر الإنترنت؛ ويوفر البعض الآخر أيضًا مجالًا لإدارة الوقت، أي يمكن ضبط الجهاز للوصول إلى الإنترنت فقط خلال ساعات معينة، يمكن للإصدارات الأكثر تقدمًا تسجيل جميع النصوص المرسلة أو المستلمة من الجهاز (Unicef, 2016, 6)

هذا وقد أكدت دراسة (Widiputera, Satria, Perdana , Zamjani & 2021, 38) أنه يجب أن ينمي الوالدين الخوف من الله حتى يعرف أن الله موجود إذا لم يكن هناك أب يشاهده، يمكن أن يؤدي ذلك بالأطفال إلى اتخاذ قراراتهم الخاصة دون تفكير سيء؛ وكذا دراسة (شفيق، ٢٠١٤، ٢٨٤) التي أكدت أن الرقابة الذاتية وتنمية القيم الأخلاقية بالفرد منذ صغره، تبقى رادعا شخصيا لمثل هذه المواقع. وبشكل عام، يتم دعم

استخدام التقنيات من قبل مواطني المملكة العربية السعودية في حالة عدم تعارضها مع تقاليد الدولة ومعاييرها الدينية؛ فلا يقللون من أهمية التقاليد على حساب الفرص الرقمية للتلاميذ؛ لذا فإن المعلمين السعوديين يعتمدون على القيم الثقافية والمعتقدات الدينية الإسلامية لتطوير مهارات المواطنة الرقمية التي يمكن أن تستخدم ليس فقط لتعزيز البصمات الرقمية الإيجابية، ولكن أيضًا للتشجيع على استخدام التكنولوجيا لبناء السلوكيات المسئولة في المدرسة.(Alqahtani, 2017, 2–3, 50).

ومن ثم يمكن الاستناد إلى قصص واقعية في مراقبة الله وخشيته بالغيب من التراث الإسلامي الذي يشتق منه القيم التربوية للمجتمع ومُثُله، نذكر منها على سبيل المثال:

(أ) ذكر هذه القصة في صفة الصفوة (ابن الجوزي، ٢٠١٢، ٣٦٥)

قال نافع: خرجت مع ابن عمر في بعض نواحي المدينة ومعه أصحابٌ له، فوضعوا سفرة فمر بهم راع، فقال له عبد الله: هلم يا راعي فأصب من هذه السفرة، فقال: إني صائم، فقال له عبد الله : في مثل هذا اليوم الشديد حره وأنت في هذه الشعاب في آثار هذه الغنم وبين الجبال ترعى هذه الغنم وأنت صائم، فقال الراعي: أبادر أيامي الخالية، فعجب ابن عمر، وقال: هل لك أن تبيعنا شاةً من غنمك نجتزرها ونطعمك من لحمها ما تقطر عليه ونعطيك ثمنها، قال : إنها ليست لي إنها لمولاي، قال: فما عسيت أن يقول لك مولاك إن قلت أكلها الذئب؟! فمضى الراعي وهو رافع إصبعه إلى السماء وهو يقول فأين الله؟ قال: فلم يزل ابن عمر يقول: قال الراعي فأين الله؛ فما عدا أن قدم المدينة فبعث إلى سيده فاشترى منه الراعي والغنم فأعتق الراعي ووهب له الغنم –رحمه الله– وهنا درس عظيم الآخر وهو تنمية الصلة بالله وخشيته في الغيب والشهادة.

(ب) ذكر هذه القصة في صفة الصفوة (ابن الجوزي، ٢٠١٢، ٩٣٤)

عن زيد بن أسلم، عن أبيه، عن جده أسلم، قال : بينا أنا مع عمر بن الخطاب رضي الله عنه وهو يعس المدينة إذ عيي فاتكأ إلى جانب جدار في جوف الليل، فإذا امرأة تقول لابنتها :يا ابنتاه قومي إلى ذلك اللبن فامذقيه بالماء، فقالت لها: يا أماه أَوَ مَا علمتِ ما كان من عزمة أمير المؤمنين اليوم؟ قالت: وما كان من عزمته يا بنية؟ قالت :إنه أمر مناديه فنادى أن لا يشاب اللبن بالماء، فقالت لها :يا بنية قومي إلى

ذلك اللبن فامذقيه بالماء فإنكِ بموضع لا يراك عمر ولا منادي عمر، فقالت الصبية لأمها: يا أمتاه والله ما كنت لأطيعه في الملأ وأعصيه في الخلاء.

(ج) بينما نفرٍ يمشونَ أخذهمُ المطرُ، فآووا إلى غارٍ في جبلٍ، فانْحطَّتْ على فمِ غارِهم صخرةٌ من الجبلِ فانطبَقتْ عليهم، فقال بعضُهم لبعضٍ: انظروا أعمالًا عمِلْتُموها صالحةً للهِ، فادعوا بها لعلَّه يُفرِّجُها عنكم، فقال أحدُهم: اللهمَّ إنه كان لي والدانِ شيخانِ كبيرانِ وامرأتي، ولي صبيةٌ صغارٌ أرعى عليهم، فإذا أرَحْتُ عليهم حلبتُ، فبدأتُ بوالدي فسقيتُهما قبلَ بَنِيَّ، وإن نأى بي ذاتَ يومٍ الشجرَ، فلم آتِ حتى أمسيتُ فوجدتُهما قد ناما، فحلبتُ كما كنتُ أحلبُ، فجئتُ بالحلابِ، فقمت عند رؤوسِهما، أكره أنْ أوقظَهما من نومِهما، وأكره أنْ أُسْقي الصبيةَ قبلَهما، والصبيةُ يتضاغونَ عند قدمي، فلم يزلْ ذلك دأْبي ودأبَهم حتى طلع الفجرُ، فإنْ كنتَ تعلمُ أني فعلتُ ذلك ابتغاءَ وجْهِك فافْرُج لنا فرجةً نرى منها السماءَ، ففرَّجَ اللهُ منها فرجةً فرأوا منها السماءَ، وقال الآخرُ: اللهمَّ إنى كنتُ استأجرْتُ أجيرًا بِفَرَقِ أرُزٍّ، فلمَّا قضى عملَه، قال لى: أعطنى حقِّي، فعرضتُ عليه فَرَقَهُ، فرغِبَ عنه، فلم أزلْ أزرعُه حتى جمعتُ منه بقرًا ورِعاءَها، فجاءني فقال: اتقِّ اللهَ ولا تظْلمْنى حقِّي، قلتُ: اذهبْ إلى تلك البقرِ ورِعائِها فخذْها، فقال: اتقِّ اللهَ ولا تستهزئْ بى، فقلت: إني لا أستهزئُ بك، خذْ ذلك البقرَ ورِعاءَها، فأخذه وذهب به، فإنْ كنتَ تعلمُ أني فعلتُ ذلك ابتغاءَ وجْهِك، فافْرُجْ ما بقيَ، ففَرَجَ اللهُ ما بقيَ. (الألباني، ١٩٨٨، ٥٥٤).

هـ- مساهمة المدارس الابتدائية في بناء قدرات المعلمين كمسئولي توعية لإدارة المخاطر السيبرانية.

في إحدى الدراسات كان يمتلك ما يقرب من ٩٠ % من معلمي المدارس هاتفًا ذكيًا، بينما تلقى ٢٧% منهم فقط تدريبًا إلزاميًا على أمن المعلومات (Richardson, Lemoine, Stephens, & Waller, 2020, 28) وفي النظام المدرسي التشيكي ربع معلمي تكنولوجيا المعلومات والاتصالات هم فقط المؤهلون بالفعل لتدريس موضوع السلامة السيبرانية (Šimandl, 2015, 52) مما يدل على نقص تأهيل المعلمين للقيام بدورهم كمسئولي توعية بالمخاطر السيبرانية.

وتوصي الدراسات بأنه يجب على المدرسة تعيين شخص يتمتع بالمعرفة والخبرة الكافية وأن يكون لديهم الاستعداد للاستماع وتقديم النصيحة؛ لتنسيق عمليات إدارة

المخاطر السيبرانية، بالإضافة إلى ضرورة تلقيهم تدريباً لإعدادهم على ذلك (Paraiso, 2019, 50) لذا توصي دراسة (Kritzinger, 2020b,4) بأنه من الضروري أن تقوم المدارس بالحصول على الهيئات الإدارية والمعلمين للوعي بالسلامة الإلكترونية ذات الصلة ببناء ثقافة أمان الإنترنت داخل المدرسة ؛ لذا تقوم بعض أنظمة المدارس بالتنمية المهنية PD للمعلمين حول الأمان عبر الإنترنت (Lester, 2018, 81)؛ لضمان حصول المعلمين على تدريب كاف ومحدّث تعزيزاً لقدرة تلاميذه على الفهم النقدي بدلا من النهج المقيّد للسلامة السيبرانية (Rahman, Malaysia, Sairi, Zizi, & Khalid, 2020, 379)

أما في اسكتلندا وإنجلترا فيلعب المعلمون دورًا رئيسًا فيما يتعلق بالتثقيف حول الأمان عبر الإنترنت من خلال منهج تعليم الصحة والرفاهية وجمعية التثقيف الشخصي والاجتماعي والصحي،(Dubicka & Theodosiou, 2020, 17) وفي إستونيا، تعتمد الحياة اليومية كلها تقريبًا على الأنشطة على الإنترنت؛ لذا كان هدفهم تعزيز أمان واستخدام أفضل للإنترنت وتقنيات الهاتف المحمول بين الأطفال والشباب؛ فاعتمدوا على إجراء أنشطة مثل تنظيم الندوات ودورات تدريبية للمعلمين والأخصائيين الاجتماعيين، وجمع ونشر مواد التوعية والتدريب لهم على المستوى الوطني (De Barros & Lazarek, 2018, 252)

كما يحرص أيضا صانعو السياسات على تدريب المعلمين والقيادة العليا في المدارس على التطبيق العملي لتمكينهم من الوصول إلى أمثلة للممارسات الجيدة من الاستخدامات الإيجابية للتقنيات الرقمية (Blum-Ross, Donoso, Dinh, Mascheroni, O'Neill, Riesmeyer, & Stoilova, 2018, 41) فيتم تشجيع المعلمين على حضور برنامج التطوير المهني للتوعية بأمان الإنترنت للمعلمين التابع لـ هيئة ACMA (Australian Communications and Media Authority) الاتصالات والإعلام الأسترالية؛ فيهدف هذا البرنامج إلى تثقيف المعلمين حول المخاطر المحتملة المرتبطة بالإنترنت، مثل سرقة الهوية والتسلط عبر الإنترنت والخداع والاتصال والمحتوى غير المناسب، كما يوفر لهم الأدوات المناسبة. (Department for Education and Child Development, 2009, 8, 12, 17).

ولأن التلاميذ في كل من ماليزيا وتايلاند لديهم حق طلب المساعدة عند مواجهة مشكلات الأمان عبر الإنترنت؛ عينت لهم المدارس الماليزية معلمين ومستشارين بحيث تكون مهمتهم تقديم المساعدة لتلاميذ المدارس عند الحاجة؛ فكل مدرسة لديها مدرسين إرشاديين جاهزين لمساعدة التلاميذ وضمان رفاهيتهم؛ من خلال تعليمهم منهج المواطنة الرقمية بهدف محو أميتهم؛ بمعنى ليس فقط فهم ما يجب فعله وما لا يجب فعله ولكن أيضًا تطوير السلوك الصحي عند تصفح الإنترنت؛ ليتمكن التلاميذ من معرفة الطرق المناسبة للتفاعل مع الآخرين عبر الإنترنت (ما هو مناسب وما هو غير ذلك) (Thah, Kaur, & Ling, 2019, 38) ويمكن أن يتم ذلك من خلال المحتوى التفاعلي Interactive content الذي يتضمن ألعابًا أو اختبارات أو بطاقات نشاط تتوافق مع عمر الطفل، واستخدامها كمصادر خارجية لزيادة وعي الأطفال (Paraiso, 2019, 54)

علاوة على اعتماد بعض مدارس الولايات المتحدة الأمريكية على مستشارين – في حالات التنمر الإلكتروني، فتعتمد بعض مدارسها بولاية كاليفورنيا على مسؤول الموارد المدرسية School Resource Officers (SRO) كمستشار؛ للمساعدة في التحقيقات؛ فيشارك SRO بطريقتين: (أ) استرداد المعلومات التي يمكن أن تساعد في التحقيق، (ب) تثقيف التلاميذ فيما يتعلق بالعواقب القانونية للتنمر الإلكتروني (Nye, 2014, 770–71)

وبناءً على ما سبق، يمكن عرض بعض أدوار المعلمين كمسئولي توعية سيبرانية يمكن أن تتم التنمية السيبرانية لهم في ضوئها:

(أ) المعلم كنموذج يتعلم منه التلاميذ؛ ينبغي ألا يُنظر إلى المعلمين في مجال السلامة السيبرانية على أنهم مجرد مُنَظِّرين ولكن أيضًا شخصيات يمكنها التأثير بشكل كبير على التلاميذ من خلال نموذجهم الخاص؛(Šimandl, 2015, 62) فيجب على المعلمين أخذ زمام المبادرة، ليكونوا نموذجًا للسلوكيات المناسبة، وتشجيع التلاميذ ليكونوا مواطنين رقميين في الفضاء السيبراني (Payne, 2016, 19) كأن يُظْهر لهم المعلم الاهتمام الذاتي بتعلم كيفية التصرف بأمان عبر الإنترنت، وسيحصلون عليه في كل مرة (Muir, 2010, 10) بل ويُفرَض على المعلمين في **أستراليا** التأكد من أن "البصمات

الرقمية" لهم تتفق مع دور المعلمين، ومدونة قواعد الأخلاق للقطاع العام (Department for Education and Child Development, 2009, 8, 12, 17).

(ب) اغتنام فرص غير مقصودة؛ كأن يدخل بعض المعلمين في مواقف غير مخطط لها –كالأخبار في وسائل الإعلام – ويستخدمونها لتحقيق مكاسب المعرفة والإلهام حول كيفية البقاء بأمان قدر الإمكان. (Šimandl, 2015, 56)

(ج) اتباع نموذج توعية التلاميذ بالعواقب؛ بمعنى توعية التلاميذ بآثار هذا السلوك غير الأخلاقي والعواقب التي تحدث عندما يتم اتخاذ قرارات سيئة في الشأن السيبراني. (Payne, 2016, 3) فقد يكون الدافع وراء السلوك الآمن لدى بعض التلاميذ هو الخوف من العواقب المحتملة وإمكانية إساءة استخدام بياناتهم الشخصية وإساءة استخدام الهوية والاحتيال عليهم. (Šimandl, 2015, 57)

(د) توجيه التلاميذ إلى النظر –بشكل عملي–في استمرارية المعلومات عبر الإنترنت؛ كأن يَطلب المعلم من التلاميذ إجراء بحث عن أسمائهم؛ فقد يجدون معلوماتٍ يشعرون بالقلق بشأنها، أو يحاولون إزالة منشور من موقع استضافة ولا يفلحوا. (Muir, 2010, 23).

وفي هذا الصدد –وبصورةٍ عملية– قامت إحدى معلمات الصف السادس في أوكلاهوما بالولايات المتحدة الأمريكية –والتي أصبحت مهتمَّة بمنشورات تلاميذها– وأرادت تعليمهم: معنى البصمة الرقمية وكيف لا يمكن محوها بالكامل؛ فقامت بإنشاء إشارة تفيد بأن تلاميذها يعتقدون أنه من المقبول نشر صور غير لائقة لأنفسهم عبر الإنترنت، ثم طلبت من مجتمع Facebook نشر تلك الإشارة ومشاركتها؛ وفي غضون ساعات وصلت تلك الإشارة إلى جميع الولايات الخمسين وعدة دول، ثم حذفت المنشور، لكن واصل المنشور التعميم، واستغلت تلك اللحظة لتعليم تلاميذها بصمتهم الرقمية، وكيف لا يمكن محوها بالكامل(Payne, 2016, 15)

(هـ) توجيه عناية التلاميذ إلى النظر للانترنت كفرصٍ لتطوير أنفسهم؛ بدلاً من توجيه نظرهم للانترنت كمجموعة من الأمور المحظورة؛ من خلال تمكين المعلم لتلاميذه من

اتخاذ خيارات واكتشافات ذكية حول ما الذي يمكنهم فعله بالتكنولوجيا؛ لمساعدتهم على أن يكونوا أكثر نجاحًا في تعليمهم وشخصيتهم وحياتهم العملية.(Muir, 2010, 9)

(و) أساليب علاجية للتنمر: بما أن المتنمرين يجدون أن العدوان هو طريق سهل للحصول على ما يريدون، فلا بد من تعليمهم في الفصل المدرسي أساليب المواجهة الأخرى، مثل التسوية والتفاوض كأساليب للحصول على ما يحتاجون. (Muir, 2010, 30)

(ز) استخدام أسلوب القصة التربوية.

تستخدم منظمة التثقيف الرقميStaySafeOnline قصة خيالية كتبها Jacalyn S.Leavitt بعنوان "فو باو القط التقني: مغامرات في الإنترنت"، هذه القصة هي أداة مرئية يمكن للمعلمين استخدامها لإعادة التأكيد على المفاهيم التي تعلموها في الأنشطة الصفية؛ فسلسلة الرسوم المتحركة ‖Faux Paw— منهج مصمم خصيصًا لأطفال المدارس الابتدائية .(Zepf & Arthur, 2013, 21, 23)

كما تستخدم منظمة التثقيف الرقمي Cyber (smart) عددًا من الموارد عبر الإنترنت للأطفال الذين تتراوح أعمارهم بين عام- سبعة أعوام، وكان أحد الموارد الأساسية الذكية للإنترنت هو التركيز على قصة تسمى "عالم هيكتور"، يقدم هذا السرد موضوعات أساسية مثل إخفاء المعلومات والتسلط عبر الإنترنت وأمن الكمبيوتر، عند استخدام هذا المنهج، يستخدم المعلمون السرد المقدم إلى جانب مجموعة متنوعة من السرد القصصي أو مقاطع الفيديو التي تناقش مواضيع مثل كلمات المرور القوية والفيروسات والنوافذ المنبثقة، وتعزز الأمان عبر الإنترنت من خلال روايات واقعية لأشخاص في الأخبار التي تأثرت سلبًا بعدم ممارسة الأمن السيبراني ,Zepf & Arthur (2013, 12-13).

هذا ويتم الاستعانة بالمعلمين بسبل مختلفة عند إدارة المخاطر السيبرانية فمثلاً: تم إعداد ٤٧ مقطعا للفيديو متاحًا وفقًا لأعمار الأطفال وسلامة الإنترنت، وتم الاستعانة بمعلم مدرسة ابتدائية لتحديد مدى ملاءمة مقاطع فيديو للفئات العمرية والفصول الدراسية النموذجية. (Paraiso, 2019, 54)

و – مساهمة المدارس الابتدائية في بناء قدرات التلاميذ تحقيقا للكفاءة الذاتية لإدارة المخاطر السيبرانية.

انتقل مفهوم إنشاء بيئة آمنة عبر الإنترنت من حماية الأشخاص إلى إكساب التلاميذ مهارات السلامة الإلكترونية الخاصة بهم والمعرفة والثقة لتعظيم الفرص الفعالة (NetSafe, 2010, 2).

ويقصد بمحو الأمية الرقمية Digitalliteracy أن تطوِّر المدرسة قدرة النشء على استخدام ومشاركة وإنشاء محتوى رقمي بطريقة تقلل من المخاطر وتعزز النتائج الإيجابية (Kritzinger, 2020, 5)، ومحو الأمية الرقمية أساس للمواطنة الرقمية؛ فهي مزيج من المهارات التقنية والاجتماعية التي تمكن الشخص أن يكون ناجحًا وآمنًا في عصر المعلومات ومشاركًا مدى الحياة (NetSafe, 2010, 3)؛ فيحتاج الأطفال والشباب إلى تعليمهم مهارات الاستخدام والإبداع ونقد التقنيات الرقمية، وإعطائهم الأدوات اللازمة للتفاوض. (Education Scotland, 2017, 13) تحقيقًا للكفاءة الذاتية وهي الإيمان بقدرات الفرد فى دفع القرار وصنع السلوك في موقف معين بناءً على القيم الأساسية والعميقة للشخص؛ فجميع القرارات منبعها قيمة، ويميل الناس إلى التصرف بطرق تتفق مع معتقداتهم. (Mark, 2014, 13)

وفي دراسة أجرتها لجنة الرخصة الأوروبية لقيادة الكمبيوتر (ECDL) عام ٢٠١٦ ذكرت فيها أن أكثر المجموعات (الضعيفة في استخدام الوسائط الرقمية عبر الإنترنت) تتكون من الأطفال والشباب وليس كبار السن، على الرغم من الوهم الواسع بأن الشباب مواطنون رقميون ويمكنهم استخدام الوسائط الرقمية بأمان وكفاءة؛ إذن هم ليسوا آمنين من مخاطر الإنترنت.(De Barros & Lazarek, 2018, 251) فالأمان لا يتعلق بسنٍ وإنما يتعلق بالتعرض للتوعية من تلك المخاطر؛ فقد وجدت الدراسات أنه من بين الأطفال الأوروبيين الذين تتراوح أعمارهم بين ٩ و ١٦ عامًا، أولئك الذين لديهم مستويات عالية من المعرفة الرقمية هم أيضًا أكثر مهارة في التنقل الآمن بين الأنشطة عبر الإنترنت. (Paraiso, 2019, 30)

١–بناء قدرات التلاميذ من خلال الاعتماد على تعليم الأقران

تزداد إمكانية التعلم من الأقران في المدارس الابتدائية؛ فيعلم الأطفال بعضهم البعض كيف يصبحون على دراية بمخاطر الفضاء الإلكتروني، وقد ثبت أن هذا الأمر فعال؛ فبالنسبة للعديد من الأطفال، يشكل أقرانهم مورداً قيماً؛ فوفق دراسة (Spiering, 2018, 22) فإن ٦٣٪ من الأطفال الأوروبيون الذين تتراوح أعمارهم بين ٩ و١٦ عامًا تلقوا نصائح حول أمان الإنترنت من أولياء أمورهم، ٥٨٪ منهم المعلمين و ٤٤٪ من أقرانهم وهي نسبة ليست بالقليلة، وفي إستونيا يتم تفويض بعض الآباء دورهم لوسطاء من أشقاء الأطفال الأكبر سناً؛ لحماية أطفالهم من المخاطر السيبرانية Older Siblings (Holloway, Green & Livingstone, 2013, 22)، "وفي دراسة حول كيفية استخدام الأجهزة اللوحية وتكنولوجيا الهاتف مع عدد كبير ممن يستخدمون الانترنت في ٦٧١ مدرسة بريطانية؛ وردا على سؤال ما النصيحة التي تعطيها للآخرين الخاصة بك؟ استجاب أكثر من ٥٤٠٠ تلميذاً وكانت نصائحهم كالتالي: فكر في العواقب قبل نشر أي شيء عبر الإنترنت، ولا تثق بالأشخاص حتى تراهم وجهًا لوجه (ودائمًا يكون معك شخص آخر عند المقابلة)، ولا تقل أي شيء لا تريد أن تسمعه، ولا تنشر أي معلومات شخصية عبر الإنترنت – مثل عنوانك أو بريدك الإلكتروني أو رقم الهاتف المحمول– فكر جيدًا قبل نشر الصور أو مقاطع الفيديو عن نفسك، ولا تضع شعار المدرسة في الصورة، بمجرد وضع صورة لك على الإنترنت، يمكن لمعظم الناس رؤيتها وقد يتمكنوا من تنزيلها، فهي ليس ملكك أنت فقط بعد الآن، احتفظ بملف إعدادات الخصوصية على أعلى مستوى ممكن، لا تعطِ كلمات مرورك أبدًا لأحد، لا تلتقِ بأناس لا تعرفهم ممن تواصلت معهم عبر الإنترنت، تحدث إلى والديك أو مقدم الرعاية حول الأشخاص الذين يقترحون عليك مقابلتهم، تذكر أنه ليس كل الأشخاص على الإنترنت هم من يقولون إنهم، فكر بعناية حول ما تقوله قبل أن تنشر شيئًا على الإنترنت، احترم آراء الآخرين حتى لو كانت لا تتفق مع آرائك ولا تكن وقحًا في الجدال، إذا رأيت شيئًا على الإنترنت جعلك تشعر بعدم الارتياح أو عدم الأمان أو القلق: اترك الموقع، وقم بإيقاف التشغيل إذا كنت ترغب في ذلك، وأخبر شخصًا بالغًا موثوقًا به على الفور، أيضا لا تذهب على Facebookأو Twitter حتى تبلغ من العمر ١٦ عامًا تقريبًا (Clarke & Crowther, 2015, 9-10).

ويمكن عرض بعض الممارسات الجيدة حول بناء قدرات التلاميذ بمساعدة أقرانهم:

(أ)- تشجيع المدرسة لتلاميذها على المشاركة في إنشاء مقاطع توعوية لأقرانهم.

لا يمكن للآباء الاعتماد فقط على استخدام الحظر لأن أبنائهم سيجدون طريقة للتغلب على القيود والفلاتر، بدلاً من ذلك، ينبغي جعلهم شركاء في الحفاظ على أنفسهم والآخرين آمنين. (Muir, 2010, 10)

ويعتبر التعلم من الأقرن من التدخلات المدرسية ذات النتائج الجيدة عند استخدامها؛ فيُطْلب من التلاميذ إنشاء مقطع فيديو ينصحون فيه أقرانهم؛ لمنع إدمان الانترنت IA في مدرستهم، بعد تثقيفهم بهذا الشأن. (Ruggieri, Santoro, Francesco De Caro, Palmieri, Capunzo, Venuleo, & Boccia, 2016, e11817-2)

أيضاً يُطلب من التلاميذ أن يصنعون مقاطع فيديو على YouTube، لتدريس أخلاقيات السلوك على الانترنت ليس فقط لزملائهم في الفصل ولكن للآخرين أيضًا.(Payne, 2016, 36, 39)

(ب)- تشجيع المدرسة لتلاميذها على المشاركة في لعب الأدوار .

تحرص المدارس على تثقيف التلاميذ حول الأخلاق، وتدريبهم على كيفية التعامل مع المواقف العامة بشكل إيجابي، وتم استخدام المحادثات باستخدام المشكلات الواقعية لاختبار سلوك أخلاقيات التلاميذ، كما تم اكتشاف أسلوب لعب الأدوار الفعال؛ لأنه يتيح للتلاميذ "الشعور بما يشعر به شخص آخر عند عكس الأدوار؛ يحتاج التلاميذ إلى التفكير في ما سيشعرون به إذا قام شخص ما بنفس الأشياء لهم؛ فعدم الراحة عند التعرض للتنمر الإلكتروني وسيلة جيدة للتعبير ولإيصال الفكرة، كما أنه يوفر لهم الإبداع والقليل من المرح، مما يحافظ على طالب مشارك في العملية. (Payne, 2016, 36, 39)

يمكن أن يكون لعب الأدوار طريقة تدريس فعالة للسلامة على الإنترنت؛ يمكن أن يكون هذا مفيدًا بشكل خاص؛ فيستخدمه التلاميذ الأكبر سنًا في المدرسة عند تعليم التلاميذ الأصغر سنًا حول الاستمالة، على سبيل المثال: أعطى التلاميذ الأكبر سنًا

مصاصات للتلاميذ الأصغر سنًا، ثم طلبوا منهم معلومات شخصية عنهم، ليشاهدوا ردة فعلهم؛ وقد كانت هذه طريقة فعالة جدًا لتعليم الاستمالة. (MacArthur, 2009, 16)

(ج)- تشجيع المدرسة لتلاميذها على القيام بالدور الإيجابي القيادي عند تعرض الأقران لتجارب سلبية عبر الانترنت.

