Entrepreneurship Journal for Finance and Business (EJFB)
2025, VOL. 06, NO. 02, 129-139, E-ISSN: 2709-4251, P-ISSN: 2708-8790
DOI: https://doi.org/10.56967/ejfb2025510

The reality of cybersecurity in five-star hotels in the golden triangle area in Jordan

Mohamed A. Al-Twaisi[1], Mohamed A. Zahry[2*]
[1,2]Department of hotel studies, faculty of tourism and hotels, Mansoura university, Dakahlia, Egypt
zohry2010@yahoo.com

Article information:
Received: 16–08– 2024
Revised: 12–09– 2024
Accepted: 25–09– 2024
Published: 25–04– 2025

[*]**Corresponding author:**
Mohamed A. Zahry
zohry2010@yahoo.com

Abstract:

In light of the expansion of the use of modern technology in hotel organizations and the transition to the post-informatics era; The importance of cybersecurity has emerged in hotels protecting their data and maintaining the confidentiality of customer data, so that cybersecurity has become one of the competitive advantages that hotel organizations seek to possess by building dynamic cybersecurity capabilities to achieve long-term competitive advantage. The research aimed to measure the extent to which the administrative leaders of five-star hotels in the Golden Triangle region of Jordan realize the importance of cybersecurity. The research followed the Qualitative approach. It also relied on a questionnaire to collect study data from five-star hotel managers, with a size of (16) items. The research recommended partnerships with international companies specialized in cybersecurity, attracting skilled human resources in the field of cybersecurity, and establishing a cybersecurity unit inside the hotel.

Keywords: Cyber security, golden triangle hotels, Jordan.

Conclusions:

1. The study sample of five-star hotel managers lacks a precise understanding of the concept of cybersecurity, despite having an initial perception of electronic security and the importance of providing data protection programs for customers and hotel operations.
2. There is no dedicated cybersecurity department in five-star hotels, as cybersecurity-related tasks are handled by the engineering maintenance or security department.
3. Repeated threats to hotel computer systems have been observed, including viruses that disrupt device functionality or reduce operational efficiency. In some cases, attempts were made to breach customer data to obtain personal phone numbers for marketing and advertising purposes.
4. There is no specific plan for improving electronic performance in the field of cybersecurity, as efforts are limited to protecting computers from viruses and unauthorized access to hotel systems.
5. Some five-star hotels have qualified personnel capable of handling information technology and general device maintenance. However, there is a shortage of specialized human resources in cybersecurity.
6. The Jordanian government has made efforts in cybersecurity, such as establishing the National Cybersecurity Center, but there are no joint initiatives to enhance cybersecurity in hotels.
7. The main form of cybersecurity implementation in hotels consists of antivirus programs to secure internal networks against malware and protect internet search engine access.
8. Most hotels do not use advanced cybersecurity systems to counter cyber interception, hacking, and cyber espionage due to the high costs of purchasing original software.
9. Five-star hotel managers in the Golden Triangle area of Jordan lack a precise awareness of the concept of cybersecurity.

مجلة الريادة للمال والاعمال
2025، المجلد السادس، العدد (02)، الصفحات 129- 139

واقع الأمن السيبراني في فنادق الخمس نجوم بمنطقة المثلث الذهبي بالأردن

محمد أحمد الطويسي[1]، محمد عبد الفتاح زهري[2*]
[1,2]قسم الدراسات الفندقية، كلية السياحة والفنادق، جامعة المنصورة، الدقهلية، مصر

معلومات البحث:
- تاريخ استلام البحث: 2024 –08–16
- تاريخ ارسال التعديلات: 2024 –09–12
- تاريخ قبول النشر: 2024 –09–25
- تاريخ النشر: 2025 –04–25

[*]المؤلف المراسل:
محمد عبد الفتاح زهري
zohry2010@yahoo.com

المستخلص:
في ظل التوسع في استخدام التكنولوجيا الحديثة في المنظمات الفندقية والانتقال الى عصر ما بعد المعلوماتية؛ ظهرت أهمية الأمن السيبراني في حماية الفنادق لبياناتها، والحفاظ على سرية بيانات العملاء، حتى أصبح الأمن السيبراني يمثل أحد الميزات التنافسية التي تسعى المنظمات الفندقية إلى امتلاكها من خلال بناء القدرات الديناميكية للأمن السيبراني لتحقيق الميزة التنافسية طويلة الأجل، وقد هدف البحث إلى قياس مدى إدراك القيادات الإدارية لفنادق الخمسة نجوم في منطقة المثلث الذهبي بالأردن لأهمية الامن السيبراني، واتبع البحث المنهج الكيفي، كما اعتمد على المقابلة الشخصية لتجميع بيانات الدراسة من مدراء الفنادق فئة الخمس نجوم في منطقة المثلث الذهبي، وبلغ حجمها (16) مقابلة، وتوصل البحث إلى غياب المفهوم الدقيق للأمن السيبراني لدى عينة الدراسة، وأوصى البحث بعقد شراكات مع الشركات العالمية المتخصصة في الامن السيبراني، واستقطاب الموارد البشرية الماهرة في مجال الامن السيبراني، وانشاء وحدة خاصة بالأمن السيبراني داخل الفندق.

الكلمات المفتاحية: الأمن السيبراني، فنادق المثلث الذهبي، الأردن.

المقدمة:

شهد القرن الحادي والعشرين ثورة جديدة اعقبت ثورة تكنولوجيا المعلومات والاتصالات التي اتسم بها القرن العشرين، وتعرف هذه الثورة الجديدة بالثورة السيبرانية (غريب ومزياني، 2020، ص36) التي تعد الميدان الخامس للصراع البشري بعد الارض والبحر والجو والفضاء (سمير، 2017، ص256)، حتى اصبحت المجتمعات تواجه تحديات الامن السيبراني لاسيما مع اتساع الفجوة بين الاداء المنوط به وبين التطورات التكنولوجية المتسارعة في الفضاء السيبراني وما يحيق به من تهديدات متعددة الابعاد تحاول الاخلال بالنظام العام بأكمله (الاصفر، 2011، ص20).

تزايد الاهتمام بالأمن السيبراني مع تزايد هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة في مختلف المجالات، وما واكبها من تزايد الجرائم والهجمات السيبرانية التي اصبحت تمثل جرائم حقيقة مكتملة الاركان، لاسيما عمليات القرصنة السيبرانية الاكثر انتشارا في بيئة العالم الرقمي (دحماني، 2018، ص1).

