

Final Project 1

Code: MGM 496-PMG496

Project Template

Faculty of Management
Midocean University

أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية
المؤسسات الحكومية للتصدي للاختراقات – دراسة ميدانية على وزارات
المنطقة الشرقية

أسم الطالب
معاذ التركي

مشروع تخرج- 2
كلية الإدارة- جامعة ميدأوشن

إشراف
د.

عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

التاريخ- الفصل الدراسي

جدول المحتويات

١	الفصل الأول: الإطار العام للدراسة.....	٣
١.١	المقدمة:.....	٤
١.٢	مشكلة الدراسة.....	٥
١.٢.١	فجوات على المستوى النظري.....	٥
١.٢.٢	فجوات على المستوى التطبيقي.....	٦
١.٣	أهمية الدراسة.....	٧
١.٣.١	على المستوى النظري:.....	٧
١.٣.٢	على المستوى التطبيقي:.....	٧
١,٤	أسئلة الدراسة.....	٨
١,٥	أهداف الدراسة.....	٩
1.6.	فرضيات الدراسة.....	٩
1.7.	نموذج الدراسة.....	١٠
1.8.	منهجية الدراسة.....	١١
١١	مجتمع وعينة الدراسة.....	١١
١٢	مصادر جمع البيانات.....	١٢
١٢	أدوات الدراسة.....	١٢
١٢	الأساليب الإحصائية المستخدمة.....	١٢
١٣	حدود الدراسة.....	١٣
١٣	أداة الدراسة (توزيع الفقرات).....	١٣
1.9.	الدراسة الميدانية.....	١٣
1.10.	مخطط المشروع المقترح (هيكل الدراسة).....	١٤
٢	الفصل الثاني: الدراسات السابقة.....	خطأ! الإشارة المرجعية غير معروفة.
٢,١	المقدمة:.....	خطأ! الإشارة المرجعية غير معروفة.
٢,٢	المتغير المستقل.....	خطأ! الإشارة المرجعية غير معروفة.
٢,٣	المتغير التابع.....	خطأ! الإشارة المرجعية غير معروفة.

العلاقة بين المتغير المستقل والمتغير التابع.....خطأ! الإشارة المرجعية غير معرفة.	٢,٤.
الخاتمة.....خطأ! الإشارة المرجعية غير معرفة.	٢,٥.
٣٠	قائمة المراجع

١. الفصل الأول: الإطار العام للدراسة

يشهد العالم اليوم تحولاً رقمياً متسارعاً أعاد تشكيل طبيعة العمل المؤسسي وأسلوب تقديم الخدمات الحكومية، إذ باتت البنى التحتية الرقمية ركيزة أساسية لاقتصادات الدول وأمنها الوطني. وقد أفرز هذا التحول واقعاً جديداً تتعاظم فيه المخاطر السيبرانية بوصفها أحد أبرز التهديدات التي تواجه الحكومات والمنظمات على حدٍ سواء؛ حيث تستهدف الهجمات السيبرانية البيانات الحساسة والأنظمة الحيوية والخدمات العامة، بما يهدد استقرار المؤسسات وثقة المواطنين فيها. وفي ضوء ذلك، أصبح الأمن السيبراني عنصراً استراتيجياً لا غنى عنه ضمن منظومة الحوكمة الرقمية الحديثة، خاصة في القطاعات الحكومية التي تتعامل مع بيانات وطنية حساسة وتُقدم خدمات لا تحتمل التوقف. (Pemmasani, 2023)

وفي هذا السياق العالمي المتغير، أولت المملكة العربية السعودية الأمن السيبراني اهتماماً بالغاً انسجاماً مع مستهدفات رؤية المملكة ٢٠٣٠، فأنشأت الهيئة الوطنية للأمن السيبراني (NCA) عام ١٤٣٨هـ بوصفها الجهة المختصة بتنظيم الأمن السيبراني على المستوى الوطني وتعزيزه وحماية المصالح الحيوية للدولة. وقد أصدرت الهيئة منظومة متكاملة من الأطر والضوابط، يأتي في مقدمتها الضوابط الأساسية للأمن السيبراني (ECC) التي تتضمن في نسختها المحدثّة (ECC-2:2024) خمسة مكونات رئيسية و(٢٩) مكوناً فرعياً و(١١٤) ضابطاً، تمثل الحد الأدنى الإلزامي الذي يتعين على الجهات الوطنية الالتزام به لحماية أصولها المعلوماتية والتقنية. كما أصدرت الهيئة ضوابط متخصصة مثل ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC) وضوابط التقنية التشغيلية (OTCC)، بهدف توحيد مستويات النضج السيبراني وتقليل المخاطر الوطنية.

ويتقاطع هذا التوجه الوطني مع توجهات دولية مماثلة تركز على بناء قدرات المؤسسات الحكومية لمواجهة الاختراقات، إذ تشير الأدبيات الحديثة إلى أن الجاهزية السيبرانية (Cybersecurity Readiness) أصبحت محدداً جوهرياً لأداء المؤسسات وقدرتها على الصمود في وجه التهديدات، وأن الالتزام بأطر الحوكمة السيبرانية ينعكس إيجاباً على فاعلية الاستجابة للحوادث وإدارة المخاطر (Mohamed Noor et al., 2026)؛ (Majeed et al., 2026) كما بينت دراسات مقارنة بين بيئات مختلفة أن وجود إطار تنظيمي وطني واضح

يُمثّل عاملاً حاسماً في رفع مستوى النضج السيبراني وتقليل الفجوة بين السياسات والتطبيق الفعلي (Rawindaran et al., 2023).

غير أن الواقع التطبيقي يكشف أن إصدار الضوابط وحده لا يكفي لتحقيق الجاهزية المطلوبة، إذ تتفاوت المؤسسات الحكومية في مستوى التزامها وقدرتها على ترجمة هذه الضوابط إلى ممارسات فعلية وإجراءات تشغيلية مؤثرة. وتتأثر هذه الجاهزية بعوامل متعددة منها: مستوى الوعي السيبراني، توافر الكفاءات البشرية، كفاية الموازنات المخصصة، ومدى تكامل الحوكمة السيبرانية مع باقي منظومات الحوكمة المؤسسية. وتُعدّ المنطقة الشرقية في المملكة العربية السعودية بيئة ذات أهمية خاصة في هذا السياق، نظراً لاحتضانها قطاعات حيوية تجعل وزاراتها وفروعها الحكومية مستهدفة بصفة متكررة من الهجمات السيبرانية.

ومن هذا المنطلق، تأتي الدراسة الحالية لتسليط الضوء على أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات، من خلال دراسة ميدانية على وزارات المنطقة الشرقية، وذلك بهدف قياس مستوى الالتزام الفعلي بهذه المعايير، وتحديد طبيعة العلاقة بينها وبين مؤشرات الجاهزية، والوقوف على الفجوات التي تحول دون تحقيق الفاعلية المرجوة، بما يُسهم في تقديم توصيات عملية تدعم صناع القرار في تعزيز المنظومة السيبرانية الوطنية.

١.٢. مشكلة الدراسة

على الرغم من الجهود التشريعية والتنظيمية التي بذلتها الهيئة الوطنية للأمن السيبراني (NCA) في إصدار حزمة متكاملة من الضوابط الإلزامية، وفي مقدمتها الضوابط الأساسية للأمن السيبراني (ECC) بنسختها الأحدث (ECC-2:2024)، إلا أن مؤشرات الواقع تشير إلى استمرار وقوع الجهات الحكومية ضحايا لاختراقات سيبرانية متفاوتة الخطورة، وإلى تباين واضح بين المؤسسات في مستوى تطبيقها للضوابط وفي درجة جاهزيتها الفعلية للتصدي للتهديدات. وهذا يطرح تساؤلاً جوهرياً حول العلاقة بين الالتزام الشكلي بالمعايير من جهة، وتحقيق الجاهزية التشغيلية الحقيقية من جهة أخرى، خاصة في ظل ندرة الدراسات الميدانية التي تناولت هذه العلاقة في السياق السعودي عموماً، وفي وزارات المنطقة الشرقية على وجه التحديد.

١.٢.١ فجوات على المستوى النظري

تتمثل الفجوات النظرية التي تسعى الدراسة إلى معالجتها في أن معظم الأدبيات السابقة التي تناولت الأمن السيبراني الحكومي ركزت على الجوانب التقنية أو السياساتية بمعزل عن قياس الأثر الفعلي للأطر الوطنية على الجاهزية المؤسسية. فقد بحثت دراسة (Pemmasani, 2023) في أطر الأمن السيبراني الوطنية للبنى التحتية الحرجة من منظور مقارن دون التعمق في إطار تنظيمي قطري بعينه، كما تناولت دراسة (Rawindaran et al., 2023) حوكمة الأمن السيبراني في المنشآت الصغيرة والمتوسطة في المملكة العربية السعودية والمملكة المتحدة دون التطرق إلى المؤسسات الحكومية. وفي المقابل، ركزت دراسة (Mohamed Noor et al., 2026) على أثر الجاهزية السيبرانية على الأداء الأمني التنظيمي في البيئة الماليزية، بينما تناولت دراسة (Majeed et al., 2026) حوكمة الأمن السيبراني في السياق الباكستاني، وهو ما يكشف عن غياب دراسات نظرية تربط مباشرة بين منظومة معايير NCA السعودية ومؤشرات الجاهزية للتصدي للاختراقات في القطاع الحكومي. كما يُلاحظ ندرة الأطر النظرية التي تُكامل بين أبعاد الحوكمة وإدارة المخاطر والصمود التنظيمي ضمن نموذج واحد يُختبر في السياق السعودي، وهو ما تسعى هذه الدراسة إلى الإسهام في معالجته من خلال بناء إطار مفاهيمي يربط بين متغيرات تطبيق الضوابط ومخرجات الجاهزية.