إن المتفرجين من التلاميذ هم عنصر أساسي في الحد من إيذاء الإنترنت، يجب أن يركز التعليم على استراتيجيات المتفرجين، والتي تُعَلِّم التلاميذ كيف يكونوا قادة فعالين بين أقرانهم؛ فبشكل عام، المعلمون وأولياء الأمور ليسوا عادة موجودين عند وقوع حوادث الإيذاء عبر الإنترنت، وغالبًا ما يكون أحد الأصدقاء هو من يتدخل للمساعدة في حل هذه المواقف؛ من خلال مساعدتهم على التحول عقليًا وعاطفيًا نحو منظور أكثر إيجابية، ومن ثم تضمنت بعض إجراءات الأقران الناجحة لمساعدة ضحايا الإنترنت: قضاء الوقت مع الضحايا، والتحدث معهم، وتشجيعهم، والاستماع إليهم، والحفاظ على علاقات اجتماعية إيجابية بين التلاميذ، ويقوم التلاميذ بهذا الدور من خلال التعلم العاطفي في المدارس؛ باعتباره العملية التي يفهم من خلالها الأطفال والبالغون ويتدربون على المهارات الاجتماعية والعاطفية ووضع أهداف إيجابية وتحقيقها، والشعور بالتعاطف مع الآخرين وإظهاره لهم، وإنشاء علاقات إيجابية والحفاظ عليها، واتخاذ قرارات مسؤولة.(Mark, 2014, 33)

ويمكن عرض دراسة حالة إحدى مدارس كاليفورنيا وتحديداً مدرسة صني فيوSunny View School التي نجحت في استحداث بروتوكل استجابة للتسلط السيبراني وتنفيذه بفاعلية، وهي مدرسة عالية الإنجاز يتجاوز مؤشر الأداء demic (API)لهذه المدرسة ٩٠٠ نقطة، ويستمر في الزيادة، تحتوي فصول العلوم على مجموعة من أجهزة IPad ؛ لاستخدامها أثناء الفصول الدراسية، فقامت Sunny View بإنشاء وتنفيذ بروتوكول للاستجابة لانتهاكات حوادث التسلط عبر الإنترنت (Nye, 2014, 62, 66)

وقد بدأت مدرسة صني فيو هذا البرنامج في عام ٢٠١٢، تُعلم تلك المدرسة مجموعة من التلاميذ كيفية التدخل عندما يرون حدوث التسلط عبر الانترنت سواء في وجودهم أو عبر الإنترنت، وإبلاغ المدرسة بالقضايا المتعلقة بمجتمع المدرسة من خلال

اجتماعات شهرية منتظمة، تساعد تلك الاجتماعات إدارة المدرسة في إدراك أنواع المواقف التي يواجهها الأطفال، والقضايا التي تؤثر عليهم، وأنواع السيناريوهات التي قد يُنظر إليها على أنها علامات أولية للتسلط، يُعَلِّم البرنامج التلاميذ أن يكونوا مسؤولين في المدرسة، لتعيين قدوة إيجابية، ومصادقة التلاميذ الذين قد لا يكون لديهم الكثير من الأصدقاء، يلعب التلاميذ في هذا البرنامج دورًا حاسمًا في الاستجابة لحوادث التسلط عبر الإنترنت (Nye, 2014, 88)

وفي إطار هذا البروتوكول يتم اختيار هؤلاء التلاميذ للمشاركة بناءً على انتمائهم إلى مجموعات متنوعة وتأثيرهم على التلاميذ الآخرين، ويشارك أكثر من ٢٠٠ طالب في هذا البرنامج، وهؤلاء ليسوا بالضرورة أكثر التلاميذ شعبية، ويتم تدريب هؤلاء التلاميذ على تحديد التنمر الإلكتروني، واستخدام الاستراتيجيات لنزع فتيل المواقف (Nye, 2014, 86-87)

٢-بناء قدرات التلاميذ بالاستناد إلى المبادئ التوجيهية الدولية:

وتمثل المبادئ التوجيهية توصيات المؤسسات الدولية للحد من المخاطر السيبرانية والاستجابة لمخاطرها بناء على خبرتها والحالات التي تُعرض عليها، ويمكن تفصيلها على النحو التالي:

(أ) المبادئ التوجيهية الدولية لإدارة مخاطر إدمان الانترنت بشكل استباقي:

-تعليم التلميذ كيفية البحث بمسؤولية وكيفية التنقل عبر مواقع الويب دون الخروج من المهمة التي يبحث عنها والإلهاء بغيرها.(Payne, 2016, 97)

- تعيين حدود زمنية توازن الوقت الذي يقضيه أمام الشاشات مع الأنشطة غير المتصلة بالإنترنت، (Widiputera, Satria, Perdana , Zamjani & 2021, 38)

- وضع حدود حول استخدام الشاشة الخاصة بولي الأمر والالتزام بها؛ فيمكن أن يساعد ذلك في الحفاظ على التوازن وتقديم مثال إيجابي للطفل أي تقليل وقت ولي الأمر على الإنترنت لنمذجة السلوك الإيجابي.

- إيقاف تشغيل الإشعارات لتطبيقات الوسائط الاجتماعية للمساعدة في تقليل التشتت.

- تضمين الأنشطة "غير المتصلة بالإنترنت" في روتين المنزل - يمكن أن يشمل ذلك، ممارسة الرياضة أو وقت القراءة أو ألعاب الطاولة

– الاتفاق على إستراتيجيات لمساعدة الأبناء على إيقاف التشغيل؛ على سبيل المثال: جهاز توقيت يرسل إشارات تفيد بأن وقت اللعبة أوشك على الانتهاء، مع وجود عواقب لعدم إيقافها. .(UNICEF, 2020, 3–11)

(ب) المبادئ التوجيهية الدولية لإدارة مخاطر التنمر الإلكتروني:

– فهم واحترام حقوقنا وحقوق الآخرين، وفهم المسئوليات في البيئة الرقمية، وتعلم التواصل باحترام.

–دور المتفرجين "حفظ الأدلة، والتحدث، والبقاء داعمين، والتحقق من الحادثة، والإبلاغ عنها، وعدم الوقوف مكتوفي الأيدي، حيث أنه من الممكن أن يكون هو الضحية التالية.(Walsh, Wallace, Ayling & Sondergeld, 2020, 35)

–تحدث الوالد إلى الطفل عن التنمر عبر الإنترنت قبل حدوثه، وطمأنتهم بأنه سيكون متواجدًا لتقديمه الدعم له.

–جمع أدلة على مواد التسلط عبر الإنترنت مثل لقطات الشاشة.

–حظر المستخدم المخالف.

– ضرورة نصيحة الطفل بعدم الرد على رسائل التنمر لأن هذا يمكن أن يؤجج الموقف.(UNICEF, 2020, 3–11)

– ضبط إعدادات الطفل على أن يتم إعلامه قبل أن يتمكن أي شخص من الإشارة إليه علىfacebook .

– الاحتفاظ بتسجيلات المكالمات والبريد الصوتي وتوثيق وتقرير الحوادث.

– جمع وحفظ أي دليل من مواقع التواصل الاجتماعي قبل طلب إزالته. ,AVA, 2020) 15)

–إبلاغ المسؤول عن الموقع بأي هجوم يمكن اعتباره تنمرًا، وتزويد المسؤول بالمعلومات الضرورية لمنع حدوث التنمر المحتمل في المستقبل داخل نفس المنصة. ,Wilbon (2020, 44)

– ألا ينزعج إذا غادر الآخرون مجموعته، فلا يريد الجميع نفس المعلومات.

–أن يُعَذِّر نفسه بأدب قبل مغادرة أي مجموعة.

-ألا ينشر في أي مجموعة دردشة بين الساعة ٢٠:٠٠ والساعة ٠٨:٠٠ ما لم تكن حالة طارئة.(Crawford International School, 2018, 8)

(ج) المبادئ التوجيهية الدولية لإدارة مخاطر الإباحية بشكل استباقي:

-توفير الأدوات للآباء والأطفال لتقييد المحتوى غير المرغوب فيه (وفقًا للمعايير الخاصة بالمجتمع) (Blum-Ross, Donoso, Dinh, Mascheroni, O'Neill, Riesmeyer, & Stoilova, 2018, 41)

-أن يثير الوالدان موضوع المواد الإباحية بأنفسهم ؛ فيوصي خبراء التربية ببدء المحادثة مبكرًا (بحلول الوقت الذي يبلغون فيه حوالي ٩ سنوات) للمساعدة في حمايتهم من التأثيرات المحتملة لمواجهته بطريق الخطأ، ويختلف كل طفل عن الآخر، لذا على الوالدين أن يقررا متى يعتقدان أنه من الصواب عرض الموضوع مع طفلهما.

-تمكين الأطفال ومساعدتهم على اتخاذ قرارات حكيمة من أجل أنفسهم، بدلاً من إخبارهم بما يجب عليهم فعله، مع محاولة توفير استراتيجيات لهم للتعامل مع التجارب السلبية عبر الإنترنت التي ستَبني لهم الثقة والمرونة.

- استخدام الأجهزة في المناطق المفتوحة من المنزل - يمكن أن يساعد ذلك في الإدارة، والوعي بالأشخاص الذين يتفاعل معهم الطفل عبر الإنترنت من خلال الهواتف والأجهزة اللوحية والألعاب والأجهزة الأخرى المتصلة.

-استخدام ميزة قفل رمز PIN على أجهزة التلفزيون الذكية، مع استخدام تدابير الرقابة الأبوية على وحدات تحكم الألعاب من خلال تنزيل أو شراء عناصر تحكم أو فلاتر أمان العائلة.(UNICEF, 2020, 3-11)

-يجب أن توضع أداة التشغيل في مكان مشترك. (Widiputera, Satria, Perdana, Zamjani & 2021, 38) تحت إشراف أحد الوالدين؛ ويجب أن يكون المكان الذي يستخدم فيه الطفل الإنترنت حيث يمكن للوالد رؤيته؛ فلا ينبغي ترك الطفل غير مراقب ووحيد على الإنترنت. (Payne, 2016, 17)

كما يجب أن يعي الآباء تصنيف الألعاب الإلكترونية الذي يشمل: E(Everyone)، T(For Teen)، M (FOR Mature) ، AO (Adult Only) (حجازي، ٢٠١٨، ٤١)

-أن يقوم الآباء بدورهم نحو بناء شخصية الطفل القادر على الاختيار الجيد للمضامين التي يتعرض لها عبر الانترنت، ومناقشته في اختياراته، بل توجيهه إذا استلزم الأمر.

-تنمية الوعي الديني والعمل على زيادة الوازع القيمي والضمير للعمل كأسلوب توجُّه داخلي للفرد لمنع الوقوع في الآثام.

-تخصيص ساعة أسبوعياً تلتقي فيا الأسرة حول مائدة النقاش، وتبادل الرأي حول ما تم التعرض له من خلال مختلف الوسائل الاتصالية.

-يمكن للآباء الذين يجيدون استخدام التكنولوجيا الرقمية أن يساهموا في توعية باقي الآباء، ويمكن أيضاً أن يكونوا بمثابة جماعات ضغط تقوم بدورها في نشر الوعي بين الصغار والكبار بأهمية سد الفجوة الرقمية ومخاطرها. (العصيمي، ٢٠٠٤، ١١١)

(د) المبادئ التوجيهية الدولية لإدارة مخاطر الاستمالة بشكل استباقي:

-تعليم التلاميذ الاستخدام المسؤول وكيفية حماية بياناتهم الشخصية، وتشمل المعلومات الشخصية: الاسم الأول والأخير، رقم الهاتف، رقم الضمان الاجتماعي أو ما يعادله، أرقام الهوية المحلية (البطاقات)، عنوان المنزل واسم الشارع أو المدينة، معلومات تحديد الموقع الجغرافي، أسماء الحيوانات الأليفة والأصدقاء وأفراد الأسرة والمدرسة، صورة أو فيديو أو ملف صوتي يحتوي على صورة الطفل أو صوته، معلومات الاتصال عبر الإنترنت أو الشاشة أو اسم المستخدم .(Unicef, 2016, 44)

-من الجيد عدم استخدام الاسم الحقيقي للطفل في مستخدم البريد الإلكتروني الخاص به؛ فالحد من عرض المعلومات هو -إلى حد بعيد- الأمر الأكثر أهمية؛ فالمعلومات سلعة؛ علاوة على الحذر عند تحميل الصور على المواقع؛ فعلاوة على أنه بمجرد مشاركة الصورة، يكاد يكون من المستحيل استعادتها أو التحكم فيها، بل ويتم توزيعها بشكل أكبر؛ علاوة على أن الصورة تساوي ألف كلمة لأي شخص مفترس عبر الإنترنت، إذا رفع الطفل صورة لنفسه واقفًا أمام منزله، مرتديًا قميص فريق المدرسة، فإن المجرم أو المفترس يمكنه العثور على ثروة من المعلومات، ما يظهر في الصورة قد تُظهر رقم الشارع والمنزل فتكشف الموقع،وقد تكشف أيضاً الوضع الاقتصادي، والمدرسة، والعمر والمظهر، كما أن لغة الجسد يمكن أن تكشف عن

الضعف العاطفي، وقد يتضح من الصورة جوانب من موقع المنزل التي تجعله سهل الاقتحام.(Muir, 2010, 7, 15, 17)

– قد لا يكون الآخرون كما يدَّعون: من المهم معرفة أن المجرمين يمكنهم إنشاء مواقع ويب زائفة بحيث تبدو شرعية، ويبدو هؤلاء الأشخاص أنهم موجودون في مجتمع الطفل، تساعد جرعةٌ صحية من الشك معظمَ الناس في التعامل مع هذه التمثيلات الزائفة، ببساطة باستخدام الحس السليم الذي يلعب دوره ؛ فمن تزييفات الحوار عبر الانترنت أنه يجعل كل الرجال أصغر من ٢٥ سنة، وجميع الأطفال مبدعين وأكبر من أعمارهم الحقيقية بسنوات. (العصيمي، ٢٠٠٤، ١٢١)

– ينبغي العلم بأن للأشخاص المفترسين أساليب معينة يستخدمونها مرارًا وتكرارًا؛ فبمجرد فهم الوالدين والطفل لتلك المخاطر المحتملة والسلوكيات والتقنيات، وتغطية كيفية اكتشاف التكتيكات، يمكن إحباط الهجمات الجنسية، وبقاء الطفل آمنًا عبر الإنترنت. (Muir, 2010, 14–15, 23)

– تعزيز الثقة بالنفس وأنه لا بأس من قول "لا".

– حذف الطلبات من الغرباء وتشجيع الطفل على حذف الصديق الذي لا يعرفه.

–من المهم التحدث مع الطفل حول العواقب المحتملة لإرسال أو مشاركة صور عارية، و**تشمل هذه المخاطر:**

- فقدان السيطرة على الصورة، حتى في العلاقات الموثوقة.
- ضغط الأقران وعدم الاحترام إذا تم إجبارهم أو الضغط عليهم لإرسال الصور أو مقاطع الفيديو بشكل صريح.
- الأذى النفسي والعاطفي، بما في ذلك الإذلال والتنمر والمضايقة أو الإضرار بسمعتهم.
- التهم الجنائية أو العقوبات في بعض القضايا – على وجه الخصوص– تشمل المشاركة في الصور الحميمة بالتراضي.(UNICEF, 2020, 3–11)
- زيادة متابعة الأسرة لأبنائها في تعاملهم مع الانترنت وخاصة الفتيات لسهولة وقوعهن في براثن من يملكون

الحيل البراقة والكلمات المنمقة، وغيرها من الأساليب غير الأخلاقية. (العصيمي، ٢٠٠٤، ١١١)

ز-الاستجابة للمخاطر السيبرانية من خلال اعتماد مخططات التصفية المتدرجة:

أما عن الموقف الياباني من برامج تصفية الإنترنت هو أن تصفية المحتوى مسألة اختيار شخصي (Lim, 2012, 6-7) فتعتمد على مخططات التصنيف عبر الإنترنت؛ بمعنى أنه توجد إرشادات للوالدين من أجل تصنيف البرامج من حيث المحتوى الجنسي الصريح والعنف التصويري والألفاظ النابية القوية واللغة الفظة في مجال الكمبيوتر وألعاب الفيديو (ENISA, 2012, 10)؛ فكل موقع مصنف بين (٠ و٤)، ويتم تشجيع مستخدمي الإنترنت على استخدام هذه التصنيفات لتقييم مواقع الويب التي يواجهونها، ويمكن للآباء والمعلمين أيضًا استخدم هذه التصنيفات لتخصيص مستوى التصفية الذي يرغبون فيه على أجهزة الكمبيوتر الخاصة بهم، علاوة على أنه قد تم إنشاء خطوط ساخنة للأفراد للإبلاغ عن المحتوى المرفوض؛ فيتم تشجيع الجميع على لعب دور إيجابي في تطوير بيئة صحية عبر الإنترنت من خلال الإبلاغ عن المحتوى المرفوض والمشاركة في تلك المهمة المجتمعية المشتركة، كما قدمت الحكومة اليابانية برنامج ترشيح مجاني للهواتف المحمولة لمعالجتها مخاوف الوالدين منذ عام ٢٠٠٠ (Lim, 2012 7, 9, 12)

ح- الاستجابة للمخاطر السيبرانية من خلال إلزامية الأنظمة التقنية لتقليل الألعاب (على سبيل المثال، الإغلاق / حجب البرمجيات).

في الصين مُنعت وحدات تحكم الألعاب الأجنبية من البيع التجاري في الفترة من ٢٠٠٠ إلى ٢٠١٤ – مثل نظام Sony PlayStation-. وفي عام ٢٠٠٧ كانت وزارة الثقافة (MoC) مسؤولة عن تنفيذ- نظام مكافحة الإدمان للألعاب عبر الإنترنت.(OGAAS)؛ فيتطلب هذا النظام من جميع مطوري خدمات ألعاب الإنترنت جمع بيانات التحقق من العمر ومراقبة استخدام الأفراد؛ فيفرض على الأفراد الذين تقل أعمارهم عن ١٨ عامًا المنع من ممارسة ألعاب الإنترنت لأكثر من ٣ ساعات في اليوم، وإذا خالف الطفل لساعات أطول تؤدي إلى إلغاء التنشيط أو تعرض آليات المكافآت في اللعبة للخطر، وبموجب هذه اللوائح يُحظر تضمين ألعاب المقامرة أو المواد الإباحية أو

العنف أو أي محتوى يعتبر انتهاكًا للقانون، ويُحظر على اللاعبين دون السن القانونية شراء العملات الافتراضية في ألعاب الإنترنت، (Taibah, Khalifa & Alshebaiki, 2020, 5) واستثمرت الحكومة الصينية مبالغ طائلة في تطوير التدابير التكنولوجية التي تهدف إلى تقييد ساعات وصول الأطفال أقل من ١٨ عامًا إلى خدمات ألعاب الإنترنت (King, Delfabbro, Doh, Wu, Kuss, Pallesen, Mentzoni, Carragher, & Sakuma, 2018, 245-246)

ويقوم الموقع الإلكتروني الرائد في الصين (Manor) والذي تتراوح أعمار زائريه بين ٧ و ١٢ عامًا بتذكير اللاعبين بأخذ استراحة كل ٤٥ دقيقة كما يتم إغلاقه من الساعة ١٢ حتى ٦ صباحًا يوميًا تقديراً لقدرة الأطفال الضعيفة على تنظيم نشاطهم عبر الإنترنت.(Lim, 2012, 11)

ط-الاستجابة للمخاطر السيبرانية من خلال التقيد بنظام التحقق من العمر:

وفي ألمانيا تم إعلان ضرورة التقيد بنظام التحقق من العمر من قِبَل المحكمة الفيدرالية الألمانية العليا باعتباره حاجز فعال لمنع القاصرين من الوصول إلى المحتوى المقيّد بالفئة العمرية عبر الإنترنت؛ بحيث يعتمد على بطاقة الهوية أو رقم جواز السفر مقرونًا بالرمز البريدي، كما هو الأمر في بلجيكا فقد تم استخدام بطاقة هوية الأطفال من سن السادسة لتحديد الهوية كأداة للتحقق من العمر عبر الإنترنت باستخدام رمز رقم التعريف الشخصي PIN؛ فيُمَكِّن الأطفال من تعريف أنفسهم على الإنترنت باستخدام بطاقة هوية الأطفال الخاصة بهم. (Macenaite & Kosta, 2017, 190)

ولجأت الصين أيضاً إلى وضع أدوات تقييد العمر والحجب، وجعلها أكثر قوة؛ بحيث يُشترط موافقة الكبار. (Blum-Ross, Donoso, Dinh, Mascheroni, O'Neill, Riesmeyer, & Stoilova, 2018, 41)

ي- استعانة المدارس الابتدائية بمنظمات المجتمع المدني لإدارة المخاطر السيبرانية بها:

لمنظمات المجتمع الدولي دور مهم في **محو الأمية الرقمية**؛ وهي عملية يصبح فيها المتلقي قادرًا على العثور على المعلومات وفهمها وتقييمها وتطبيقها بأشكال مختلفة على حل المشكلات الشخصية أو المهنية أو المجتمعية أو الإقليمية أو الاجتماعية أو

حتى العالمية، وتبني نوع خاص من التفكير، بما يسمح للمستخدمين بالعمل بشكل حدسي في البيئات الرقمية (Milenkova & Lendzhova, 2021, 3).

لذا عملت الحكومة الاسكتلندية مع مؤسسة ماري كولينز البريطانية لتجريبها الوحدة التدريبية "النقرة CLICK: الطريق إلى الحماية" في اسكتلندا، وكانت تستهدف جميع المهنيين المكلفين بحماية الأطفال الذين تعرضوا للاعتداء والاستغلال الجنسي عبر الإنترنت، وعملت الحكومة الاسكتلندية مع جامعة إدنبرة البريطانية، ومؤسسة (أوقفه الآن !) في إجراء بحث عن رادع مشاهدة الصور غير اللائقة للأطفال على الإنترنت، وتعاونت الحكومة الاسكتلندية مع حكومة المملكة المتحدة أثناء تطويرها أحكام التحقق من العمر ضمن مشروع قانون الاقتصاد الرقمي؛ للترويج ليوم الإنترنت الآمن في اسكتلندا.(Education Scotland, 2017, 11).

وعملت الحكومة الاسكتلندية ومؤسسة (التربية الاسكتلندية) لتعزيز وتحديث أداة 360 degree safe tool ٣٦٠ درجة؛ لاستخدامها في التقييم الذاتي للمخاطر السيبرانية، وتم عقد ورشة عمل في فبراير ٢٠١٧ مع المفوضين الشباب حول الحقوق الرقمية بما في ذلك مخاطر وفوائد أن تكون متصلاً بالإنترنت. (Education Scotland, 2017, 8, 10)

وكذا اشتركت منظمات المجتمع المدني الكبرى مثل منظمة Sense Media Common –وسائل إعلام الحس السليم– وهي منظمة غير ربحية أمريكية توفر التعليم والتأييد للعائلات تعزيزاً للتكنولوجيا والوسائط الآمنة للأطفال–؛ فطورت دروسًا حول المواطنة الرقمية، ليتكون منهج المواطنة الرقمية الخاص بهم من أكثر من ٧٠ درسًا للتلاميذ من الروضة إلى الصف ١٢، علاوة على أنها تهدف لتزويد المعلمين بموضوعات السلامة السيبرانية (Malecki, 2018, 5) فيتناول ذلك المنهج الدراسي ثماني فئات هي: أمان الإنترنت، الخصوصية والأمان، العلاقات والتواصل، التنمر عبر الإنترنت، البصمة الرقمية والسمعة، الصورة الذاتية والهوية، المعرفة المعلوماتية، والائتمان الإبداعي وحقوق التأليف والنشر؛ بإجمالي خمسة عشر درسًا لكل مستوى صف من K–8th الصف الثامن؛ هناك عشرون درسًا للصفوف الثانوية ٩–١٢، كل درس

يستخدم في التدريس إما واحدة أو أكثر من الفئات الرئيسة الثمانية، ويُرَاعى في تنظيم الوحدات ملاءمة العمر .(Zepf & Arthur, 2013, 13–14, 41)

ويعد برنامج محو الأمية الرقمية خطوة مهمة في معالجة الفجوة ما بين الفرص والمخاطر السيبرانية؛ فيقدَّم البرنامج بالتوازي مع المنهج الدراسي الذي يطلق عليه "العلاقات المحدثة والتربية الجنسية". (Joynes, Rossignoli & Amonoo–Kuofi, 2019, 14–15)

وحتى عام ٢٠١٣، كانت محاولات دمج أمن معلومات الحاسب الآلي ومبادئها في التعليم الابتدائي ضئيلة للغاية، ثم اتبعت العديد من الدول خطى مؤسسة (المبادرات الوطنية لتعليم الأمن السيبراني) National Initiative for Cybersecurity Education (NICE) الأمريكية، وبدأت في إنشاء مناهجهم الخاصة بأمن الكمبيوتر؛ بهدف دمجها في مدارس المرحلة الابتدائية والثانوية، ومن أشهر الجهود المجتمعية في هذا المجال i–SAFE برنامج (أنا آمن) وهو برنامج تعليمي للسلامة الإلكترونية تم إنشاؤه لتقديمه للمدارس والمناطق التعليمية بمواد المناهج ومجموعة متنوعة من منصات التعلم، ويوفر هذا المنهج أدوات التدريس التي تهدف إلى تزويد التلاميذ بالتفكير النقدي ومهارات اتخاذ القرار التي يحتاجون إليها ليكونوا مواطنين سيبرانيين، وقد دربت أكثر من ٣٤ مليون طفل على الأمن السيبراني، وتغطي المناهج الدراسية نطاقاً واسعاً لأطفال مدارس المرحلة ما قبل الابتدائية إلى الثانوية .(Zepf & Arthur, 2013, 2, 4, 17)

كما تم إنشاء برنامج CyberCitz في ولاية فرجينيا بالولايات المتحدة الأمريكية من قبل جامعة جيمس ماديسون–وهي إحدى جامعات الأبحاث العامة في هاريسونبورغ، فرجينيا –؛ بهدف مساعدة المعلمين في دمج التدريب على الأمن السيبراني والمعايير الأخلاقية في المناهج الحالية؛ فيعزز استخدامهم للويب بشكل أكثر حكمة ومسؤولية، ويركز على موضوعات مثل الشبكات الاجتماعية والألعاب السيبرانية، كما أنشأ التحالف الوطني للأمن السيبراني في الولايات المتحدة منظمة StaySafeOnline المكرسة للتثقيف السيبراني وبالتالي تمكين المجتمع الرقمي من استخدام الإنترنت بأمان في المنزل والعمل والمدرسة، .(Zepf & Arthur, 2013, 15, 20)

وتعمل مؤسسة تكنولوجيا المعلومات للتعليم (HITSA) في إستونيا كمصدر أساسي للتدريب وحملات توعية في إستونيا، وتبدأ برامجها التدريبية للأطفال في سن ما قبل المدرسة، علاوة على البرامج التعليمية المقامة على مستوى المدارس الابتدائية والمتوسطة والكليات(Lewis, Porrúa, Catalina & Díaz, 2016, 15). وتوجد مبادرة عالمية تشجع بقوة جميع الدول على تبنيها وهي الاعتراف بشهر أكتوبر باعتباره شهر التوعية بالأمن السيبراني. (Cybersecurity Tech Accord, 2020, 1)

خامساً- تتبع المخاطر وتحديث إدارتها.

أ-تعديل أساليب إدارة المخاطر السيبرانية وفقا لمخرجات تطبيقها.

فبعد سنوات من محاولة كندا حظر الهواتف المحمولة في المدارس، تحاول العديد من المدارس الآن استخدامها في العمل في الفصل، وتَرَاجَعَ أكبر مجلس مدرسة في كندا عن حظر الهواتف بعد أربع سنوات، والآن يُسمح للمعلمين بإملاء أفضل ما يناسب فصولهم الدراسية.(Quaglio & Millar, 2020, 28)

ب- تعديل أساليب إدارة المخاطر السيبرانية استجابة للمتغيرات المجتمعية.

وفي الصين قد لقي نظام الرقابة -الملقب بـ السد الأخضر -الذي استخدموه في إدارة المخاطر السيبرانية - إدانة واسعة النطاق من المستخدمين، وتم بالفعل سحبه قبل منتصف عام ٢٠٠٩. (Faris & Zittrain, 2009, 92) حيث أظهرت نتائج الاستطلاعات التي أجريت على مواقع رائدة في الصين أن أكثر من ٨٠٪ من الناس رفضوا التثبيت، وأن مشروع السد الأخضر كان فاشلاً بوجود عيوب وثغرات في تصميمه؛ فكانت وسائل التقنية للتحايل على السد الأخضر GFW وفيرة؛ فقد تم كسر الملايين من جدران الرقابة بشكل يومي؛ فهم بارعون في الالتفاف عليه، علاوة على أن هذا القيد يتم تطبيقه-فقط-عندما يقوم المستخدمون بتوصيل أجهزتهم عبر الإنترنت، أما الأجهزة غير المتصلة بالانترنت فلا يتمكن البرنامج من مراقبة أنشطتها (Zhao, 2016, 80, 82)، كما تم انتقاد تلك السياسات الصينية للتصفية باعتبارها سياسات ذات دوافع سياسية ومعادية للديمقراطية، وتم إلغاء هذا المشروع في أغسطس من ذات العام ٢٠٠٩ بسبب احتجاج شعبي قوي ليصبح برنامج التصفية في النهاية مطلوباً فقط

لأجهزة الكمبيوتر في المدارس ومقاهي الإنترنت؛ فتصفية الإنترنت على مستوى البوابة أو في الطبقة العليا تتكبد تكاليف أقل بكثير؛ ومن الواضح أنها أكثر فعالية من مبادرة السد الأخضر الفاشلة. (Lim, 2012, 6) وكانت إحدى المحاولات الرئيسة في أوائل عام ٢٠١١ قيام اللجنة المركزية الشيوعية الصينية لرابطة الشباب في بكين بالتعاون مع تشاينا موبايل لتصميم منصة الوصول إلى الإنترنت عبر الهاتف المحمول على الصعيد الوطني للقُصَّر (Ning, 2011, 37) بالوصول إلى قائمة بيضاء بمواقع الويب المحددة والمعتمدة مسبقًا فكانت جاهزة للاستخدام عند عودة الأطفال إلى المدرسة بعد العطلة الصيفية في عام ٢٠١١(Ning, 2011, 38) ، كما جربت الصين أيضًا معسكرات لعلاج إدمان الانترنت تقدم أكثر من ٢٠٠ منظمة، بعضها ممول من الحكومة، كما تجبر الأطفال على الانخراط في الأنشطة البدنية.(Lim, 2012, 11)

ويتضح لنا من تحليل ما سبق أن الإساءة الرقمية أضحت شكلاً جديداً من أشكال إساءة معاملة التلاميذ، تخالف مبادئ اتفاقية حقوق الطفل على أن حماية الطفل ومصالحه لها الأولوية، بما في ذلك الحق في الحماية و"الترفيه الآمن"، لذا كانت هناك نداءات متزايدة من صانعي السياسات والأكاديميين لتغيير حقوق الأطفال، لتلبية الاحتياجات الرقمية للعمر ولاسيما الحق في الإتاحة والمشاركة بعد إذن الوالدين. ودفعنا ذلك إلى تناول الممارسات الدولية الخاصة بإدارة المخاطر السيبرانية بإجراءاتها المتميزة حتى نتمكن من استعارة ما يناسبنا منها؛ الأمر الذي يتطلب النزول للميدان للكشف عن واقع إدارة المخاطر السيبرانية في المدارس الابتدائية، ومعرفة أوجه القصور والقوة والإجراءات التي تحتاج لدعمها بالمزيد من الممارسات الدولية، وهذا ما سيتناوله المحور التالي.