وقد أدت التطورات السريعة لاستخدامات الواسعة للفضاء السيبراني في مختلف المنظمات الوطنية والاقليمية والدولية الى تزايد اهميته الحيوية، وعلى الرغم من ذلك فقد ارتبط هذا الفضاء السيبراني بتحديات متعاظمة بسبب الترابط العضوي بين الفضاء السيبراني والامن السيبراني والبنية التحتية للدول والمنظمات الحكومية وغير الحكومية، مما جعل الامن السيبراني يأتي على رأس اولويات الامن الوطني (الشمري، 2021، ص150)، لهذا ظهرت أهمية الأمن السيبراني في حماية الفنادق لبياناتها والمعلومات التشغيلية الخاصة بها، والحفاظ على سرية بيانات العملاء، وعليه يركز موضوع البحث على واقع الأمن السيبراني في فنادق الخمس نجوم بمنطقة المثلث الذهبي في الاردن.

مشكلة البحث:

تسعى المنظمات الفندقية المعاصرة إلى مواكبة التطور التكنولوجي، والتوسع في استخدام التطبيقات الكترونية في الفنادق، للمساعدة في انجاز العديد من المهام الاساسية مثل الحجوزات الإلكترونية والدفع الإلكتروني والتسويق الالكتروني وغيرها، إلا ان هذا المسعى، وعلى الرغم مما يجنيه من فوائد وإيجابيات، فقد أدى الى ظهور مخاطر لم تكن معروفة في السابق، ومنها نظم الامن السيبراني، والمرتبط بإمكانية سرقة البيانات المعلومات وتعديلها او فقدانها، من خلال أفراد داخل او خارج المنظمة، مع إمكانية اطلاع المنافسين على البيانات أو المعلومات ضمن قواعد البيانات للفندق او المؤسسة.

اشارت دراسة الحميري وبريس (2006) إلى أن قطاع الفنادق يواجه تحديات كبيرة بسبب التطور الهائل والمستمر في التكنولوجيا الحديثة التي فرضت تغييرات جذرية في بيئات العمل الداخلية والخارجية، وقد انعكس ذلك على تراجع ترتيب الاردن في مؤشر تنافسية السياحة والسفر العالمي من المركز (54) في عام 2009م الى المركز (64) في عام 2021م (World Economic Forum, 2009-2021)،

وقد اشارت دراسة بظاظو (2020) الى تراخي مشغلي القطاع السياحي في الأردن على مواكبة التقنيات الحديثة في تكنولوجيا العرض والطلب، مما ادى الى ضعف الحصة السوقية من السياحة العالمية، وضعف الايدي العاملة المدربة في قطاع السياحة الرقمية، نتيجة لضعف عملية دمج التكنولوجيا في قطاع الضيافة الأردني، وانه لا يرقى الى المقومات التي يمتلكها الأردن،

وقد لاحظ الباحث من خلال عمله في القطاع الفندقي بمنطقة المثلث الذهبي الأردني (مدينة العقبة، البترا، وادي رم) انخفاض إدراك الادارات الفندقية لأثر تطبيق تدابير الامن السيبراني، مما أدي إلى ضعف الأداء والقدرة التنافسية، لهذا فإن مشغلي قطاع الفنادق بحاجة إلى معرفة ابعاد الامن السيبراني في القطاع الفندقي، وطرق تطويرها،

وانطلاقاً مما سبق؛ يمكن صياغة مشكلة الدراسة في ضوء التساؤل الرئيس التالي: ما مدى إدراك القيادات الإدارية لفنادق الخمسة نجوم في منطقة المثلث الذهبي بالأردن بأهمية الامن السيبراني؟

أهمية البحث:

أكدت العديد من الدراسات السابقة على أهمية الأمن السيبراني إلى جانب الأمن المادي في قطاع السياحة والفنادق (Shabani, & Munir, 2020)، حيث أصبح مفهوم الأمن السيبراني مؤخرًا تحديًا كبيرًا في نمو السياحة العالمية والسفر، خاصة مع انتشار السياحة الرقمية والسياحة الذكية، وتوسعها الهائل في القرن الحالي في تطبيق أنظمة الحجز الإلكتروني، وفي جميع جوانب صناعة السياحة والفنادق، وهو المفتاح في عملية تطوير وتسويق وإدارة المواقع السياحية والفنادق في الوقت الحالي (Bazazo, et.al., 2019).

تأتي أهمية البحث من أهمية القطاع الفندقي في الاقتصاد الوطني الأردن اذ شكل الدخل السياحي 16% لعام 2019 من اجمالي الدخل القومي الأردني (إحصاءات وزارة السياحة والآثار، 2020)، كما استمد البحث أهميته من الدور الذي يلعبه الأمن السيبراني وأثره على الميزة التنافسية، كونها مرتكزات مهمة في زيادة القدرة التنافسية للمؤسسات الفندقية، وعليه يمكن تحديد أهمية البحث من خلال:

1. توضيح مدى إدراك الادارات الفندقية لأهمية الأمن السيبراني في منطقة المثلث الذهبي في الأردن.
2. المساهمة في تكوين نظام معرفي عن مدى تطبيق الادارات الفندقية العالمية والأهلية (الفنادق المحلية) لأنظمة الامن السيبراني
3. توضيح مدى قدرة الإدارات الفندقية على التعامل مع الامن السيبراني بفاعليه لإدارة مؤسساتهم.
4. تعتبر الدارسة من الدارسات الحديثة في مجال البحوث العلمية المتعلقة بالأمن السيبراني حيث محدودية المكتبة العلمية لمثل هذه الدارسات.

فرضية البحث:

لتحقيق اهداف البحث تم صياغة الفرضية التالية:

يوجد إدراك دقيق لدى مدراء فنادق الخمس نجوم بمنطقة المثلث الذهبي بالأردن لمفهوم الأمن السيبراني.