١.٢.٢. فجوات على المستوى التطبيقي

أما على المستوى التطبيقي، فإن قاعدة الدراسات الميدانية التي قُيِّمت الأثر الفعلي لتطبيق معايير NCA على جاهزية الجهات الحكومية السعودية لا تزال محدودة، ولم يُرصد حسب علم الباحث وجود دراسة ميدانية مخصصة لوزارات المنطقة الشرقية تحديداً، مع ما تتميز به هذه المنطقة من ثقل اقتصادي وحضور لقطاعات حيوية يجعل مؤسساتها هدفاً متكرراً للهجمات السيبرانية. كما يُلاحظ في الواقع التطبيقي تفاوت واضح بين الجهات الحكومية في مستوى نضج الأمن السيبراني، وفي مدى ترجمة الالتزام التنظيمي بالضوابط إلى ممارسات تشغيلية فاعلة على أرض الواقع، إضافة إلى وجود تحديات تتعلق بنقص الكوادر المتخصصة، ومحدودية الوعي السيبراني لدى الموظفين، وضعف تكامل منظومات الاستجابة للحوادث، وهو ما أشارت إليه ضمناً تقارير الجهات الرقابية ومؤشرات النضج السيبراني الوطنية. ويُضاف إلى ذلك غياب أدوات قياس عملية تربط بين كل بُعد من أبعاد الضوابط الأساسية ومؤشر محدد من مؤشرات الجاهزية للتصدي للاختراقات، مما يُصعّب على الجهات الحكومية تشخيص فجواتها الفعلية وتحديد أولويات التحسين.

وفي ضوء ما تقدّم من فجوات نظرية وتطبيقية، يمكن صياغة السؤال الرئيسي للدراسة على النحو الآتي:

ما أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية؟

١.٣. أهمية الدراسة

تستمد هذه الدراسة أهميتها من حداثة موضوعها وارتباطه المباشر بأحد أهم محاور رؤية المملكة ٢٠٣٠ المتعلق ببناء اقتصاد رقمي آمن ومستدام، فضلاً عن كونها تتناول قطاعاً حساساً يتمثل في المؤسسات الحكومية التي تُعدّ خط الدفاع الأول عن البيانات الوطنية والخدمات العامة. وتنقسم أهمية الدراسة إلى بُعدين متكاملين:

١.٣.١. على المستوى النظري:

تُسهّم الدراسة في إثراء الأدبيات العربية والسعودية المتعلقة بالأمن السيبراني الحكومي من خلال تقديم إطار نظري يربط بين معايير – NCA بوصفها متغيراً مستقلاً متعدد الأبعاد يشمل الحوكمة وتعزيز الأمن السيبراني وصموده ومكوناته المتعلقة بالأطراف الخارجية والحوسبة السحابية والأنظمة الصناعية – ومتغير الجاهزية للتصدي للاختراقات بوصفه متغيراً تابعاً يشمل أبعاد الوقاية والاكتشاف والاستجابة والتعافي. كما تُعدّ الدراسة إضافة معرفية تُقلّص الفجوة في الأبحاث التي تناولت أثر الأطر التنظيمية الوطنية على الأداء السيبراني للمؤسسات الحكومية في السياق السعودي، وتفتح المجال أمام دراسات لاحقة لاختبار النموذج في قطاعات أو مناطق جغرافية أخرى، أو لإجراء دراسات مقارنة مع أطر مماثلة في دول الخليج والشرق الأوسط. ويُتوقع أن تُسهّم نتائج الدراسة في تطوير الأدوات المفاهيمية المستخدمة في قياس النضج السيبراني المؤسسي، وفي تعميق فهم العلاقة بين الامتثال التنظيمي والصمود السيبراني الفعلي.

١.٣.٢. على المستوى التطبيقي:

تكتسب الدراسة أهميتها التطبيقية من كونها تقدّم تشخيصاً ميدانياً لواقع تطبيق معايير NCA في وزارات المنطقة الشرقية، وتوفّر للقيادات الحكومية ومسؤولي الأمن السيبراني صورة واضحة عن مستوى الجاهزية الفعلية ومواطن القوة والضعف في تطبيق الضوابط. كما تُسهّم نتائج الدراسة في تزويد الهيئة الوطنية للأمن السيبراني (NCA) بمؤشرات ميدانية مفيدة في مراجعة آليات الإشراف والمتابعة ودعم الجهات الحكومية في رحلة الامتثال، بما يُعزّز فاعلية المنظومة الوطنية ككل. ومن المتوقع أن تُفيد الدراسة الجهات الحكومية في توجيه

استثماراتها في الأمن السيبراني نحو الأبعاد الأكثر تأثيراً في الجاهزية، وفي تطوير برامج بناء القدرات والتدريب وفقاً للفجوات المُشخَّصة. كما قد تُشكّل التوصيات العملية للدراسة مرجعاً مساعداً لصنّاع القرار في تطوير السياسات الداخلية للوزارات، وتعزيز ثقافة الأمن السيبراني، وبناء قدرات الاستجابة للحوادث، بما يُسهم في النهاية في حماية الأصول الوطنية وتعزيز ثقة المستفيدين بالخدمات الحكومية الرقمية.

١,٤. أسئلة الدراسة

السؤال الرئيسي : ما أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية؟

ويتفرع من السؤال الرئيسي مجموعة من الأسئلة الفرعية على النحو الآتي:

١. ما أثر تطبيق بُعد حوكمة الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

٢. ما أثر تطبيق بُعد تعزيز الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

٣. ما أثر تطبيق بُعد صمود الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

٤. ما أثر تطبيق بُعد الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

٥. ما أثر تطبيق بُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

١,٥. أهداف الدراسة

تهدف هذه الدراسة إلى دراسة أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية.

وينبثق من هذا الهدف الرئيسي مجموعة من الأهداف الفرعية التي تُسهم مجتمعة في تحقيقه، وهي على النحو الآتي:

- قياس أثر بُعد حوكمة الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد تعزيز الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد صمود الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- الخروج بمجموعة من التوصيات والمقترحات العملية التي تُسهم في رفع كفاءة تطبيق معايير NCA، وتعزيز جاهزية المؤسسات الحكومية للتصدي للاختراقات، بما يدعم صناع القرار في الهيئة الوطنية للأمن السيبراني وفي الوزارات المعنية.

1.6. فرضيات الدراسة

في ضوء مشكلة الدراسة وأسئلتها وأهدافها، تسعى الدراسة إلى اختبار الفرضية الرئيسية الآتية:

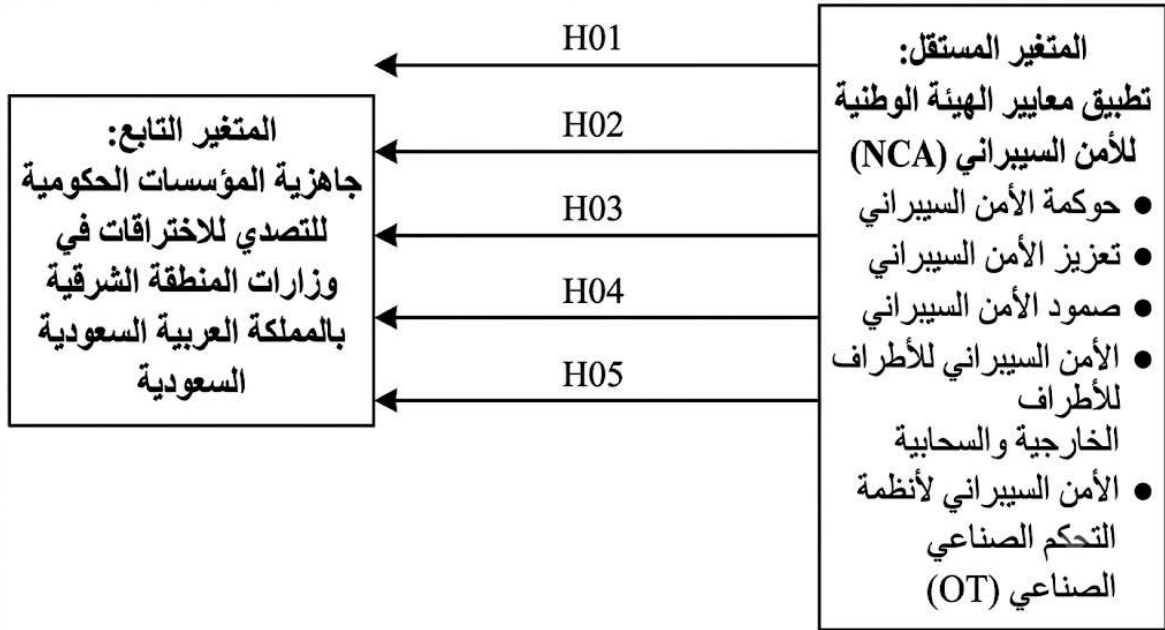
الفرضية الرئيسية: (H_0) لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لتطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها مجتمعةً (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية.

وتتفرع من الفرضية الرئيسية الفرضيات الفرعية الآتية:

- **H_{01} :** لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لتطبيق بُعد حوكمة الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- **H_{02} :** لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لتطبيق بُعد تعزيز الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- **H_{03} :** لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لتطبيق بُعد صمود الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- **H_{04} :** لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لتطبيق بُعد الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- **H_{05} :** لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) لتطبيق بُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.

1.7. نموذج الدراسة

يوضح نموذج الدراسة العلاقة السببية بين المتغير المستقل المتمثل في تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعاده الخمسة، والمتغير التابع المتمثل في جاهزية المؤسسات الحكومية للتصدي للاختراقات، وذلك على النحو الآتي:



1.8. منهجية الدراسة

سوف يعتمد الباحث في هذه الدراسة على **المنهج الوصفي التحليلي**، باعتباره الأنسب لطبيعة الدراسة وأهدافها، إذ سيقوم بوصف الظاهرة محل الدراسة وصفًا دقيقًا من خلال استعراض الإطار النظري والدراسات السابقة المتعلقة بمعايير الهيئة الوطنية للأمن السيبراني (NCA) وجاهزية المؤسسات الحكومية للتصدي للاختراقات، ثم تحليل البيانات التي سيتم جمعها ميدانيًا للوصول إلى نتائج علمية دقيقة تُسهم في اختبار فرضيات الدراسة والإجابة عن تساؤلاتها.

كما سوف يستخدم الباحث **المنهج الكمي** في مرحلة الدراسة الميدانية، من خلال تصميم استبانة إلكترونية تُوزَّع على مجتمع الدراسة، ثم معالجة البيانات إحصائيًا باستخدام برنامج (SPSS) للوصول إلى استنتاجات تعكس واقع تطبيق معايير NCA وأثرها على جاهزية المؤسسات الحكومية في وزارات المنطقة الشرقية بالمملكة العربية السعودية.