المحور الرابع: واقع ادارة المخاطر السيبرانية في المدارس الابتدائية بمصر (بورسعيد أنموذجاً)

ومن خلال الاطلاع على بعض الأدبيات التربوية المعاصرة حول المخاطر السيبرانية وإدارتها، اتضحت معالم الدراسة الميدانية، فقد دعت الحاجة إلى رصد الواقع مؤسساً على إجراءات منهجية، وقبل عرض إجراءات الدراسة الميدانية التي تم القيام بها،

نوضح التحليل النظري لواقع إدارة المخاطر السيبرانية بمصر، ويمكن تناول ذلك في سياق ما يلي:

أولاً: الواقع النظري لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر (وفقاً للأدبيات والتقارير العالمية).

أ–واقع استخدام الانترنت في مصر:

يرتفع عدد مستخدمي الإنترنت في مصر باستمرار فزاد بمقدار ٤.٥ مليون (+٨.١٪) في عامٍ واحد بين عاميّ ٢٠٢٠ و٢٠٢١، وبلغ معدل انتشار الإنترنت في مصر ٥٧.٣٪ من جملة السكان في يناير ٢٠٢١، كما ارتفع عدد مستخدمي وسائل التواصل الاجتماعي في مصر في يناير ٢٠٢١ ليبلغ ٤٩ مليون نسمة؛ فارتفع عددهم بمقدار ٧ مليون (+١٧٪) بين عاميّ ٢٠٢٠ و ٢٠٢١.(Kemp, 2021b, 17–18) .

أفادت إحصائيات Google Trends عام ٢٠٠٨ أن مصر احتلت المركز الثاني عالمياً في البحث عن كلمة جنس، واحتلت المركز الرابع في البحث عن كلمة لواط. كما أفادت إحدى الدراسات التي أجريت عام ٢٠٠٩ على عينة مكونة من ٣٩٦ من تلاميذ المدارس الثانوية بمدينتيّ المنيا والقاهرة أن ٤١.٩٪ يتعرضون للمواقع الإباحية أحياناً، و٥٣٪ يتعرضون لها دائماً، وقد نوه تقرير إخباري أوردته جريدة "ميل أند جارديان" البريطانية تحت عنوان : المتحرشون الجنسيون يجوبون شوارع مصر، بتنامي ظاهرة التحرش الجنسي بالنساء؛ فتحول لسرطان اجتماعي يهدد كيان المجتمع المصري؛ استنادا لما رصده تقرير المركز المصري لحقوق المرأة، وقد اعترف أحد المتهمين في قضية هتك عرض الأطفال بالقوة في مصر أنه اعتاد وأدمن مشاهدة الأفلام الإباحية مما دفعه نحو ارتكاب مثل هذه الجرائم.(مرعي، ٢٠١٣، ١٨٦، ٢١٣)

وعليه قام مجموعة من طلاب جامعة الإسكندرية بحملة لمقاطعة المواقع والقنوات الإباحية باعتبارها تهدد الأمن القومي المصري تحت شعار "اوع تميل"، وطالب الشباب بضرورة تضافر جهود الدولة ومنظمات المجتمع المدني لحجب هذه المواقع، وإجراء تشريع لمقاضاة شركات الاستضافة، وتعقب المستخدمين وتقديمهم للمحاكمة، كما قدمت شركة TEDATA (إحدى الشركات مزودة خدمة Family Internet المعتمدة

على نظام الفلاتر filter باشتراك رمزي؛ لحجب ومنع المواقع المنافية للأخلاق بهدف حماية الأطفال والمراهقين والشباب(مرعي، ٢٠١٣، ٣٠٧-٣١١)

ب-جهود الدولة في إدارة المخاطر السيبرانية بها.

تحرص وزارتا التربية والتعليم والاتصالات وتكنولوجيا المعلومات في مصر على توفير عنصر الأمان لمستخدمي شبكة الانترنت في مصر من الأطفال والشباب؛ ومن ثم فقد اتخذت الوزارتان العديد من الخطوات الملموسة لردع المجرمين عن استغلال الأطفال عبر الانترنت. ويمكن عرض بعض هذه الجهود فيما يلي:

١-الجهود التشريعية:

اهتم دستور ٢٠١٤ في مادته رقم ٢٥ بتأكيد التزام الدولة بوضع خطة شاملة للقضاء على الأمية الرقمية بين المواطنين في جميع الأعمار، وتلتزم بوضع آليات تنفيذها بمشاركة مؤسسات المجتمع المدني، وذلك وفق خطة زمنية محددة. (جمهورية مصر العربية، وزارة التربية والتعليم، ٢٠١٤، الخطة الإستراتيجية للتعليم قبل الجامعي ٢٠١٤-٢٠٣٠، ١٤)

كما يوجد في مصر جهود حثيثة ومستمرة لمكافحة الإباحية؛ فقد نصت المادة ١٧٨ بالعقوبات الخاصة بانتهاك حرمة الآداب العامة بعد تعديلها بالقانون رقم ١٤٧ لسنة ٢٠٠٦ المادة الثالثة على أنه " يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن خمسة ألاف جنيه ولا تزيد على عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من نشر أو صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو مخطوطات أو رسومات أو إعلانات أو صورًا محفورة أو منقوشة أو رسوما يدوية أو فوتوغرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عامة إذا كانت خادشة للحياء العام". (جمهورية مصر العربية، رئاسة الجمهورية، ١٥ يولية ٢٠٠٦، ١١)

كما نصت المادة ١١٦ مكرر (أ) من قانون الطفل المصري رقم ١٢ لسنة ١٩٩٢ المعدل بالقانون ١٢٦ لسنة ٢٠٠٨المتعلقة بجرائم الحاسب الآلي والانترنت" يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن عشرة الأف جنية ولا تجاوز خمسين ألف جنيه كل من أستورد أو صدر أو أنتج أو أعد أو عرض أو طبع أو روج

أو حاز أو بث أي أعمال إباحية يشارك فيها أطفال أو تتعلق بالاستغلال الجنسي للطفل ، ويحكم بمصادرة الأدوات والآلات المستخدمة في ارتكاب الجريمة والأموال المتحصلة منها ، وغلق الأماكن محل ارتكابها ، مدة لا تقل عن ستة أشهر وذلك كله مع عدم الإخلال بحقوق الغير الحسن النية. ومع عدم الإخلال بأي عقوبة أشد ينص عليها في قانون آخر، يعاقب بذات العقوبة كل من :

(أ) استخدم الحاسب الآلي أو الانترنت أو شبكات المعلومات أو الرسوم المتحركة لأعداد أو لحفظ أو لمعالجة أو لعرض أو لطباعة أو لنشر أو لترويج أنشطة أو أعمال إباحية تتعلق بتحريض الأطفال أو استغلالهم في الدعارة والأعمال الإباحية أو التشهير بهم أو بيعهم .

(ب) استخدم الحاسب الآلي أو الانترنت أو شبكات المعلومات أو الرسوم المتحركة لتحريض الأطفال علي الانحراف أو لتسخيرهم في ارتكاب جريمة أو علي القيام بأنشطة أو أعمال غير مشروعة أو منافية للأداب ، ولو لم تقع الجريمة فعلاً. (عبدالعزيز، ٢٠١٦، ٤٩٩)

٢-الجهود التنفيذية:

وضعت وزارة التربية والتعليم في خطتها الأخيرة أحد الأهداف الإستراتيجية الخاصة بموضوع الدراسة وهو بناء تشريعات تختص بتنظيم مصادر جمع وتدقيق ومعالجة ونشر المعلومات، وتدعيم الثقافة والقيم المعلوماتية بقطاع التعليم قبل الجامعي. ومن الاستراتيجيات الحاكمة والموجهة لأنشطة الخطة الاستراتيجية للتعليم في مصر تنمية قدرات التلاميذ على التعامل مع التقنية في إطار قيمي ينمي شخصية الطفل في جوانبها كافة، وإكساب المتعلم كفايات اكتساب قيم المواطنة الرقمية. (جمهورية مصر العربية، وزارة التربية والتعليم، ٢٠١٤، الخطة الإستراتيجية للتعليم قبل الجامعي ٢٠١٤-٢٠٣٠، ٧٠، ٩٤)

كما يسعى قطاع الاتصالات وتكنولوجيا المعلومات إلى تعزيز مبادئ المواطنة الرقمية في مصر، والتعريف بحقوق ومسئوليات المواطن في المجتمع الافتراضي فكانت رؤيته" نحو مواطنة رقمية عادلة، واقتصاد معرفي متطور في ظل التحول الديمقراطي"، ومن الأهداف الاستراتيجية له تعزيز المواطنة الرقمية ومجتمع المعلومات وبرنامج أمان

الأسرة على الانترنت، وبرنامج تعزيز القدرات البشرية القومية ومحو الأمية الإلكترونية.(جمهورية مصر العربية، وزارة الاتصالات وتكنولوجيا المعلومات، يونيو ٢٠١٢ ، ٦، ١٠) بل كانت أحد المحاور الاستراتيجية الرئيسة للإستراتيجية القومية للاتصالات الأخيرة: تفعيل المواطنة الرقمية، وركزت الخطة على مجال أمان الطفل والأسرة على الانترنت **واستهدفت فيه:** (جمهورية مصر العربية، وزارة الاتصالات وتكنولوجيا المعلومات، يونيو ٢٠١٢ ، ٦٣)

-تطوير المحتوى الخاص بالاسخدام الآمن للانترنت مع إيلاء اهتمام خاص بالسياسات والبرامج الموجهة للأطفال.

-تطوير مناهج الاستخدام الآمن للانترنت بما يتماشى مع التطورات الحادثة في عالم الاتصالات وتكنولوجيا المعلومات.

-التوسع في إتاحة تطبيقات نظم الحماية التكنولوجية على الانترنت والموبايل لاختيار الفرد والأسرة.

-الاهتمام بالأبحاث والدراسات الخاصة بحماية الأسرة عبر الانترنت.

-تعزيز فرص التعاون الدولي من أجل خدمة محور الحماية على الانترنت في مصر.

-تعزيز فرص التعاون العربي باتخاذ خطوات فعلية على طريق تنفيذ مشروع حماية النشء العربي على الانترنت، وتوقيع مذكرات تفاهم مع الدول العربية لتعزيز التعاون وتبادل الخبرات في مجال الحماية على الانترنت.

-تشجيع مقدمي الخدمة وشركات المحمول على تبني حملات رفع الوعي وإتاحة آليات الحماية.

كما استهدف برنامج الأمن السيبراني حمايةَ الهوية الرقمية وتأهيل الكوادر البشرية وتوفير الخبرات مع التعاون مع الدول الصديقة والمنظمات الدولية ذات الصلة؛ لتبادل الخبرات في مجال الأمن السيبراني ومكافحة الجرائم السيبرانية (جمهورية مصر العربية، وزارة الاتصالات وتكنولوجيا المعلومات، يونيو ٢٠١٢ ، ٥٥) وقد بلغ عدد الخريجين الحاصلين على تدريب على البرمجيات من قبل هيئة تنمية صناعة تكنولوجيا المعلومات حتى مارس ٢٠٢١ ٢٩.٩٣ ألف متدرب.(MCIT, 2021, 1-11)

كذا تم تأسيس اللجنة الوطنية المعنية بالاستخدام الآمن للأطفال عام ٢٠١٣ يهدف توحيد وتنسيق الجهود المبذولة في هذا الموضوع، وتوفير عنصر الأمان في عالم الانترنت، فضلاً عن وقايتهم من المخاطر المرتبطة بعالم الانترنت، وفي هذا الإطار أنشئت شبكات البيانات وجرائم الانترنت داخل الإدارة العامة للمعلومات والتوثيق التابعة لوزارة الداخلية؛ وقد شرعت الإدارة في ابتكار عدة طرق للإبلاغ عن الجريمة السيبرانية، ولعل أكثر هذه الطرق فعالية هو الخط الساخن ١٠٨، كما قامت وزارة التربية والتعليم بإنشاء "المجموعة المعنية بأن المعلمين على الانترنت" بالتعاون مع وزارة الاتصالات وتكنولوجيا المعلومات؛ إيماناً منها بأهمية إعداد معلمين ملمين بقواعد الأمان على الانترنت داخل وارة التربية والتعليم، وقد تم تدريب حوالي ٦٥٠٠ معلماً عام ٢٠١٠ بمساعدة الشركات المتخصصة في تكنولوجيا المعلومات والخبراء المحليين والدوليين. (عبدالعزيز، ٢٠١٦، ٥٠١، ٥١٣)

ج–بعض المؤشرات الدالة على قصور إدارة المخاطر السيبرانية بالمدارس الابتدائية بمصر:

١–التقارير العالمية. (IQ INSTITUTE Website, 2020)

يقيِّم معهد الذكاء الرقمي DQ مؤشر أمان الطفل على الإنترنت، ويصدر تقاريراً دولية؛ بهدف مراقبة التقدم العالمي في بناء المهارات الرقمية بشكل شامل في جميع أنحاء العالم، وبهدف تمكين كل فرد ومنظمة في كل دولة لتكون جاهزة رقميًا آمنة وأخلاقية، ويتم التقييم بناء على المعايير التالية:

المعيار ١–المخاطر السيبرانية.

يقيِّم ما إذا كان الأطفال يتعرضون لمخاطر الإنترنت مثل التسلط عبر الإنترنت أو جهات الاتصال المحفوفة بالمخاطر أو الاستخدام المضطرب للتكنولوجيا.

المعيار ٢–الاستخدام الرقمي المنضبط.

يقيِّم ما إذا كان الأطفال يقضون وقتًا طويلاً مع الأجهزة الإلكترونية والوسائط.

المعيار ٣–الكفاءة الرقمية.

يقيّم ما إذا كان الأطفال لديهم مهارات رقمية ، مثل التعاطف الرقمي وإدارة البصمة الرقمية ، التي تقلل من المخاطر الإلكترونية وتسمح لهم بأن يكونوا مواطنين رقميين جيدين.

المعيار ٤ –التوجيه والتعليم.

يقيّم ما إذا كان الأطفال يتلقون الدعم من خلال توجيهات مقدمي الرعاية والتعليم المدرسي حول الأمان عبر الإنترنت.

المعيار ٥ –البنية التحتية الاجتماعية.

يقيّم ما إذا كانت الحكومات والصناعات تعمل بطرق تحمي الأطفال من مخاطر الإنترنت.

المعيار ٦ –الاتصال.

يقيّم ما إذا كان يمكن للأطفال الوصول إلى الإنترنت بسرعاتٍ كافية.

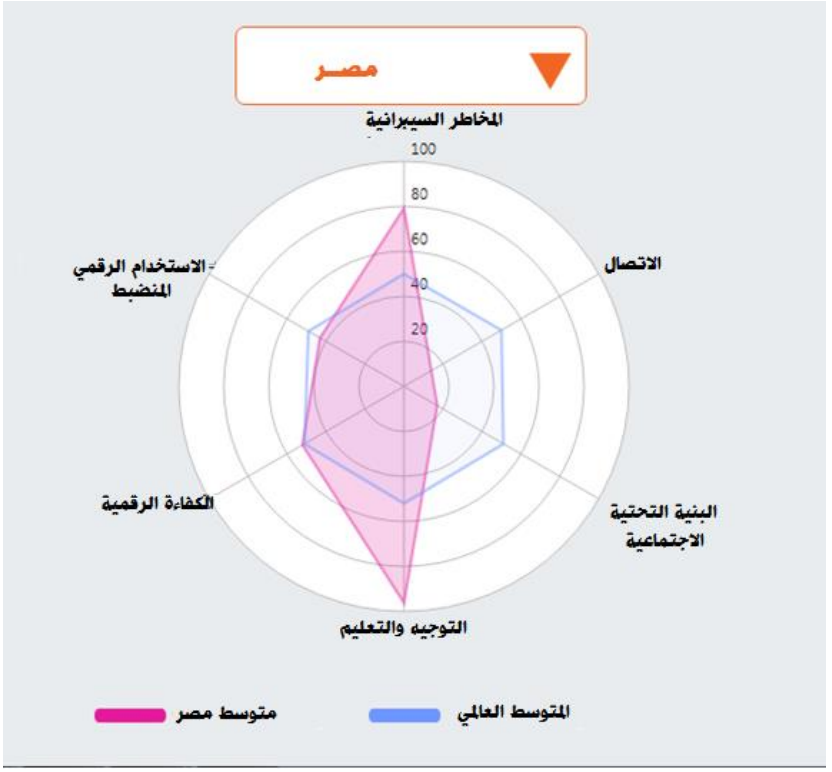
جدول (٥) التقرير الدولي عن واقع الذكاء الرقمي لمصر وفق مؤسسة الذكاء الرقمي لعام ٢٠٢٠

الملخص	الترتيب	النقاط	المتوسط العالمي للنقاط
الذكاء الرقمي الكلي	١٧	٤٠	٤٢
المخاطر السيبرانية	٧	٧٩	٥٠
الاستخدام الرقمي المنضبط	١٧	٤٣	٤٩
الكفاءة الرقمية	١٧	٥٢	٥١
التوجيه والتعليم	١	٩٦	٥٢
البنية التحتية الاجتماعية	٢٧	١٧	٥١
الاتصال	٢٦	١٤	٥٠

النتائج الرئيسية:

احتلت مصر المرتبة ١٧ من أصل ٣٠ بدرجة إجمالية ٤٠.١ – وهذا مصنف على أنه أداء متوسط؛ تتسم بأداء ضعيف في البنية التحتية الاجتماعية (١٧) وارتفاع

مستويات المخاطر السيبرانية (٧٩) – المجالات الرئيسة للتحسين هي الإطار القانوني (٢٤) ومشاركة الصناعة (٢٢) درجة عالية في التوجيه والتعليم (الأول).



شكل (٥) رسم بياني لواقع الذكاء الرقمي لأطفال مصر ٢٠٢٠ وفق مؤشر أمان الطفل على الانترنت.

المصدر: (IQ INSTITUTE Website, 2020)

٢- نتائج الدراسات السابقة عن واقع المخاطر السيبرانية وإدارتها في المدارس الابتدائية بمصر.

أما دراسة (عبد الرازق، ٢٠٢٠، ١٣٦)؛ فأشارت إلى زيادة ظاهرة التلوث الثقافي والتكنولوجي، خاصةً بعد العديد من الثورات التي انطلقت من أساليب تكنولوجية وخاصة ثورة ٢٥ يناير، وأن أكثر المضايقات التي يعاني منها التلاميذ كانت إرسال

صور غيرأخلاقية والاستيلاء على الحساب بعد اختراقه، ومحاولات للتعارف، بالإضافة إلى تفاعل الأطفال مع عدد من الأغاني والألعاب والبرامج غير المناسبة لطبيعة المرحلة السِّنية التي يمرون بها في ظل تدني وعي الأمهات والمعلمين.

كما أشارت نتائج دراسة (المسلماني، ٢٠١٤، ٦٨-٧٠) إلى انخفاض نسبة الأسر التي تضع حدوداً لاستخدام أبنائها للانترنت لتصل ٢٠٪؛ مما يمثل خطراُ على الأبناء وخصوصاً من ينقصهم الوعي بالاستخدام الصحيح، كما أكدت نتئج الدراسة ارتفاع نسبة التلاميذ الذين يستخدمون التكنولوجيا بصورة يومية، وانخفاض نسبة أولياء الأمور ممنهم على وعي باستخدام التكنولوجيا الحديثة، وانخفاض نسبة التلاميذ الذين تدربوا على استخدام التكنولوجيا بمساعدة الأسرة (٢٦.٧٪) ومن خلال المدرسة (٢٦.٧٪)، وعدم اهتمام المدارس بقضية التكنولوجيا وضرورة تدريب التلاميذ عليها، وأن نسبة كبيرة من التلاميذ (٤٦.٧٪) يعتمدون على أصدقائهم في التدريب على استخدام التكنولوجيا –وهو ما ينطوي على جانب من الخطورة فيما يتعلق بأصدقا السوء ودورهم في إفساد أقرانهم وإكسابهم سلوكيات غير أخلاقية، وأن ثلث العينة (٣٣.٣٪) تعرضوا لتهديدات من خلال البريد الإلكتروني، كما تعرض نصف العينة تقريباً (٤٦.٧٪) لسرقات من خلال الانترنت، كما توصلت الدراسة إلى نتيجة تشير إلى انخفاض دور المعلم في تدريب التلاميذ على المعايير الأخلاقية المرتبطة باستخدام التكنولوجيا استخداماً آمناً، وكيفية التحقق من مصداقية المواقع التي يتصفحونها؛ حيث تراوحت النسب ما بين ١٣.٣٪ إلى ٢٠٪، وأقر ٥٣.٣٪ من التلاميذ أنهم يستمتعون بغرف الدردشة مما يمثل خطورة في التواصل مع الغرباء، فضلاً عن ارتفاع نسبة من يلجأون إلى استخدام الرسائل الفورية أثناء الحصص الدراسية والتي بلغت ٦٦.٧٪، وأشار نحو (٦٠٪) من أفراد العينة إلى أن استخدامهم للتكنولوجيا أدى إلى انطوائهم، كما تعلم (٤٦.٧٪) منهم سلوكيات غير سليمة من خلال التكنولوجيا، كما أقر (٧٣.٣٪) أن التكنولوجيا أثرت سلباً على مذاكرة دروسهم، وهي نسبة كبيرة جدا؛ وقد يرجع هذا الخلل في كثير من جوانبه إلى ضعف إدارة المخاطر السيبرانية في المدارس الابتدائية.

وكذا أشارت دراسة (حشيش، ٢٠١٨، ٤١٠-٤١١) التي أجرتها على ١٥٠ تلميذا بالصف السادس الابتدائي بإحدى المدارس الخاصة؛ بهدف التعرف على أكثر

المواقع الإلكترونية التي يفضلون استخدامها وحجم استخدامهم للانترنت، وهل هناك من يقوم بالإشراف عليهم وتوجيههم بالمواقع الإلكترونية المناسبة لهم؛ فكانت النتائج كالآتي: أكثر المواقع التي يترددون عليها الفيسبوك ثم اليوتيوب، ٧٢٪ من عينة البحث لا يقوم أولياء أمورهم بالإشراف عليهم أثناء استخدامهم للانترنت، ٧٠٪ من عينة البحث لا يوجد هناك من يقوم بإرشادهم بالمواقع الإلكترونية المناسبة لهم مثل المعلم أو ولي الأمر، ٧٠٪ من عينة البحث يلجأون للاستعانة بأصدقائهم عندما يواجهون أية مشكلة خاصة بالكمبيوتر أو الانترنت.

كما أشارت دراسة (العصيمي، ٢٠٠٤، ١٠٨) إلى أن بعض الخبراء أكدوا أن انتشار الألعاب والبرامج التي تمثل شخصيات وهمية أو أجنبية جعلت أبناءنا لا يعرفون رموز أمتنا؛ ففي إحدى الدراسات اتضح أن ٦٨٪ من أطفال العرب أقل من ١٠ سنوات لا يعرفون صحابياً مثل خالد بن الوليد مع معرفتهم برموز الألعاب والبرامج الأجنبية.

كان من أهم نتائج دراسة (حجازي، ٢٠١٨، ١١٤، ١٤٣، ١٤٦) التي أجرتها على ٦٠ تلميذاً في للمرحلة الابتدائية تعرض الأطفال للألعاب الإلكترونية (بصفة دائمة) في المقام الأول بنسبة ٧٠.٥٪ مما يؤكد على أن التعرض للألعاب الإلكترونية أصبح سلوكاً شائعاً بين الأطفال في المجتمع المصري، وأنها تشغل حيزا كبيرا من وقت ونشاط الطفل. وعكست نتائج الدراسة التحليلية انخفاض عدد القيم الإيجابية التي تتضمنها الألعاب الإلكترونية بوجه عام، وتصدرت السمات السلبية للصورة التي يظهر بها الشخصيات الرئيسة حيث بلغ إجمالي نسبة السلبية للصورة التي يظهر بها الشخصيات الرئيسة ٥٦.٣٪؛ مما يدلل على أن مصممي الألعاب الإلكترونية لا يهتمون بالصورة التي تظهر بها الشخصيات الرئيسة، أما ما يهم مصممي الألعاب الإلكترونية هو كيف يجعلون اللعبة الإلكترونية جذابة بالنسبة لأكبر عدد من الأطفال، وتغلبت السمات السلبية على الصورة التي تظهر بها الشخصيات الرئيسة حيث جاءت فئة (أخرى بنسبة ٧٥٪ شملت سمات (سلبية– مثيرة للجنس– كاذبة)، كما جاءت سمة (مؤذية للآخرين بنسبة ٢٥٪)، لذا أوصت الباحثة بضرورة تنبه أولياء الأمور إلى طبيعة المحتوى الذي تقدمه الألعاب الإلكترونية التي يتعرض لها أطفالهم والتوجه إلى الألعاب ذات الطابع التعليمي والترفيهي

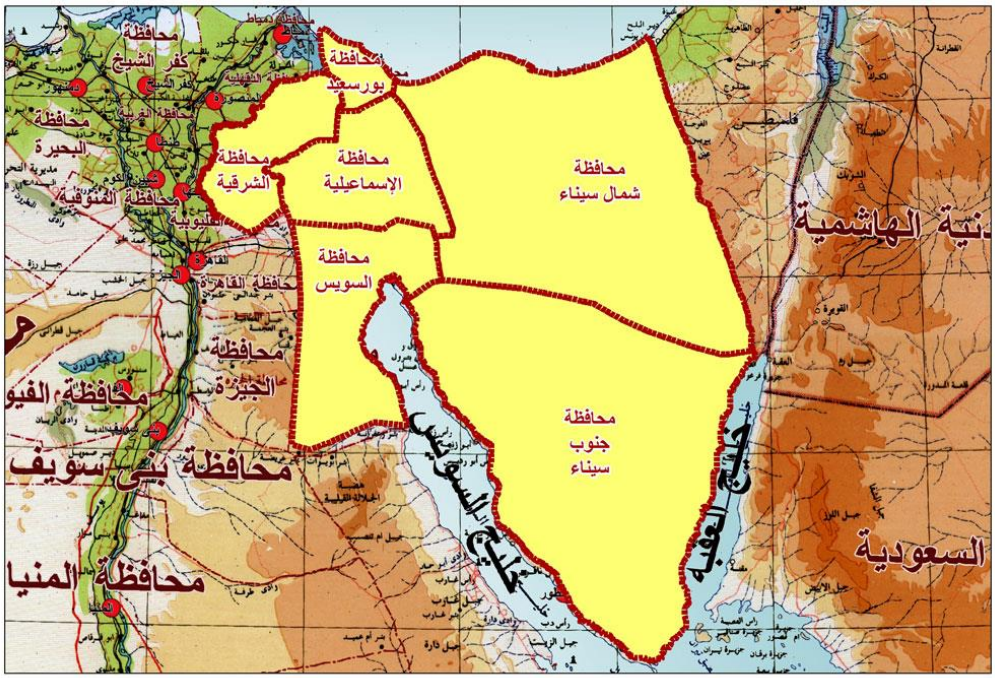
بدلا من الألعاب ذات المحتوى القتالي العدواني والذي قد يتضمن قيم وسلوكيات مخالفة لقيم المجتمع المصري.

ثانياً: الواقع الميداني لإدارة المخاطر السيبرانية في المدارس الابتدائية بمحافظة بورسعيد.

أ-نبذة عن محافظة بورسعيد.

١- السمات العامة للمحافظة:

محافظة بورسعيد هي إحدى محافظات جمهورية مصر العربية، وإحدى المحافظات الثلاث المكونة لإقليم قناة السويس بجانب كل من محافظات الإسماعيلية، السويس كما في شكل (٦)، وترجع نشأة بورسعيد إلى بداية حفر قناة السويس في ٢٥ إبريل ١٨٥٩ ، وافتتاح القناة للملاحة العالمية في نوفمبر عام ١٨٦٩، وتتمع محافظة بورسعيد بِموقع جغرافي وإستراتيجي متميز، **وبمقومات تنموية هائلة تمكنها من تحقيق التنمية الشاملة في شتى المجالات؛**



شكل (٦) موقع محافظة بورسعيد من إقليم قناة السويس.