الإطار النظري:

أولاً: مفهوم الأمن السيبراني

ويقصد بالأمن السيبراني القدرة على تحقيق النتائج المستهدفة من استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، لإيجاد مزايا وفوائد للدولة والتأثير على الاحداث المتعلقة بالبيئات التشغيلية الاخرى من خلال الادوات السيبرانية (Nye, 2010, p.3)

وهو تبني الوسائل والاليات التي تتمكن من الحد من مخاطر الهجوم الالكتروني على اجهزة الحاسب الالي والبرمجيات وشبكات المعلومات والاتصالات واكتشاف الفيروسات ومنع تأثيرها على المعدات والبرمجيات (Amoroso, 2007, p.1)

ويقصد بالأمن السيبراني مجموعة الانشطة والاجراءات التي تؤمن حماية الموارد المالية والبشرية المتعلقة بتقنيات المعلومات والاتصالات، والحد من الاضرار والخسائر التي يمكن ان تحدث جراء التهديدات والمخاطر، وإعادة السيطرة على الاوضاع بأسرع وقت ممكن دون تحول الاضرار الى خسائر دائمة (جبور، 2012، ص3)

يتضمن الامن السيبراني مجموعة القواعد والاجراءات والاطر القانونية والتنظيمية التي تضعها الاجهزة الامنية المعنية لتوفير الحماية لسرية المعلومات والبيانات الالكترونية، من خلال تنسيق الجهود المشتركة بين القطاعين العام والخاص وكذلك تنسيق الجهود المحلية والدولية لغرض حماية الفضاء السيبراني عن طريق تطبيق نظم المعلومات الرقمية الدفاعية عالية الخصوصية والسرية (العلي، 2019، ص57)

يعد الأمن السيبراني عبارة عن مصفوفة من الأدوات التنظيمية والتقنية والإجرائية التي تهدف الى حماية الحواسيب الالية والشبكات الالكترونية، وما تحتويه من معلومات وبيانات من تهديدات الاختراق أو الاتلاف او التغيير أو تعطل الوصول الى الخدمات او المعلومات على مستوى الدول أو المنظمات الحكومية أو الشركات الخاصة (منصور، 2021، ص226).

ويشير الامن السيبراني الى الوسائل التقنية والادارية والتنظيمية والتشغيلية التي تهدف الى التصدي للاستخدامات غير القانونية او غير المصرح بها لاستخدام المعلومات الالكترونية او استرجاعها لغرض توفير الحماية والسرية والخصوصية للبيانات الخاصة بالأفراد والمنظمات الوطنية (الجنفاوي، 2021، ص81).

في ضوء التعريفات السابقة يمكن تحديد المفهوم الاجرائي للأمن السيبراني في المنظمات الفندقية بانه مجموع الإجراءات التقنية والإدارية التي تتضمن القواعد والعمليات والآليات التي يتم اتخاذها لمنع أي تدخل مقصود او غير مقصود لاستخدام أو سوء الاستغلال كل ما يتعلق بنظم المعلومات والاتصالات الخاصة بالمنظمة الفندقية، وضمان تأمين وحماية وسرية وخصوصية البيانات الشخصية للنزلاء.

ثانياً: اهمية الأمن السيبراني:

اوضح الحربي (2021، ص14) الى ارتفاع التكلفة المادية والزمنية لمعالجة اختراق الامن السيبراني حيث يمكن ان يستغرق كشف ومعالجة اختراق البيانات نحو 6 اشهر كما تخصص الولايات المتحدة الامريكية ميزانية خاصة للأمن السيبراني تبلغ حوالى 15 مليار دولار سنوياً كما اشار الى تزايد معدلات الانفاق العالمي على الامن السيبراني حيث بلغت في عام 2021م حوالى 6 تريليون دولار مما يعكس الاهتمام المتنامي بالأمن السيبراني، كما اوضح العلي، (2019،

ص56) الى اعتماد المجتمعات المعاصرة على تكنولوجيا المعلومات والاتصالات الحديثة المتصلة بشبكة الانترنت والتي تنطوي على العديد من المخاطر والتهديدات المتعلقة بالأمن السيبراني وامن المعلومات، كما تعتبر منطقة الشرق الاوسط منطلقا جيوسيبرانيا عالميا بحكم موقع الدول في بؤرة ربط شبكات الانترنت الممتدة تحت البحر المتوسط، مما يجعل المنطقة مستهدفة سيبرانيا على كافة المستويات (رقولي ولخضر، 2019، ص75).

ثالثاً: أنواع الأمن السيبراني:

1.3 أمن الشبكات: يقصد به الاجراءات التي يتم اتخاذها لتامين شبكات الحاسب الآلي الداخلية والخارجية من التهديدات السيبرانية التي تتضمن كل من المهاجمين المستهدفين، أو البرامج الضارة، بالإضافة الى تامين الدخول على محركات البحث على شبكة الانترنت (Jain & Pal, 2017, p.791).

2.3 أمن التطبيقات: يقصد به الحفاظ على برامج نظم المعلومات، والأجهزة الالية داخل المنظمة بعيدا عن التهديدات السيبرانية، حيث من الممكن أن يوفر التطبيق المخترق الوصول إلى المعلومات والبيانات المصممة للحماية، لذلك فان مفهوم الأمان السيبراني الناجح يجب ان يبدأ من مرحلة التصميم الاولى قبل نشر البرنامج أو الجهاز (السمحان، 2020، ص14).

3.3 أمن المعلومات: يختص بتوفير السلامة والخصوصية للمعلومات والبيانات، سواء في مرحلة التخزين أو التبادل داخل المنظمة وخارجها (Jain & Pal, 2017, p.791)

4.3 أمن العمليات: يقصد به الامن التشغيلي الذي يتضمن مختلف الممارسات والمهام التي تتعامل مع أصول البيانات داخل المنظمة، والتكفل بحمايتها واتاحة الوصول اليها في الوقت المناسب (الجنفاوي، 2021، ص85).

رابعاً: اهداف الامن السيبراني في المنظمات الفندقية:

تتضمن اهداف الامن السيبراني سواء بشكل عام او في المنظمات الفندقية ما يلي:

- الانتقال بشكل مباشر من العمل التقليدي الى استخدام العمل التقني من خلال الوسائل والادوات التكنولوجية الحديثة بأنواعها المختلفة واستخدامها في تامين عمليات الاطلاع على المعلومات والاتصالات اللازمة لممارسة الاعمال الرقابية (الجنفاوي، 2021، ص87).
- مواجهة مخاطر العولمة والانتشار المعلوماتي الكثيف في مختلف جوانب الحياة العامة والمهنية، والتوسع المستمر في استخدام اجهزة الحاسب الالي والهواتف الذكية وما تتطلبه من ضرورة توفير نظم الامن السيبراني (الخضري واخرون، 2020، ص222).
- توفير الحماية للبيانات والمعلومات الالكترونية والتطبيقات والبرمجيات المشغلة لها على المستوى الفردي والمؤسسي لمنع دخول اي شخص او جهة غير مصرح لها بالتعامل مع البيانات والمعلومات ذات الصلة (ماشوش، 2018، ص50).
- حماية شبكات المعلومات والاتصالات من التهديدات السيبرانية من خلال امتلاك أحدث التقنيات والنماذج للأمن السيبراني لكشف الاهداف المعادية والتصدي لها بأسلوب علمي (عسيري، 2020، ص6)
- تامين البني التحتية المعلوماتية وحماية الانظمة الالكترونية للدولة وما تتضمنه من بيانات ومعلومات ذات اهمية قصوى (المقصودي، 2017، ص13).
- رصد واكتشاف الهجمات السيبرانية القائمة او المحتملة والتعامل معها وتحديد التقنيات التكنولوجية المتعلقة بأمن المعلومات والتصدي لها على نحو سريع قبل ان تحدث اثارا تخريبية في انظمة المعلومات (الجموسي، 2016، ص120).
- معالجة نقاط الضعف في أنظمة تامين المعلومات والحواسيب الآلية والأجهزة المحمولة باختلاف أنواعها، وسد الثغرات في أنظمة أمن المعلومات (السمحان، 2020، ص12).
- تشفير مختلف التعاملات الرقمية على شبكات الانترنت مما يحميها من الهجمات السيبرانية التي تسعى لاختراقها والتلاعب بها او تدميرها (الخضري واخرون، 2020، ص223).