مجتمع وعينة الدراسة

سوف يتكون **مجتمع الدراسة** من العاملين في إدارات تقنية المعلومات والأمن السيبراني في الوزارات والجهات الحكومية العاملة في المنطقة الشرقية بالمملكة العربية السعودية، والبالغ عددهم التقريبي (١,٢٥٠) موظفًا موزعين على مختلف الوزارات والفروع الحكومية في المنطقة.

وسوف يقوم الباحث بسحب **عينة عشوائية طبقية** حجمها (٢٩٥) مفردة، وقد تم تحديد هذا الحجم بالاعتماد على معادلة (Steven K. Thompson) عند مستوى ثقة (٩٥٪) وهامش خطأ (٥٪)، حيث سيتم توزيع (٣٣٠) استبانة إلكترونية تحسبًا لعدم اكتمال بعض الاستجابات، ويُتوقع استرداد ما لا يقل عن (٣٠٠) استبانة صالحة للتحليل الإحصائي.

مصادر جمع البيانات

سوف يعتمد الباحث في جمع البيانات على مصدرين رئيسيين هما: **المصادر الثانوية**، والتي تشمل الكتب والمراجع العلمية والدوريات المحكمة والرسائل الجامعية والتقارير الرسمية الصادرة عن الهيئة الوطنية للأمن السيبراني، إضافةً إلى قواعد البيانات العلمية ذات الصلة بموضوع الدراسة؛ **والمصادر الأولية**، والتي ستُجمع بياناتها من الميدان مباشرةً عبر استبانة إلكترونية مصممة خصيصًا لأغراض هذه الدراسة.

أدوات الدراسة

سوف يستخدم الباحث **الاستبانة** أداةً رئيسيةً لجمع البيانات، وسيتم تصميمها وفقًا لمقياس ليكرت الخماسي، بعد التحقق من صدقها وثباتها من خلال عرضها على مجموعة من المحكمين الأكاديميين والمهنيين المتخصصين، وحساب معامل ثبات ألفا كرونباخ للتأكد من الاتساق الداخلي لفقراتها.

الأساليب الإحصائية المستخدمة

سوف يعتمد الباحث على مجموعة من الأساليب الإحصائية المناسبة لطبيعة الدراسة، تشمل: مقاييس الإحصاء الوصفي (المتوسطات الحسابية والانحرافات المعيارية والتكرارات والنسب المئوية)، ومعامل ألفا كرونباخ لقياس الثبات، ومعامل ارتباط بيرسون للصدق البنائي، واختبار التوزيع الطبيعي، ومعاملات VIF و Tolerance

لاختبار التداخل الخطي، فضلاً عن تحليل الانحدار الخطي المتعدد لاختبار الفرضيات وقياس أثر المتغيرات المستقلة على المتغير التابع.

حدود الدراسة

تقتصر حدود الدراسة على النحو الآتي: **الحدود الموضوعية** وتتمثل في دراسة أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها الخمسة على جاهزية المؤسسات الحكومية للتصدي للاختراقات؛ **والحدود المكانية** وتشمل الوزارات والجهات الحكومية في المنطقة الشرقية بالمملكة العربية السعودية؛ **والحدود البشرية** وتتضمن العاملين في إدارات تقنية المعلومات والأمن السيبراني في تلك الوزارات؛ **والحدود الزمانية** وتتمثل في الفترة الزمنية التي سيتم فيها تنفيذ الدراسة الميدانية خلال عام ٢٠٢٦م.

أداة الدراسة (توزيع الفقرات)

سوف تتكون الاستبانة من قسمين رئيسيين؛ يتضمن القسم الأول البيانات الديموغرافية للمستجيبين، بينما يشتمل القسم الثاني على فقرات قياس متغيرات الدراسة موزعةً على النحو الآتي:

المحور	المتغير	عدد الفقرات
المتغير المستقل	حوكمة الأمن السيبراني	4
المتغير المستقل	تعزيز الأمن السيبراني	4
المتغير المستقل	صمود الأمن السيبراني	4
المتغير المستقل	الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية	4
المتغير المستقل	الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية	4
المتغير التابع	جاهزية المؤسسات الحكومية للتصدي للاختراقات	10
إجمالي فقرات المقياس		30

1.9. الدراسة الميدانية

سوف يقوم الباحث بتنفيذ الدراسة الميدانية وفق خطوات علمية منظمة، تبدأ بتصميم الاستبانة الإلكترونية اعتمادًا على الإطار النظري والدراسات السابقة والوثيقة التنظيمية لمعايير الهيئة الوطنية للأمن السيبراني (NCA)، ثم عرضها على مجموعة من المحكمين المتخصصين للتحقق من صدقها الظاهري والمحتوى، يليها تطبيق دراسة استطلاعية على عينة محدودة قوامها (٣٠) مفردة من مجتمع الدراسة لاختبار ثبات الأداة وصلاحياتها.

وبعد التأكد من صلاحية الأداة، سوف يتم توزيعها إلكترونياً على أفراد العينة المستهدفة في وزارات المنطقة الشرقية، ثم تُجمع الاستجابات وتُفَرَّغ في برنامج (SPSS) لإجراء التحليلات الإحصائية اللازمة، وصولاً إلى النتائج التي سيتم مناقشتها في ضوء فرضيات الدراسة والدراسات السابقة، لتخرج الدراسة في نهايتها بمجموعة من التوصيات العملية.

1.10. مخطط المشروع المقترح (هيكل الدراسة)

سوف يتم تنظيم الدراسة في خمسة فصول رئيسية على النحو الآتي:

الفصل الأول: الإطار العام للدراسة يتضمن: المقدمة، مشكلة الدراسة، أهمية الدراسة، أسئلة الدراسة، أهداف الدراسة، فرضيات الدراسة، نموذج الدراسة، منهجية الدراسة، حدود الدراسة، ومصطلحات الدراسة.

الفصل الثاني: الإطار النظري والدراسات السابقة

- المبحث الأول: معايير الهيئة الوطنية للأمن السيبراني (NCA) وأبعادها.
- المبحث الثاني: جاهزية المؤسسات الحكومية للتصدي للاختراقات.
- المبحث الثالث: الدراسات السابقة العربية والأجنبية، والتعليق عليها، وموقع الدراسة الحالية منها.

الفصل الثالث: منهجية الدراسة وإجراءاتها يتضمن: منهج الدراسة، مجتمع وعينة الدراسة، أداة الدراسة، صدق الأداة وثباتها، الأساليب الإحصائية المستخدمة، وإجراءات تطبيق الدراسة الميدانية.

الفصل الرابع: عرض نتائج الدراسة الميدانية ومناقشتها يتضمن: الخصائص الديموغرافية للعينة، تحليل نتائج المحاور، اختبار الفرضيات، ومناقشة النتائج في ضوء الدراسات السابقة.

الفصل الخامس: النتائج والتوصيات يتضمن: خلاصة النتائج، التوصيات العملية، المقترحات للدراسات المستقبلية.

قائمة المراجع والملاحق.

الفصل الثاني: الدراسات السابقة

2.1 المقدمة

يُعدّ هذا الفصل حجر الأساس في البناء المعرفي والنظري للدراسة الحالية، إذ يستعرض الأدبيات والدراسات السابقة المرتبطة بمتغيرات البحث، ويسهم في تكوين رؤية علمية متكاملة حول موضوع الدراسة. وتتبع أهمية هذا الفصل من كونه يوفر خلفية نظرية عميقة حول تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بوصفه المتغير المستقل، وجاهزية المؤسسات الحكومية للتصدي للاختراقات بوصفها المتغير التابع، فضلاً عن استعراض العلاقة التي تربط بينهما في ضوء التحوّل الرقمي المتسارع الذي تشهده المؤسسات الحكومية في المملكة العربية السعودية عموماً، وفي وزارات المنطقة الشرقية على وجه الخصوص.

ويسعى هذا الفصل إلى تقديم إطار مفاهيمي متكامل لكل متغير من متغيرات الدراسة، بدءاً بتوضيح المفهوم والأهمية والأهداف والأبعاد، ومروراً باستعراض مجموعة من الدراسات العربية والأجنبية الحديثة التي تناولت هذه المتغيرات في سياقات متنوعة، ووصولاً إلى تحليل طبيعة العلاقة التي تربط بين المتغيرين المستقل والتابع. كما يهدف الفصل إلى تحديد الفجوة البحثية التي تسعى الدراسة الحالية إلى سدّها، من خلال المقارنة بين ما تم تناوله في الأدبيات السابقة وما ستضيفه هذه الدراسة من إسهام علمي جديد.

وقد جاء تنظيم هذا الفصل ليعكس التسلسل المنطقي في عرض المتغيرات ومناقشتها، حيث يبدأ بعرض المتغير المستقل ودراساته المرتبطة، ثم ينتقل إلى المتغير التابع بالمنهجية ذاتها، ثم يتناول العلاقة بين المتغيرين، ويُختتم بخاتمة تُلخّص أبرز ما تم استعراضه من أدبيات ودراسات.

2.2 المتغير المستقل: تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA)

2.2.1 تمهيد ومفهوم تطبيق معايير الهيئة الوطنية للأمن السيبراني

شهد العالم في العقدين الأخيرين تحولاً رقمياً عميقاً غير ملامح العمل المؤسسي في كافة القطاعات، وأصبحت البيانات والمعلومات الرقمية من أهم الأصول الاستراتيجية التي تمتلكها المؤسسات الحكومية والخاصة. وفي ظل تصاعد التهديدات السيبرانية وتنوّع أساليب الاختراق، برزت الحاجة الملحة إلى إرساء منظومات وطنية متكاملة للأمن السيبراني تضمن حماية البنى التحتية الحيوية والمعلومات الحساسة. وفي هذا السياق، أنشأت المملكة العربية السعودية الهيئة الوطنية للأمن السيبراني (NCA) عام ٢٠١٧ لتكون الجهة المختصة بالأمن السيبراني في المملكة، والمرجع الوطني في شؤونه، وتعمل على تعزيزه لحماية المصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

ويُعزف تطبيق معايير الهيئة الوطنية للأمن السيبراني بأنه المنظومة المتكاملة من الضوابط والسياسات والإجراءات التي أصدرتها الهيئة، والتي تلتزم الجهات الوطنية بتطبيقها لتحقيق الحد الأدنى من متطلبات الأمن السيبراني، بهدف حماية الأصول المعلوماتية والتقنية من التهديدات الداخلية والخارجية. ويشير أبو دولة والشوابة (٢٠٢٥) إلى أن معايير الأمن السيبراني تمثل مجموعة من الأطر التنظيمية والفنية والإدارية التي تُوفّر بيئة عمل آمنة، وتضمن سلامة البيانات وسريتها وتوافرها، وتُعزّز من قدرة المؤسسات على الاستمرارية في أداء مهامها. ويُضيف الفلاح والنسور والعربيات (٢٠٢٣) أن هذه المعايير تُشكّل خارطة طريق تنظيمية تُساعد المؤسسات على مواكبة التطورات التقنية المتسارعة، وتُوفّر مرجعية موحّدة تُقاس بها مستويات النضج السيبراني.