فاحتلت بورسعيد المرتبة الأولى على مستوى الجمهورية **فى مجال التنمية الشاملة** لما تزخر به المدينة من مستوى تعليمي وثقافي وصحي مرتفع، وتقوم المحافظة بإنشاء العديد من المشروعات الخدمية فى مجالات الصرف الصحى والطرق والإسكان، وتحتل المرتبة الأولى **فى مجال الاتصال**، بالإضافة للمشروعات الزراعية والتعدينية والبترولية العملاقة فى جنوب وغرب المدينة وهى رائدة فى مجال مكافحة محو الأمية وأيضًا فى مجال الحفاظ على البيئة من التلوث لأن معظم منشآتها تدار بالغاز الطبيعي، وتسير مشروعات الرعاية الاجتماعية فى الطريق الصحيح. (محافظة بورسعيد، جهاز شئون البيئة، ٢٠٠٧، ١-٢)

ويتمتع إقليم قناة السويس ببعض الاستثمارات المركزية المتمثلة فى قناة السويس، فضلا عن توطن بعض المشروعات الكبرى بالإقليم مثل مشروع ترعة السلام لاستصلاح الأراضى، ومشروع ميناء الحاويات بشرق بورسعيد، ويوجد في المحافظة مطار بورسعيد: وهو مطار محلى تم تطويره حديثا وإنارته لاستقبال الطيران الليلي، وبه

صالتان للسفر والوصول تتسعان لعدد ٢٥٠ راكب / ساعة.(وزارة الإسكان والمرافق والتنمية العمرانية، ٢٠٠٨، ١٥،٦٢، ٦٣، ٨٦)

٢- المساحة وعدد السكان والتقسيم الإداري:

تبلغ مساحة بورسعيد ١٣٥٤ كم٢ أي ٣٢١ ألف فدان، وتمثل ١.٧ % من مساحة إقليم قناة السويس، ٠.١٣% تقريبا من مساحة مصر، وبلغ عدد السكان ٧٧٨٨٣٤ نسمة، وبذلك يمثل سكان بورسعيد ٠.٨ % من جملة سكان مصر.(جمهورية مصر العربية، وزارة التخطيط والمتابعة والإصلاح الإداري، ٢٠١٨، ٤١٤)

وتعد محافظة بورسعيد محافظة حضارية، وتضم سبعة أحياء هي: حي الزهور –حى المناخ – حى العرب– حى الضواحي – حى الشرق – حى الجنوب – حى بورفؤاد، كما يتبع كل من حي الزهور وحي الجنوب عددٌ من القرى؛ فيتبع حي الزهور القرى الآتية :الديبة – المناصرة – الجرابعة وتقع فى غرب بورسعيد (بينما يتبع حى الجنوب) بحر البقر –أم خلف – الكاب وتقع فى جنوب بورسعيد وتبلغ المساحة الكلية لمحافظة بورسعيد ١٣٥٤كم ٢ (جامعة بورسعيد، ٢٠١٧-٢٠٢٢، ٢٠١٧، ٦)

٣ – مؤشرات التنمية الأساسية الخاصة بمحافظة بورسعيد: (وزارة التخطيط والمتابعة والإصلاح الإداري، ٢٠١٥، ٩-١٣) (جمهورية مصر العربية، وزارة التخطيط والمتابعة والإصلاح الإداري، مايو ٢٠١٨، ٤١٥، ٤٤٠) (جمهورية مصر العربية، الجهاز المركزي للتعبئة والإحصاء، يناير ٢٠٢١أ، ٤)

تطرح فكرة التنمية ذاتها ضرورة القياس سواء لصياغة السياسات والخطط وتحديد الأهداف أم لتقييم النتائج، ونظراً للتحولات الواسعة في مفهوم التنمية؛ فإن المؤشرات عرفت بدورها تطورات مهمة على محاور عدة بدءاً من مقاييس النمو الاقتصادي إلى المؤشرات الاجتماعية كدليل للتنمية البشرية، لذا تعرض الدراسة فيما يلي مؤشرات التنمية الأساسية العامة المتعلقة بمحافظة بورسعيد:

المؤشر	القيمة	السنة
مؤشرات السكان: – إجمالي عدد السكان. –ذكور –إناث	 ٧٧٨٨٣٤ نسمة ٣٩٩٦٩٤ نسمة ٣٧٩١٤٠ نسمة	٢٠٢١
مؤشرات العمل: – نسبة المشتغلين (١٥سنة فأكثر) بالمحافظة لإجمالي عدد المشتغلين (١٥سنة فأكثر)على مستوى الجمهورية.	٠.٨٪	٢٠١٤
– معدل البطالة ١٥ سنة فأكثر.	٢٥.٩٪	
– نسبة العاملين بالقطاع الحكومي في المحافظة لإجمالي عدد العاملين بالقطاع الحكومي بالدولة.	١٪	
مؤشرات الثقافة: – نسبة عدد قصور الثقافة بالمحافظة إلى الإجمالي على مستوى الجمهورية:	٣٪	٢٠١٣
التقسيمات المحلية والإدارية: –عدد المدن: – عدد الأحياء: – عدد أقسام الشرطة: – عدد الشياخات: – عدد إدارات شرطة الميناء:	 ١ ٦ ١١ ٢٢ ١	٢٠١٤
–نسبة الاستثمارات الحكومية (التنمية المحلية) بمحافظة بورسعيد	١٤٥ مليوناً	٢٠١٨
–مؤشرات الفقر: يعد إقليم قناة السويس أقل أقاليم مصر في	١٥٪	٢٠١٥

المؤشر	القيمة	السنة
نسبة الفقر؛ مقارنةً بجنوب الصعيد وهي الأعلى فقراً (٥٣.٤٪)		
مؤشرات نسبة الأمية:	١٤.١٪	٢٠١٧

يرتبط كون محافظة بورسعيد مدينة حضرية بزيادة في فرص الوصول الشامل والميسور إلى شبكة الإنترنت بخلاف المدن الريفية التي لا توجد فيها تغطية لشبكات الاتصالات المتنقلة على الإطلاق، أما عن مؤشر كون محافظة بورسعيد من أقل محافظات جمهورية مصر العربية فقرا؛ يدلنا على أن أولياء الأمور لديهم القدرة المادية على شراء أجهزة لوحية موصلة بالانترنت لأبنائهم ما يشكل نقطة انطلاق للمخاطر السيبرانية.

ب- أهداف التعليم ومؤشراته في المدارس الابتدائية بمحافظة بورسعيد.

١-أهداف التعليم الابتدائي بمصر:

وفيما يلي نعرض تأكيد أهداف التعليم -وفقا للقوانين- على ترسيخ القيم التربوية وتزويد التلاميذ بالسلوك المناسب، وهو ما تقوم عليه إدارة المخاطر السيبرانية:

نصت المادة رقم (١٩) من دستور ٢٠١٤ على أن التعليم حق لكل مواطن، هدفه بناء الشخصية المصرية، والحفاظ على الهوية الوطنية، وترسيخ القيم الحضارية والروحية، وإرساء مفاهيم المواطنة (جمهورية مصر العربية، وزارة التربية والتعليم، ٢٠١٤، ١٣)

وقد نصت المادة ١ من قانون رقم ١٣٩ لسنة ١٩٨١ على أن من أهداف التعليم قبل الجامعي تكوين الدارس تكوينا ثقافيا وعلميا وقوميا، من النواحي الوجدانية والقومية والعقلية والاجتماعية والصحية والسلوكية، بقصد إعداد الإنسان المصري المؤمن بربه ووطنه وبقيم الخير والحق والإنسانية، وتزويده بالقدر المناسب من القيم التي تحقق إنسانيته وكرامته. (جمهورية مصر العربية، رئاسة الجمهورية: قانون رقم ١٣٩ لسنة ١٩٨١ بإصدار قانون التعليم، ٢١٤٨)

أما التعليم الأساسي خاصةً فيهدف إلى تزويد الطلاب بالقدر الضروري من القيم والسلوكيات. (جمهورية مصر العربية، وزارة التربية والتعليم، ٢٠١٤، الخطة الإستراتيجية للتعليم قبل الجامعي ٢٠١٤-٢٠٣٠، ٥٥)

وعن المادة ١٧ الخاصة بتنظيم الدراسة في مرحلة التعليم الأساسي(جمهورية مصر العربية ، رئاسة الجمهورية : قانون رقم ١٣٩ لسنة ١٩٨١ بإصدار قانون التعليم، ٢١٥١) فقد نصت على أن من أغراض تلك المرحلة: التأكيد على التربية الدينية والوطنية والسلوكية والرياضية خلال مختلف سنوات الدراسة.

ونلاحظ مما سبق اتفاق الدستور وقانون التعليم المصري والخطة الاستراتيجية للتعليم قبل الجامعي في التأكيد على ترسيخ القيم وتزويد التلاميذ بالسلوك المناسب خلال مختلف سنوات الدراسة، وهو ما تقوم عليه إدارة المخاطر السيبرانية كمستحدثات تربوية.

٢-اسراتيجية التعليم في محافظة بورسعيد (محافظة بورسعيد، مديرية التربية والتعليم، إدارة قياس الجودة، ديسمبر ٢٠١٤)

ونلاحظ فيها الاعتماد بشكل جذري على **البعد التكنولوجي والتقني** سواء بتوظيف التكنولوجيا في المدارس، أو بالاستخدام الأمثل لها من قبل الطلاب للتعلم، أو بتفعيل دور وحدة التطوير التكنولوجي، والاستفادة من إمكانات مركز التطوير التكنولوجي، مع الإغفال التام لتدريب الطلاب وتوعيتهم بالمخاطر السيبرانية وتأمين دخولهم على شبكات الانترنت، ومع الاعتراف بتدني استخدام البعد التقني كمعوق لتحقيق التجديد الذاتي، ويظهر ذلك جليا فيما يلي:

(أ) الرؤية:

تطوير عناصر المنظومة التعليمية لتنشئة طالب قادر على التعليم والتعلم المستمر.

(ب)الرسالة:

تهيئة بيئة تعليمية محفزة للابتكار والإبداع من خلال توظيف التكنولوجيا الحديثة، وتفعيل إستراتيجيات التعليم والتعلم المتمركزة حول المتعلم، والتنمية

المهنية المستدامة للقوى البشرية في إطار المحاسبية واللامركزية والشراكة المجتمعية الفعالة.

(ج) الأهداف:

-العمل على تكوين رؤية لدى مديري عموم الإدارات التعليمية كلاً في إدارته.

-تحقيق روح الانتماء للمؤسسة التعليمية وحب الوطن.

-تنمية مهارات مديري إدارت المؤسسات التعليمية بالمديرية على كيفية وضع خطة عمل بما يتناسب ومهام كل إدارة ومؤسسة.

-تفعيل وحدات التدريب والجودة بالمؤسسات التعليمية.

-نشر ثقافة التغير من أجل الإصلاح التربوي.

-تحقيق مؤشرات ضبط الجودة الشاملة بالمؤسسات التعليمية.

-ضبط وتقييم الأداء في ضوء المعايير القومية للتعليم.

-توسيع قاعدة المشاركة المجتمعية واللامركزية في إدارة العملية التعليمية لتعميق المشاركة بين المؤسسة التعليمية والمجتمع.

-الاهتمام ورعاية ذوي الاحتياجات الخاصة (موهوبين- صعوبات تعلم-إعاقات بدنية- تأخر دراسي).

-تعميق روح الإبداع والابتكار العلمي ودعم ثقافة البحث العلمي.

-الاستخدام الأمثل لتكنولوجيا التعلم للوصول إلى الجودة الشاملة.

(د) إستراتيجيات التنفيذ:

وضع خطط التحسين المبنية على التقييم الذاتي في ضوء مجالات ومعايير الهيئة القومية لضمان جودة التعليم لاعتماد المديريات والإدارات التعليمية.

(هـ) متطلبات إنجاح الرؤية:

-المساندة والدعم من قبل المديرية والإدارة التعليمية ومنظمات المجتمع المدني.

-إجراء البحوث التي تتضمن مسح للبيئة الخارجية والداخلية لاكتشاف إمكانياتها واستغلالها، وربطها بالمؤسسة التعليمية.

-تحديد الجهات والمؤسسات القادرة على تقديم الدعم المادي والإداري والفني.

-وضع نظام محاسبي.

-وضع مؤشرات للأداء المالي.

-تفعيل دور وحدة التطوير التكنولوجي داخل المؤسسات التعليمية.

-الاستفادة من إمكانات مركز التطوير التكنولوجي (قسم البرمجيات- قسم الشبكات).

(و) القضايا التي تعوق تحقيق التجديد الذاتي:

-تدني كفاءة وقدرة العنصر البشري.

-ضعف الاستفادة من الوحدات المستحدثة داخل المؤسسات التعليمية (الوحدة المنتجة- وحدة التدريب والجودة-وحدة الإحصاء)

-محدودية الموارد المالية اللازمة للوفاء بمتطلبات التجديد للمدرسة.

-تدني استخدام البعد التقني.

-انعزال المؤسسة التعليمية عن البيئة الخارجية مما يقلل من فرص استثمار إمكانات البيئة، والإفادة من إمكانات المؤسسة التعليمية.

-البيروقراطية والروتين.

(ز) الفترة الزمنية المقترحة للتنفيذ:

حوالي من ٥-٧ سنوات تبدأ من العام ٢٠١٥/٢٠٢٠ وذلك تماشيا مع متطلبات التطوير والتجديد والخطة العامة لاعتماد المؤسسات التعليمية من قبل مديرية التربية والتعليم ببورسعيد.

٣- مؤشرات التنمية التعليمية الخاصة بالمدارس الابتدائية بمحافظة بورسعيد:

وفيما يلي مؤشرات التنمية التعليمية الخاصة بالمدارس **الابتدائية** بمحافظة بورسعيد للعام الدراسي ٢٠٢٠/٢٠٢١: (وزارة التربية والتعليم والتعليم الفني، الإدارة العامة لنظم المعلومات ودعم اتخاذ القرار، ٢٠٢١أ،) (وزارة التربية والتعليم والتعليم الفني، الإدارة العامة لنظم المعلومات ودعم اتخاذ القرار، ٢٠٢١ب، ١٧) (جمهورية مصر العربية، الجهاز المركزي للتعبئة والإحصاء، ٢٠٢٠، مصر في أرقام (التعداد)، ١٧، ٢٤)

المؤشر	القيمة	النسبة	السنة
مؤشرات التحاق سكان بورسعيد بالتعليم:	٣٥١٩٦٢	٥١.٣٪	٢٠١٧
-التحق وأنهى.	١٣٠١٨٤	٢٦.٨٪	
-ملتحق حالياً.	٣٨٠٢٩	٥.٥٪	
-التحق وتسرب.	١١١٧٧١	١٦.٣٪	
-لم يلتحق.	٦٥٨٩٢	١٠٠٪	
-الجملة.			
نسبة الأمية بين السكان:			٢٠٢١/٢٠٢٠
-ذكور.	-	١٢.٥٪	
-إناث.	-	١٥.٨٪	
-جملة.	-	١٤.١٪	
عدد المدارس الابتدائية -حكومي وخاص	١٦٥	-	٢٠٢١/٢٠٢٠
عدد الفصول الابتدائية: -حكومي وخاص	٢١١٨	-	٢٠٢١/٢٠٢٠
عدد التلاميذ: -حكومي وخاص	٩١٠٣١	-	٢٠٢١/٢٠٢٠
-أعداد أعضاء التعليم والعاملين بالمدارس الابتدائية:			٢٠٢١/٢٠٢٠
-معلمون+ معلمون متعاقدون	٥١٠٢	-	
-إدارة مدرسية	١٣٧		
-أخصائيون	٥٨٧		
-إداريون +إداريون متعاقدون	١١٩٢		
-عمال	٣١٢		
-جملة	٧٣٣٠		

المؤشر	القيمة	النسبة	السنة
-أعداد المعلمين وفقا للدرجة بالمدارس الابتدائية:			
-وكيل يدرس	٥		
-كبير + خبير مشرف	١١١		
-معلم خبير	١١٧٢		
-معلم أول أ مشرف	٠	-	٢٠٢١/٢٠٢٠
-معلم أول أ	١٢٢١		
-معلم أول مشرف	١		
-معلم أول غير مشرف	٧١٨		
-معلم	١٩٦٩		
-جملة	٥٠٩٧		
-مؤهلات معلمي المدارس الابتدائية:	٤٠٣٠		
-ممتازة وعليا تربوية.	١٥٥		
-ممتازة وعليا غير تربوية.	٨٣٤		
-فوق متوسطة ومتوسطة تربوية	٧٨		٢٠٢١/٢٠٢٠
-فوق متوسطة ومتوسطة غير تربوية	٠		
-مؤهلات أخرى	٥٠٩٧		
-إجمالي عدد المعلمين			

اعتماداً على الإحصاءات والبيانات جدير بالذكر أن بورسعيد أقل محافظات الجمهورية في نسبة الأمية بعد محافظة البحر الأحمر التي تمثل (١٢.٠)%، فضلاً عن أن نسبة النجاح (الحكومي): ٩٨.٨٪ (الخاص): ٩٩.٧٪ ، ونسبة التسرب للمرحلة

الابتدائية بين عاميّ ٢٠١٨/٢٠١٩-٢٠١٩/٢٠٢٠: ١٤١ طالبا بما يعادل ١٧.٠٪، كما أن نسبة المعلمين التربويين: (حكومي) ٩٧.٣٤٪ (خاص) ٧٦.٦٠٪ (إجمالي) ٩٥.٤٣٪، ونصيب المعلم من التلاميذ: ١٧.٨٤، بالإضافة إلى أن متوسط كثافة الفصل: ٤٢.٩٨.

ج- إجراءات الدراسة الميدانية، وتشمل ما يلي:

١-أهداف الدراسة الميدانية:

تعرف واقع إدارة المخاطر السيبرانية بالمدارس الابتدائية في محافظة بورسعيد.

٢-أداة الدراسة، وعينة الدراسة:

تمثلت استبانة استقصت فيها الباحثة آراء عينة من مديري المدارس الابتدائية بمحافظة بورسعيد؛ للتعرف على واقع إدارة المخاطر السيبرانية في المدارس الابتدائية بمحافظة بورسعيد؛ تناولت فيه الباحثة مجموعة من العمليات والإجراءات التي استخلصتها من الدراسة النظرية، وقد تم تطبيقها على عينة عشوائية بلغت (٧٨) مديراً.

البيان	المجتمع الأصلي	العينة	النسبة المئوية
مديري المدارس	١٣٧	٧٨	٥٦.٩٪

٣-ثبات وصدق الاستبانة:

(أ)- صدق الاستبانة.

(١)-الصدق الظاهري.

تم التحقق من الصدق الظاهري من خلال:

عرض الاستبانة على المحكمين: قامت الباحثة بعرض الصيغة الأولية للاستبانة على محكمين من ذوى الخبرة والاختصاص العلمى، ملحق(٤) قائمة بأسماء أعضاء لجنة التحكيم، حيث طُلب منهم التفضل بإبداء الرأى حول سلامة الصياغة اللغوية لكل فقرة من الفقرات، وبيان مدى انتماء كل فقرة للمجال الذى تندرج تحته، ومدى مناسبة فقرات الاستبانة مع عينة الدراسة، وقد كانت نسبة الإتفاق(٨٠ %) فأكثر بين آراء أعضاء لجنة التحكيم؛ وبناء على ذلك تم إجراء التعديلات المطلوبة.

(٢)- صدق الاتساق الداخلى.

٢-١-معامل ارتباط كل مفردة مع البعد الخاص بها:

تم حساب معاملات الارتباط بين المفردات وأبعاد الاستبانة لدى العينة الاستطلاعية (ن= ٤٤) وهذا ما يسمى بالتجانس أو الاتساق الداخلي، كما هو موضح بالجدول التالي:

جدول (٦) معاملات ارتباط مفردات أبعاد إدارة المخاطر السيبرانية

رقم المفردة	البعد الأول	رقم المفردة	البعد الثاني	رقم المفردة	البعد الثالث	رقم المفردة	البعد الرابع	رقم المفردة	البعد الخامس
١	**٠.٦٠٦	٨	*٠.٣٨٠	١٥	**٠.٠٦١١	٢٢	**٠.٤٧١	٢٩	**٠.٦٤٦
٢	**٠.٧٠٤	٩	**٠.٨١٤	١٦	**٠.٤٠٤	٢٣	**٠.٥٧٠	٣٠	**٠.٤٣٠
٣	**٠.٧٠٧	١٠	**٠.٧٤٥	١٧	**٠.٤٦٢	٢٤	*٠.٣٠١	٣١	**٠.٥٢٨
٤	**٠.٦٦١	١١	**٠.٧٧٧	١٨	٠.١٧٠	٢٥	**٠.٥٧٦	٣٢	**٠.٣٩٢
٥	**٠.٤٠٢	١٢	**٠.٦٩٧	١٩	*٠.٣٥١	٢٦	**٠.٤٦٩	٣٣	*٠.٣٧٧
٦	*٠.٣٥٠	١٣	*٠.٣٤٣	٢٠	*٠.٣٥٠	٢٧	*٠.٣٢٩	٣٤	**٠.٤٧٠
٧	*٠.٣٤٥	١٤	**٠.٦٢١	٢١	**٠.٤٦٨	٢٨	*٠.٣٣٧	٣٥	**٠.٥٢٤

(*) دال إحصائيا عند مستوى (٠,٠٥) (**) دال إحصائيا عند مستوى (٠,٠١)

ويتضح من الجدول السابق أن جميع المفردات مرتبطة بأبعادها ارتباط دال إحصائياً عند مستوى(٠,٠١)، فيما عدا المفردات رقم (٦، ٧، ٨، ١٣، ١٩، ٢٠، ٢٤، ٢٧، ٢٨، ٣٣) دال إحصائياً عند مستوى(٠,٠٥)، بينما كانت المفردة (١٨) غير دالة إحصائياً لذلك وجب حذفها في الصورة النهائية للاستبانة.

٢-٢معامل الارتباط بين أبعاد الاستبانة والدرجة الكلية:

تم حساب معامل الارتباط بين أبعاد إدارة المخاطر السيبرانية والدرجة الكلية للاستبانة كما هو موضح بالجدول التالي :

جدول (٧) معاملات الارتباط بين أبعاد إدارة المخاطر السيبرانية **والدرجة الكلية للاستبانة**

البعد	الدرجة الكلية للاستبانة
الأول	**٠.٨٠٧
الثاني	**٠.٨٥٨
الثالث	**٠.٥٥٧
الرابع	**٠.٤٩٨
الخامس	**٠.٥٧٠

(**) دال إحصائيا عند مستوى (٠,٠١)

يتضح من الجدول السابق وجود ارتباط دال إحصائياً عند مستوى دلالة (٠.٠١) بين البعد الأول والدرجة الكلية للاستبانة، حيث بلغ قيمة معامل الارتباط (ر = ٠,٨٠٧)، كما وجد ارتباط دال إحصائياً عند مستوى (٠.٠١) بين بعد الثاني والدرجة الكلية للاستبانة ، حيث بلغ قيمة معامل الارتباط (ر=٠,٨٥٨)، كما وجد ارتباط دال إحصائياً عند مستوى (٠.٠١) بين بعد الثالث والدرجة الكلية للاستبانة ، حيث بلغ قيمة معامل الارتباط (ر=٠,٥٥٧)، كما وجد ارتباط دال إحصائياً عند مستوى (٠.٠١) بين بعد الرابع والدرجة الكلية للاستبانة ، حيث بلغ قيمة معامل الارتباط (ر=٠,٤٩٨)، كما وجد ارتباط دال إحصائياً عند مستوى (٠.٠١) بين بعد الخامس والدرجة الكلية للاستبانة ، حيث بلغ قيمة معامل الارتباط (ر=٠,٥٧٠)، مما يشير إلي اتساق البناء الداخلي للاستبانة.

(ب) ثبات الاستبانة

(١)-ثبات مفردات الاستبانة بطريقة معامل ألفا كرونباخ :

تم حساب ثبات مفردات الاستبانة باستخدام برنامج الإحصاء SPSS(20) وذلك بطريقة معامل ألفا كرونباخ Cronbach's Alpha لمفردات الاستبانة لدى العينة

المكونة من (ن = ٤٤) مديراً ، وفي كل مرة يتم حذف درجة إحدى المفردات من الدرجة الكلية للاستبانة، وذلك كما هو موضح بالجدول التالي:

جدول (٨)

معاملات ثبات مفردات استبانة إدارة المخاطر السيبرانية **لدى العينة الاستطلاعية (ن= ٤٤)**

المفردة	معامل ألفا	المفردة	معامل ألفا	المفردة	معامل ألفا	المفردة	معامل ألفا	المفردة	معامل ألفا
١	٠.٧٧٥	٨	٠.٧٧٨	١٥	٠.٧٦٥	٢٢	٠.٧٦٨	٢٩	٠.٧٧٧
٢	٠.٧٦٣	٩	٠.٧٦٠	١٦	٠.٧٨١	٢٣	٠.٧٧٩	٣٠	٠.٧٧٣
٣	٠.٧٥٦	١٠	٠.٧٥٥	١٧	٠.٧٧٩	٢٤	٠.٧٧٩	٣١	٠.٧٧٥
٤	٠.٧٦٩	١١	٠.٧٤٤	١٨	٠.٧٨٥	٢٥	٠.٧٨٠	٣٢	٠.٧٨١
٥	٠.٧٧٤	١٢	٠.٧٦٦	١٩	٠.٧٧٤	٢٦	٠.٧٨٩	٣٣	٠.٧٨٠
٦	٠.٧٧٦	١٣	٠.٧٨٠	٢٠	٠.٧٧٧	٢٧	٠.٧٨٠	٣٤	٠.٧٦٨
٧	٠.٧٧٤	١٤	٠.٧٦٨	٢١	٠.٧٧٧	٢٨	٠.٧٨١	٣٥	٠.٧٧٢

معامل ألفا للاستبانة بدون حذف أى مفردة=٠,٧٨١

يتضح من الجدول السابق أن:

معاملات ألفا لكل مفردة عند حذف درجة المفردة من الدرجة الكلية للاستبانة أقل من معامل ألفا العام للاستبانة ، أي أن جميع المفردات ثابتة، حيث إن تدخل المفردة لا يؤدى إلي خفض معامل الثبات الكلي للاستبانة ، وذلك باستثناء المفردات ذات الأرقام (١٨، ٢٦)، حيث وجد أن تدخل هذه المفردات يؤدى إلي خفض معامل الثبات الكلى للاستبانة واستبعادها يؤدى إلي رفع معامل الثبات الكلى للاستبانة ، لذا تم حذف هذه المفردات، حيث تراوحت قيم ثبات مفردات الاستبانة من (٠.٧٤٤) إلي (٠.٧٨١).

(٢)-الثبات الكلى للاستبانة بطريقة معامل ألفا كرونباخ:

تم حساب ثبات الأبعاد والاستبانة ككل بطريقة معامل ألفا كرونباخ لدى العينة الكلية (ن = ٤٤) مديراً ، حيث يمثل معامل ألفا متوسط المعاملات الناتجة عن تجزئة الاستبانة

إلي أجزاء بطريقة مختلفة، وبذلك فإنه يمثل معامل الارتباط بين أي جزأين من أجزاء الاستبانة، وتتضح نتائج هذا التحليل من الجدول التالي:

جدول (٩)

معامل ثبات ألفا كرونباخ لأبعاد استبانة إدارة المخاطر السيبرانية والدرجة الكلية

الأبعاد الرئيسة	معامل ثبات ألفا كرونباخ
البعد الأول	٠,٧٤٨
البعد الثاني	٠,٧٦٩
البعد الثالث	٠,٧٥٠
البعد الرابع	٠,٧٨٣
البعد الخامس	٠.٧٤٥
الدرجة الكلية للأبعاد	٠.٧٨١

ويتضح من الجدول السابق ثبات الاستبانة ككل والأبعاد الخمسة المتمثلة في: تحديد المخاطر السيبرانية، تحليل المخاطر السيبرانية، تقييم المخاطر السيبرانية، الاستجابة للمخاطر السيبرانية، تتبع المخاطر وتحديث آليات المواجهة لدى أفراد عينة الدراسة الحالية.

(٣)- الثبات الكلى للاستبانة باستخدام التجزئة النصفية:

حيث تم حساب معامل الثبات الكلي بطريقة التجزئة النصفية باستخدام معادلتي سبيرمان / براون، وجتمان بعد حذف المفردات غير الثابتة، حيث وجد أن معامل الثبات الكلي للاستبانة يساوي(٠,٨٠٧) بطريقة سبيرمان / براون، ويساوي (٠,٧٢١) بطريقة جتمان، وهو معامل ثبات مرتفع مما يدل على الثبات الكلي للاستبانة.

الصورة النهائية للاستبانة: ملحق(٣)

بعد التحقق من الخصائص السيكومترية للاستبانة، تبين أن المفردات(١٨، ٢٦) افتقدت مؤشرات الصدق والثبات؛ وبالتالي تم حذف تلك المفردات من الصورة النهائية للاستبانة ، وأصبحت مفردات الاستبانة (٣٣) مفردة، موزعة على أبعاد الاستبانة، (٧) مفردات للبعد الأول ،(٧) مفردات للبعد الثانى، (٦) مفردات للبعد الثالث، (٦) مفدرات للبعد الرابع، (٧) مفردات للبعد الخامس.

(ج)-المعالجة الإحصائية:

وتم استخدام المعالجات الإحصائية التالية:

-حساب التكرارات ونسبتها المئوية لكل مفردة .