خامساً: أبعاد الامن السيبراني في المنظمات الفندقية:

يتسم الامن السيبراني بتعدد ابعاده الاقتصادية والاجتماعية والقانوني والسياسي والعسكري.

1. **البعد الاقتصادي:**

يعد الفضاء السيبراني احد ابرز القطاعات الجاذبة للاستثمارات طويلة الاجل، باعتباره محركا قويا للابتكار وتحديث الانتاج ودفع النمو الاقتصادي نحو المنافسة، حيث يعد تركيز الجهود على تقنيات تكنولوجيا المعلومات من العوامل الاساسية للنهوض باقتصاد المعرفة والاقتصاد الرقمي في القرن الحادي والعشرين، مما دفع الدول الكبرى لتعظيم الاستثمار في المعرفة السيبرانية، بهدف التحكم في الاقتصاد العالمي الرقمي (سمير، 2017، ص261)، ونظرا لتزايد الاعتماد على تكنولوجيا المعلومات وما واكبها من تزايد الهجمات السيبرانية فقد دعت الحاجة الى اهمية توفير الامن السيبراني لحماية المعلومات والبيانات وما يمثله اختراقها من تهديدات مباشرة لنمو الاقتصاد العالمي (مختار، 2015، ص6).

2. **البعد الاجتماعي:**

نتيجة لتطور تكنولوجيا الانترنت وانشاء مواقع التواصل الاجتماعي والمدونات اصبح لكل فرد الحق في التعبير عن آرائه وتطلعاته وطموحاته الاجتماعية المختلفة بمشاركة واسعة من جميع فئات وشرائح المجتمع ومكوناته مما اعطى فرصة لتبادل وانتشار الافكار والمعلومات (الدلابيح، 2021، ص13)، ويتمثل البعد الاجتماعي للأمن السيبراني في تامين شبكات التواصل الاجتماعي لاسيما فيما يتعلق بحرية التعبير عن الآراء السياسية والفكرية بمشاركة واسعة من جميع فئات المجتمع مما يقتضي الحفاظ على الاستقرار الاجتماعي للفضاء السيبراني لدعم التبادل الايجابي للأفكار والخبرات وتأسيس افاق التعاون والتكامل (شفيق، 2014، ص40).

وفي هذا الصدد ينبغي تامين الشبكة الدولية للمعلومات واتاحتها لجميع مستخدمي شبكة الانترنت للاستفادة من

المعلومات والخدمات والبنى التحتية الرقمية دون تحمل المخاطر الامنية السيبرانية مما يتطلب بلورة المبادئ الاساسية لأخلاقيات الامن السيبراني من قبل جميع مستخدمي الفضاء السيبراني (الاتحاد الدولي للاتصالات، 2006، ص16)

3. البعد القانوني:

تعد العلاقة بين الامن السيبراني والجوانب القانونية علاقة تبادلية حيث ان تطور التكنولوجيا الحديثة يقتضى وجود التشريعات القانونية المنظمة لاستخدامها (قادير، 2016، ص5)، حيث يؤدي الاستخدام المكثف للفضاء السيبراني على المستوى الفردي والمنظمي والحكومي الى ترتيبات قانونية تستوجب حل ما يمكن ان ينشا من نزاعات او خلافات لمواكبة التحولات الرقمية التي تجتاح العالم وفي مقدمتها حق الوصول الى الشبكة العالمية للمعلومات وحق استخدام تقنيات المعلومات والاتصالات وانشاء المواقع الالكترونية والمدونات الالكترونية وتوفير الحماية القانونية لملكية البرمجيات وحقوق الملكية الفكرية فضلا عن ما استحدث من حقوق قانونية تتعلق بحق الاحتفاظ ببيانات الاتصالات وحق الابلاغ عن التجاوزات والمخالفات والجرائم السيبرانية (سمير، 2017، ص263).

4. البعد السياسي:

يتضمن البعد السياسي للأمن السيبراني حماية الوثائق السرية من التسريبات المختلفة لتحقيق اهداف سياسية شائنة، مما يتطلب ضرورة توفير الامن السيبراني في العمليات ذات الطابع السياسي مثل تنظيم الانتخابات او تابعة الاحتجاجات الالكترونية (عسيري، 2020، ص7)، وعلى المستوى الاستراتيجي الوطني، يجب ان تقوم الحكومات بتأمين الرقابة العامة على انظمة المعلومات، وتبادل المعلومات بين المؤسسات المعنية، وزيادة الوعي بأفضل الممارسات المتبعة في مجال الأمن السيبراني، التي تتوافق مع التشريعات القانونية التي تصدرها السلطة التشريعية، بهدف تنظيم قطاع المعلومات والاتصالات، وتحديد الجهات الرسمية المسؤولة عن الأمن السيبراني، وصياغة التعليمات والأنظمة الاحترازية الخاصة بالأمن السيبراني وتشريعها وتحديثها (العوادي، 2016، ص8).

5. البعد العسكري:

اخيرا يجب الاشارة الى البعد العسكري للأمن السيبراني على الرغم من عدم تعلقه بصناعة الفنادق، حيث نشأة الانترنت كانت ذات صبغة عسكرية في المقام الاول، لخدمة الاغراض الحربية، وتتصاعد في الآونة الاخيرة الصراع السيبراني ذو البعد العسكري لاسيما بين روسيا والولايات المتحدة الامريكية وقد ظهر هذا الصراع جليا في الصراعات الناشئة في استونيا وجورجيا وإيران وكوريا الجنوبية، التي ظهر بها اهمية الامن السيبراني بعد تعرضها للهجمات السيبرانية التي خلفت اثارا تقنية ومادية كبيرة (الاشقر، 2012، ص15).