كما يُعرّفها الهاجري والبشاشة (٢٠٢١) بأنها منظومة متكاملة من الضوابط الأساسية التي تُعالج الجوانب المتعلقة بالحوكمة والمخاطر والامتثال، وتُغطّي كافة الجوانب التشغيلية والفنية والاستراتيجية للأمن السيبراني. وفي السياق الدولي، يرى Pemmasani (2023) أن الأطر الوطنية للأمن السيبراني تُمثّل الركيزة الأساسية لبناء المرونة السيبرانية على مستوى الدول، وتُساهم في حماية البنى التحتية الحيوية من الهجمات المتطورة. ويؤكد Gambo, Danasabe, Binbeshr, Imam, (2026) Shinwari, and Mahmoud (2026) على أن معايير الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية تُعدّ من أكثر الأطر شمولاً في المنطقة، إذ تُغطّي كافة الجوانب المتعلقة بالحوكمة والحماية والصمود والأطراف الخارجية وأنظمة التحكم الصناعي.

2.2.2 أهمية تطبيق معايير الهيئة الوطنية للأمن السيبراني

تتبع أهمية تطبيق معايير الهيئة الوطنية للأمن السيبراني من الدور المحوري الذي تلعبه في حماية المؤسسات من المخاطر السيبرانية المتزايدة، وتعزيز الثقة في الخدمات الرقمية الحكومية، وضمان استمرارية الأعمال في ظل بيئة تقنية شديدة التعقيد. وقد تناول العديد من الباحثين هذه الأهمية من زوايا متعددة، مما يعكس الاهتمام الأكاديمي والعملية المتنامي بهذا الموضوع.

ويشير الحلافي والعباس والمطيري (٢٠٢٦) إلى أن أهمية تطبيق معايير الأمن السيبراني تتجلى في عدة محاور، أبرزها: أولاً، الحدّ من المخاطر السيبرانية التي تواجه المؤسسات المالية والحكومية من خلال توفير ضوابط استباقية تُقلّل من احتمالية وقوع الاختراقات؛ ثانياً، تعزيز قدرة المؤسسات على الامتثال للتشريعات والأنظمة الوطنية والدولية ذات العلاقة؛ ثالثاً، حماية سمعة المؤسسات وتعزيز ثقة العملاء والمستفيدين في الخدمات المُقدّمة؛ رابعاً، تحسين الكفاءة التشغيلية من خلال تبني ممارسات أمنية موحّدة وفعّالة.

ويرى الحسيني والدعيمي (٢٠٢٥) أن أهمية معايير الأمن السيبراني تتمثّل في قدرتها على الحدّ من القصور الذاتي للمؤسسات، من خلال: تعزيز الوعي السيبراني لدى العاملين، وبناء ثقافة أمنية مؤسسية راسخة، وتوفير آليات واضحة للاستجابة للحوادث

السيبرانية، وضمان التعافي السريع بعد وقوع الاختراقات، فضلاً عن حماية الأصول المعلوماتية باعتبارها ثروة استراتيجية للمؤسسة.

ويُضيف نوار (٢٠٢٥) أن أهمية تطبيق متطلبات الأمن السيبراني تظهر في: دعم الحوكمة الرقمية داخل المؤسسات، وتحقيق التكامل بين الأنظمة التقنية المختلفة، وتوفير بيئة آمنة لتبادل البيانات والمعلومات، وتعزيز الشفافية والمساءلة في الأداء المؤسسي، وتمكين المؤسسات من مواكبة رؤية المملكة ٢٠٣٠ في مجال التحوّل الرقمي.

وفي السياق الدولي، يشير Majeed, Majeed, and Minhas (2026) إلى أن أهمية حوكمة الأمن السيبراني تتجلى في: بناء المرونة التنظيمية في مواجهة التهديدات المتطورة، ودمج إدارة المخاطر السيبرانية ضمن الاستراتيجية العامة للمؤسسة، وتعزيز الرقابة التنظيمية على الأصول الرقمية، وضمان استمرارية الأعمال في ظل الأزمات السيبرانية. كما يؤكد Rawindaran and Nawaf (2023) على أن معايير الأمن السيبراني تُشكّل عاملاً حاسماً في تعزيز تنافسية المؤسسات في عصر الصناعة ٥.٠، من خلال بناء ثقة الأطراف المعنية وتوفير بيئة رقمية آمنة تدعم الابتكار والنمو.

2.2.3 أهداف تطبيق معايير الهيئة الوطنية للأمن السيبراني

تسعى معايير الهيئة الوطنية للأمن السيبراني إلى تحقيق جملة من الأهداف الاستراتيجية والتشغيلية التي تخدم الرؤية الوطنية في بناء منظومة سيبرانية متكاملة. وقد تناول الباحثون هذه الأهداف بأساليب متعددة تعكس تنوّع الزوايا التي يمكن النظر منها إلى هذا الموضوع.

ويشير السرحان والمشاغبة (٢٠٢٠) إلى أن أهداف تطبيق سياسة الأمن السيبراني تتمثل فيما يلي: أولاً، حماية سرية المعلومات المؤسسية من الوصول غير المصرّح به؛ ثانياً، ضمان سلامة البيانات من التعديل أو التلاعب غير المشروع؛ ثالثاً، توفير المعلومات في الوقت المناسب للمستخدمين المصرّح لهم؛ رابعاً، تعزيز جودة المعلومات المحاسبية والإدارية في المؤسسات المالية؛ خامساً، بناء منظومة رقابية فعّالة تحدّ من المخاطر التشغيلية.

كما يشير صمادي والعليمات (٢٠٢٠) إلى أن أهداف تطبيق سياسة الأمن السيبراني تتضمن: تحسين جودة التدقيق الإلكتروني، وتعزيز الثقة في المخرجات الرقمية، وتوفير بيئة آمنة للتعاملات الإلكترونية، ودعم اقتصاد المعرفة من خلال حماية الأصول المعرفية، وبناء منظومة تكامل بين المؤسسات المختلفة تُتيح تبادلاً آمناً للمعلومات.

ويرى الفلاح والنسور والعربيات (٢٠٢٣) أن الأهداف الجوهرية لتطبيق معايير الأمن السيبراني تشمل: تحسين الأداء المؤسسي في قطاع الاتصالات، وتعزيز رضا العملاء عن الخدمات المُقدّمة، وحماية البنية التحتية الحيوية للاتصالات، والحدّ من الخسائر المالية الناجمة عن الحوادث السيبرانية، وتمكين المؤسسات من التوسّع الرقمي بثقة وأمان.

وفي السياق الدولي، يشير (Mohamed Noor, Moghavvemi, and Tajudeen (2026) إلى أن أهداف الجاهزية السيبرانية تتضمن: تعزيز الأداء الأمني للمؤسسات، وبناء قدرات استباقية للكشف عن التهديدات، وتطوير آليات فعالة للاستجابة للحوادث، وتحقيق التوافق بين الاستراتيجية الأمنية والاستراتيجية العامة للمؤسسة، وتعزيز ثقافة الأمن السيبراني على كافة المستويات التنظيمية. كما يُشير (Gambo and Danasabe (2026 إلى أن أهداف تطبيق المعايير السعودية للأمن السيبراني تشمل: بناء منظومة وطنية متكاملة، وتوحيد الممارسات الأمنية عبر القطاعات، وتعزيز التعاون الدولي في مجال الأمن السيبراني، ودعم التحول الرقمي للأمن ضمن رؤية ٢٠٣٠.

2.2.4 أبعاد تطبيق معايير الهيئة الوطنية للأمن السيبراني

تم تحديد أبعاد تطبيق معايير الهيئة الوطنية للأمن السيبراني بناءً على دراسة الحلافي والعباس والمطيري (٢٠٢٦) ودراسة (Gambo and Danasabe (2026 ودراسة أبو دولة والشوابكة (٢٠٢٥)، والتي تناولت الضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية. وتتضمن هذه الأبعاد خمسة محاور رئيسة تُشكل الإطار المتكامل لتطبيق المعايير، وفيما يلي شرح مفصل لهذه الأبعاد:

البُعد الأول: حوكمة الأمن السيبراني، ويُمثل هذا البُعد الركيزة الاستراتيجية التي تُبنى عليها منظومة الأمن السيبراني في المؤسسة، إذ يتضمن وضع السياسات والإجراءات الحاكمة، وتحديد الأدوار والمسؤوليات، وبناء الهيكل التنظيمي المناسب لإدارة الأمن السيبراني. ويشمل هذا البُعد إعداد استراتيجية الأمن السيبراني بما يتوافق مع الاستراتيجية العامة للمؤسسة، وتخصيص الموارد البشرية والمالية اللازمة، وضمان الالتزام بالتشريعات والأنظمة ذات العلاقة. كما يُركز على إدارة المخاطر السيبرانية من خلال تحديدها وتقييمها ومعالجتها ومراقبتها بشكل مستمر، إضافة إلى بناء برامج التوعية والتدريب لتعزيز الثقافة السيبرانية داخل المؤسسة.

البُعد الثاني: تعزيز الأمن السيبراني، ويتناول هذا البُعد الجوانب الفنية والتشغيلية المتعلقة بحماية الأصول المعلوماتية والتقنية للمؤسسة. ويتضمن إدارة الأصول من خلال حصرها وتصنيفها، وإدارة هويات المستخدمين وصلاحيات الوصول بحيث لا يحصل أي مستخدم على صلاحيات تزيد عن حاجته الوظيفية، وحماية الأنظمة والأجهزة من خلال التحديثات الأمنية الدورية وتطبيق الإعدادات الآمنة. كما يشمل حماية البريد الإلكتروني وشبكات الاتصال، وإدارة التشفير لحماية البيانات أثناء تخزينها ونقلها، وإدارة النسخ الاحتياطية لضمان استعادة البيانات عند الحاجة، وإدارة الثغرات الأمنية من خلال الفحص الدوري والمعالجة السريعة.