-حساب التقدير الرقمى لكل عبارة من خلال المعادلة التالية :

-التقدير الرقمى= (ك١ ×١)+(ك ١ × ٢) + (ك ٣ × ٣)

-حساب الوزن النسبي= التقدير الرقمي/ ن

واستعانت الباحثة بأسلوب حساب الوزن النسبي ، ومستوى الموافقة وفقاً لتدرج مقياس ليكرت الخماسي (١-١.٨٠= ضعيفة جداً، ١.٨١-٢.٦١= ضعيفة، ٢.٦١-٣.٤٠= متوسطة، ٣.٤١-٤.٢٠= كبيرة، ٤.٢١-٥= كبيرة جداً)

د- عرض وتحليل نتائج الدراسة الميدانية.

نتائج المحور الأول: واقع تحديد المخاطر السيبرانية بالمدارس الابتدائية بمحافظة بورسعيد.

يتكون هذا المحور من عدد (٧) عبارات، سيتم توضيح استجابات العينة الكلية للدراسة حول هذه العبارات بالتفصيل، كما هو موضح بالجدول التالي:

جدول (١٠) استجابات عينة الدراسة حول واقع تحديد المخاطر السيبرانية بالمدارس الابتدائية بمحافظة بورسعيد (ن= ٧٨)

من خلال نتائج الجدول السابق يتضح أن م	العبارة	التكرار	درجة التحقق					التقدير الرقمي	الوزن النسبي	اتجاه العبارة	الترتيب
		النسبة	ضعيفة جدا	ضعيفة	متوسطة	كبيرة	كبيرة جدا				
١	-تُجري إدارة المدرسة مسحاً داخليا لتحديد المخاطر السيبرانية.	ك	60	14	3	1	0	101	1.29	قليلة جدا	5
		%	76.9	17.9	3.8	1	0				
٢	-تُجري إدارة المدرسة مسحاً خارجيا لتحديد المخاطر السيبرانية.	ك	61	10	7	0	0	102	1.31	قليلة جدا	4
		%	78.2	12.8	9.0	0	0				
٣	-تحدد إدارة المدرسة آليات للكشف المبكر عن المخاطر السيبرانية.	ك	59	15	2	1	1	104	1.33	قليلة جدا	3
		%	75.6	19.2	2.6	1.3	1.3				
٤	-تستعين إدارة المدرسة بالخبراء عند تحديد المخاطر السيبرانية.	ك	56	17	5	0	0	105	1.35	قليلة جدا	2
		%	71.8	21.8	6.4	0	0				
٥	-تستخدم إدارة المدرسة أسلوب SWOT عند تحديد المخاطر	ك	55	15	6	1	1	112	1.44	قليلة جدا	1

من خلال نتائج الجدول السابق يتضح أن م	العبارة	التكرار	درجة التحقق					التقدير الرقمي	الوزن النسبي	اتجاه العبارة	الترتيب
		النسبة	ضعيفة جدا	ضعيفة	متوسطة	كبيرة	كبيرة جدا				
	السيبرانية.	%	70.5	19.2	7.7	1.3	1.3				
٦	-تستعين المدرسة بأصحاب المصلحة للمساندة في تحديد المخاطر السيبرانية.	ك	63	15	0	0	0	93	1.19	قليلة جدا	6
		%	80.8	19.2	0.0	0	0				
٧	-تحرص إدارة المدرسة على تحديد سياق إدارة المخاطر السيبرانية.	ك	58	14	6	0	0	104	1.33	قليلة جدا	3 مكرر
		%	74.4	17.9	7.7	0	0				

من خلال نتائج الجدول السابق يتضح ما يلي:

بالنسبة لترتيب أعلى عبارة حسب الوزن النسبي لها فكانت:-تستعين إدارة المدرسة بالخبراء عند تحديد المخاطر السيبرانية؛ وتُرجع الباحثة ذلك إلى ربط مديري المدارس بين مجهوداتهم في الجودة وبين إدارة المخاطر السيبرانية باعتبارها علاقة الكل بالجزء؛ فاعتبروا استقدام خبراء لضمان الجودة جهود لإدارة كل ما في المنظمة ومنها إدارة المخاطر السيبرانية.

وجاء ترتيب أقل عبارة حسب الوزن النسبي لها: -تستعين المدرسة بأصحاب المصلحة للمساندة في تحديد المخاطر السيبرانية. وقد يرجع ذلك لمعاناة المدارس بشكل عام من ضعف المشاركة المجتمعية كما تشير معظم الدراسات.

نتائج المحور الثاني: واقع تحليل المخاطر السيبرانية بالمدارس الابتدائية بمحافظة بورسعيد.

يتكون هذا المحور من عدد (٧) عبارات، سيتم توضيح استجابات العينة الكلية للدراسة حول هذه العبارات بالتفصيل، كما هو موضح بالجدول التالي:

جدول (١١) استجابات عينة الدراسة حول واقع تحليل المخاطر السيبرانية بالمدارس الابتدائية بمحافظة بورسعيد (ن= ٧٨)

م	العبارة	التكرار	درجة التحقق					التقدير الرقمي	الوزن النسبي	اتجاه العبارة	الترتيب
		النسبة	ضعيفة جدا	ضعيفة	متوسطة	كبيرة	كبيرة جدا				
١	– تحتفظ إدارة المدرسة بقاعدة بيانات تتضمن معلومات عن المخاطر السيبرانية التي يتعرض لها الطلاب.	ك	60	12	6	0	0	102	1.31	قليلة جدا	1
		%	77	15	8	0	0				
٢	–تهتم إدارة المدرسة بتكاملية المعلومات الخاصة بإدارة المخاطر السيبرانية.	ك	63	10	5	0	0	98	1.26	قليلة جدا	4
		%	80.8	12.8	6.4	0	0				
٣	– تحلل إدارة المدرسة المخاطر باستخدام أدوات مناسبة.	ك	61	13	3	1	0	100	1.28	قليلة جدا	2
		%	78.2	16.7	3.8	1.3	0				
٤	–تدرس إدارة المدرسة العوامل المسببة للمخاطر السيبرانية.	ك	60	15	2	1	0	100	1.28	قليلة جدا	2 مكرر

م	العبارة	التكرار	درجة التحقق					التقدير الرقمي	الوزن النسبي	اتجاه العبارة	الترتيب
		النسبة	ضعيفة جدا	ضعيفة	متوسطة	كبيرة	كبيرة جدا				
		%	76.9	19.2	2.6	1.3	0				
٥	-تدرس إدارة المدرسة تأثير المخاطر السيبرانية على الأهداف الاستراتيجية للمدرسة.	ك	63	12	2	1	0	97	1.24	قليلة جدا	5
		%	80.8	15.4	2.6	1.3	0				
٦	-تدرس إدارة المدرسة الضوابط الوقائية التي يمكن وضعها لتقليل احتمالية حدوث المخاطر السيبرانية.	ك	64	9	4	1	0	98	1. 26	قليلة جدا	4 مكرر
		%	82	12	5	1	0				
٧	-تعد إدارة المدرسة إستراتيجية واضحة لإدارة المخاطر السيبرانية	ك	62	11	5	0	0	99	1.27	قليلة جدا	3
		%	79.5	14.1	6.4	0	0				

من خلال نتائج الجدول السابق يتضح ما يلي:

بالنسبة لترتيب أعلى عبارة حسب الوزن النسبي لها فكانت:- تحتفظ إدارة المدرسة بقاعدة بيانات تتضمن معلومات عن المخاطر السيبرانية التي يتعرض لها الطلاب وإن كان اتجاه العبارة قليل جداً تحققه. **وجاء ترتيب أقل عبارة حسب الوزن**

النسبي لها: :- تدرس إدارة المدرسة تأثير المخاطر السيبرانية على الأهداف الاستراتيجية للمدرسة.

نتائج المحور الثالث: واقع تقييم المخاطر السيبرانية بالمدارس الابتدائية بمحافظة بورسعيد.

يتكون هذا المحور من عدد (٦) عبارات، سيتم توضيح استجابات العينة الكلية للدراسة حول هذه العبارات بالتفصيل، كما هو موضح بالجدول التالي:

جدول (١٢) استجابات عينة الدراسة حول واقع تقييم المخاطر السيبرانية بالمدارس الابتدائية بمحافظة بورسعيد (ن= ٧٨)

م	العبارة	التكرار	درجة التحقق					التقدير الرقمي	الوزن النسبي	اتجاه العبارة	الترتيب
		النسبة	ضعيفة جدا	ضعيفة	متوسطة	كبيرة	كبيرة جدا				
١	-تقوم إدارة المدرسة بتقييم الآثار المحتملة للمخاطر السيبرانية على البيئة المدرسية.	ك	60	12	4	1	1	105	1.35	قليلة جدا	1
		%	76.9	15.4	5.1	1.3	1.3	97			
٢	- تقوم إدارة المدرسة بجدولة المخاطر السيبرانية وفقا للأشد خطراً فالأقل.	ك	62	13	3	0	0	100	1.24	قليلة جدا	5
		%	79.5	16.7	3.8	0	0				
٣	-تقوم إدارة المدرسة بتقييم نقاط القوة في التعامل مع المخاطر السيبرانية.	ك	61	13	3	1	0	98	1.28	قليلة جدا	3
		%	78.2	16.7	3.8	1.3	0				

م	العبارة	التكرار	درجة التحقق					التقدير الرقمي	الوزن النسبي	اتجاه العبارة	الترتيب
		النسبة	ضعيفة جدا	ضعيفة	متوسطة	كبيرة	كبيرة جدا				
٤	-تدرس إدارة المدرسة تأثير المخاطر السيبرانية على الأهداف الاستراتيجية للمدرسة.	ك	62	12	4	0	0	101	1.26	قليلة جدا	4
		%	79.5	15.4	5.1	0	0				
٥	-تدرس إدارة المدرسة الضوابط الوقائية التي يمكن وضعها لتقليل احتمالية حدوث المخاطر السيبرانية.	ك	60	14	3	1	0	98	1.29	قليلة جدا	2
		%	76.9	17.9	3.8	1.3	0				
٦	-تعِد إدارة المدرسة إستراتيجية واضحة لإدارة المخاطر السيبرانية	ك	63	10	5	0	0	98	1.26	قليلة جدا	مكرر 4
		%	80.8	12.8	6.4	0	0				

من خلال نتائج الجدول السابق يتضح ما يلي:

بالنسبة لترتيب أعلى عبارة حسب الوزن النسبي لها فكانت:- تقوم إدارة المدرسة بتقييم الآثار المحتملة للمخاطر السيبرانية على البيئة المدرسية. **وجاء ترتيب أقل عبارة حسب الوزن النسبي لها:** - تقوم إدارة المدرسة بجدولة المخاطر السيبرانية وفقا للأشد خطراً فالأقل.

نتائج المحور الرابع: واقع الاستجابة للمخاطر السيبرانية بالمدارس الابتدائية بمحافظة بورسعيد.

يتكون هذا المحور من عدد (٦) عبارات، سيتم توضيح استجابات العينة الكلية للدراسة حول هذه العبارات بالتفصيل، كما هو موضح بالجدول التالي:

جدول (١٣) استجابات عينة الدراسة حول واقع الاستجابة للمخاطر السيبرانية بالمدارس الابتدائية بمحافظة بورسعيد (ن= ٧٨)

من خلال نتائج الجدول السابق يتضح أن م	العبارة	التكرار	درجة التحقق					التقدير الرقمي	الوزن النسبي	اتجاه العبارة	الترتيب
		النسبة	ضعيفة جدا	ضعيفة	متوسطة	كبيرة	كبيرة جدا				
١	–تنسق إدارة المدرسة جهود فريق إدارة المخاطر السيبرانية.	ك	60	16	2	0	0	98	1.26	قليلة جدا	4
		%	76.9	20.5	2.6	0	0				
٢	–تنظم إدارة المدرسة ورش عمل لتوعية الطلبة بشأن المخاطر السيبرانية.	ك	28	20	20	10	0	168	2.15	قليلة	1
		%	35.9	25.6	25.6	13	0				
٣	–تذلل إدارة المدرسة صعوبات الاتصال بالجهات المساعدة في إدارة المخاطر السيبرانية.	ك	64	10	3	1	0	97	1.24	قليلة جدا	5
		%	82.1	12.8	3.8	1.3	0				
٤	–تستخدم إدارة المدرسة صفحتها على الانترنت لتوعية أولياء أمور الطلبة.	ك	40	11	17	10	0	153	1.96	قليلة	2
		%	51.3	14.1	21.8	13	0				
٥	–تعد إدارة المدرسة برامج تدريبية للمعلمين في مجال إدارة المخاطر السيبرانية.	ك	59	19	0	0	0	97	1.24	قليلة جدا	5 مكرر
		%	75.6	24.4	0	0	0				
٦	–تنتهج إدارة المدرسة نظما ولوائح وقائية للسلامة من المخاطر السيبرانية.	ك	60	13	4	1	0	102	1.31	قليلة جدا	3
		%	76.9	16.7	5.1	1.3	0				

من خلال نتائج الجدول السابق يتضح ما يلي:

- **بالنسبة لترتيب أعلى عبارة حسب الوزن النسبي لها فكانت:-** تنظم إدارة المدرسة ورش عمل لتوعية الطلبة بشأن المخاطر السيبرانية.

- **وجاء ترتيب أقل عبارة حسب الوزن النسبي لها:** :- تذلل إدارة المدرسة صعوبات الاتصال بالجهات المساعدة في إدارة المخاطر السيبرانية.وكذا العبارة-تعد إدارة المدرسة برامج تدريبية للمعلمين في مجال إدارة المخاطر السيبرانية.

نتائج المحور الخامس: واقع تتبع المخاطر السيبرانية وتحديث إدارتها بالمدارس الابتدائية بمحافظة بورسعيد.

يتكون هذا المحور من عدد (٧) عبارات، سيتم توضيح استجابات العينة الكلية للدراسة حول هذه العبارات بالتفصيل، كما هو موضح بالجدول التالي:

جدول (١٤) استجابات عينة الدراسة حول واقع تتبع المخاطر السيبرانية وتحديث إدارتها بالمدارس الابتدائية بمحافظة بورسعيد (ن= ٧٨)

م	العبارة	التكرار	درجة التحقق					التقدير الرقمي	الوزن النسبي	اتجاه العبارة	الترتيب
		النسبة	ضعيفة جدا	ضعيفة	متوسطة	كبيرة	كبيرة جدا				
١	-تجري إدارة المدرسة تقويما مستمرا لأساليب التخطيط المتبعة في الكشف المبكر عن المخاطر السيبرانية.	ك	60	12	6	0	0	102	1.31	قليلة جدا	1
		%	76.92	15.38	7.69	0	0				
٢	-تجري إدارة المدرسة مراجعة دورية لأساليب إدارة مخاطرها السيبرانية.	ك	62	12	3	1	0	99	1.27	قليلة جدا	3
		%	79.5	15.4	3.8	1.3	0				
٣	-تُقَيِّم إدارة المدرسة خطط إدارة المخاطر السيبرانية بقصد تطويرها.	ك	63	11	4	0	0	97	1.24	قليلة جدا	5
		%	80.8	14.1	5.1	0	0				
٤	-تتابع إدارة المدرسة نتائج إستراتيجيات التحديث المتخذة في مواجهة المخاطر السيبرانية.	ك	62	13	3	0	0	97	1.24	قليلة جدا	5 مكرر
		%	79.5	16.7	3.8	0	0				
٥	- تتابع إدارة المدرسة نتائج	ك	60	15	3	0	0	99	1.27	قليلة جدا	3

م	العبارة	التكرار	درجة التحقق					التقدير الرقمي	الوزن النسبي	اتجاه العبارة	الترتيب
		النسبة	ضعيفة جدا	ضعيفة	متوسطة	كبيرة	كبيرة جدا				
	إستراتيجيات الوقاية المتخذة في مواجهة المخاطر السيبرانية.	%	76.9	19.2	3.8	0	0				مكرر
٦	–تعيد إدارة المدرسة تقييم احتمالية المخاطر السيبرانية بعد اتخاذ بعض إستراتيجيات الاستجابة.	ك	62	13	2	1	0	98	1.26	قليلة جدا	4
		%	79.5	16.7	2.6	1.3	0				
٧	– تقوم إدارة المدرسة بتجديد قاعدة البيانات حسب ما يستجد من مخاطر سيبرانية.	ك	61	12	5	0	0	100	1.28	قليلة جدا	2
		%	78.2	15.4	6.4	0	0				

من خلال نتائج الجدول السابق يتضح ما يلي:

بالنسبة لترتيب أعلى عبارة حسب الوزن النسبي لها فكانت:– –تجري إدارة المدرسة تقويما مستمرا لأساليب التخطيط المتبعة في الكشف المبكر عن المخاطر السيبرانية.

وجاء ترتيب أقل عبارة حسب الوزن النسبي لها: :– تُقَيِّم إدارة المدرسة خطط إدارة المخاطر السيبرانية بقصد تطويرها. وكذا عبارة –تتابع إدارة المدرسة نتائج إستراتيجيات التحديث المتخذة في مواجهة المخاطر السيبرانية.

نلاحظ من كل مما سبق أن متوسط الوزن النسبي لكل المحاور يقع في نطاق درجة تحقق قليل جداً، وتفسر الدراسة ذلك بأنه من الطبيعي أن تكون إجراءات وعمليات إدارة المخاطر السيبرانية كجزء من إدارة المخاطر بشكل عام (قليلة جداً)؛ فهي إدارة مستحدثة في العالم كله، بالإضافة إلى قصور إدارة المخاطر في مصر على مفهومها التقليدي من حدوث حريق أو زلزال وقصور عملياتها على التدريب كل فترة في المدرسة على النزول بنظام عند سماع أجهزة الإنذار تحت مسمى "خطة الإخلاء في الحالات الطارئة"؛ بإخلاء تلك المباني التعليمية من شاغليها والنصح بعدم استخدام مصاعد كهربية وعدم الركض أو نحو ذلك، أما إدارة المخاطر السيبرانية بمفهومها المستحدث فلم

يلق الاهتمام الكافي في مصر وإن بدأ بمحاولات تنمية الوعي لدى طلابها بتلك المخاطر من خلال ورش العمل أو صفحتها على الانترنت كما أشارت نتائج الدراسة الميدانية.

ويتضح لنا من التحليل الإحصائي وباستقراء واقع إدارة المخاطر السيبرانية أن هناك قصور ملحوظ في إدارة المخاطر السيبرانية؛ فهناك نقص واضح في السياسات والممارسات والإجراءات المتعلقة بإدارة المخاطر السيبرانية وبالتالي ضعف الالتزام التنظيمي للمدارس بإدارة المخاطر السيبرانية بها؛ حيث أن مجرد وجود الرغبة دون سياسات وإجراءات مدروسة لا يكفي لخلق ثقافة مناهضة للمخاطر السيبرانية في المدارس، علاوة على أن الإجراءات المطبقة لم ترق إلى الدرجة المطلوبة التي تنشدها متطلبات العصر، وهذا القصور إنما يرجع للعديد من الظواهر منها أن هؤلاء التلاميذ لديهم القليل جدًا من التعليم المتعلق بالسلوك الصحيح في الفضاء السيبراني داخل المدارس، كما أن معظم المعلمين لديهم معرفة وخبرة محدودة بموضوع المخاطر السيبرانية والسلامة على الإنترنت، بالإضافة إلى أنهم لم يتلقَّوْا تدريبًا محددًا خلال تعليمهم الجامعي، ونقص دور منظمات المجتمع المدني، مما يستلزم الاستعانة بالممارسات الدولية في هذا الصدد لتقديم إجراءات مقترحة عما يمكن فعله لإدارة المخاطر السيبرانية على نحوٍ سليم.

المحور الخامس: إجراءات مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء الممارسات الدولية.

انطلاقاً من الإطار النظري للدراسة الذي تضمن عرضًا تحليلياً نظرياً للمخاطر السيبرانية متضمناً عرضاً لعمليات إدارة المخاطر، وتناول أيضًا عرضًا للاتجاهات العالمية المعاصرة لإدارة المخاطر السيبرانية في المدارس الابتدائية، ومن خلال الاطلاع على بعض الأدبيات التربوية المعاصرة، واستناداً إلى التحليل النظري لواقع إدارة المخاطر السيبرانية بمصر، وتأسيساً على الواقع الميداني المعاصر لإدارة المخاطر السيبرانية في المدارس الابتدائية بالتطبيق على محافظة بورسعيد، اتضحت الإجراءات المقترحة في ضوء الممارسات الدولية، وقد حرصت الباحثة على تأسيسها على إجراءات منهجية، وقد عرضت تلك الإجراءات على مجموعة من المحكمين المصريين لمعرفة مدى قابليتها للتطبيق ومناسبتها للواقع المصري ومخاطره السيبرانية وعدلت الباحثة

المقترح في ضوء توجيهاتهم؛ ومن ثم يتناول هذا المحور عرض إجراءات مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء الممارسات الدولية.

وقد سارت الإجراءات المقترحة متوافقة مع منهجية إدارة المخاطر بالالتزام بالخطوات التالية:

أولاً: توفير سياق لإدارة المخاطر السيبرانية في المدارس الابتدائية: بتحديد الأهداف من إدارة تلك المخاطر.

ثانياً: تحليل واقع القدرات التنظيمية للمدارس الابتدائية والمخاطر السيبرانية، من خلال:

١-تحديد المخاطر السيبرانية بطريقة منهجية اعتمادا على الدراسة الاستطلاعية باستطلاع آراء ٤٦٢ ولي أمر، وتحديد الأولويات في مواجهتها.

٢-تحديد القدرات التنظيمية.

٣-تقييم آثار المخاطر.

ثالثاً: تحديد إجراءات مقترحة لإدارة المخاطر السيبرانية بصورة استباقية والحد من آثارها السلبية، وقد صاغتها الباحثة في ضوء الممارسات الدولية.

ويمكن عرض ذلك فيما يلي:

أولاً -توفير سياق لإدارة المخاطر السيبرانية في المدارس الابتدائية:

-الأهداف.

*هدف وقائي: يتمثل في أن يصبح تلاميذ المدارس الابتدائية محصنين من احتمالية التعرض لمجموعة من الأفكار والمشاهد والممارسات الخاطئة الناتجة عن المخاطر السيبرانية أو الوقوع فريسة لتلك المخاطر والتي قد تسبب لهم أضرارا جمّة.

*هدف إرشادي: يتمثل في أن يوجَّه أصحاب المصلحة من الآباء والتلاميذ والمعلمين، وتزويدهم بالمبادئ التوجيهية للقيام بأدوارهم في إدارة المخاطر السيبرانية.

*هدف نمائي: يتمثل في أن يُخَفَّف من الآثار السلبية للمخاطر السيبرانية ومنع تفاقمها، وإتاحة الفرصة لتلاميذ المدارس الابتدائية للوصول للنمو المتكامل نفسياً ومعرفياً ووجدانياً، وتقديم مقترحاتٍ تربوية لكيفية التعامل البنّاء مع تلك المخاطر، خاصةً مع المطالبة القوية لأولياء الأمور بذلك.

ثانياً: تحليل واقع إدارة المخاطر السيبرانية في المدارس الابتدائية:

١-تحديد المخاطر السيبرانية بطريقة منهجية.

بناءً على نتائج الدراسة الاستطلاعية أمكن تحديد المخاطر السيبرانية على النحو التالي:

-**إدمان تلاميذ المدارس للانترنت:** وتعني استخدام الإنترنت بشكل مفرط "لغرض واحد" مثل الألعاب أو المواد الإباحية بواقع ٣٠ ساعة أسبوعياً.

-**التنمر الإلكتروني:** ويعني استخدام التكنولوجيا الإلكترونية كوسيلة لإيذاء الآخرين أو عدم راحتهم؛ بتخويف المتلقي أو التحكم فيه أو التلاعب به أو إذلاله أو إهانته بإبداء تعليقات بذيئة، أو بالإدلاء بملاحظات جنسية حول الملابس والمظهر، ويتم ذلك من خلال البريد الإلكتروني أو مجموعات مناقشة غرفة الدردشة أو المراسلة الفورية أو صفحات الويب أو الرسائل القصيرة ، وتكمن خطورته في أنه قد يُحْدِث انتهاك كرامة الطفل و/ أو يخلق بيئة معادية أو مسيئة؛ فيتَّسِم التنمر عبر الإنترنت بِسِمتين: تكرار الفعل ونية إلحاق الأذى بالضحية.

-**مشاهدة عناصر غير لائقة:** تعرض الطفل لمحتوى غير مرحب به وغير مناسب، يمكن أن يشمل ذلك المحتوى الجنسي والإباحي والصور العنيفة، بعض أشكال الإعلان، المواد العنصرية أو التمييزية أو خطاب الكراهية؛ ومواقع الويب التي تدعو إلى سلوكيات غير صحية أو خطيرة، مثل إيذاء النفس والانتحار وفقدان الشهية والانضمام لجماعات مشبوهة.

-**الاستمالة:** وهي الاستدراج المقصود للأطفال من مشتهي الأطفال خلال الدردشة عبر الإنترنت أو داخل اللعبة ؛ بهدف ممارسة الجنس، أو للحصول على صور أو مقاطع فيديو جنسية لهم، أو البث المباشر لذلك، ومن إستراتيجياته تعريض الطفل تدريجيًا لمواد جنسية صريحة لتقليل المقاومة أو الموانع المتعلقة بالجنس (الاعتداء الجنسي) وتعليم الأطفال ما يريدونه منهم بالضبط، وتهدئتهم بأن هذا النشاط الجنسي ممتع لا خوف منه، مما يسبب ضررا جسيما للطفل.

٢-تحديد القدرات التنظيمية.

ويمكن رصد القدرات التنظيمية الحالية المتوفرة في مدارس مصر–والتي يمكن استغلالها في إدارة المخاطر السيبرانية– فيما يلي:

(أ) استغلال زيادة صلاحيات المدارس الابتدائية مالياً وإدارياً وتربوياً بإنشاء مجالس الأمناء وإصدار تنظيم جديد لها عام ٢٠١١؛ بما يمكنها من اتخاذ القرارات التنفيذية للتعامل مع المخاطر السيبرانية على المستوى المدرسي.

(ب) استثمار محاولات إعداد المدارس للاعتماد التربوي في إطار الخطة الاستراتيجية للتعليم قبل الجامعي ؛ وما يصاحبها من الاهتمام المتنامي بتحسين جودة الأداء المدرسي من كافة النواحي العامة والإدارية.

(ج) استغلال الأكاديمية المهنية للمعلمين والقيادات التربوية لتسهم بشكل فاعل ويكون لها دور في تنمية الكوادر البشرية من المعلمين والمديرين على إدارة المخاطر السيبرانية على مستوى المدرسة.

(د) الاستفادة من تطور تكنولوجيا المعلومات والاتصالات في دعم التواصل مع الآباء والمجتمع المحلي؛ من أجل نشر الوعي بالمخاطر السيبرانية.

٣–تقييم آثار المخاطر.