لقد حدث تحول جذري في ادارة الحروب في الوقت الحاضر بحيث تحولت معطيات الانتصار العسكري من الاعتماد على القوة العسكرية التقليدية او تحالفات الدول الكبرى الى الحروب التكنولوجية التي تقوم في الاساس على شبكات الانترنت فيما أصبح يعرف بالحروب السيبرانية (غريب ومزياني، 2020، ص38).

تكمن الميزة التنافسية للأمن السيبراني في المجال العسكري في قدرته الفائقة على ربط الوحدات العسكرية مع بعضها البعض بشبكة الكترونية عسكرية عبر الفضاء السيبراني، مما يسمح بسهولة وسرية تبادل المعلومات وسرعة اتخاذ القرارات الحربية، فضلا عن تامين الجيوش في الميدان من الهجمات السيبرانية المضادة التي تسعى لتدمير قواعد البيانات والمعلومات وقطع الاتصالات مما يشكل مخاطر كبيرة في الاوقات الحرجة (مختار، 2015، ص6).

سادساً: انواع الامن السيبراني في المنظمات الفندقية:

تتضمن مجموعة متنوعة من العمليات التي تستهدف تحقيق الامن السيبراني والتي تشمل الانواع التالية: امن الشبكات، وامن التطبيقات، وأمن المعلومات، وامن العمليات (Jain & Pal, 2017, p.791).

- **أمن الشبكات:**

يقصد به الاجراءات التي يتم اتخاذها لتامين شبكات الحاسب الآلي الداخلية والخارجية من التهديدات السيبرانية التي تتضمن كل من المهاجمين المستهدفين، أو البرامج الضارة، بالإضافة الى تامين الدخول على محركات البحث على شبكة الانترنت.

- **أمن التطبيقات:**

يقصد به الحفاظ على برامج نظم المعلومات، والأجهزة الالية داخل المنظمة بعيدا عن التهديدات السيبرانية، حيث من الممكن أن يوفر التطبيق المخترق الوصول إلى المعلومات والبيانات المصممة للحماية، لذلك فان مفهوم الأمان السيبراني الناجح يجب ان يبدأ من مرحلة التصميم الاولى قبل نشر البرنامج أو الجهاز (السمحان، 2020، ص14).

ويتضمن كذلك امن التطبيقات تامين التطبيقات الالكترونية المستخدمة لاسيما البريد الالكتروني، بالإضافة الى توفير التامين لأجهزة الهواتف المحمولة.

- **أمن المعلومات**

يختص بتوفير السلامة والخصوصية للمعلومات والبيانات، سواء في مرحلة التخزين أو التبادل داخل المنظمة وخارجها.

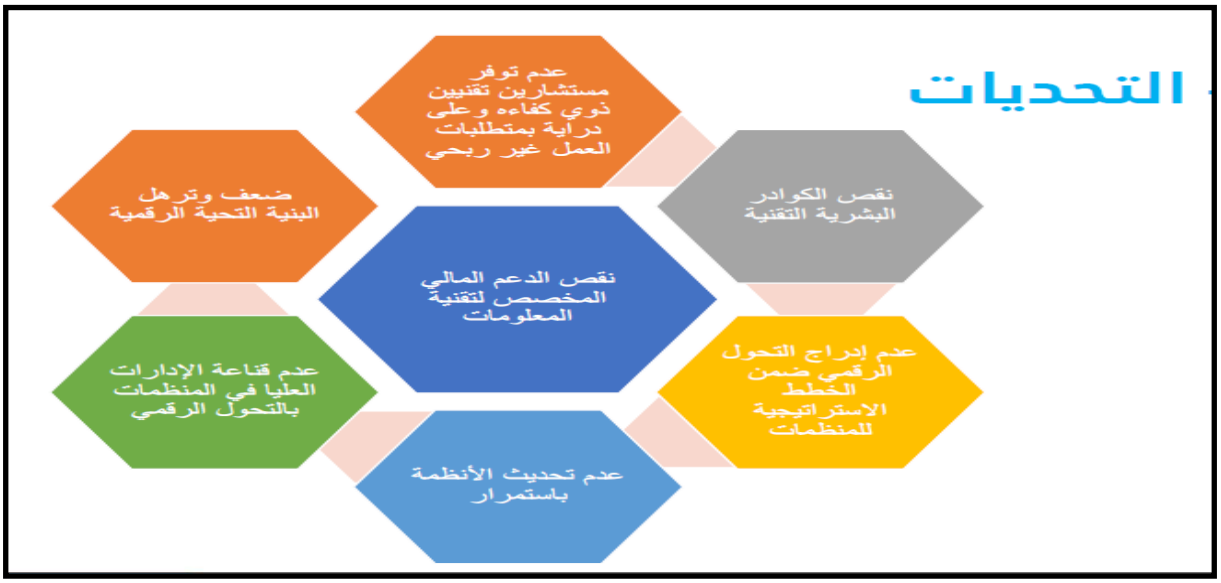
- **أمن العمليات:**

ويقصد به الامن التشغيلي الذي يتضمن مختلف الممارسات والمهام التي تتعامل مع أصول البيانات داخل المنظمة، والتكفل بحمايتها واتاحة الوصول اليها في الوقت المناسب (الجنفاوي، 2021، ص85).

سابعاً: تحديات الامن السيبراني في المنظمات الفندقية:

يواجه الامن السيبراني في المنظمات الفندقية العديد من التحديات التي تستوجب تكاتف مختلف القوى الفاعلة والجهات المعنية لتوفير بيئة امنة في الفضاء السيبراني لممارسة الانشطة الفندقية التي تحقق امن المنظمات الفندقية والعاملين والسائحين على حد سواء.