البُعد الثالث: صمود الأمن السيبراني، ويُعنى هذا البُعد بقدرة المؤسسة على الاستمرار في تقديم خدماتها ووظائفها الأساسية في مواجهة الحوادث السيبرانية والأزمات الطارئة. ويتضمن بناء خطط استمرارية الأعمال بما يشمل الجوانب السيبرانية، وإعداد خطط التعافي من الكوارث السيبرانية، وتحديد أزمدة الاستعادة المستهدفة، وإجراء اختبارات دورية للتأكد من فاعلية هذه الخطط. كما

يُركّز على بناء قدرات المؤسسة في الاستجابة للحوادث من خلال تشكيل فرق متخصصة، ووضع إجراءات واضحة للتعامل مع الحوادث، وتوثيق الدروس المستفادة لتحسين الأداء المستقبلي.

البُعد الرابع: الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، ويتناول هذا البُعد المخاطر السيبرانية الناجمة عن التعامل مع الأطراف الخارجية كالموردين ومقدّمي الخدمات، فضلاً عن استخدام خدمات الحوسبة السحابية. ويتضمن تقييم المخاطر المرتبطة بهذه الأطراف قبل التعاقد معها، وتضمن متطلبات الأمن السيبراني في العقود، والرقابة على التزامها بهذه المتطلبات طوال فترة التعاقد. كما يشمل وضع ضوابط خاصة باستخدام الخدمات السحابية بما يضمن حماية بيانات المؤسسة وسريتها، وتحديد مواقع تخزين البيانات، وضمان استعادتها عند إنهاء التعاقد.

البُعد الخامس: الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية، ويُعنى هذا البُعد بحماية الأنظمة التقنية التشغيلية وأنظمة التحكم الصناعي التي تُدير البنى التحتية الحيوية كالطاقة والمياه والاتصالات. ويتضمن الفصل بين الشبكات التشغيلية وشبكات تقنية المعلومات، وتطبيق ضوابط أمنية متخصصة تُراعي طبيعة هذه الأنظمة، وحمايتها من الهجمات المتطورة التي قد تستهدف تعطيل الخدمات الحيوية أو الإضرار بالبنية التحتية. كما يشمل إدارة الوصول إلى هذه الأنظمة بشكل صارم، ومراقبة الأنشطة عليها بشكل مستمر، وتحديث أنظمة الحماية بما يتوافق مع طبيعة التهديدات المتغيرة.

وإلى جانب هذه الأبعاد الخمسة، تجدر الإشارة إلى وجود عناصر مكملة تدعم تطبيق هذه المعايير، منها: التقييم الذاتي الدوري لمستوى الالتزام بالمعايير، والمراجعة الخارجية من قِبل جهات متخصصة، والتحسين المستمر بناءً على نتائج التقييمات والمراجعات، فضلاً عن التكامل مع المعايير الدولية كالأيزو ٢٧٠٠١ وإطار NIST لتعزيز الفاعلية والشمولية.

2.2.5 الدراسات السابقة المرتبطة بالمتغير المستقل

أولاً: الدراسات العربية

دراسة أبو دولة والشوابكة (2025) هدفت الدراسة إلى التعرف على أثر تطبيق معايير الأمن السيبراني بأبعاده (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني) على ممارسات إدارة الموارد البشرية في وكالة الأمم المتحدة لإغاثة وتشغيل اللاجئين الفلسطينيين (الأونروا) في إقليم الأردن. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (٢٨٥) موظفاً في الوكالة. وتوصلت نتائج الدراسة إلى وجود أثر ذي دلالة إحصائية لتطبيق معايير الأمن السيبراني على ممارسات إدارة الموارد البشرية، وأوصت بضرورة تعزيز برامج التوعية السيبرانية وتطوير السياسات المتعلقة بحماية بيانات الموظفين.

دراسة الفلاح والنسور والعربيات: (2023) هدفت الدراسة إلى التعرف على أثر تطبيق معايير الأمن السيبراني بأبعاده (السياسات والإجراءات، البنية التحتية، الوعي والتدريب، إدارة المخاطر) على أداء شركات الاتصالات الأردنية. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (٣١٠) موظفين في شركات الاتصالات. وتوصلت نتائج الدراسة إلى وجود أثر إيجابي ذي دلالة إحصائية لتطبيق معايير الأمن السيبراني على الأداء المؤسسي، وأوصت بضرورة الاستثمار في البنية التحتية السيبرانية وتطوير برامج التدريب المتخصصة.

دراسة الحلافي والعباس والمطيري: (2026) هدفت الدراسة إلى التعرف على أثر تطبيق معايير الأمن السيبراني بأبعاده (الحوكمة، التعزيز، الصمود، الأطراف الخارجية) في الحدّ من المخاطر في البنوك التجارية بمدينة الرياض. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (٢٤٠) موظفاً في البنوك التجارية. وتوصلت نتائج الدراسة إلى وجود أثر قوي لتطبيق معايير الأمن السيبراني في الحدّ من المخاطر المصرفية، وأوصت بتعزيز التعاون بين البنوك والهيئة الوطنية للأمن السيبراني.

ثانياً: الدراسات الأجنبية

:

دراسة: (2023) Pemmasani هدفت الدراسة إلى التعرف على دور الأطر الوطنية للأمن السيبراني في حماية البنية التحتية الحيوية، من خلال استخلاص الدروس المستفادة من المبادرات الحكومية للمرونة السيبرانية. واستخدمت الدراسة المنهج التحليلي المقارن، وتكونت العينة من مراجعة أطر الأمن السيبراني في عشر دول. وتوصلت نتائج الدراسة إلى أن الأطر الوطنية الشاملة تُعزّز بشكل كبير من مرونة البنية التحتية الحيوية، وأوصت الدراسة بتبني مقاربات متكاملة تجمع بين الحوكمة والضوابط الفنية والتعاون الدولي.

دراسة: (2023) Rawindaran and Nawaf هدفت الدراسة إلى التعرف على تعزيز حوكمة وسياسات الأمن السيبراني للمؤسسات الصغيرة والمتوسطة في ظل الصناعة ٥.٠، من خلال دراسة مقارنة بين المملكة العربية السعودية والمملكة المتحدة. واستخدمت الدراسة المنهج الوصفي المقارن، وتكونت العينة من (٢٠٠) مؤسسة صغيرة ومتوسطة موزعة بين البلدين. وتوصلت نتائج الدراسة إلى وجود فروق جوهرية في مستوى نضج ممارسات الأمن السيبراني بين البلدين، وأوصت الدراسة بتعزيز برامج النوعية وتبني أفضل الممارسات الدولية في المؤسسات الصغيرة والمتوسطة.

دراسة: (2026) Gambo and Danasabe هدفت الدراسة إلى التعرف على معايير الأمن السيبراني في المملكة العربية السعودية ومعوقات تطبيقها، وتحليل المشهد السيبراني في المملكة. واستخدمت الدراسة المنهج التحليلي النوعي، وتكونت العينة

من (٣٥) خبيراً ومسؤولاً في مجال الأمن السيبراني. وتوصلت نتائج الدراسة إلى تحديد عدد من معوقات التطبيق، منها: محدودية الكوادر البشرية المؤهلة، وقيود الميزانية، وتحديات الثقافة المؤسسية، وأوصت الدراسة بتعزيز برامج بناء القدرات، وتقوية التعاون بين الهيئة الوطنية للأمن السيبراني والمؤسسات في مختلف القطاعات.

2.3.2 المتغير التابع: جاهزية المؤسسات الحكومية للتصدي للاختراقات

2.3.1.1 تمهيد ومفهوم جاهزية المؤسسات الحكومية

تُعدّ جاهزية المؤسسات الحكومية للتصدي للاختراقات السيبرانية من أهم المفاهيم الحديثة في مجال الإدارة العامة والأمن السيبراني، إذ تعكس قدرة هذه المؤسسات على مواجهة التهديدات الرقمية المتطورة وحماية أصولها المعلوماتية وضمان استمرارية خدماتها. وقد اكتسب هذا المفهوم أهمية متزايدة في ظل التوسّع الرقمي الذي تشهده الحكومات حول العالم، وارتفاع وتيرة الهجمات السيبرانية التي تستهدف القطاع الحكومي بشكل خاص لما يمتلكه من بيانات حساسة وبنى تحتية حيوية.

ويُعرّف (Mohamed Noor and Moghavvemi (2026) الجاهزية السيبرانية بأنها الحالة التي تكون فيها المؤسسة مُهيأةً تنظيمياً وفنياً وبشرياً لمواجهة التهديدات السيبرانية، والاستجابة الفعّالة للحوادث، والتعافي السريع منها بأقل قدر من الخسائر. ويرى (Gorenšek and Trivunčević (2025 أن الجاهزية السيبرانية تتجاوز مجرد امتلاك الأدوات التقنية إلى بناء منظومة متكاملة تشمل الاستراتيجية والحوكمة والقدرات البشرية والثقافة المؤسسية.

ويُشير (Zubaidah and Monalisa (2024 إلى أن الجاهزية الإلكترونية للمؤسسات الحكومية تُمثّل مقياساً لمدى استعدادها للتحوّل الرقمي وتقديم الخدمات الإلكترونية بكفاءة وأمان. كما يُعرّفها (Yusuf (2021 بأنها القدرة المؤسسية على تبني التقنيات الحديثة والتكيف مع المتطلبات الرقمية المتغيرة، مع ضمان توفّر الكفاءات البشرية والبنية التحتية اللازمة. وفي السياق العربي، يُشير الهاجري والبشاشة (٢٠٢١) إلى أن جاهزية المؤسسات الحكومية تتضمن قدرتها على استشعار التهديدات مبكراً، والاستجابة لها بفاعلية، والتعافي منها بأقل التكاليف الممكنة، مما يُعزّز من ثقة المواطنين في الخدمات الحكومية الرقمية.