ويمكن عرض المخاطر السيبرانية وآثارها فيما يلي:

المخاطر السيبرانية	الآثار السلبية
–مشاهدة الأطفال للمواد الإباحية	<u>التأثير السلبي على النسق التربوي للتلميذ من خلال:</u> –إيقاظ الرغبة الجنسية مبكراً Awaking Sexual Passions وزيادة النشاط الجنسي عن طريق التفاصيل المرئية للممارسة الجنسية؛ فَتُقْصِي قيم الحياء، وتشكل صدمة شعورية للطفل في بداية رؤيتها سرعان ما يعتاد عليها من كثرة التعرض، الأمر الذي يدفعه إلى محاولة تجربتها في الواقع! مما يسهم في زيادة جرائم التحرش الجنسي أو زنا المحارم، خاصة في ظل غياب الرقابة الأسرية. –غرس الفكر الجنسي المتجرد من الفطرة والشريعة، وتوسيع مساحة الغرائز في حياته. –التغير الفسيولوجي وما يتبعه من زيادة معدلات ضربات القلب والآثار

المخاطر السيبرانية	الآثار السلبية
	السلوكية behavioral effects التي ترتبط بإجراء معين بعد التعرض لوسيلة إعلامية. -يصبح الطفل مهووساً أسيراً لها، مدفوعاً بشكل لاإرادي نحوها، مصاباً بوابل من الأمراض النفسية والاجتماعية التي تصعب مقاومتها. -ينجرف الفرد نحو إشباع ملذاته دون وضع أي قيود على سلوكه. -تُحْدِث له نوع من التصادم الذي لايكون في مصلحته أو مصلحة الوطن؛ حيث يفرز شخصاً غير قادر على الإبداع أو الإنتاج منساقاً وراء ما تروجه دول الغرب من إرواء الغرائز الجنسية؛ فيتجرد من هويته الدينية والأخلاقية ويهدد مستقبل مجتمعه وأمته العربية. -تشكيل اتجاهات سلبية فيما يتعلق بالعلاقات الحميمية Intimate Relationships؛ فالأشخاص الذين يتعرضون لمثل هذه المحتويات قد يعتقدون بأن ما يشاهدونه طبيعي وملائم للتطبيق في الحياة اليومية. -تكوين صورة ذهنية عن الأنثى في عقول مشاهديها؛ بحيث تتحول من كائن يحترمه ويتعايش معه إلى مجرد رمز جنسي. - ارتفاع معدلات التحرش بين شريحة المراهقين، وزيادة معدل الجرائم الجنسية.
إدمان الألعاب الإلكترونية الأجنبية	<u>التأثير السلبي على النسق الأكاديمي للتلميذ من خلال ما يلي:</u> - هناك أدلة تشير إلى أن النمو المعرفي للأطفال يمكن أن يتضرر بفترات طويلة من استخدام الإنترنت، بما في ذلك تطوير مهارات الذاكرة، ومدى الانتباه، وقدرات التفكير النقدي، واكتساب اللغة والقراءة والتعلم، ويكون لديه استدعاء أقل للمعلومات. - ثبت الارتباط المباشر بين المشاركة المفرطة في الألعاب عبر الإنترنت والعجز البنيوي في منطقة الدماغ . - وفقًا لتحليل المحتوى الذي أجرته منظمة معلومات الألعاب الأوروبية: 89 ٪ من الألعاب على الانترنت تحتوي على عناصر عنف ودم -بشكل

المخاطر السيبرانية	الآثار السلبية
	صريح- بما يؤدي لزيادة العدوانية بل قد يقلل من الشعور بالضمير، كما يؤدي اللعب المفرط إلى انخفاض الدافع للتعلم، وتؤثر سلبًا على الصحة البدنية والعقلية، وتشير دراسات التصوير بالرنين المغناطيسي إلى تغييرات هيكلية في القشرة الأمامية للمخ مرتبطة بخلل وظيفي لدى مدمن الإنترنت. -الاعتلال المشترك هو القاعدة وعادة ما يشمل الاكتئاب الاجتماعي، واضطراب القلق، والرهاب الاجتماعي، والوسواس القهري، واضطراب فرط الحركة ونقص الانتباه، والعداء، واضطرابات تعاطي المخدرات. -أشار الاستطلاع الذي أجري على العديد من المدارس الأمريكية التي تسمح بدخول أجهزة متعددة إلى الفصل الدراسي: أن أكثر الأمور إلحاحًا بين المعلمين كان الإلهاء، والذي تجاوز قضايا الخصوصية والأمان . -هناك ألعاب ذات عناصر شبيهة بالمقامرة والتي يمكن أن تجعل لعب القمار أمرًا طبيعيًا بالنسبة للأطفال بالإضافة إلى تكاليف الإنفاق داخل اللعبة. -يؤثر على الدماغ الأيمن فيجعلها متخلفة وهي المرتبطة بالتركيز وتخزين الذاكرة وتنظيم العاطفة، كما يؤدي لامتصاص إشعاع الموجات الكهرومغناطيسية، والإضرار بسرعة نمو دماغ الأطفال. -التعرض (غير المنضبط وغير المحدود) للتكنولوجيا بين الأطفال الصغار يؤدي إلى العديد من المخاطر الفسيولوجية والصحية المتعلقة بالرؤية، وكذلك المخاطر العقلية والنفسية والسلوكية مثل الانعزال، والإدمان.
التنمر الإلكتروني	<u>التأثير السلبي على النسق التربوي والأكاديمي للتلميذ على النحو التالي:</u> تشمل العواقب المرتبطة بالإيذاء السيبراني تدني احترام الذات وزيادة مستويات الاكتئاب لدى الضحايا، وكذلك ضعف الأداء الأكاديمي، والتسرب من المدرسة، والعنف الجسدي والانتحار، كما تشمل عواقب التنمر عبر الإنترنت على المتعلم، المشاكل الأكاديمية، والعنف المدرسي، والسلوك المنحرف.

المخاطر السيبرانية	الآثار السلبية
الاستمالة	التأثير السلبي على النسق التربوي والأكاديمي للتلميذ على النحو التالي: يمكن أن تؤدي النتيجة إلى حالات بغاء القصر وخطر الاتجار بالأطفال؛ حيث يُنظر إلى استغلال الأطفال في المواد الإباحية على أنها مشكلة واسعة الانتشار ومتفاقمة في مجتمع العصر الحديث، بدليل أن المواد الإباحية المشارك بها أطفال هي صناعة مربحة بمليارات الدولارات، فيتراوح إجمالي أرباحها من ١ إلى ٥ مليارات دولار سنويًا.

ثالثاً: تحديد إجراءات مقترحة لإدارة المخاطر السيبرانية بصورة استباقية والاستجابة لها للحد من آثارها السلبية في ضوء الممارسات الدولية.

أ- متطلبات إدارة المخاطر السيبرانية في المدارس الابتدائية (على المستوى المركزي) وفقا للمارسات الدولية :

فقد أشارت الأدبيات المعاصرة إلى أنه من الناحية المثالية، يجب أن يكون تحسين الأمان عبر الإنترنت وإدارة مخاطره نهجًا من أعلى إلى أسفل يبدأ بالحكومة وقسم التعليم، **ويمكن عرض متطلبات إدارة المخاطر السيبرانية فيما يلي:**

-أن تكون الحكومة في طليعة جهود الوقاية، وليس منظمات الخدمات الخاصة والمنظمات غير الربحية. (ممارسة كوريا الجنوبية)

-الاستجابة المنسقة لتهديدات الصحة السيبرانية العامة بمبادرات حكومية واسعة واستراتيجية خطط طويلة المدى على جميع مستويات الوقاية. (ممارسة كوريا الجنوبية)

- الاعتراف بشهر أكتوبر باعتباره شهر التوعية بالأمن السيبراني، مع إدراج يوم وطني أكثر أمانًا في التقويم، ليقام في ٩ تشرين فبراير من كل عام ؛ فتوثق الإجراءات المتخذة خلال هذا اليوم لتبادل الوعي حول هذه المسألة. (ممارسة المملكة المتحدة)

-استحداث هيئة (مفوض السلامة الإلكترونية للأطفال) وهو جهة تنظيمية مستقلة وطنية للإنترنت، تتضمن منصة أمان عبر الإنترنت بكمية هائلة من المحاكاة للمعلومات والموارد؛ لمساعدة المدارس والمجتمعات لتعزيز مسؤولية التلاميذ عبر الانترنت والمرونة لبناء ثقافة مدرسية إيجابية، وتتمثل مهمتها في الترويج للسلامة الرقمية من خلال تعزيز

التربية الإيجابية حول المواطنة الرقمية بين الأطفال والشباب، ومن مهامها أيضاً احتواؤها نظام شكاوى مكثف لمساعدة الأطفال والشباب؛ فإذا لم يلتزم موقع التواصل الاجتماعي بامتثال المعايير الواردة في مدونة قواعد الممارسة، فيمكن للفرد أن يلجأ إلى مفوض السلامة الرقمية، الذي يمكنه توجيه موقع التواصل الاجتماعي للامتثال للمعايير الواردة في المدونة. (خبرتيّ نيوزيلندا، أستراليا)

– رفع مستوى الوعي العام حول الأمن السيبراني باعتماد جهود الوقاية الاستباقية، وبمبادرات حكومية وطنية واسعة وخطط طويلة المدى. (ممارستيّ كوريا والولايات المتحدة الأمريكية)

–تبادل أفضل ممارسات الأمن السيبراني من خلال المشاركة في الندوات وورش العمل والمؤتمرات ذات الصلة. (ممارسة ماليزيا)

–الحوكمة الفعالة بوضع استراتيجية وخطة عمل لمعالجة المخاطر السيبرانية. (ممارسة ماليزيا)

– مراجعة جميع سياسات وإجراءات إدارة المخاطر السيبرانية في المدارس على الأقل كل سنتين. (ممارسة أستراليا)

– استحداث وظيفة (مرشد أو مستشار سيبرانية) ليُعَيَّن في المدارس وهو شخص يتمتع بسلامة كافية عبر الإنترنت ومعرفة وخبرة لتنسيق عمليات إدارة المخاطر السيبرانية؛ تكون مهمته تقديم المساعدة السيبرانية لطلاب المدرسة عند الحاجة (ممارسة ماليزيا وتايلاند)

–بدء البرامج التوعوية حول أمان الانترنت للأطفال في سن ما قبل المدرسة. (ممارسة إستونيا)

–الاستعانة بفريق عمل من بعض المتخصصين أكاديمياً مع معلمي المدارس الابتدائية لتحديد مدى ملاءمة مقاطع الفيديو التوعوية ووحدات تعليم الأمن السيبراني للفئات العمرية.

–تشجيع جميع المدارس والمحافظات على تناول مواضيع الأمن السيبراني وإدارة مخاطره

– توجيه القائمين على إدارة المخاطر السيبرانية من المعلمين والقيادة العليا في المدارس إلى التطبيق العملي للممارسات الجيدة من الاستخدامات الإيجابية للتقنيات الرقمية.

– الاهتمام بالجوانب الاجتماعية أكثر من الجوانب التقنية في الأمن السيبراني مثل تحضير الأطفال للمواقف التي قد يتعرضون لها على الإنترنت مثل ما يجب فعله إذا طلب شخص غريب الاجتماع وجهًا لوجه.

– إنشاء موقع تفاعلي مثيرًا لاهتمام الوالدين يحتوي على إرشادات للآباء –كملخص لشروحات قابلة للطباعة– في صورة كتاب إرشادي أو مقاطع فيديو ومقالات عن مستويات الاستخدام الصحي لأبنائهم للانترنت وكيفية مساعدة الأطفال في الأمان على الإنترنت، يعطي ذلك معلومات قيمة حول أدوات الرقابة الأبوية المتاحة ويعلمها، كما يعطي الموقع تلميحات حول التطبيقات التي قد يستخدمها أطفالهم، والمخاطر المرتبطة بها، ويشرح دور الآباء حسب عمر الطفل، ويساعد الآباء على تحديد التهديدات السيبرانية وإجراءات الإبلاغ عن تهديدات السلامة الإلكترونية (خبرتيّ أستراليا وماليزيا)

–تقديم المدارس دروساً ليلية للآباء والمعلمين حول الأمان عبر الإنترنت (ممارسة شمال كارولينا)

–أن يفرض على المعلمين التأكد من أن تتفق "بصماتهم الرقمية" من هوياتهم الشخصية على الإنترنت بما في ذلك مواقع الشبكات الاجتماعية مع دورهم كمعلمين، ومع أخلاقيات مهنة التدريس – والبصمة الرقمية هي الآثار التي يتركها شخص ما في البيئة الرقمية ويمكن تتبعها وتحليلها – (ممارسة جنوب أستراليا).

–توجيه المعلمين لدورهم كمسئولي توعية سيبرانية ليقوموا بـ:

*اغتنام فرص غير مقصودة؛ غير مخطط لها –كالأخبار في وسائل الإعلام – ويستخدمونها لإلهام التلاميذ حول كيفية البقاء بأمان عبر الانترنت.

* اتباع نموذج توعية التلاميذ بالعواقب المحتملة للاستخدام غير المسئول للانترنت.

* توجيه نظر التلاميذ إلى استمرارية المعلومات عبر الإنترنت.

* استخدام أسلوب القصة التربوية لقصص واقعية لأشخاص في الأخبار تأثروا سلبًا بعدم ممارسة الأمن السيبراني، وبقصص عن مراقبة الله وخشيته بالغيب.

– إظهار المعلم لتلاميذه الاهتمام الذاتي بتعلم كيفية التصرف بأمان عبر الإنترنت، فيقتدي به تلاميذه.

– تنمية مهاراته الخاصة بتوصيل القيم الثقافية والمعتقدات الدينية لتطوير مهارات المواطنة الرقمية (ممارسة السعودية)

–استهداف وزارة التربية والتعليم تنمية الكفاءة الذاتية والمسئولية الرقمية لتلاميذ المدارس.

–تنمية مهارات القرن الحادي والعشرين لدى التلاميذ الخاصة بمحو الأمية الرقمية؛ ليتم تعليمها للأطفال في التعليم الابتدائي، وليكونوا: التفكير الحاسوبي، المهارات الأساسية لتكنولوجيا المعلومات والاتصالات، محو الأمية الإعلامية، ومهارات المعلومات. (هولندا)

–توجيه المتخصصين إلى استخدام خطوات علمية مدروسة للمساعدة في عملية كتابة مناهج المواطنة الرقمية لبناء قدرات التلاميذ هي: تحديد الموظفين والتلاميذ وأولياء الأمور للعمل في لجنة كتابة المناهج، ومراجعة واستخدام المبادئ التوجيهية لمناهج المواطنة الرقمية التي وضعتها المدارس الأخرى، وإنشاء أسئلة أساسية لتوجيه عمل كتابة المناهج مثل: كيف يمكننا (أي فريق العمل والتلاميذ وأولياء الأمور والمجتمع) استخدام التكنولوجيا لتكون فعالة؟ كيف ندير المعلومات والأدوات لاستخدامها بأمان وفعالية وقانونية؟ مع ضرورة التخطيط لعملية مراجعة منهج المواطنة الرقمية كل عامين، وتوجيههم إلى ضرورة تماشي الأنشطة الحالية مع الاتجاهات الرقمية. (ولاية كونيتيكت الأمريكية)

–أن تتضمن مناهج تنمية قدرات التلاميذ في الأمن السيبراني ثماني فئات هي: أمان الإنترنت، الخصوصية والأمان، العلاقات والتواصل، التنمر عبر الإنترنت، البصمة الرقمية والسمعة، الصورة الذاتية والهوية، المعرفة المعلوماتية، والائتمان الإبداعي وحقوق التأليف والنشر؛ بإجمالي خمسة عشر درسًا لكل مستوى صف حتى الصف الثامن. (المنظمات الدولية)

– تقييم محتوى مناهج المواطنة الرقمية فتتم من قِبَل أربعة هيئات تدريسية ممن يتفاعلون مع تلاميذ المرحلة الابتدائية على أساس منتظم؛ ليتم التقييم حول معايير: (أ) قيمة العرض التقديمي للغرض المقصود، (ب) ملاءمة المواد للمستويات العمرية، (ج) احتمالية أن يشارك التلاميذ بنشاط، (د) الموضوعات التي ينبغي إضافتها أو حذفها.

–العمل على إكساب الطلاب الإحساس الشخصي بالخطأ؛ فقد نُقل عن كونفوشيوس قوله "إذا حكمت الناس لوجستيًا وتحكمت بهم من خلال العقاب سوف يتجنبون الجريمة، لكن

لن يكون لديهم إحساس شخصي بالعار أما إذا كنت تحكمهم عن طريق الفضيلة والسيطرة عليهم بلياقة، سوف يكتسبون إحساسهم بالرفض الاجتماعي والعار، وهكذا يصححون أنفسهم. (كونفوشيوس)

– عقد المدارس ورش عمل مع التلاميذ في المدارس حول الحقوق الرقمية بما في ذلك مخاطر وفوائد أن تكون متصلاً بالإنترنت (ممارسة اسكتلندا)

–توفير المدارس محتوى تفاعلي للطفل يتضمن ألعابًا أو اختبارات أو بطاقات نشاط تتوافق مع عمر الطفل، واستخدامها كمصادر خارجية لزيادة الوعي السيبراني للأطفال.

– تشجيع الجميع على لعب دور في تطوير بيئة صحية عبر الإنترنت من خلال الإبلاغ عن المحتوى المرفوض من خلال إنشاء خطوط ساخنة للإبلاغ (ممارسة الصين واليابان وكوريا)

– استحداث وظيفة مسؤول الموارد المدرسية School Resource Officers (SRO) في المدارس الابتدائية لتعتمد عليه المدرسة في المساعدة على التحقيقات؛ لتكون مهمته: استرداد المعلومات التي يمكن أن تساعد في التحقيق، وتثقيف التلاميذ فيما يتعلق بالعواقب القانونية للتنمر الإلكتروني. (ممارسة جنوب كاليفورنيا).

– تجنيد سفراء المشاهير للتحدث في التلفزيون والراديو عن حماية البيانات الشخصية.(ممارسة كوريا)

– إقامة مبادرات لحماية البيانات الشخصية باستخدام لافتات وإعلانات على قطارات الأنفاق والحافلات ومراكز التسوق وفي قاعات الألعاب.(ممارسة كوريا)

* معالجة المخاطر السيبرانية من خلال إلزامية الأنظمة التقنية لتقليل الألعاب (على سبيل المثال، إغلاق / حجب البرمجيات) ويمكن تفصيل الإجراءات المقترحة في ذلك الصدد على النحو التالي:

– تصفية الدولة لمحتوى جميع المواقع ذات المخاطر على النسق التربوي والأكاديمي للطلاب باستخدام أجهزة التوجيه والخوادم، ومراقبة مقدمي الخدمات (خبرتيّ الصين والسعودية)

–الاعتماد على تقنيات الحظر واستخدام خوادم تسيطر عليها الدولة (ممارسة السعودية)

-تثبيت آليات تتبع في المدارس بحيث تُطْلَق صفارات إنذار تحذيرية عند وصول التلاميذ أو العاملين بالمدرسة إلى مواقع غير مناسبة (ممارسة شيكاغو)

-اعتماد مخططات التصنيف عبر الانترنت من أجل تصنيف البرامج من حيث المحتوى الجنسي الصريح والعنف التصويري والألفاظ النابية القوية ؛ فكل موقع مصنف من (٠-٤)؛ لكي يقوم الآباء والمعلمون بتخصيص مستوى التصفية الذي يرغبون به. (ممارسة اليابان)

- تعليق أو تقييد أوقات اللعب بأن تغلق الألعاب من الساعة ١٢ صباحًا حتى الساعة ٦ صباحًا يوميًا.(ممارسة الصين)

- أن تُمنع مواقع الألعاب التفاعلية التلاميذ من ممارسة ألعاب الانترنت لأكثر من ٣ ساعات يوميا، وإجبارهم على أخذ استراحة كل ٤٥ دقيقةً، وإذا خالف الطفل لساعات أطول تؤدي إلى إلغاء التنشيط أو تعرض آليات المكافآت في اللعبة للخطر.(ممارسة الصين)

- منع وحدات تحكم الألعاب الأجنبية، مثل نظام Sony PlayStation من البيع التجاري في مصر.(ممارسة الصين)

- تقديم ترشيح مجاني للهواتف المحمولة لمعالجة مخاوف الوالدين وتطوير برامج التصفية بشكل دوري وتوزيعها مجانا على المدارس (ممارسة اليابان).

- تقديم برنامج ترشيح مجاني للهواتف المحمولة وبرامج تصفية وتوزيعه مجانًا على المدارس.(ممارسة اليابان)

- أن يشرع حظر تضمين الألعاب محتوى المقامرة أو المواد الإباحية أو العنف أو أي محتوى يعتبر انتهاكًا للقانون.(ممارسة الصين)

- وضع قيود استباقية على المواقع التكنولوجية، بحيث يُطالب الأطفال بأن يكون لديهم تطبيقات لتصفية المحتوى مثبتة على هواتفهم (ممارسة كوريا الجنوبية)

ب- إجراءات مقترحة لإدارة المخاطر السيبرانية. (على مستوى المدارس الابتدائية) وفقا للمارسات الدولية :

١-تحديد المخاطر السيبرانية:

(أ)-اتخاذ نسب بعض الظواهر المرتبطة مؤشراً لتحديد المخاطر السيبرانية.

(ب)- إيلاء مهمة تحديد المخاطر السيبرانية للآباء مع توفير سبل المساعدة.

(ج)- مطابقة الوضع الحالي لاستخدام أطفال المدارس للانترنت بمؤشرات الاستخدام الصحي للانترنت.

(د)- إجراء مسح داخلي وخارجي في المدارس الابتدائية للمخاطر السيبرانية.

(هـ)- تحديد آليات مدرسية للكشف المبكر عن المخاطر السيبرانية.

(و)-استعانة إدارة المدرسة بالخبراء عند تحديد المخاطر السيبرانية.

(ز)-استخدام إدارة المدرسة أسلوب SWOT عند تحديد المخاطر السيبرانية.

(ح)-استعانة إدارة المدرسة بأصحاب المصلحة للمساندة في تحديد المخاطر السيبرانية.

(ط)-حرص إدارة المدرسة على تحديد سياق إدارة المخاطر السيبرانية.

٢-تحليل المخاطر السيبرانية:

(أ)-أن تحتفظ إدارة المدرسة بقاعدة بيانات تتضمن معلومات عن المخاطر السيبرانية التي يتعرض لها الطلاب.

(ب)-أن تحلل إدارة المدرسة المخاطر باستخدام أدوات مناسبة.

(ج)- أن تدرس إدارة المدرسة العوامل المسببة للمخاطر السيبرانية.

(د)- أن تدرس إدارة المدرسة تأثير المخاطر السيبرانية على الأهداف الاستراتيجية للمدرسة.

(هـ)- أن تدرس إدارة المدرسة العواقب المحتملة للمخاطر السيبرانية.

(و)- أن تدرس إدارة المدرسة الضوابط الوقائية التي يمكن وضعها لتقليل احتمالية حدوث المخاطر السيبرانية.

(ز)-تعِد إدارة المدرسة إستراتيجية واضحة لإدارة المخاطر السيبرانية

(ح)-تهتم إدارة المدرسة بتكاملية المعلومات الخاصة بإدارة المخاطر السيبرانية.

٣-تقييم المخاطر السيبرانية:

(أ)- أن تقوم إدارة المدرسة بتقييم الآثار المحتملة للمخاطر السيبرانية على البيئة المدرسية.

(ب)- أن تقوم إدارة المدرسة بجدولة المخاطر السيبرانية وفقا للأشد خطراً فالأقل.

(ج)- أن تقوم إدارة المدرسة بتقييم نقاط القوة في التعامل مع المخاطر السيبرانية.

(د)- أن تقوم إدارة المدرسة بتقييم التهديدات الحالية.

(هـ)-أن تستعين إدارة المدرسة بمتخصصين عند إعداد خطط إدارة المخاطر السيبرانية.

(و) -أن تحلل إدارة المدرسة عوامل التخفيف المنفذة.

(ز)-أن تقارن إدارة المدرسة احتمالية حدوث المخاطر السيبرانية الحالية بتقييم الاحتمالية المسبق لها.

(ح)-أن تضع المدرسة الخطط بناء على تحليل الاحتمالية.

٤-الاستجابة للمخاطر السيبرانية على مستوى المدارس الابتدائية:

وذلك كما في الجدول التالي:

المخاطر	استراتيجيات الاستجابة للمخاطر	الإجراءات المقترحة للاستجابة للمخاطر
(أ) إدمان الانترنت	(١)استراتيجية الإنهاء/ التجنب	١-أ-بناء قدرات أولياء الأمور كمسئولي توعية لإدارة المخاطر السيبرانية. - توفير الموارد التعليمية في المدارس لأولياء الأمور، لتوعيتهم بالمعلومات العلمية عن مستويات الاستخدام الصحي لأبنائهم للانترنت: لتكون على النحو التالي: * لا ينبغي توفير أي وقت أمام الشاشة للأطفال أقل من عام واحد، أما الأطفال الذين تتراوح أعمارهم بين (٢-٤) أعوام الحد الأقصى لهم ساعة واحدة يوميا؛ ويجب خلالها على البالغين من أفراد الأسرة مشاهدة الشاشات مع الأطفال لتمكينهم من فهم ما يشاهدون؛ فيجب تنظيم الاستخدام اليومي لمدة لا تزيد عن ساعة واحدة لمدة ٥ مرات في الأسبوع. * العلم بأن مقدار الاستخدام المؤذي أو المكثف للإنترنت بواقع ٤ ساعات يوميًا أو ٣٠ ساعة أسبوعياً؛ ليكون الاستخدام الصحي ساعة واحدة يومياً لمدة ٥ مرات في الأسبوع. * الالتزام بالتقييد الرسمي لسن عمل حساب على وسائل التواصل الاجتماعي عند بلوغ ١٣- ١٦ عامًا. * إيقاف تشغيل إشعارات تطبيقات الوسائط الاجتماعية للأبناء للمساعدة في تقليل الإلهاءات.

المخاطر	استراتيجيات الاستجابة للمخاطر	الإجراءات المقترحة للاستجابة للمخاطر
		* إدراك العلامات الأساسية لإدمان الانترنت، واقتراح أنشطة بديلة. * التركيز على المهمة عند البحث في الانترنت وعدم الإلهاء بغيرها. * التفاوض مع الأبناء في أوقات خالية من الشاشة مثل أوقات الوجبات وقبل النوم بساعة. * ضبط الجهاز للوصول إلى الانترنت فقط خلال ساعات معينة. (توصيات اليونيسيف) – تشجيع المدارس للآباء على التواصل ومتابعة استخدام الإنترنت باعتبار ذلك أداة واعدة للآباء للمساهمة –بشكل ملحوظ– في تقليل مخاطر الاستخدام القهري للإنترنت.(هولندا) – تشجيع المدارس للآباء على الجمع بين الأشكال المتنوعة للوساطة الأبوية من: وساطة تقنية، ووساطة تقييدية –بتوفير قواعد للوقت والمواقع والمحتوى المسموح به– ووساطة المشاهدة المشتركة، ووساطة بناء عادات جيدة، والوساطة النشطة –ببناء علاقة ثقة مفتوحة حول التكنولوجيا، والمراقبة بطريقة حازمة غير مخيفة، وتوجيههم بطريقة صحيحة وتعريفهم بعواقب الاستخدام السيء–. – تشجيع المدارس للآباء على تزويد الأنشطة العائلية في الهواء الطلق، وممارسة التلاميذ للرياضة أو القراءة أو ألعاب الطاولة. ١–ب بناء قدرات المعلمين كمسئولي توعية لإدارة المخاطر السيبرانية. – تشجيع المعلمين على حضور برامج التطوير المهني للتوعية بأمان الإنترنت؛ لتثقيف المعلمين حول المخاطر المحتملة المرتبطة بالإنترنت. –تدريب المعلمين على دورهم كمسئولي توعية سيبرانية ، كما يوفر لهم الأدوات المناسبة لاستخدامها. (ممارسة أستراليا، وشمال كارولينا) ١–ج بناء قدرات الطلاب لإدارة المخاطر السيبرانية. –إقامة برامج تربوية نفسية تستمر من ٣ إلى ٦ أسابيع للأطفال في سن المدرسة؛

المخاطر	استراتيجيات الاستجابة للمخاطر	الإجراءات المقترحة للاستجابة للمخاطر
		لتقديم المعلومات حول مخاطر الإفراط في استخدام الانترنت، وتقنيات ضبط النفس، ومهارات تحديد وإدارة الوقت، والأنشطة البديلة. (خبرتيّ كوريا والصين). – أن تطلب المدرسة من بعض التلاميذ إنشاء مقاطع فيديو في مدرستهم بمساعدة المعلمين لإرشاد زملائهم لمنع إدمان الانترنت؛ فتُستخدم كتدخلات مدرسية لها نتائج جيدة. – جهود استباقية للمدرسة بتوفير دورات توعية حول الاستخدام الصحي ومقداره وكيفيته، توفير معسكرات آمنة في الإجازة الصيفية وفتح أبواب المدارس للأنشطة الصيفية مع توفير الإمكانات للأنشطة المختلفة والمكتبات ومدربي الرياضات المختلفة. –إقامة ورش عمل موجزة عن خطورة الاستخدام المتواصل للألعاب أو الإنترنت كاضطراب (ممارسة إسبانيا).
	(٢)استراتيجية المعالجة	٢–أ معالجة المخاطر السيبرانية من خلال حظر استخدام الطلاب للأجهزة اللوحية في المدارس. ٢–ب معالجة المخاطر السيبرانية من خلال برامج التدخل المبكر في المدرسة ومعسكرات العلاج من إدمان الانترنت: – إقامة معسكرات لتلاميذ المدارس لعلاج إدمان الانترنت بإجبارهم على الانخراط في الأنشطة البدنية (ممارسة الصين) –جهود علاجية بتوفير مراكز علاج إدمان الانترنت (الصين وكوريا)
(ب)التنمر الإلكتروني	(١)استراتيجية الإنهاء/ التجنب	١–أ وضع بروتوكول لانضباط المدارس محدد فيه عواقب المخاطر السيبرانية. – أن يخوَّل لمدير المدرسة سلطة تعليق أو استبعاد أي طالب من الحضور في المدرسة إذا كان الطالب يتصرف عبر الإنترنت بطريقة تهدد رفاهية طالب أو ولي أمر أو عضو المجتمع المدرسي حتى لو حدث هذا خارج موقع المدرسة و/ أو

المخاطر	استراتيجيات الاستجابة للمخاطر	الإجراءات المقترحة للاستجابة للمخاطر
		خارج ساعات المدرسة. (ممارسة أستراليا) – تطبيق مصفوفة الانضباط بالمدارس مع توجيههم إلى ممارسة التأديب التدريجي لتحديد العواقب حسب الاقتضاء والضرورة من الإنذار بالتعليق إلى الطرد حسب خطورة الحادث (ممارسة كاليفورنيا). ١–ب دمج المواطنة الرقمية في المناهج الدراسية. –اعتماد مناهج تبين للطلاب حقوقهم وواجباتهم في العالم الرقمي. – إنشاء برامج تعليمية عن التسلط عبر الانترنت وأمان الانترنت على مستوى المدارس الابتدائية (ممارسة إستونيا، وبعض الولايات في الولايات المتحدة الأمريكية) ١–ج بناء قدرات أولياء الأمور كمسئولي توعية لإدارة المخاطر السيبرانية. – تفعيل مواقع تفاعلية وكتيبات للآباء تابعة لوزارة التربية والتعليم تحتوي إرشادات تساعد الآباء على تحديد التهديدات السيبرانية وإجراءات الإبلاغ عن تهديدات السلامة الإلكترونية (خبرتيّ أستراليا وماليزيا) –أن يتعلم الوالدين إقناع الطفل بإبلاغها بأي تنمر يتعرض له، وإقناعه بأنه سيكون موجوداً في أي وقت لحمايته. ١–د بناء قدرات المعلمين كمسئولي توعية لإدارة المخاطر السيبرانية. – تشجيع المعلمين على حضور برامج التطوير المهني للتوعية بأمان الإنترنت؛ لتثقيف المعلمين حول المخاطر المحتملة المرتبطة بالإنترنت. –تدريب المعلمين على دورهم كمسئولي توعية سيبرانية ، كما يوفر لهم الأدوات المناسبة لاستخدامها. (ممارسة أستراليا، وشمال كارولينا) ١–هـ بناء قدرات التلاميذ تحقيقا للكفاءة الذاتية لإدارة المخاطر السيبرانية. – استخدام لعب الأدوار في المدرسة لأنه يتيح للتلاميذ معرفة كيف يمكن أن يشعر شخص آخر عند عكس الأدوار؛ للتفكير في ما سيشعرون به إذا قام شخص ما بنفس الأشياء لهم، وتوفر لهم هذه الطريقة الإبداع والقليل من المرح والمحافظة على

المخاطر	استراتيجيات الاستجابة للمخاطر	الإجراءات المقترحة للاستجابة للمخاطر
		مشاركة التلاميذ في العملية. (ممارسة الولايات المتحدة الأمريكية) – اختيار مجموعة من تلاميذ الفصول كمشاركين نشطين في جهود مكافحة التسلط عبر الإنترنت بناءً على تأثيرهم على التلاميذ الآخرين وأن يكونوا قدوة إيجابية لضمهم في برنامج لتعليمهم أن يكونوا مسؤولين في المدرسة ؛ فيتم تدريب هؤلاء التلاميذ على تحديد التنمر السيبراني واستخدام استراتيجيات نزع فتيل المواقف، ومصادقة التلاميذ الذين قد لا يكون لديهم الكثير من الأصدقاء، فيجتمعون بانتظام مع المعلمين لإبلاغ الإدارة بنظرة ثاقبة لما يواجهه التلاميذ والقضايا التي تؤثر عليهم والعلامات الأولية للتسلط والإبلاغ عن الحوادث.(ممارسة جنوب كاليفورنيا). –تنمية مهارات الثقة بالنفس وضبط النفس وحفظ أدلة التنمر السيبراني والإبلاغ عبر المواقع من خلال دورات مكثفة. – تعليم التلاميذ حقوقهم وحقوق الآخرين، وتعلم التواصل باحترام. (اليونيسيف) – تعليم التلاميذ أن يفكروا بعناية قبل أن ينشروا أي شيء على الإنترنت. – تعليم التلاميذ احترم آراء الآخرين حتى لو كانت لا تتفق مع آرائهم وألا يكونوا وقحين في الجدال. – تعليم التلاميذ إذا رأوا شيئًا على الإنترنت جعلهم يشعرون بعدم الارتياح أو عدم الأمان أو القلق: أن يتركوا الموقع، ويقوموا بإيقاف التشغيل، وإخبار شخص بالغ موثوق به على الفور . – تعليم المتنمرين عبر الانترنت في المدارس أساليب المواجهة الأخرى، مثل التسوية والتفاوض للحصول على ما يريدون كي لا يلجئوا للعدوان. –تعليم التلاميذ جمع الأدلة على مواد التسلط عبر الانترنت مثل لقطات الشاشة. (اليونيسيف) –تعليم الطفل عدم الرد على التنمر السيبراني كي لا يؤجج الموقف. (اليونيسيف) – تعليم الطفل إبلاغ المسؤول عن الموقع بأي هجوم يمكن اعتباره تنمرًا.