يتضح من الشكل (1) اهم تحديات الامن السيبراني والتي يمكن القاء الضوء عليها كما يلي:

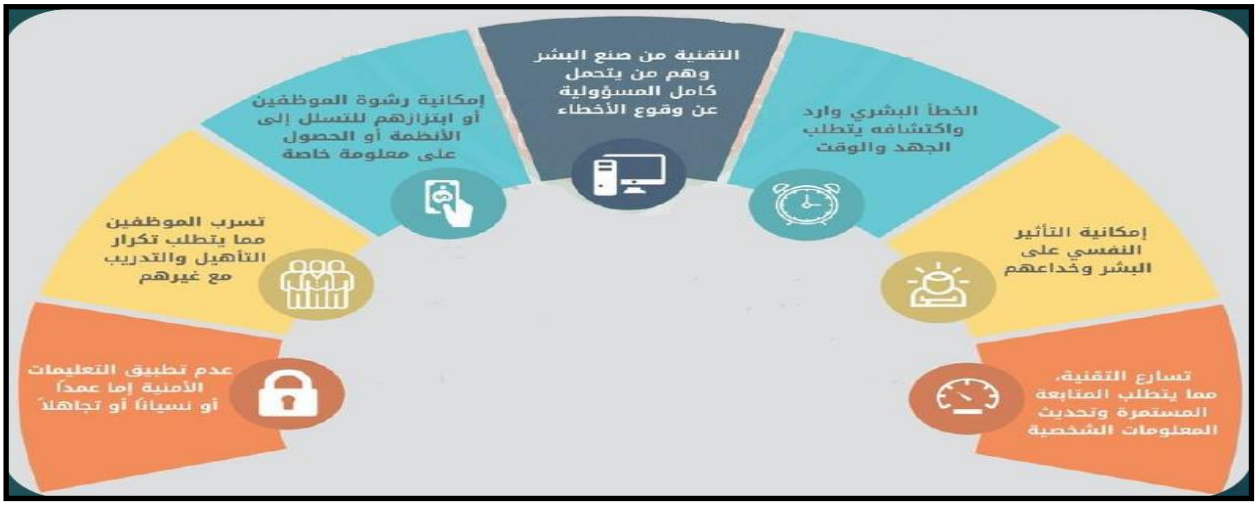


شكل (1) التحديات الرئيسية للأمن السيبراني
المصدر: (الحربي، 2019، ص28)

- عدم ادراج التحول الرقمي والامن السيبراني

في الخطط الاستراتيجية للمنظمات على الرغم مما اشارت اليه رؤية المملكة الأردنية الهاشمية في الأمن السيبراني بالنص التالي: (أردن واثق وآمن ضمن العالم الرقمي ومقاوم للتهديد السيبراني)، ويمكن تحقيق هذه الرؤية الامنية عن طريق انشاء وتطوير وتنمية الكفاءات الوطنية في مجالات الأمن السيبراني، لتحقيق التميز على المستوى الوطني والعالمي (وزارة الاتصالات وتكنلوجيا المعلومات، 2018، ص11).

- ضعف البنية التحتية الرقمية اللازمة لتحقيق الامن السيبراني لاسيما مع صعوبة اثبات مصادر الهجمات السيبرانية بسبب استخدام الوسائل التقنية الحديثة عالية التقنية التي قد توفق قدرات الامن السيبراني (الخضري واخرون، 2020، ص223).
- الطبيعية غير الوطنية للجريمة السيبرانية، مما يصعب في ظلها اتخاذ إجراءات وطنية في غياب وجود تعاون قضائي دولي، أو اتفاقيات ومعاهدات تلتزم بها جميع دول العالم (العوادي، 2016، ص10).
- ضعف قدرات الاجهزة الامنية في مجال الامن السيبراني مما يسبب قصور الامكانات في التعامل مع الهجمات السيبرانية فضلا عن نقص الخبرة التكنولوجية في العديد من المنظمات (الملاحي، 2015، ص129)
- قصور التشريعات والقوانين المنظمة لاستخدام الفضاء السيبراني والتي توفر الحماية القانونية للمستخدمين مما ينقص من سيادة الدولة على فضائها السيبراني (يحيى، 2013، ص67).
- نقص الكوادر البشرية وضعف تأهيلها وهي تعد من أخطر نقاط الضعف في منظومة الامن السيبراني، نظرا لأنه يقع على عاتق الافراد المسئولية الكاملة في تسرب المعلومات والبيانات السرية، سواء بعمد عن طريق الفساد والرشوة، او بغير عمد، عن طريق الجهل او الاهمال او تجاهل التعليمات واللوائح القانونية المستخدمة للأمن السيبراني شكل (2).



شكل (2) التحديات الانسانية (البشرية) للأمن السيبراني
المصدر: (الفريق الوطني للاستجابة للأحداث السيبرانية، 2018، ص8)

- عدم تحديث الانظمة باستمرار خاصة في المجالات التكنولوجية المستحدثة مثل الذكاء الاصطناعي الذي يستخدم على نطاق واسع في تهديد الامن السيبراني، كأداة للحصول على المعلومات والبيانات المطلوبة، مما يتطلب ضرورة المواكبة المستمرة لتكنولوجيا الذكاء الاصطناعي ووضع الخطط المناسبة للتعامل مع التطورات التكنولوجية الحديثة، كما تشكل تكنولوجيا الحوسبة السحابية مصدر تهديد مهم للأمن السيبراني، في ظل الانتشار الكبير للخدمات الإلكترونية التي تقدمها مما جعل معظم المنظمات تفضل استخدام هذه التكنولوجيا لأنها توفر الجهد والوقت والمال، إلا أنها تنطوي على تهديدات كبيرة في مجال الأمن السيبراني بسبب تعرض معلومات العملاء الاجتماعية والاقتصادية والمالية عرضة للهجمات السيبرانية (الفارس، 2022، ص1)، كما تستخدم تكنولوجيا انترنت الاشياء لتعزيز فرص النمو الاقتصادي والاندماج والحراك المجتمعي والتواصل الاجتماعي، الا ان هذه التكنولوجيا ما تزال تعاني من الثغرات الامنية مما يشكل تهديدا سيبرانيا يمكن من خلاله شن هجمات سيبرانية خطيرة (المبيضين، 2022، ص1).
- ضعف السيادة الوطنية للعديد من دول الشرق الاوسط بسبب التهديدات الامنية المتراكمة وما تتعرض له من تضليل سيبراني يؤثر على التماسك الوطني والاجتماعي للدول (رقولي ولخضر، 2019، ص75).

الدراسة الميدانية:

أولاً: منهجية الدراسة الميدانية

1. حدود البحث:

- **الحدود المكانية:** اقتصرت الدراسة على فنادق الخمس نجوم في منطقة المثلث الذهبي في الاردن.
- **الحدود الزمنية:** تم إجراء هذه الدراسة خلال فترة زمنية من 2023/4/15 ولغاية 2023/5/5.
- **الحدود البشرية**: شملت المدراء في فنادق منطقة المثلث الذهبي في الاردن والمصنفة خمس نجوم والبالغ عددها 16 فندقا، نظرا لامتلاكها بيانات مفيدة للدارسة، للخروج بنتائج أو مؤشرات يمكن تعميمها.