2.3.2 أهمية جاهزية المؤسسات الحكومية للتصدي للاختراقات

تتبع أهمية جاهزية المؤسسات الحكومية للتصدي للاختراقات من الطبيعة الاستراتيجية للقطاع الحكومي والدور المحوري الذي يلعبه في تقديم الخدمات للمواطنين وحماية المصالح الوطنية. وقد تناول الباحثون هذه الأهمية من زوايا متعددة تعكس أبعاد هذا الموضوع.

ويشير (Murad and Qudah (2025) إلى أن أهمية الجاهزية السيبرانية للمؤسسات الوطنية تتمثل فيما يلي: أولاً، حماية الأمن الوطني من التهديدات السيبرانية التي قد تستهدف البنى التحتية الحيوية؛ ثانياً، ضمان استمرارية الخدمات الحكومية المُقدّمة للمواطنين دون انقطاع؛ ثالثاً، حماية البيانات الحساسة للمواطنين والمؤسسات؛ رابعاً، تعزيز الثقة العامة في الحكومة الإلكترونية والخدمات الرقمية؛ خامساً، الحدّ من الخسائر المالية الناجمة عن الاختراقات السيبرانية.

ويرى (Gorenšek and Trivunčević (2025 أن أهمية الجاهزية السيبرانية تتجلى في: بناء المرونة الوطنية في مواجهة الحرب السيبرانية، وتعزيز التنافسية الرقمية للدولة على المستوى الدولي، ودعم التحوّل الرقمي بشكل آمن ومستدام، وحماية الاستثمارات التقنية الضخمة التي تضخّها الحكومات، وبناء منظومة تعاون إقليمي ودولي في مجال الأمن السيبراني.

ويُضيف الهاجري والبشاشة (٢٠٢١) أن أهمية جاهزية المؤسسات الحكومية تظهر في: تعزيز قدرة الأجهزة الحكومية على إدارة الأزمات السيبرانية بفاعلية، وتوفير بيئة رقمية آمنة لتنفيذ الاستراتيجيات الوطنية، وبناء ذكاء استراتيجي يُمكن من استشعار التهديدات مبكراً، ودعم اتخاذ القرارات المبنية على معلومات دقيقة وآمنة.

ويشير نوار (٢٠٢٥) إلى أن أهمية الجاهزية السيبرانية للمؤسسات الحكومية تتمثل في: دعم الحوكمة الرقمية وتحقيق أهدافها، وضمان جودة الخدمات الرقمية المُقدّمة، وتعزيز الشفافية والمساءلة في العمل الحكومي، وتمكين المؤسسات من مواكبة التطورات التقنية المتسارعة، وحماية سمعة المؤسسات الحكومية من الأضرار الناجمة عن الاختراقات.

كما يرى (Almaiah and Alfaisal (2022 أن أهمية الجاهزية المؤسسية تتضمن: تعزيز قدرة المؤسسات على تبني التقنيات الناشئة كالذكاء الاصطناعي بشكل آمن، وبناء ميزة تنافسية مستدامة، وتحسين تجربة المستخدمين، ودعم الابتكار المؤسسي، وتحقيق التميز في الأداء التشغيلي.

2.3.3 أهداف تحقيق جاهزية المؤسسات الحكومية للتصدي للاختراقات

تسعى المؤسسات الحكومية إلى تحقيق جاهزيتها السيبرانية من خلال مجموعة من الأهداف الاستراتيجية والتشغيلية التي تخدم رسالتها ورؤيتها. وقد تناول الباحثون هذه الأهداف بأساليب متنوعة.

ويشير (Mohamed Noor and Moghavvemi (2026 إلى أن أهداف الجاهزية السيبرانية تتضمن ما يلي: أولاً، تحقيق الأداء الأمني الأمثل للمؤسسة من خلال بناء قدرات دفاعية متكاملة؛ ثانياً، الكشف المبكر عن التهديدات السيبرانية قبل تحويلها إلى حوادث فعلية؛ ثالثاً، الاستجابة السريعة والفعالة للحوادث السيبرانية عند وقوعها؛ رابعاً، التعافي السريع من الحوادث بأقل الخسائر الممكنة؛ خامساً، التعلم المستمر من الحوادث لتحسين الأداء المستقبلي.

كما يشير (Gorenšek and Trivunčević 2025) إلى أن أهداف الجاهزية السيبرانية على المستوى الوطني تشمل: بناء استراتيجيات وطنية متكاملة، وتطوير مؤشرات قياس عالمية للجاهزية السيبرانية، وتعزيز التعاون الإقليمي في منطقة الاتحاد الأوروبي المتوسطي، وبناء قدرات وطنية في مجال الاستخبارات السيبرانية، وتحسين ترتيب الدول في المؤشرات الدولية للأمن السيبراني.

ويرى (Kulin and Johansson Sevä 2021) أن أهداف بناء الثقة في المؤسسات الحكومية تتضمن: تعزيز الشفافية في اتخاذ القرارات، وبناء علاقات إيجابية مع المواطنين، ودعم المشاركة العامة في السياسات الحكومية، وضمان الحيادية والنزاهة في الأداء المؤسسي، وتحقيق التوازن بين الأهداف الأمنية والحقوق الفردية.

ويشير (Zubaidah and Monalisa 2024) إلى أن أهداف الجاهزية الإلكترونية للمؤسسات الحكومية تتمثل في: تسريع التحول نحو الحكومة الإلكترونية، وتحسين كفاءة تقديم الخدمات، وخفض التكاليف التشغيلية، وتعزيز التكامل بين المؤسسات الحكومية المختلفة، وبناء منظومة بيانات موحدة تدعم اتخاذ القرارات.

كما يشير الحسيني والدعيمي (٢٠٢٥) إلى أن الأهداف التي تسعى الجاهزية السيبرانية إلى تحقيقها تتضمن: الحد من القصور الذاتي للمؤسسات، وتعزيز قدرتها على التكيف مع المتغيرات، وبناء ثقافة الابتكار والتحسين المستمر، ودعم اتخاذ القرارات الاستراتيجية بمعلومات دقيقة وآمنة، وتحقيق التميز المؤسسي المستدام.

2.3.4 أبعاد جاهزية المؤسسات الحكومية للتصدي للاختراقات

تم تحديد أبعاد جاهزية المؤسسات الحكومية للتصدي للاختراقات بناءً على دراسة (Mohamed Noor and Moghavvemi 2026) ودراسة (Gorenšek and Trivunčević 2025) ودراسة (Murad and Qudah 2025)، والتي تناولت هذه الجاهزية بشكل شامل ومتكامل. وتتضمن هذه الأبعاد المحاور الرئيسية التالية:

البُعد الأول: الجاهزية الاستراتيجية والتخطيطية، ويمثل هذا البُعد الركيزة الأساسية للجاهزية السيبرانية، إذ يتضمن وجود استراتيجية واضحة للأمن السيبراني على مستوى المؤسسة، تتوافق مع الاستراتيجية الوطنية للأمن السيبراني، وتتضمن رؤية ورسالة وأهدافاً واضحة قابلة للقياس. كما يشمل هذا البُعد التخطيط طويل المدى لمواجهة التهديدات المستقبلية، وتخصيص الميزانيات اللازمة، وبناء خارطة طريق زمنية لتطوير القدرات السيبرانية، فضلاً عن ربط الاستراتيجية السيبرانية بالخطط التنموية الوطنية ومواءمتها مع رؤية المملكة ٢٠٣٠.

البُعد الثاني: الجاهزية التقنية والبنية التحتية، ويتناول هذا البُعد الجوانب الفنية والتكنولوجية اللازمة لبناء منظومة أمنية فعّالة. ويتضمن توفير البنية التحتية التقنية المتطورة، وتطبيق أحدث تقنيات الحماية كأنظمة كشف التسلل وأنظمة منع الاختراق وجدران

الحماية المتقدمة، واستخدام تقنيات التشفير الحديثة، وتطبيق تقنيات التحليل الذكي للتهديدات باستخدام الذكاء الاصطناعي وتعلم الآلة. كما يشمل هذا البُعد بناء مراكز عمليات أمنية (SOC) تعمل على مدار الساعة، وتوفير أدوات الاستجابة للحوادث، وضمان التحديث المستمر للأنظمة والبرامج.

البُعد الثالث: الجاهزية البشرية والكوادر المتخصصة، ويُعنى هذا البُعد بتوفر الكوادر البشرية المؤهلة والمتخصصة في مجال الأمن السيبراني. ويتضمن استقطاب المواهب المتميزة، وتطوير برامج التدريب والتأهيل المستمر للعاملين، وبناء مسارات مهنية واضحة للمتخصصين في الأمن السيبراني، وتنظيم برامج التوعية السيبرانية لجميع العاملين في المؤسسة. كما يشمل بناء الشراكات مع الجامعات ومراكز التدريب المتخصصة، والاستفادة من الشهادات المهنية الدولية، وتطوير قدرات القيادات في اتخاذ القرارات المتعلقة بالأمن السيبراني.

البُعد الرابع: الجاهزية التنظيمية والإدارية، ويتناول هذا البُعد الجوانب المتعلقة بالهيكل التنظيمي والسياسات والإجراءات الداعمة للأمن السيبراني. ويتضمن وجود هيكل تنظيمي واضح لإدارة الأمن السيبراني، وتحديد الأدوار والمسؤوليات، ووضع السياسات والإجراءات المكتوبة والمعتمدة، وبناء نظام إدارة المخاطر السيبرانية. كما يشمل تفعيل مبدأ الفصل بين المهام، وبناء آليات الرقابة الداخلية، وتوثيق الإجراءات، وضمان التحسين المستمر للممارسات التنظيمية.

البُعد الخامس: الجاهزية للاستجابة والتعافي، ويُركز هذا البُعد على قدرة المؤسسة على الاستجابة الفعالة للحوادث السيبرانية والتعافي منها. ويتضمن وجود خطط مكتوبة للاستجابة للحوادث، وتشكيل فرق متخصصة (CERT/CSIRT)، وإجراء تمارين محاكاة دورية، ووجود قنوات اتصال واضحة مع الجهات المعنية داخلياً وخارجياً. كما يشمل بناء خطط استمرارية الأعمال، وضمان توفر النسخ الاحتياطية، وتحديد أزمّة الاستعادة المستهدفة، وتوثيق الدروس المستفادة من كل حادثة.