المخاطر	استراتيجيات الاستجابة للمخاطر	الإجراءات المقترحة للاستجابة للمخاطر
		– تعليم الطفل ألا ينزعج إذا غادر الآخرون مجموعته، فلا يريد الجميع نفس المعلومات. – تعليم الطفل أن يعذر نفسه بأدب قبل مغادرة المجموعة. – تعليم الطفل ألا ينشر في أي مجموعة دردشة بين الساعة ٢٠:٠٠ والساعة ٠٨:٠٠ ما لم تكن حالة طارئة.
	(٢)استراتيجية المعالجة	–إنشاء نظام شكاوى مكثف في المدارس لمساعدة من يتعرضون للتنمر (ممارسة أستراليا)
(ج)مشاهدة عناصر غير لائقة	(١)استراتيجية الإنهاء/ التجنب	١–أ دمج المواطنة الرقمية في المناهج الدراسية. – دمج التثقيف التوعوي لتعزيز الوعي الجنسي لأطفال المدارس الابتدائية من خلال تضمينه في المناهج. ١–ب بناء قدرات أولياء الأمور كمسئولي توعية لإدارة المخاطر السيبرانية. – تدريب أولياء الأمور على استخدام برامج حجب المحتوى الإباحي للآباء وتصفية المواقع غير المرغوب فيها. – تدريب أولياء الأمور على استخدام برامج تعتيم الشاشة كل ٣ دقائق إذا كان يكتشف أن المستخدم يزور مواقع غير مشروعة. – توجيه أولياء الأمور إلى الحرص ألا يكون للطفل هاتف شخصي "ذكي" دون سن ١٤ عاما . – توجيه أولياء الأمور إلى أن يثيروا موضوع المواد الإباحية بأنفسهم؛ فيوصي خبراء التربية ببدء المحادثة مبكرًا (بحلول الوقت الذي يبلغون فيه حوالي ٩ سنوات) للمساعدة في حمايتهم من التأثيرات المحتملة لمواجهته بطريق الخطأ. (اليونيسيف) – توجيه أولياء الأمور إلى استخدام الأجهزة في المناطق المفتوحة المشتركة من

المخاطر	استراتيجيات الاستجابة للمخاطر	الإجراءات المقترحة للاستجابة للمخاطر
		المنزل.(اليونيسيف) – توجيه أولياء الأمور إلى استخدام ميزة قفل رمز PIN على أجهزة التلفزيون الذكية.(اليونيسيف) – توجيه أولياء الأمور إلى أن يقوموا بدورهم نحو بناء شخصية الطفل القادر على الاختيار الجيد للمضامين التي يتعرض لها عبر الانترنت ومناقشته في اختياراته بل توجيهه إذا استلزم الأمر. – توجيه أولياء الأمور إلى تنمية الوعي الديني للطالب والعمل على زيادة الوازع القيمي والضمير للعمل كأسلوب توجُّه داخلي للفرد لمنع الوقوع في الآثام. – توجيه أولياء الأمور إلى تخصيص ساعة أسبوعياً تلتقي فيها الأسرة حول مائدة النقاش وتبادل الرأي حول ما تم التعرض له من خلال مختلف الوسائل الاتصالية. ١–ج– بناء قدرات المعلمين كمسئولي توعية لإدارة المخاطر السيبرانية. –تشجيع المعلمين على حضور برامج التطوير المهني للتوعية بأمان الإنترنت؛ لتثقيف المعلمين حول المخاطر المحتملة المرتبطة بالإنترنت، مثل مخاطر المحتوى وسرقة الهوية والتسلط عبر الإنترنت والخداع والاتصال غير المناسب، وتوفير الأدوات المناسبة لهم لاستخدامها. (ممارسة أستراليا، وشمال كارولينا) ١–د –بناء قدرات التلاميذ تحقيقا للكفاءة الذاتية لإدارة المخاطر السيبرانية. –إقامة برامج تدريبية على مستوى المدرسة حول عواقب مخاطر مشاهدة عناصر غير لائقة. – إقامة ندوات توعوية للتلاميذ؛ مساعدةً في تطوير تفكيرهم النقدي وقدرتهم على اتخاذ خيارات جيدة؛ فمن المستحيل المراقبة المستمرة لهم في العالم السيبراني. –التركيز على القصص التربوية والنموذج القدوة.
	(٢)استراتيجية المعالجة	٢–أ معالجة المخاطر السيبرانية من خلال حظر استخدام الطلاب للأجهزة اللوحية في المدارس.

المخاطر	استراتيجيات الاستجابة للمخاطر	الإجراءات المقترحة للاستجابة للمخاطر
		– فرض حظر على استخدام تلاميذ المدارس الذين تتراوح أعمارهم بين ٣ و ١٥ عامًا للهواتف الذكية والأجهزة اللوحية أثناء التواجد في المدرسة، بما في ذلك أيضاً فترات الراحة ووقت الغداء (ممارسة فرنسا وبريطانيا). – أن يكون للمدرسة الحق في مراقبة واعتراض الاتصالات الإلكترونية؛ وعلى الطالب المشتبه في استخدامه جهازًا إلكترونيًا بالمخالفة لهذه الشروط أن يخضع لإجراءات تأديبية لسوء السلوك، بموجب قانون المدرسة؛ وفي حالة صدور حكم بالإدانة، قد يفقد الطالب الحق في حمل جهاز إلكتروني في المدرسة بالإضافة إلى أي لوم آخر؛ وتنطبق هذه القواعد على استخدام أي جهاز إلكتروني مملوك للمدرسة أو موجود في مبنى المدرسة، أو أي جهاز إلكتروني قيد الاستخدام سواء كان الجهاز مرتبط بمزود خدمة المدرسة على حساب المدرسة أم لا (ممارسة كينيا) ٢–ب معالجة المخاطر السيبرانية من خلال التقيد بنظام التحقق من العمر. – إنشاء نظام التحقق من العمر يعتمد على بطاقة الهوية أو رقم جواز السفر مقرونًا بالرمز البريدي يستخدمها الأطفال من سن السادسة لمنع وصول القاصرين إلى المحتوى المقيّد بالفئة العمرية عبر الإنترنت. (ممارسة ألمانيا وبلجيكا) ٢–ج معالجة المخاطر السيبرانية من خلال توفير المنصات البيضاء ومستشارين للطلاب. – تفعيل منصة تعليمية تابعة لوزارة التربية والتعليم للوصول إلى الإنترنت عبر الهاتف المحمول على الصعيد الوطني للقصر؛ لتحوي قائمة بيضاء بمواقع الويب المحددة والمعتمدة مسبقًا جاهزة للاستخدام عند عودة الأطفال إلى المدرسة بعد العطلة الصيفية. (ممارسة الصين وماليزيا وأستراليا ونيوزيلندا)
(د)الاستمالة	(١)استراتيجية الإنهاء/	١–أ– دمج المواطنة الرقمية في المناهج الدراسية. ١–ب– بناء قدرات أولياء الأمور كمسئولي توعية لإدارة المخاطر السيبرانية.

المخاطر	استراتيجيات الاستجابة للمخاطر	الإجراءات المقترحة للاستجابة للمخاطر
	التجنب	–توجيه المدارس لأولياء الأمور من خلال ورش العمل والبرامج التدريبية بالانتباه لأي شخص بالغ حصل على مكانة بارزة في حياة الطفل أو يبدو الآن أنه بطل في نظر الطفل. –توجيه المدارس لأولياء الأمور من خلال البرامج التدريبية بالانتباه لعلامات الاستمالة وهي: أن ينسحب الطفل–أو يتلقى مكالمات في أوقات غريبة من اليوم أو يتلقى هدايا من أشخاص لا يعرفهم ، فضلاً عن بدء الطالب في عزل نفسه عن الأصدقاء والعائلة. – تعريف أولياء الأمور على سلوكيات المستميلين بما يساعد على تجنب وقوع أبنائهم ضحية. ١–ج– بناء قدرات المعلمين كمسئولي توعية لإدارة المخاطر السيبرانية. ١–د –بناء قدرات التلاميذ تحقيقا للكفاءة الذاتية لإدارة المخاطر السيبرانية. –استخدام لعب الأدوار طريقة تدريس فعالة للسلامة على الإنترنت؛ حيث يمكن للتلاميذ الأكبر سنًا تعليم التلاميذ الأصغر سنًا عن الاستمالة كأن يعطى التلاميذ الأكبر سنًا مصاصات التلاميذ الأصغر سنًا ثم يطلبون منهم معلوماتٍ شخصية عنهم. – توعية التلاميذ بـ: *الالتزام بالتقييد الرسمي لسن عمل حساب على وسائل التواصل الاجتماعي عند بلوغ ١٣– ١٦ عامًا. * حذف طلبات الصداقة من الغرباء، وحذف الأصدقاء الذين لا يعرفهم. * العواقب المحتملة لإرسال أو مشاركة صور عارية. لتشمل هذه المخاطر: +فقدان السيطرة على الصورة، حتى في العلاقات الموثوقة. +ضغط الأقران بعدم احترامهم لهذا الفرد. + الأذى النفسي والعاطفي، بما في ذلك الإذلال والتنمر والمضايقة أو الإضرار

المخاطر	استراتيجيات الاستجابة للمخاطر	الإجراءات المقترحة للاستجابة للمخاطر
		بسمعتهم. +التهم الجنائية أو العقوبات في بعض القضايا – على وجه الخصوص – وتشمل مشاركة الصور الحميمة بالتراضي. * أن المعلومات سلعة لذا وجب الحد من عرض المعلومات ؛ فعند رفع الطالب الصور لنفسه على مواقع التواصل الاجتماعي؛ فالصورة تساوي حقًا ألف كلمة لأي شخص مفترس عبر الإنترنت، إذا رفع الطفل صورة لنفسه واقفًا أمام منزله؛ يظهر مع المنزل ورقم إشارة الشارع، مرتديًا قميص فريق المدرسة، يمكن لأي مجرم العثور على ثروة من المعلومات؛ فالصورة قد تكشف ■:الموقع ■الوضع الاقتصادي ■المدرسة ■العمر والمظهر ■لغة الجسد التي يمكن أن تكشف عن الضعف العاطفي. * استمرارية المعلومات عبر الانترنت؛ مثلما فعلت إحدى معلمات الصف السادس من أوكلاهوما والتي قامت بإنشاء علامة تفيد بأن تلاميذها يعتقدون بأنه من المقبول نشر صور غير لائقة لأنفسهم عبر الإنترنت، ثم طلبت من مجتمع Facebook مشاركتها وفي غضون ساعات وصلت إلى جميع الولايات الخمسين وعدة دول .ثم حذفت المنشور، لكن واصل التعميم .واستغلت تلك اللحظة لتعليم تلاميذها بصمتهم الرقمية، وكيف لا يمكن محوها بالكامل. * ضرورة تمسكهم بجرعة صحية من الشك في التعامل مع هذه التمثيلات الزائفة؛ فقد لا يكون الآخرون كما يدّعون. * التحدث إلى الوالدين حول الأشخاص الذين يقترحون مقابلتهم.
	(٢)استراتيجية المعالجة	–إنشاء نظام شكاوى مكثف في المدارس لمساعدة من يتعرضون للاستمالة (ممارسة أستراليا).

٥-متابعة المخاطر السيبرانية وتحديث إدارتها:

(أ)- أن تجري إدارة المدرسة تقويما مستمرا لأساليب التخطيط المتبعة في الكشف المبكر عن المخاطر السيبرانية.

(ب)- أن تجري إدارة المدرسة مراجعة دورية لأساليب إدارة مخاطرها السيبرانية.

(ج) -أن تُقَيِّم إدارة المدرسة خطط إدارة المخاطر السيبرانية بقصد تطويرها.

(د)- أن تتابع إدارة المدرسة نتائج إستراتيجيات التحديث المتخذة في مواجهة المخاطر السيبرانية.

(هـ)- أن تتابع إدارة المدرسة نتائج إستراتيجيات الوقاية المتخذة في مواجهة المخاطر السيبرانية.

(و)- أن تعيد إدارة المدرسة تقييم احتمالية المخاطر السيبرانية بعد اتخاذ بعض إستراتيجيات الاستجابة.

(ز)- أن تقوم إدارة المدرسة بتجديد قاعدة البيانات حسب ما يستجد من مخاطر سيبرانية.

المراجع العربية:

إبراهيم، عيده .(٢٠١٩، أبريل). إدارة المخاطر مدخل لتعزيز تنافسية الجامعات المصرية: تصور مقترح، *دراسات في التعليم الجامعي*، كلية التربية – جامعة عين شمس، مركز تطوير التعليم الجامعي، (٤٣).

ابن الجوزي، جمال الدين أبي الفرج .(٢٠١٢). *صفوة الصفوة*، تحقيق: طرطوسي، خالد، دار الكتاب العربي، لبنان.

أبو بكر، منى محمود .(٢٠١٧، يونية). تصور مقترح لمواجهة إدمان الألعاب الإلكترونية في المرحلة الابتدائية بالمملكة العربية السعودية في ضوء خبرتيّ كل من الولايات المتحدة الأمريكية وكوريا الجنوبية، *مجلة التربية المقارنة والدولية*، الجمعية المصرية للتربية المقارنة والإدارة التعليمية، ٣(٧).

الألباني، أبو عبد الرحمن محمد ناصر الدين .(١٩٨٨). *صحيح الجامع الصغير وزياداته*، الجزء الأول، ط٣، المكتب الإسلامي، لبنان.

المدرع، سفر بخيت .(٢٠١٩). تقويم إدارة مخاطر الموارد البشرية بالجامعات السعودية وفقا لمعيار المنظمة الدولية للمعايير لإدارة الخطر (ISO 31000: 2018). دراسة مقارنة بين الجامعات الحكومية والأهلية. *مجلة كلية التربية (أسيوط)*, ٣٥(٥), ٥٢-١٠٣.

جامعة بورسعيد .(٢٠١٧). الخطة الإستراتيجية لجامعة بورسعيد ٢٠١٧-٢٠٢٢، جامعة بورسعيد، ص ص ١-١٧٢.

جمهورية مصر العربية، الجهاز المركزي للتعبئة والإحصاء .(٢٠٢٠). *مصر في أرقام (التعداد)*. الجهاز المركزي للتعبئة والإحصاء، القاهرة.

جمهورية مصر العربية، الجهاز المركزي للتعبئة والإحصاء .(٢٠٢١، يناير). *مصر في أرقام (السكان)*. الجهاز المركزي للتعبئة والإحصاء، القاهرة.

جمهورية مصر العربية، رئاسة الجمهورية: قانون رقم ١٣٩ لسنة ١٩٨١ بإصدار قانون التعليم ، **أحدث تعديلاته بتاريخ ٨ أبريل ٢٠١٩ بالقانون ١٦ لسنة ٢٠١٩،** وزارة التربية والتعليم ، التشريعات واللوائح التى تحكم أنشطة العمل بوزارة التربية والتعليم.

جمهورية مصر العربية، رئاسة الجمهورية. (٢٠٠٦، ١٥ يولية). قانون رقم ١٤٧ لسنة ٢٠٠٦ ببتعديل بعض أحكام قانون العقوبات، الجريدة الرسمية، ع ٢٨ مكرر.

جمهورية مصر العربية، وزارة الاتصالات وتكنولوجيا المعلومات. (يونيو ٢٠١٢). الإستراتيجية القومية للاتصالات وتكنولوجيا المعلومات ٢٠١٤-٢٠١٧ المجتمع الرقمي في ظل اقتصاد المعرفة، وزارة الاتصالات وتكنولوجيا المعلومات، القاهرة.

جمهورية مصر العربية، وزارة التخطيط والمتابعة والإصلاح الإداري .(٢٠١٨، مايو). *الخطة متوسطة المدى للتنمية المستدامة ٢٠١٨/٢٠١٩-٢٠٢١/٢٠٢٢*، وزارة التخطيط والمتابعة والإصلاح الإداري، القاهرة.

جمهورية مصر العربية، وزارة التربية والتعليم (٢٠١٤). الخطة الإستراتيجية للتعليم قبل الجامعي ٢٠١٤-٢٠٣٠، التعليم المشروع القومي لمصر، وزارة التربية والتعليم، القاهرة.

حجازي، نهاد فتحي. (٢٠١٨، يناير). *القيم التي تعكسها الألعاب الإلكترونية وتأثيرها على الأطفال دراسة مسحية*، دار العلوم، القاهرة.

الحراحشة، محمد. (٢٠١٩). درجة تطبيق إدارة المخاطر في مدارس المرحلة المتوسطة في دولة الكويت، رسالة ماجستير، كلية العلوم التربوية، جامعة آل البيت، الأردن.

حريري، رندة ؛ المنتشري، فاطمة .(٢٠٢٠، يوليو). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، *المجلة العربية للتربية النوعية*، ٤(١٣).

حشيش، نشرين. (٢٠١٨). مهارات المواطنة الرقمية اللازمة لتلاميذ مرحلة التعليم الأساسي، *دراسات في التعليم الجامعي*، جامعة عين شمس، (٣٩).

الخليفة، نورة والعبيكان، ريم .(٢٠١٩). تحليل محتوى كتب الحاسب وتقنية المعلومات للمرحلة الثانوية بالمملكة العربية السعودية في ضوء أبعاد المواطنة الرقمية لمنظمة تعليم الفطرة السلمية Education Sense Common ، *رسالة الخليج العربي*، مكتب التربية العربي لدول الخليج، ٤٠(١٥١).

الخياط، أحمد. (٢٠١٩، ديسمبر). تصور مقترح لتطوير إدارة الأعمال في ضوء مدخل إدارة المخاطر بمؤسسات الأعمال الكويتية، *المجلة العلمية للاقتصاد والتجارة*، كلية التجارة–جامعة عين شمس، (٤).

خيري، السيد.(١٩٩٩). *الإحصاء في البحوث النفسية*، دار الفكر العربي، القاهرة.

الريح، موسى. (٢٠١٩). الاتجاهات الحديثة للمراجعة الداخلية ودورها في تفعيل إدارة المخاطر: دراسة ميدانية على عينة من المصارف السودانية، رسالة ماجستير، كلية الدراسات العليا بجامعة النيلين بالخرطوم.

الزهراني، معجب. (٢٠١٩). إسهام المدرسة في تحقيق المواطنة الرقمية لدى طلابها في ظل التحديات المعاصرة، *المجلة التربوية* – جامعة سوهاج، (٦٨).

شفيق، حسنين. (٢٠١٤). *مستجدات الإعلام الجديد والتحولات المستقبلية*. دار فكر وفن، القاهرة.

عبد الرازق، ابتسام ؛ نصر، نوال ؛ حسن، سماح. (يناير ٢٠٢٠). تفعيل التربية على المواطنة الرقمية بمدارس الحلقة الثانية من التعليم الأساسي على ضوء خبرات بعض الدول الأجنبية، *مجلة البحث العلمي* في التربية، كلية البنات للآداب والعلوم والتربية– جامعة عين شمس، ١(٢١).

عبد العزيز، عبدالعاطي حلقان .(٢٠١٦). تعليم المواطنة الرقمية في المدارس المصرية والأوروبية: دراسة مقارنة، *المجلة التربوية*، جامعة سوهاج، (٤٤).

عبيدات، ذوقان .(٢٠٠٠). *البحث العلمى مفهومه وأداوته وأساليبه* ، دار أسامة للنشر والتوزيع، عمان.

العصيمي، عبد المحسن. (٢٠٠٤). *الآثار الاجتماعية للانترنت*، دار قرطبة، الرياض.

العياشي، وردة .(٢٠١٦، سبتمبر). إدارة المخاطر والاستراتيجيات المستقبلية دراسة حالة شركة المعادن بالمملكة العربية السعودية، *دراسات قانونية*، مركز البصيرة للبحوث والاستشارات والخدمات التعليمية، ع ٢٣.

قارة عشرة، نصر الدين وحبار، عبد الرازق .(٢٠٢٠). إدارة مخاطر الائتمان باستخدام الحوكمة معيار كفاءة رأس المال التوريق المشتقات الائتانية، *مجلة الريادة لاقتصاديات الأعمال*، ٦(٢)، جامعة حسيبة بن بو علي الشلف.

القريوتي، محمد قاسم ؛ زويلف، مهدي حسن .(١٩٩٣). *المفاهيم الحديثة في الإدارة*، ط ٣، المكتبة الوطنية، عمان.

لوفيل، ك.؛ لوسون، ك.س. (١٩٨١). حتى نفهم البحث التربوي، *ترجمة عميرة، إبراهيم بسيوني*، ط٣، دار المعارف، القاهرة.

محافظة بورسعيد، جهاز شئون البيئة .(٢٠٠٧). *التوصيف البيئي لمحافظة بورسعيد*، جهاز شئون البيئة، بورسعيد.

محافظة بورسعيد، مديرية التربية والتعليم، إدارة قياس الجودة .(٢٠١٤، ديسمبر). الرؤية والرسالة والأهداف، مديرية التربية والتعليم، بورسعيد.

المخلفي، تركي .(٢٠١٩، يناير). درجة تطبيق إدارة المخاطر لدى قادة المدارس الحكومية في منطقة القصيم، *مجلة القراءة والمعرفة*، كلية التربية–جامعة عين شمس، (٢٠٧).

المدرع، سفر .(٢٠١٩، مايو). تقويم إدارة مخاطر الموارد البشرية بالجامعات السعودية وفقاً لمعيار المنظمة الدولية للمعايير لإدارة الخطر ISO 31000: 2018 دراسة مقارنة بين الجامعات الحكومية والأهلية، *مجلة كلية التربية–جامعة أسيوط*، ٣٥(٥).

مرعي، دينا عمر. (٢٠١٣). *مكافحة المواقع الإباحية على شبكة الانترنت المشكلة والتأثير وأساليب المكافحة*. دار العالم العربي، القاهرة.

المنتشري، فاطمة. (٢٠٢٠، يوليو). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، *المجلة العربية للعلوم التربوية والنفسية*، ٤(١٧).

ناصف، مرفت صالح. (٢٠١٢، نوفمبر). إدارة المخاطر مدخل لتحقيق سلامة المدارس الثانوية الصناعية في جمهورية مصر العربية. التربية:المجلس العالمي لجمعيات التربية المقارنة – الجمعية المصرية للتربية المقارنة والإدارة التعليمية، ١٥(٣٨).

النجار، عمر والفرا، ماجد. (٢٠١٩). أثر إدارة المخاطر على التميز المؤسسي لجامعة الأقصى بقطاع غزة، رسالة ماجستير، كلية الاقتصاد والعلوم الإدارية، الجامعة الإسلامية بغزة.

وزارة الإسكان والمرافق والتنمية العمرانية، الهيئة العامة للتخطيط العمراني (٢٠٠٨). إستراتيجية التنمية لمحافظات الجمهورية إقليم قناة السويس، الهيئة العامة للتخطيط العمراني، القاهرة.

وزارة التخطيط والمتابعة والإصلاح الإداري (٢٠١٥). دليل المواطن للخطة الالستثمارية بمحافظة بورسعيد ٢٠١٥/٢٠١٦، وزارة التخطيط والمتابعة والإصلاح الإداري، القاهرة.

وزارة التربية والتعليم والتعليم الفني، الإدارة العامة لنظم المعلومات ودعم اتخاذ القرار (٢٠٢١أ). *كتاب الإحصاء السنوي للعام الدراسي ٢٠٢٠/٢٠٢١*، الإدارة العامة لنظم المعلومات ودعم اتخاذ القرار، القاهرة.

وزارة التربية والتعليم والتعليم الفني، الإدارة العامة لنظم المعلومات ودعم اتخاذ القرار (٢٠٢١ب). *الملخص الإحصائي للتعليم ما قبل الجامعي للعام الدراسي ٢٠٢٠/٢٠٢١*، الإدارة العامة لنظم المعلومات ودعم اتخاذ القرار، القاهرة.

المراجع الأجنبية:

Alqahtani, A. S. (2017). The Extent of Comprehension and Knowledge with Respect to Digital Citizenship Among Saudi Arabia Teachers. (Doctoral dissertation, University of Northern Colorado). *ProQuest LLC*.

Australian Centre to Counter Child Exploitation (2020, February). Tanding Community Awareness, Perceptions, Attitudes and Reventative Behaviours Research Report, ACCCE.

Authority, C. A. S. (2002). Safety management systems. *Getting started. Canberra, ACT, Australia: PMP*.

AVA (2020), Digital Safeguarding Source Pack, commissioned AVA (Against Violence and Abuse).

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), 1-13.

Bica, I., & Petruta, A. (2021, June). The risk assessment, a decision-making tool for the management of contaminated sites. In *E3S Web of Conferences* (Vol. 265, p. 04001). EDP Sciences.

Blum-Ross, A., Donoso, V., Dinh, T., Mascheroni, G., O'Neill, B., Riesmeyer, C., & Stoilova, M. (2018). Looking forward: Technological and social change in the lives of European children and young people. *Report for the ICT Coalition for Children Online. Bruxelas: ICT Coalition.*

Buchholz, B. A., DeHart, J., & Moorman, G. (2020). Digital citizenship during a global pandemic: Moving beyond digital literacy. *Journal of Adolescent & Adult Literacy*, 64(1), 11-17.

Buganová, K., & Šimíčková, J. (2019). Risk management in traditional and agile project management. *Transportation Research Procedia*, *40*, 986-993.

Centers for Medicare & Medicaid Services Information Security and Privacy Group.(2021). *Risk Management Handbook (RMH)*. Chapter 14: Risk Assessment (RA).Version 1.3.

Charmaraman, L., Richer, M., & Moreno, A. (2020). Social and behavioral health factors associated with violent and mature gaming in early adolescence*. International journal of environmental research and public health*, 17(14), 4996.

Cilliers, L., & Chinyamurindi, W. (2020). Perceptions of cyber bullying at primary andsecondary school level amongst

student teachers in the Eastern Cape province of South Africa. *South African Computer Journal*, 32 (1), 27-42.

Clarke, B., & Crowther, K. (2015). *Children internet safety report: Key findings*. London: Family Kids and Youth. Techknowledge for schools.

Council of Europe Project Combating violence against children in Ukraine (2020). Solicitation of Children for Sexual Purposes. ARTICLE 23. The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse.