الجدول (1) عينة الدراسة من فنادق الخمس نجوم بمنطقة المثلث الذهبي بالأردن

المنطقة		اسم الفندق
العقبة	فنادق ادارة دولية	انتركونتيننتال - موفنبيك ريزورت اند ريزيدانس العقبة - كيمبنسكى العقبة
	فنادق ادارة محليه	منتجع وسبا موفنبيك تالا باى - اوريكس العقبة – المنارة
وادي رم	فنادق ادارة دولية	لا يوجد
	فنادق ادارة محليه	وادي رم بوللي لوكسوتيل - اريانا وادي رم كامب - وادي رم زياد كامب
البتراء	فنادق ادارة دولية	منتجع موفمبيك البتراء - موفمبيك نباتيان كاستل - ماريوت البتراء
	فنادق ادارة محليه	اولد فلج البتراء - حياة زمان البترا - بترا مون لوكسري - اتش لوكسري البترا

منهج الدراسة والبحث:

استخدمت الدراسة المنهج الكيفي الذي يتناسب مع موضوع الدراسة، في تحليل اراء عينة الدراسة حول واقع الامن السيبراني في فنادق منطقة المثلث الذهبي في الاردن.

2. تصميم اداة البحث:

صممت استمارة المقابلة الشخصية على شكل أسئلة مفتوحة تتعلق بواقع الأمن السيبراني في فنادق الخمس نجوم بمنطقة المثلث الذهبي في الاردن، وتكونت المقابلة من سبعة اسئلة.

نتائج المقابلة الشخصية:

1. ما هو مفهوم الامن السيبراني من وجهة نظر سيادتكم؟

تبين من تحليل اراء المدراء غياب المفهوم الدقيق للأمن السيبراني وان كان معظمهم قد اشار الى وجود تصور مبدئي حول مفهوم الامن الالكتروني واهمية توفير برامج الحماية البيانات والمعلومات المتعلقة بالعملاء واعمال الفندق حيث اوضح معظم المدراء ان الامن السيبراني من وجهة نظرهم يرتبط بالأدوات والبرامج الالكترونية الدفاعية التي تكتشف محاولات اختراق المعلومات والبيانات التي يقوم بها القراصنة او الفيروسات الحاسوبية التي تعطل عمل اجهزة الحاسب الآلي وكيفية التصدي لها.

2. هل يوجد في الهيكل التنظيمي للفندق قسم مختص بالأمن السيبراني؟

اوضح غالبية المدراء انه لا يوجد لدى الفنادق قسم خاص بالأمن السيبراني ولكن يتم الحاق الاعمال المرتبطة به الى قسم الصيانة الهندسية او قسم الامن نظرا لحداثة مفهوم الامن السيبراني وانه يتطلب توفر خبرة يختص بها العاملون في قسم الصيانة.

3. هل تعرض الفندق من قبل لمشكلات متعلقة بالأمن السيبراني؟

اشار معظم المدراء الى تكرار حدوث اصابة اجهزة الحاسب الالي بالفندق بالفيروسات التي تعطل عمل الاجهزة او تقلل من قدراتها بالإضافة الى حدوث حالات محاولة اختراق البيانات الخاصة بالعملاء للحصول على ارقام الهواتف الشخصية لاستخدامها في اعمال الدعاية والتسويق من قبل بعض الشركات وتسبب هذه الاختراقات تهديدات كبيرة لأمن الفندق وثقة العملاء مما يؤثر على الميزة التنافسية للفندق.

4. هل يوجد بالفندق خطة لتطوير الاداء الالكتروني في مجال الامن السيبراني؟

اوضح غالبية المدراء عدم وجود خطة محددة لتطوير الاداء الالكتروني في مجال الامن السيبراني بشكل محدد على الرغم من وجود إدراك لأهمية وجود برامج الحماية الالكترونية التي تستخدمها بعض الفنادق لحماية اجهزة الحاسب الالي من الفيروسات ومحالات الاختراق او الدخول غير المسموح به لأنظمة الفندق.

5. هل يوجد بالفندق افراد مؤهلين للعمل في مجال الامن السيبراني؟

اشار غالبية المدراء الى وجود افراد مؤهلين في التعامل مع تكنولوجيا المعلومات وصيانة الاجهزة والمعدات بشكل عام ولكن الموارد البشرية المختصة بالأمن السيبراني لا تزال في حاجة الى التدريب والتأهيل المتخصص لرفع كفاءتهم في تصميم البرامج الالكترونية المتخصصة في الامن السيبراني.

6. هل يوجد إلزام من الجهات الحكومية المختصة بتطبيق معايير الامن السيبراني؟

أكد معظم المدراء الى وجود جهود حكومية في مجال الامن السيبراني تمثلت في انشاء المركز الوطني للأمن السيبراني الاردني الذي يقدم العديد من الخدمات في هذا المجال ولكن نظرا لحداثة انشائه فانه لم يتم حتى الان تفعيل مبادرات مشتركة لتوفير الامن السيبراني في مجال الفنادق كما ان وزارة السياحة لا تلزم الفنادق باتباع تدابير واجراءات الامن السيبراني.

7. ما اشكال تطبيق الامن السيبراني في الفندق؟

اوضح معظم المدراء ان اهم اشكال تطبيق الامن السيبراني في الفنادق تتمثل في برامج الحماية من الفيروسات الحاسوبية لتامين الشبكات الداخلية من التهديدات الالكترونية أو البرامج الضارة وتامين الدخول على محركات البحث على شبكة الانترنت، وبصفة خاصة فيروسات احصنة طروادة ودودة الحاسب الاكثر انتشارا في اجهزة الحاسب بالفنادق ولكن لا تستخدم معظم الفنادق انظمة الامن السيبراني فائقة القدرة التي تتعامل مع تهديدات الاعتراض السيبراني والقرصنة السيبرانية والتجسس السيبراني نظرا للتكاليف المرتفعة لشراء البرامج الاصلية.