وإلى جانب هذه الأبعاد، تُضاف عناصر مكملة تُعزز جاهزية المؤسسات الحكومية، منها: الجاهزية الثقافية التي تعكس مستوى الوعي السيبراني ودمج قيم الأمن في ثقافة المؤسسة، والجاهزية للتعاون والشراكات مع الجهات الوطنية والدولية لتبادل المعلومات والخبرات، والجاهزية للتقييم والتحسين المستمر من خلال إجراء تقييمات دورية ذاتية وخارجية، ومقارنة الأداء بأفضل الممارسات العالمية.

2.3.5 الدراسات السابقة المرتبطة بالمتغير التابع

أولاً: الدراسات العربية

دراسة الهاجري والشاباشة: (2021) هدفت الدراسة إلى التعرف على أثر الذكاء الاستراتيجي على استراتيجيات إدارة الأزمات من خلال استراتيجية الأمن السيبراني بأبعادها (الاستشعار، الاستجابة، التعافي) بالتطبيق على الأجهزة الحكومية في دولة قطر.

واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (350) موظفاً في الأجهزة الحكومية القطرية. وتوصلت نتائج الدراسة إلى وجود دور وسيط للأمن السيبراني في العلاقة بين الذكاء الاستراتيجي وإدارة الأزمات، وأوصت بضرورة تعزيز الجاهزية السيبرانية للأجهزة الحكومية وبناء استراتيجيات متكاملة لإدارة الأزمات السيبرانية.

دراسة نوار: (2025) هدفت الدراسة إلى التعرف على أثر تطبيق متطلبات الأمن السيبراني بأبعاده (الحوكمة، الحماية، الصمود) على الحوكمة الرقمية بمديرية الشباب والرياضة بمحافظة الإسكندرية. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (١٨٠) موظفاً في المديرية. وتوصلت نتائج الدراسة إلى وجود أثر إيجابي قوي لمتطلبات الأمن السيبراني على الحوكمة الرقمية، وأوصت بتطوير برامج التوعية وتحديث البنية التحتية التقنية.

دراسة السرحان والمشاقبة: (2020) هدفت الدراسة إلى التعرف على أثر تطبيق سياسة الأمن السيبراني بأبعادها (السرية، السلامة، التوافر) على جودة المعلومات المحاسبية في البنوك التجارية الأردنية. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (٢٢٠) موظفاً في البنوك التجارية. وتوصلت نتائج الدراسة إلى وجود أثر ذي دلالة إحصائية لسياسة الأمن السيبراني على جودة المعلومات المحاسبية، وأوصت بضرورة الاستمرار في تطوير السياسات الأمنية وتحديثها بشكل دوري.

ثانياً: الدراسات الأجنبية

:

دراسة: (2026) Mohamed Noor and Moghavvemi هدفت الدراسة إلى التعرف على أثر الجاهزية السيبرانية على الأداء الأمني للمؤسسات بأبعادها (الجاهزية الاستراتيجية، الجاهزية التقنية، الجاهزية البشرية، الجاهزية التشغيلية) على المؤسسات المالية. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (٣١٢) مديراً ومختصاً في المؤسسات المالية. وتوصلت نتائج الدراسة إلى وجود أثر إيجابي قوي للجاهزية السيبرانية على الأداء الأمني، وأوصت الدراسة بالاستثمار في بناء قدرات سيبرانية متكاملة وتطوير برامج التدريب المتخصصة.

دراسة: (2025) Gorenšek and Trivunčević هدفت الدراسة إلى التعرف على الجاهزية السيبرانية في منطقة الاتحاد الأوروبي المتوسطي، من خلال مراجعة مقارنة للأدبيات المتعلقة بالاستراتيجيات الوطنية والمؤشرات العالمية. واستخدمت الدراسة منهج المراجعة المنهجية للأدبيات، وتكونت العينة من (٨٥) دراسة وتقريراً حول الجاهزية السيبرانية الوطنية. وتوصلت نتائج الدراسة إلى وجود تفاوت كبير في مستويات الجاهزية السيبرانية بين دول منطقة الاتحاد الأوروبي المتوسطي، وأوصت الدراسة بتعزيز التعاون الإقليمي وتوحيد معايير التقييم.

دراسة: (Murad and Qudah (2025) هدفت الدراسة إلى التعرف على اتجاهات الإعلاميين نحو الأمن السيبراني فيما يتعلق بالأمن والسلامة في المؤسسات الوطنية بأبعادها (الوعي، الالتزام، المشاركة). واستخدمت الدراسة المنهج الوصفي المسحي، وتكونت العينة من (٢٧٥) (إعلامياً في المؤسسات الوطنية الأردنية. وتوصلت نتائج الدراسة إلى وجود اتجاهات إيجابية نحو الأمن السيبراني، مع وجود فجوة في التطبيق العملي، وأوصت الدراسة بتطوير برامج التوعية وتعزيز ثقافة الأمن السيبراني في المؤسسات الوطنية.

2.4 العلاقة بين المتغير المستقل والمتغير التابع

تُعدّ العلاقة بين تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) وجاهزية المؤسسات الحكومية للتصدي للاختراقات من العلاقات المحورية التي تحظى باهتمام بالغ في الأدبيات الأكاديمية والممارسات المهنية على حدٍ سواء. وتنطلق هذه العلاقة من فرضية أساسية مفادها أن تطبيق معايير أمنية موحدة وشاملة يُسهم بشكل مباشر في رفع مستوى الجاهزية السيبرانية للمؤسسات وتعزيز قدرتها على مواجهة التهديدات المتنامية.

ويمكن تحليل هذه العلاقة من خلال عدة زوايا مترابطة. فمن الناحية الاستراتيجية، تُوفّر معايير الهيئة الوطنية للأمن السيبراني إطاراً استراتيجياً واضحاً يُمكن المؤسسات الحكومية من بناء رؤيتها الأمنية وربطها بالاستراتيجية الوطنية. فبعد حوكمة الأمن السيبراني في معايير NCA يُسهم بشكل مباشر في تعزيز الجاهزية الاستراتيجية والتخطيطية للمؤسسات، من خلال إلزامها بوضع سياسات واستراتيجيات مكتوبة ومعتمدة، وتحديد الأدوار والمسؤوليات، وبناء إطار متكامل لإدارة المخاطر. وقد أكد Majeed (2026) على أن حوكمة الأمن السيبراني تُعدّ الركيزة الأساسية لبناء المرونة التنظيمية والاستعداد الاستراتيجي للمؤسسات في مواجهة التهديدات السيبرانية.

ومن الناحية الفنية والتقنية، يرتبط بُعد تعزيز الأمن السيبراني في معايير NCA ارتباطاً وثيقاً بالجاهزية التقنية للمؤسسات، إذ يفرض تطبيق مجموعة من الضوابط الفنية كإدارة الأصول والهويات وحماية الأنظمة والتشفير، مما يُسهم في بناء بنية تحتية تقنية قوية قادرة على التصدي للاختراقات. ويؤكد Pemmasani (2023) على أن الأطر الوطنية للأمن السيبراني تُسهم بشكل كبير في تعزيز البنية التحتية التقنية للمؤسسات، وتُوفّر لها الأدوات والآليات اللازمة للكشف عن التهديدات والاستجابة لها.

ومن الناحية التشغيلية، يُعزّز بُعد صمود الأمن السيبراني الجاهزية للاستجابة والتعافي، من خلال إلزام المؤسسات ببناء خطط استمرارية الأعمال والتعافي من الكوارث، وتشكيل فرق متخصصة للاستجابة للحوادث. وقد أشارت دراسة الحلافي والعباس والمطيري (٢٠٢٦) إلى أن تطبيق هذا البُعد يُسهم بشكل مباشر في الحدّ من الآثار السلبية للاختراقات وتقليل زمن التعافي منها. كما أكدت دراسة Mohamed Noor and Moghavvemi (2026) على وجود علاقة إيجابية قوية بين مستوى الجاهزية السيبرانية والأداء الأمني للمؤسسات، مما يُدعم فرضية أن تطبيق المعايير يُنتج جاهزية أعلى وأداءً أمنياً أفضل.

وعلى صعيد إدارة المخاطر الخارجية، يُسهم بُعد الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية في تعزيز جاهزية المؤسسات الحكومية للتعامل مع المخاطر الناجمة عن الاعتماد المتزايد على مقدّمي الخدمات الخارجيين وخدمات السحابة. ويرى (Rawindaran and Nawaf (2023 أن إدارة مخاطر الأطراف الخارجية أصبحت من أهم متطلبات الجاهزية السيبرانية في العصر الحالي، خاصة في ظل التوسّع في استخدام الحوسبة السحابية وتقنيات إنترنت الأشياء.

كما يرتبط بُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية بجاهزية المؤسسات الحكومية لحماية البنى التحتية الحيوية التي تُدير الخدمات الأساسية للمواطنين. فتطبيق هذا البُعد يُعزّز من قدرة الوزارات والجهات الحكومية على حماية أنظمتها التشغيلية من الهجمات المتطورة التي قد تستهدف تعطيل الخدمات العامة. وقد أكّد (Gambo and Danasabe (2026 على أن حماية الأنظمة التشغيلية تُشكّل تحدياً كبيراً في المملكة العربية السعودية، وأن معايير NCA تُوفّر إطاراً متكاملًا لمعالجة هذا التحدي.

ومن الناحية البشرية والثقافية، يُسهم تطبيق معايير NCA بشكل عام في تعزيز الجاهزية البشرية للمؤسسات من خلال ما تفرضه من متطلبات للتدريب والتوعية وبناء القدرات. وقد أشارت دراسة أبو دولة والشوابكة (٢٠٢٥) إلى أن تطبيق معايير الأمن السيبراني يُسهم بشكل ملموس في تطوير الكوادر البشرية وبناء ثقافة مؤسسية داعمة للأمن السيبراني، مما يُعزّز من الجاهزية الشاملة للمؤسسة.

وتُشير الأدبيات كذلك إلى أن العلاقة بين المتغيرين ليست علاقة خطية بسيطة، بل علاقة تفاعلية معقدة تتأثر بعوامل وسيطة عدة، منها: مستوى الدعم القيادي، وتوفّر الموارد المالية، ومدى نضج الثقافة المؤسسية، وطبيعة القطاع الذي تعمل فيه المؤسسة. فقد أوضح (Murad and Qudah (2025 أن الجاهزية السيبرانية لا تتحقق بمجرد وجود معايير مكتوبة، بل تتطلب التزاماً قيادياً واعياً وثقافة مؤسسية داعمة وموارد كافية للتطبيق الفعلي.