Crawford International School. (2018). Digital Citizenship Guidelines for Remote Learning, ADTCH GROUP, Kenya.

Cybersecurity Tech Accord. (2020) .Cybersecurity Awareness in the Commonwealth of Nations. https://cybertechaccord.org/new-whitepaper-cybersecurityawareness-in-the-com-monwealth-of-nations/.

De Barros, M. J. Z., & Lazarek, H. (2018, January). A Cyber Safety Model for Schools in Mozambique. In Proceedings of the 4th International Conference on *Information Systems Security and Privacy*, Funchal, Portugal (pp. 251-258).

De Giusti, A. (2020). Policy Brief: Education during COVID-19 and beyond. *Revista Iberoamericana de Tecnología En Educación y Educación En Tecnología*, (26), e12-e12.

Department for Education and Child Development. (2009). *Cyber-safety: Keeping children safe in a connected world. Guidelines for schools and preschools*. Adelaide: DECD. AUSTRALIA.

Department for Education. (2014). Keeping children safe in education: Statutory guidance for schools and colleges. Retrieved 30/6/2021 from www.gov.uk/government/publications/keeping-children-safe-in-education--2

Department for Education. (2017). Preventing and tackling bullying: Advice for headteachers, staff and governing bodies. London, UK: Department for Education.

Department of Education and Children's Services. (2009, June). Cyber Safety: Maintaining Morality in a Digital World, Government of South Australia, South Australia.

Dresp, B. (2020). Internet Addiction Disorder (IAD). Encyclopedia, *section Psychiatry and Mental Health Studies*. hal-02615330

Dubicka B, Theodosiou L. (2020, January). *Technology use and the mental health of children and young people*. Royal College of Psychiatrists, College Report 225.

Education Scotland. (2017). The National Action Plan on Internet Safety for Children and Young People, Education Scotland.

Faltýnková, A., Blinka, L., Ševˇcíková, A., & Husarova, D. (2020). The associations between family-related factors and excessive internet use in adolescents. *International journal of environmental research and public health*, 17(5), 1754.

Faris, R., & Zittrain, J. (2009). Web tactics. *Index on Censorship*, 38(4), 90-96.

Fernández-Prados, J. S., Lozano-Díaz, A., & Ainz-Galende, A. (2021, March). Measuring digital citizenship: A comparative analysis. In *Informatics* (Vol. 8, No. 1, p. 18). Multidisciplinary Digital Publishing Institute.

Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2020). *Youth internet safety education: Aligning programs with the evidence base*. Trauma, Violence, & Abuse, 1-15.

Fourie, I., Bothma, T. J., & Bitso, C. (2013). Trends in transition from classical censorship to Internet censorship: selected country overviews. *Innovation: journal of appropriate librarianship and information work in Southern Africa*, 2013(46), 166-191.

Georgia, M., Elizabeth, L. & Leah, E. (2020). Validation of the Sexual Grooming Model of Child Sexual Abusers, *Journal of Child Sexual Abuse,* 29(7), 855-875.

Gioe, D. V., Goodman, M. S., & Wanless, A. (2019). Rebalancing cybersecurity imperatives: patching the social layer. *Journal of Cyber Policy*, 4(1), 117-137.

Göldag, B. (2020). The Relationship between the Digital Game Dependence and Violence Tendency Levels of High School Students. *International Education Studies*, 13(8), 118-129.

Hasebrink, U., Görzig, A., Haddon, L., Kalmus, V., & Livingstone, S. (2011). Patterns of risk and safety online: In-depth analyses from the EU Kids Online survey of 9-to 16-year-olds and their parents in 25 European countries. *London, UK: EU Kids Online*.

Hassan, M. A. (2021). The Role of Secondary School in The Development of the Values of Digital Citizenship for Students Under the Coronavirus Pandemic (Covid-19). *Multicultural Education*, 7(3).

Hidayati, I., Afiatin, T., & Susanti, M. (2019). Parental Mediation and Excessive Internet Use Behaviour in Teenagers. In *Education Innovation and Mental Health in Industrial Era 4.0* . Sciendo.

Holloway, D., Green, L. and Livingstone, S. (2013). *Zero to eight. Young children and their internet use*. London: EU Kids Online, LSE.

Hopkin, P. (2012). Fundamentals of Risk Management (2nd edt.) – Understanding, Evaluating and Implementing Effective Risk Management. London: Kogan Limited.

Hopkin, P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.

Hornor, G. (2020). Child and adolescent pornography exposure. *Journal of Pediatric Health Care*, 34(2).

IJM's Center to End Online Sexual Exploitation of Children (2020, October). COVID-19 Brief on Online Sexual Exploitation of Children ASEAN Focus, endosec.

IQ INSTITUTE Website. (2020). 2020 CHILD ONLINE SAFETY INDEX, Retrieved 22 March 2021 from https://www.dqinstitute.org/impact-measure/#cosi_page

Jemeļjanenko, A. (2019). Risk Management in the Educational Sector of Latvia, Human, Technologies and Quality of Education= *Cilvēks, tehnoloģijas un izglītības kvalitāte: konferences rakstu krājums*. University of Latvia.

Joynes, C., Rossignoli, S., & Amonoo-Kuofi, E. F. (2019). 21st Century Skills: evidence of issues in definition, demand and delivery for development contexts.

Kemp, S. (2021). Digital 2021: Global Digital Overview .Retrieved 22 May 2021 from https://wearesocial.com/blog/2021/01/digital-2021-the-latest-insights-into-the-state-of-digital

Kemp, S. (2021b). DIGITAL 2021: EGYPT .Retrieved 22 May 2021 from https://datareportal.com/reports/digital-2021-egypt

King, D. L., Delfabbro, P. H., Doh, Y. Y., Wu, A. M., Kuss, D. J., Pallesen, S., Mentzoni, R., Carragher, N., & Sakuma, H. (2018). Policy and prevention approaches for disordered and hazardous gaming and internet use: An international perspective. *Prevention Science*, 19(2), 233–249.

Klucka, J., Gruenbichler, R., & Ristvej, J. (2021). Relations of COVID-19 and the Risk Management Framework. *Sustainability*, *13*(21), 11854.

Kritzinger, E. (2020). Improving Cybersafety Maturity of South African Schools. *Information*, 11(10), 471.

Kritzinger, E. (2020b). *Cybersafety Guidelines to Prepare South African Schools for the 4th Industrial Revolution*. (Master Thesis, University of Johannesburg -South Africa).

Kritzinger, E., Bada, M., & Nurse, J. R. (2017, May). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In *IFIP World Conference on Information Security Education*. Springer, Cham.

Kurbalija, J. (2016). *An introduction to internet governance*. 7th edition, Diplo Foundation.

Lee, J. A., & Liu, C. U. (2012). Forbidden City enclosed by the Great Firewall: The law and power of Internet filtering in China. *Minn. JL Sci. & Tech.*, 13, 125.

Lester, T. M. (2018). *An Investigation on Cyber Safety Awareness Among Teachers and Parents* (Doctoral dissertation, Gardner-Webb University).

Lewis, J. A., Porrúa, M. A., Catalina, A., De, G., & Díaz, A. (2016). Advanced Experiences in Cybersecurity Policies and Practices. *no. July*.

Lewis, L. (2020). Experiences in Online Grooming from Initial Contact with Offender to Relationship Ending, doctoral dissertation, Walden University ScholarWorks.

Lim, S. (2012). Regulatory initiatives for managing online risks and opportunities for youths—The East Asian experience. In M. Walrave (Ed.), e-Youth: Balancing between opportunities and risks? (pp. 271–290). Brussels: Peter Lang.

Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S. and Lagae, K. (2015). *How parents of young children manage digital devices at home: The role of income, education and parental style.* London: EU Kids Online, LSE.

Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C., & Nandi, A. (2017). Children's online activities, risks and safety: a literature review by the UKCCIS evidence group.

Livingstone, S. Lievens, E, Carr, J. (2020, November). *Handbook for policy makers on the rights of the child in the digital environment*. Council of Europe.

Lopez-Fernandez, O., & Kuss, D. J. (2020). Preventing harmful internet use-related addiction problems in Europe: A literature review

and policy options. *International journal of environmental research and public health*, 17(11), 3797.

MacArthur, L. (2009) "Internet Safety for Students in Elementary Schools". All Regis University Theses. 64.

Macenaite, M., & Kosta, E. (2017). Consent for processing children's personal data in the EU: following in US footsteps?. *Information & Communications Technology Law*, 26(2), 146-197.

Malecki, A. (2018) "Cybersecurity in the Classroom: Bridging the Gap Between Computer Access and Online Safety". Cyber Security Capstone Research Project Reports. 1.

Maphorisa, S. (2021). LEADERSHIP AND THE RISK MANAGEMENT CONUNDRUM IN BOTSWANA'S PUBLIC SECONDARY SCHOOLS, *Mosenodi Journal*, 24(1).

Mark, L. (2014). *Reducing cyber victimization through home and school partnerships: The effects of a cyber safety workshop on parent and educator perceptions of self-efficacy and attitudes toward family-school collaboration* (Doctoral dissertation, [Honolulu]: [University of Hawaii at Manoa], [2014, May]).

MCIT (Ministry of Communications and Information Technology). (2021, March). ICT Indicators Bulletin. Quarterly Issue.

Milenkova, V., & Lendzhova, V. (2021). Digital Citizenship and Digital Literacy in the Conditions of Social Crisis. *Computers*, *10*(4), 40

MOHAN, S. C., & LEE, Y. (2020). Sexual grooming as an offence in Singapore. Singapore Academy of Law Journal, 1.

Moulton, P. (2021). *Decision Factors Used by Risk Managers for Cyber Insurance Purchasing in US Organizations*. (Doctoral dissertation, Wilmington University -Delaware).

Muir, Nancy. (2010). Guide to Teaching Cyber Safety to the Digital Generation, Wiley Publishing Inc (con el auspicio de las compañías Dell y Microsoft).

Munawar, M., & Nisfah, N. (2020). The Effect of Assertive Discipline on Early-Aged Children's Gadget Addiction. *JECCE (Journal of Early Childhood Care and Education)*, 2(2), 64-70.

NetSafe. (2010). *Digital Citizenship in New Zealand Schools Overview*. Retrieved from: http://www.netsafe.org.nz/Doc_Library/Digital_Citizenship_in_New_Zealand_Schools_Overview.pdf

Ning, Y. M. (2011). China's tackling of online pornography: Puzzles, issues and trends.' In 8th International Telecommunications Society (ITS) Asia-Pacific Regional Conference. Taiwan.

Nye, M. R. (2014). *A case study of promising practices of anti-cyberbullying efforts in a middle school*. (Doctoral dissertation, University of Southern California).

Ofcom. (2016). *Children and parents: Media use and attitudes report.* Retrieved from www.ofcom.org.uk/ data/assets/pdf file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf.

Ofcom. (2020). Children and parents: Media use and attitudes report 2019. Ofcom.

Paraiso, E. (2019). *Towards a cyber safety information framework for South African parents* (Doctoral dissertation, University of Pretoria).

Payne, J. L. (2016). *A case study of teaching digital citizenship in fifth grade* (Doctoral dissertation, University of Alabama Libraries).

Pest Management Regulatory Agency Health Canada. (2021). A Framework for Risk Assessment and Risk Management of Pest Control Products, PMRA Guidance Document, Canada.

Psotka, J. (2013). Educational games and virtual reality as disruptive technologies. *Journal of Educational Technology & Society*, *16*(2), 69-80.

Puddephatt, A. (2011). FREEDOM OF EXPRESSION RIGHTS IN THE DIGITAL AGE. *Open Society Foundation: Washington*.

Quaglio, G & Millar, S.(2020, May) . Potentially negative effects of internet use, IN-*DEPTH ANALYSIS Panel for the Future of Science and Technology*, Scientific Foresight Unit (STOA), European Parliamentary Research Service (EPRS).

Quinn, S., Ivy, N., Barrett, M., Feldman, L., Witte, G., & Gardner, R. (2021). *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management* (No. NIST Internal or Interagency Report (NISTIR) 8286A). National Institute of Standards and Technology.

Rahman, A., Malaysia, N. A., Sairi, M. T. U. K., Zizi, I. K., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. International Journal of Information and Education Technology, 10(5), 378-382.

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, 27(2), 23-39.

Ruggieri, R. A., Santoro, E., Francesco De Caro, M. D., Palmieri, L., Capunzo, M., Venuleo, C., & Boccia, G. (2016). Internet addiction: A prevention action-research intervention. *Epidemiol Biostat Public Health*, 13(3). e11817-1- e11817-5.

Salamzada, K. H. O. S. R. A. W., Shukur, Z., & Bakar, M. A. (2015). A framework for cybersecurity strategy for developing countries: Case study of Afghanistan. *Asia-Pacific Journal of Information Technology and Multimedia*, 4(1), 1-10.

Saluja, S., Bansal, D. & Saluja, S. (2012). "Cyber Safety Education in High Schools", *International Conference on Computer Technology and Science (ICCTS)*. vol. (47), IPCSIT Press, Singapore.

Schubart, R. C. (2021). Leading in the Digital Age: A Multi-case Study of Leading Digital Citizenship. *Theses and Dissertations-Education Sciences*. 79. https://uknowledge.uky.edu/edsc_etds/79

Shersad, F., & Salam, S. (2020). Managing Risks of E-learning During COVID-19. *International Journal of Innovation and Research in Educational Sciences*, 7(4), 2349-5219.

Šimandl, V. (2015). ICT teachers and technical e-safety: Knowledge and routines. *International Journal of Information and Communication Technologies in Education*, 4(2), 50-65.

Sitarz, R; Rogers, M; Bentley, L; & Jackson, E, (2014). "Internet Addiction to Child Pornography". Annual ADFSL Conference on Digital Forensics, *Security and Law*. 6. https://commons.erau.edu/adfsl/2014/wednesday/6

Sityata, I., Botha, L., & Dubihlela, J. (2021). Risk Management Practices by South African Universities: An Annual Report Disclosure Analysis. *Journal of Risk and Financial Management*, 14(5), 195.

Soares, F., & Lopes, A. (2020). Active citizenship skills and active digital citizenship skills in teaching and learning in the digital age, European Education Policy Network, Brussels

Spiering, M. A. (2018, February). Improving cyber safety awareness education at Dutch elementary schools. Master Thesis of Cyber Security, Cyber Security Academy, Hague.

Suppo, C. A. (2013). *Digital citizenship instruction in Pennsylvania public schools: School leaders expressed beliefs and current*

practices (Doctoral dissertation, Indiana University of Pennsylvania).

Swanton, T. B., Blaszczynski, A., Forlini, C., Starcevic, V., & Gainsbury, S. M. (2021). Problematic risk-taking involving emerging technologies: A stakeholder framework to minimize harms. *Journal of behavioral addictions*, 9(4), 869-875.

SWGfL/UK Safer Internet Centre, University of Plymouth United Kingdom, Netsafe New Zealand, & eSafety Commissioner Australia. (2017). Young People and Sexting - Attitudes and Behaviours.

Taibah, W. M., Khalifa, H. K., & Alshebaiki, A. M. (2020) Strengthening the convention on the rights of the child (CRC). Governing children's digital world.

Thah, S., Kaur, K., & Ling, P. (2019, April). CYBERSAFETY IN EDUCATION FOR THE 21ST CENTURY: A COMPARATIVE STUDY OF MALAYSIA AND THAILAND. In *ICE 2019 CONFERENCE PROCEEDINGS*.

THE UNIVERSITY OF LEEDS (2019) Risk management: guidance for UEG, faculties, schools, professional services, programme and project leads, THE UNIVERSITY OF LEEDS. Retrieved 30 May 2021 from https://www.leeds.ac.uk/secretariat/documents/risk_management_guidance.pdf

Tosun, N., & Mihci, C. (2020). An Examination of Digital Parenting Behavior in Parents with Preschool Children in the Context of Lifelong Learning. *Sustainability*, 12(18), 7654.

Tsai, M., Wang, Y., & Weng, C. (2020). A Study on Digital Games Internet Addiction, Peer Relationships and Learning Attitude of Senior Grade of Children in Elementary School of Chiayi County. *Journal of Education and Learning*, 9(3), 13-26.

UNICEF. (2016, April) Guide to using the child online safety assessment tool: empowering technology companies to promote a safe online environment for children. UNICEF

UNICEF. (2017). The State of The World's Children: Children in a Digital World 2017.

UNICEF, Lao PDR (2020). Keeping children safe online during the COVID-19 pandemic. UNICEF

Ünübol, H., Koç, A. Ş., Sayar, G. H., Stavropoulos, V., Kircaburun, K., & Griffiths, M. D. (2020). Measurement, profiles, prevalence, and psychological risk factors of problematic gaming among the

Turkish community: A large-scale national study. *International Journal of Mental Health and Addiction*, 1-21.

Vallor, S. & Rewak, S.J. (2018). An Introduction to Cybersecurity Ethics, Markkula Center for Applied Ethics, https://www.scu.edu/ethics/focus-areas/technology-ethics/resources/an-introduction-tocybersecurity-ethics.

Walsh, K., Wallace, L., Ayling, N., & Sondergeld, A. (2020). Best practice framework for online safety education (Stage 1). eSafety Commissioner, Australia.

Warf, B. (2011). Geographies of global Internet censorship. *GeoJournal*, 76(1), 1-23.

Webster, J. P. (2018). *Teacher perceptions and implementation of digital citizenship curriculum in one-to-one high schools in Missouri* (Doctoral dissertation, Southwest Baptist University).

Weis, J. E. (2020). Play therapy interventions promoting intrinsic characteristics of resilience.: A systematic literature review. Master Thesis Interventions in Childhood, School of Education and Communication (HLK), Jönköping University.

White, J. M. (2013). *Cyber Bullying: In the Educational Setting*. (Doctoral Dissertation, University of Phoenix).

Widiputera, F, Satria, N, Perdana & Zamjani, I .(2021). Digital Kids Asia-Pacific Insights into Children's Digital Citizenship, Country Report –Indonesia, UNESCO Bangkok.

Wilbon Sr, K. (2020). *Cyber Bullying Prevention and Effective Coping Strategies for Middle School Students: A Case Study of Middle School Teachers in Maryland* (Doctoral dissertation, Northcentral University).

World Health Organisation (WHO). (2018). International Classification of Diseases, 11th Revision, Available at: https://icd.who.int/en

World Health Organisation. (2019). *Guidelines on physical activity, sedentary behaviour and sleep for children under 5 years of age* [Online]. Available: https://apps.who.int/iris/handle/10665/311664 [Accessed 28 April 2019].

Yancey, M. (2017). Cyber Bullying: Examining Curriculum and Policy in Eastern North Carolina High Schools; A Qualitative Case Study. (Doctoral dissertation, Northcentral University). *ProQuest LLC*.

Yang, K. C. (2011). The aborted Green dam-youth escort censor-ware project in China: A case study of emerging civic participation in

Online ISSN\2735-3192 ISSN\2682-3489

China's internet policy-making process. *Telematics and Informatics*, 28(2), 101-111.

Zepf, I. V., & Arthur, L. (2013). *Cyber-security curricula for basic users*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA. (Master Thesis-Naval Postgraduate School).

Zhao, Y. (2016). *Protocols of Control in Chinese Online News Media: The Case of Wenzhou News* (Doctoral dissertation, University of Sheffield).

Zulkifli, Z., Molok, N. N. A., Abd Rahim, N. H., & Talib, S. (2020). Cyber Security Awareness Among Secondary School Students in Malaysia. *Journal of Information Systems and Digital Technologies*, 2(2), 28-41.

جامعة بورسعيد

كلية التربية

قسم التربية المقارنة والإدارة التربوية

ملحق (١)

دراسة استطلاعية مع مديري المدارس الابتدائية بمحافظة بورسعيد.

- كيف تشارك المدرسة الابتدائية في إدارة المخاطر السيبرانية؟

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

- **كيف** يشارك معلمو المدارس الابتدائية في إدارة المخاطر السيبرانية ؟

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

- هل هناك ضرورة لإدارة المخاطر السيبرانية في المدارس الابتدائية؟

.....
.....
.....
.....
.....
.....
.....

ملحق (٢)

دراسة استطلاعية لأولياء أمور تلاميذ الابتدائية بمحافظة بورسعيد.

- ما المخاطر السيبرانية التي تواجه أبناءكم تلاميذ المدارس الابتدائية في محافظة بورسعيد؟

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

- هل هناك ضرورة لإدارة المخاطر السيبرانية في المدارس الابتدائية؟

.....
.....

.....

.....

.....

.....

.....

- ما الإجراءات التي اتخذتموها لمواجهة تلك المخاطر السيبرانية التي تعرض لها أبناؤكم؟ (اختر واحدة)

أ- منع الأبناء من الدخول على الانترنت مطلقاً.

ب-بدء فرض قيود على الاستخدام وإلزام الأبناء بها.

ج- محاولة وضع قيود على الاستخدام مع صعوبة إلزام الأبناء بها نتيجة لسنوات الاستخدام الطويلة؛ مما يؤدي لعدم الالتزام بالقيود المفروضة.

د- أتيح الانترنت بلا قيود.

ملحق (٣)

الصور النهائية لاستبانة موجهة لمديري المدارس الابتدائية لرصد واقع إدارة المخاطر السيبرانية في المدارس الابتدائية

م	العبارة	بدرجة كبيرة جدا	بدرجة كبيرة	بدرجة متوسطة	بدرجة قليلة	بدرجة قليلة جدا
أولا: نحديد المخاطر السيبرانية						
١	-تُجري إدارة المدرسة مسحاً داخليا لتحديد المخاطر السيبرانية.					
٢	-تُجري إدارة المدرسة مسحاً خارجيا لتحديد المخاطر السيبرانية.					
٣	-تحدد إدارة المدرسة آليات للكشف المبكر عن المخاطر السيبرانية.					
٤	-تستعين إدارة المدرسة بالخبراء عند تحديد المخاطر السيبرانية.					
٥	-تستخدم إدارة المدرسة أسلوب SWOT عند تحديد المخاطر السيبرانية.					
٦	-تستعين إدارة المدرسة بأصحاب المصلحة للمساندة في تحديد المخاطر السيبرانية.					
٧	-تحرص إدارة المدرسة على تحديد سياق إدارة المخاطر السيبرانية.					
ثانيا: تحليل المخاطر السيبرانية:						
٨	- تحتفظ إدارة المدرسة بقاعدة بيانات تتضمن معلومات عن المخاطر السيبرانية التي يتعرض لها الطلاب.					
٩	-تهتم إدارة المدرسة بتكاملية المعلومات الخاصة بإدارة					

م	العبارة	بدرجة كبيرة جدا	بدرجة كبيرة	بدرجة متوسطة	بدرجة قليلة	بدرجة قليلة جدا
	المخاطر السيبرانية.					
١٠	– تحلل إدارة المدرسة المخاطر باستخدام أدوات مناسبة.					
١١	–تدرس إدارة المدرسة العوامل المسببة للمخاطر السيبرانية.					
١٢	–تدرس إدارة المدرسة تأثير المخاطر السيبرانية على الأهداف الاستراتيجية للمدرسة.					
١٣	–تدرس إدارة المدرسة الضوابط الوقائية التي يمكن وضعها لتقليل احتمالية حدوث المخاطر السيبرانية.					
١٤	–تعِد إدارة المدرسة إستراتيجية واضحة لإدارة المخاطر السيبرانية					
ثالثا: تقييم المخاطر السيبرانية						
١٥	–تقوم إدارة المدرسة بتقييم الآثار المحتملة للمخاطر السيبرانية على البيئة المدرسية					
١٦	– تقوم إدارة المدرسة بجدولة المخاطر السيبرانية وفقا للأشد خطراً فالأقل.					
١٧	–تقوم إدارة المدرسة بتقييم نقاط القوة في التعامل مع المخاطر السيبرانية.					
١٨	–تقوم إدارة المدرسة بتقييم التهديدات الحالية المتعلقة بالمخاطر السيبرانية.					
١٩	–تستعين إدارة المدرسة بمتخصصين عند إعداد خطط إدارة المخاطر السيبرانية.					
٢٠	– تحلل إدارة المدرسة عوامل التخفيف المنفذة.					
٢١	–تقارن إدارة المدرسة تقييم احتمالية حدوث المخاطر السيبرانية الحالية بتقييم الاحتمالية المسبق لها.					

م	العبارة	بدرجة كبيرة جدا	بدرجة كبيرة	بدرجة متوسطة	بدرجة قليلة	بدرجة قليلة جدا
رابعا: الاستجابة للمخاطر السيبرانية						
٢٢	-تنسق إدارة المدرسة جهود فريق إدارة المخاطر السيبرانية.					
٢٣	-توفر إدارة المدرسة نظاما فعالا للتعامل مع أية مخاطر سيبرانية محتملة.					
٢٤	-تذلل إدارة المدرسة صعوبات الاتصال بالجهات المساعدة في إدارة المخاطر السيبرانية.					
٢٥	-تستخدم إدارة المدرسة صفحتها على الانترنت لتوعية أولياء أمور الطلبة.					
٢٦	-تنظم إدارة المدرسة ورش عمل لتوعية الطلبة بشأن المخاطر السيبرانية.					
٢٧	-تعد إدارة المدرسة برامج تدريبية للمعلمين في مجال إدارة المخاطر السيبرانية.					
٢٨	-تنتهج إدارة المدرسة نظما ولوائح وقائية للسلامة من المخاطر السيبرانية.					
خامسا: تتبع المخاطر وتحديث آليات المواجهة.						
٢٩	-تجري إدارة المدرسة تقويما مستمرا لأساليب التخطيط المتبعة في الكشف المبكر عن المخاطر السيبرانية.					
٣٠	-تجري إدارة المدرسة مراجعة دورية لأساليب إدارة مخاطرها السيبرانية.					
٣١	-تُقَيِّم إدارة المدرسة خطط إدارة المخاطر السيبرانية بقصد تطويرها.					
٣٢	-تتابع إدارة المدرسة نتائج إستراتيجيات التحديث المتخذة في مواجهة المخاطر السيبرانية.					

م	العبارة	بدرجة كبيرة جدا	بدرجة كبيرة	بدرجة متوسطة	بدرجة قليلة	بدرجة قليلة جدا
٣٣	– تتابع إدارة المدرسة نتائج إستراتيجيات الوقاية المتخذة في مواجهة المخاطر السيبرانية.					
٣٤	–تعيد إدارة المدرسة تقييم احتمالية المخاطر السيبرانية بعد اتخاذ بعض إستراتيجيات الاستجابة.					
٣٥	– تقوم إدارة المدرسة بتجديد قاعدة البيانات حسب ما يستجد من مخاطر سيبرانية.					

ملحق (٤)

قائمة بأسماء السادة المحكمين (•) لأدوات الدراسة

م	الاسم	الوظيفة
١	أ.د/ حسن مختار حسين سليم.	أستاذ الإدارة والتخطيط والدراسات المقارنة- جامعة الأزهر.
٢	أ.د شيرين الدسوقي.	أستاذ علم النفس التربوي، وعميد كلية التربية جامعة بورسعيد.
٣	أ.د/ محمد يوسف نصر.	أستاذ الإدارة والتخطيط والدراسات المقارنة- جامعة الأزهر.
٤	أ.د/ مصطفى رجب.	أستاذ أصول التربية، بكلية التربية جامعة سوهاج.
٥	أ.م.د/ إيمان حمدي رجب.	أستاذ مساعد الإدارة التربوية وسياسات التعليم، بكلية التربية- جامعة الفيوم.
٦	أ.م.د/ عبد السلام الشبراوي عباس.	أستاذ مساعد التربية المقارنة والإدارة التربوية المتفرغ، بكلية التربية-جامعة بورسعيد.

(•) ترتيب أسماء السادة المحكمين طبقا للدرجة العلمية ثم الترتيب الأبجدي.

ملحق (٥)

قائمة بأسماء السادة المحكمين (•) للإجراءات المقترحة

م	الاسم	الوظيفة
١	أ.د/ أحمد عبد الفتاح الزكي.	أستاذ ورئيس قسم أصول التربية، بكلية التربية– جامعة دمياط.
٢	أ.د/ سيد سلامة الخميسي.	أستاذ أصول التربية المتفرغ، بكلية التربية–جامعة دمياط.
٣	أ.د/ السيدة محمود إبراهيم سعد.	أستاذ الإدارة التربوية وسياسات التعليم – بكلية التربية– جامعة الإسكندرية.
٤	أ.م.د/ أحمد غانم.	أستاذ مساعد الإدارة التعليمية المتفرغ، بكلية التربية– جامعة بني سويف
٥	أ.م.د/ إيمان حمدي رجب.	أستاذ مساعد الإدارة التربوية وسياسات التعليم، بكلية التربية– جامعة الفيوم
٦	أ.م.د/ حسنية حسين عبد الرحمن عويس.	أستاذ مساعد التربية المقارنة، وقائم بعمل رئيس قسم التربية المقارنة، بكلية التربية– جامعة الفيوم .
٧	أ.م.د/ عبد السلام الشبراوي عباس.	أستاذ مساعد التربية المقارنة والإدارة التربوية المتفرغ، بكلية التربية– جامعة بورسعيد.
٨	أ.م.د/ نهى العاصي.	أستاذ التربية المقارنة والإدارة التربوية ، بكلية التربية بالاسماعيلية– جامعة قناة السويس.

(•) ترتيب أسماء السادة المحكمين طبقا للدرجة العلمية ثم الترتيب الأبجدي.