وعلى المستوى النظري، يُمكن تفسير هذه العلاقة من خلال عدة نظريات، منها: نظرية المؤسسات (Institutional Theory) التي تُشير إلى أن الالتزام بالمعايير المؤسسية يُعزّز من شرعية المؤسسة وقدرتها على البقاء، ونظرية النضج المؤسسي (Organizational Maturity Theory) التي تربط بين مستوى تطبيق الممارسات المعيارية ومستوى النضج المؤسسي. كما يُمكن الاستناد إلى نظرية إدارة المخاطر التي تُقدّم إطاراً لفهم كيف يُسهم تطبيق الضوابط المعيارية في تقليل المخاطر وتعزيز الجاهزية.

وفي السياق التطبيقي للمملكة العربية السعودية، تكتسب هذه العلاقة أهمية استثنائية في ضوء التوجّهات الاستراتيجية لرؤية المملكة ٢٠٣٠ التي تُركّز على التحوّل الرقمي وبناء اقتصاد المعرفة. فتطبيق معايير NCA في وزارات المنطقة الشرقية يُمثّل

ركيزة أساسية لبناء جاهزية سيبرانية تُمكن هذه الوزارات من تقديم خدماتها الرقمية بأمان وفعالية، وحماية البيانات الحساسة للمواطنين، والمساهمة في بناء منظومة حكومية رقمية متكاملة وآمنة.

وخلاصة القول، فإن العلاقة بين تطبيق معايير الهيئة الوطنية للأمن السيبراني وجاهزية المؤسسات الحكومية للتصدي للاختراقات هي علاقة إيجابية تكاملية، إذ يُشكّل كل بُعد من أبعاد المعايير رافداً مباشراً لأحد أبعاد الجاهزية أو أكثر، ويُساهم في المحصلة النهائية في بناء منظومة سيبرانية وطنية قوية قادرة على مواجهة التحديات الراهنة والمستقبلية.

2.5 الخاتمة

استعرض هذا الفصل الأدبيات والدراسات السابقة المرتبطة بمتغيرات الدراسة الحالية، حيث تم تناول المتغير المستقل المتمثل في تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) من خلال عرض مفهومه وأهميته وأهدافه وأبعاده الخمسة (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية). كما تم استعراض المتغير التابع المتمثل في جاهزية المؤسسات الحكومية للتصدي للاختراقات بأبعاده المتعددة، وتحليل العلاقة التي تربط بين المتغيرين.

وقد اتضح من خلال استعراض الدراسات السابقة العربية والأجنبية أن هناك اهتماماً أكاديمياً متزايداً بموضوع الأمن السيبراني عموماً، ومعايير الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية خصوصاً. كما تبين أن معظم الدراسات السابقة أكّدت على وجود علاقة إيجابية بين تطبيق معايير الأمن السيبراني والأداء المؤسسي والجاهزية للتصدي للتهديدات السيبرانية، وإن تفاوتت هذه الدراسات في السياقات التطبيقية والقطاعات المدروسة.

وعلى الرغم من ثراء الأدبيات السابقة، إلا أن الدراسة الحالية تُميّز نفسها بتركيزها على وزارات المنطقة الشرقية بالمملكة العربية السعودية، ودراسة الأثر الشامل لأبعاد معايير NCA الخمسة على جاهزية المؤسسات الحكومية للتصدي للاختراقات، مما يُشكّل إضافة نوعية للأدبيات المتوفرة ويُسدّ فجوة بحثية ملموسة. كما تستفيد الدراسة الحالية من الأطر النظرية والمنهجية التي قدّمتها الدراسات السابقة، وتبني عليها لتقديم رؤية متكاملة تخدم صانعي القرار والممارسين في مجال الأمن السيبراني في القطاع الحكومي السعودي.

ويُشكّل هذا الفصل الأساس المعرفي والنظري الذي ينطلق منه الفصل التالي في بناء المنهجية والإجراءات المتبعة في الدراسة، والذي سيتناول تصميم الدراسة ومجتمعها وعينيتها وأدواتها والمعالجات الإحصائية المستخدمة للإجابة عن أسئلة الدراسة واختبار فرضياتها.

قائمة المراجع

- أبو دولة، سناء إسماعيل محمود، و الشوابكة، زياد علي عيد. (٢٠٢٥). أثر تطبيق معايير الأمن السيبراني على ممارسات إدارة الموارد البشرية في وكالة الأمم المتحدة لإغاثة وتشغيل اللاجئين الفلسطينيين في الشرق الأدنى – إقليم الأردن (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من <http://search.mandumah.com/Record/1608363>
- الهاجري، راشد محمد علي الفهيد، و البشاشة، سامر عبدالمجيد هزيم. (٢٠٢١). أثر الذكاء الاستراتيجي على استراتيجيات إدارة الأزمات من خلال استراتيجية الأمن السيبراني بالتطبيق على الأجهزة الحكومية في دولة قطر (رسالة دكتوراه غير منشورة). جامعة مؤتة، مؤتة. مسترجع من <http://search.mandumah.com/Record/1277187>
- الفلاح، حسام محمد سليمان، النسور، مروان محمد عبد، و العريبات، أيمن عبدالهادي. (٢٠٢٣). أثر تطبيق معايير الأمن السيبراني على أداء شركات الاتصالات الأردنية (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من <http://search.mandumah.com/Record/1460405>
- الحسيني، سرور حافظ، و الدعيمي، وليد عباس جبر. (٢٠٢٥). أثر الأمن السيبراني في الحد من القصور الذاتي للمصارف. مجلة الغري للعلوم الاقتصادية والإدارية، مج ٢١، ع ٢٤، ٤١٥ - ٤٤٧. مسترجع من <http://search.mandumah.com/Record/1604136>
- صمادي، نور الهدى أحمد يوسف، و العليمات، نوفان حامد محمد. (٢٠٢٠). أثر اقتصاد المعرفة على جودة التدقيق الإلكتروني في ظل تطبيق سياسة الأمن السيبراني: دراسة ميدانية على مكاتب التدقيق الأردنية (رسالة ماجستير غير منشورة). جامعة آل البيت، المفرق. مسترجع من <http://search.mandumah.com/Record/1140998>
- السرхан، حنين عبدالمهدي سالم، و المشاقبة، محمد ناصر موسى حمدان. (٢٠٢٠). أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة آل البيت، المفرق. مسترجع من <http://search.mandumah.com/Record/1094365>
- نوار، سلمى عصام محمد. (٢٠٢٥). أثر تطبيق متطلبات الأمن السيبراني على الحوكمة الرقمية بمديرية الشباب والرياضة بمحافظة الإسكندرية. المجلة العلمية للبحوث والدراسات في التربية الرياضية، ع ٤٩٤، ١٥٤ - ٢٠٨. مسترجع من <http://search.mandumah.com/Record/1591679>
- الحلافي، حسن خضر، العباس، المعتصم خليل، و المطيري، منى بنت جزاء. (٢٠٢٦). أثر تطبيق معايير الأمن السيبراني في الحد من المخاطر في البنوك التجارية بمدينة الرياض خلال العام ٢٠٢٥. مجلة العلوم الاقتصادية والإدارية والقانونية، مج ١٠، ع ٢٤، ١ - ١٠. مسترجع من <http://search.mandumah.com/Record/1666230>

Pemmasani, P. K. (2023). National cybersecurity frameworks for critical infrastructure: Lessons from governmental cyber resilience initiatives. *International Journal of Acta Informatica*, 2(1), 209-218

Mohamed Noor, A. F., Moghavvemi, S., & Tajudeen, F. P. (2026). Assessing the impact of cybersecurity readiness on organizational security performance: a study on Malaysian organizations. *Journal of Enterprise Information Management*, 39(3), 907-927.

Majeed, Y., Majeed, A., & Minhas, M. T. (2026). Cybersecurity Governance in the Digital Era and IT: Integrating Regulatory Oversight, Risk Management, and Organisational Resilience in Pakistan. *Social Science Review Archives*, 4(1), 1806-1829

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in industry 5.0: a comparative study between Saudi Arabia and the United Kingdom. *Digital*, 3(3), 200-231.

Majeed, Y., Majeed, A., & Minhas, M. T. (2026). Cybersecurity Governance in the Digital Era and IT: Integrating Regulatory Oversight, Risk Management, and Organisational Resilience in Pakistan. *Social Science Review Archives*, 4(1), 1806-1829.

Gambo, M. L., Danasabe, A., Binbeshr, F., Imam, M., Shinwari, M. W., & Mahmoud, A. (2026). Navigating the cyber landscape: Saudi Arabia's cybersecurity standards and implementation barriers. *Arabian Journal for Science and Engineering*, 51(5), 5589-5607.

Murad, H. A., & Qudah, M. (2025). The attitudes of communicators toward cybersecurity concerning security, safety in national institutions. *Frontiers in Communication*, 10, 1552520.

Mohamed Noor, A. F., Moghavvemi, S., & Tajudeen, F. P. (2026). Assessing the impact of cybersecurity readiness on organizational security performance: a study on Malaysian organizations. *Journal of Enterprise Information Management*, 39(3), 907-927.

Gorenšek, T., & Trivunčević, R. (2025). Cybersecurity Readiness in the Euro-Mediterranean: A Comparative Review of Literature on National Strategies and Global Indices. *Journal of Criminal Justice and Security*, 1-32.

Zubaidah, E., Monalisa, M., Rusadi, S., & Handoko, T. (2024). E-Readiness Analysis to Accelerate Transformation Towards E-Government in Regional Government in Indonesia. *Jurnal Bina Praja*, 16(1), 37-53.

Almaiah, M. A., Alfaisal, R., Salloum, S. A., Hajjej, F., Shishakly, R., Lutfi, A., ... & Al-Marooof, R. S. (2022). Measuring institutions' adoption of artificial intelligence applications in online learning environments: integrating the innovation diffusion theory with technology adoption rate. *Electronics*, 11(20), 3291b

Kulin, J., & Johansson Sevä, I. (2021). Who do you trust? How trust in partial and impartial government institutions influences climate policy attitudes. *Climate Policy*, 21(1), 33-46.

Yusuf, F. (2021). The independent campus program for higher education in Indonesia: The role of government support and the readiness of institutions, lecturers, and students. *Journal of Social Studies Education Research*, 12(2), 280-304