الاستنتاجات والتوصيات

أولا: الاستنتاجات:

1. غياب المفهوم الدقيق للأمن السيبراني لدى عينة الدراسة من مدراء الفنادق الخمس نجوم على الرغم من وجود تصور مبدئي حول مفهوم الامن الالكتروني واهمية توفير برامج الحماية البيانات والمعلومات المتعلقة بالعملاء واعمال الفندق.
2. عدم وجود قسم خاص بالأمن السيبراني الفنادق الخمس نجوم حيث تتم الاعمال المتعلقة به في قسم الصيانة الهندسية او قسم الامن.
3. تبين تكرار حدوث تهديدات لأجهزة الحاسب الالي بالفندق بالفيروسات التي تعطل عمل الاجهزة او تقلل من قدرتها العملية كما حدث في بعض الاحيان محاولات لاختراق البيانات الخاصة بالعملاء للحصول على ارقام الهواتف الشخصية لاستخدامها في اعمال الدعاية والتسويق.
4. عدم وجود خطة محددة لتطوير الاداء الالكتروني في مجال الامن السيبراني واقتصارها على حماية اجهزة الحاسب الالي من الفيروسات او الدخول غير المسموح به لأنظمة الفندق.
5. يوجد في بعض الفنادق الخمس نجوم عدد من الافراد المؤهلين في التعامل مع تكنولوجيا المعلومات وصيانة الاجهزة والمعدات بشكل عام ولكن يوجد قصور في الموارد البشرية المختصة في مجال الامن السيبراني.
6. توجد جهود حكومية في مجال الامن السيبراني تمثلت في انشاء المركز الوطني للأمن السيبراني الاردني الا انه لا توجد مبادرات مشتركة لتوفير الامن السيبراني في الفنادق.
7. تتمثل اهم اشكال تطبيق الامن السيبراني في الفنادق تتمثل في برامج الحماية من الفيروسات الحاسوبية لتامين الشبكات الداخلية من البرامج الضارة وتامين الدخول على محركات البحث على شبكة الانترنت.
8. لا تستخدم معظم الفنادق انظمة الامن السيبراني فائقة القدرة للتعامل مع تهديدات الاعتراض السيبراني

والقرصنة السيبرانية والتجسس السيبراني نظرا للتكاليف المرتفعة لشراء البرامج الاصلية.

9. غياب الادراك الدقيق لدى مدراء فنادق الخمس نجوم بمنطقة المثلث الذهبي بالأردن لمفهوم الأمن السيبراني.

ثانيا: التوصيات:

1. اعتبار الامن السيبراني مجالا مهما من مجالات تحقيق الميزة التنافسية الفندقية نظرا لتأثيره على العديد من الابعاد التنافسية
2. التنسيق بين نظم الحماية الامنية الالكترونية في الفنادق وبين الجهات الامنية المسئولة عن الامن السيبراني في الاردن.
3. عقد المزيد من الدورات التدريبية والتثقيفية للعاملين في الفنادق حول اهمية الاهتمام بإدارة الامن السيبراني في الفنادق لتحقيق الميزة التنافسية.
4. عقد شراكات مع الشركات العالمية المتخصصة في الامن السيبراني لتعزيز قدرات الفنادق في مجال الحماية الالكترونية للبيانات لمواكبة أحد النظم العالمية في الامن السيبراني.
5. استقطاب الموارد البشرية الماهرة في مجال الامن السيبراني لتكوين راس المال البشري القادر على تولى مسؤولية الامن السيبراني داخل الفندق مما يحقق ميزة تنافسية للفنادق
6. تشجيع العاملين على الابتكار التكنولوجي في مجال الامن السيبراني عن طريق تقديم الحوافز المادية والمعنوية للخبرات والكفاءات الفردية.
7. انشاء وحدة خاصة بالأمن السيبراني داخل الفندق تتبع قسم الامن الفندقي وتوفير كافة الاجهزة والمعدات والبرامج الالكترونية لها.

توافر البيانات:

تم تضمين البيانات المستخدمة لدعم نتائج هذه الدراسة في المقالة.

تضارب المصالح:

يعلن المؤلفون أنه ليس لديهم تضارب في المصالح.

موارد التمويل:

لم يتم تلقي اي دعم مالي.

شكر وتقدير:

لا أحد.

References:

1. Ministry of Tourism and Antiquities. (2020). Statistics 2020. Retrieved in April 2020, from https://www.mota.gov.jo/Contents/Statistics_2018_2ndAr.aspx.
2. International Telecommunication Union. (2006). Cybersecurity Guide for Developing Countries. Geneva, Switzerland.
3. Al-Ashqar, M. (2012). Al-amn al-saybiri: Al-tahadiyat wa mustalazimat al-muwajaha [Cybersecurity: Challenges and Requirements for Confrontation]. First Annual Meeting of Cybersecurity Experts, Arab Center for Legal and Judicial Research, Cairo, Egypt.
4. Al-Asfar, A. A. (2011). ‘Awamil irtifa‘ mu‘addalat al-jarima al-mustahdatha wa subul muwajahatiha [Factors of the Increase in Emerging Crimes and Ways to Combat Them]. Scientific Symposium on Analyzing Emerging Crimes and Criminal Behavior, College of Training, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.
5. Al-Jamousi, J. (2016). Al-iftiḍar wa al-thawra: Makanat al-internet fi nash’at mujtama‘madani ‘Arabi [Virtualization and Revolution: The Role of the Internet in the Rise of an Arab Civil Society]. Arab Center for Research and Policy Studies, Beirut, Lebanon.
6. Al-Janfawi, K. M. (2021). Al-tahawul al-raqmi lil-mu’assasat al-wataniyah wa tahadiyat al-amn al-saybiri min wijhat nazar dubbat al-shurta al-akademiyin fi al-Kuwait [Digital Transformation of National Institutions and Cybersecurity Challenges from the Perspective of Academic Police Officers in Kuwait]. Al-Majalla Al-Arabiya lil-Adab wa al- ‘Ulum al-Insaniya, The Arab Institution for Education, Science, and Literature, 5(19).
7. Al-Harbi, A. (2019). Nafidha ‘ala al-amn al-saybiri fi zill ru’ya 2030 [A Window on Cybersecurity under Vision 2030]. Ministry of Communications and Information Technology, Riyadh, Saudi Arabia.
8. Al-Harbi, A. (2021). Muqaddima fi al-amn al-saybiri [Introduction to Cybersecurity]. Institute for Research and Consultancy Studies, Umm Al-Qura University, Saudi Arabia.

9. Al-Hamiri, B. A., & Baris, A. K. (2006). Athar teknulujia al-ma‘lumat fi jawdat al-khidmat al-fundukiya: Dirasa maydaniya ‘ala ‘ayina min al-fanadiq al-siyahiya [The Impact of Information Technology on the Quality of Hotel Services: A Field Study on a Sample of Tourist Hotels]. Majallat Jami‘at Ahl al-Bayt, (4).

10. Al-Khudari, J. S. M., Salami, H. J. A., & Kulaibi, N. N. M. (2020). Al-amn al-saybiri wa al-dhaka’ al-sina‘i fi al-jami‘at al-Su‘udiyah: Dirasa muqarana [Cybersecurity and Artificial Intelligence in Saudi Universities: A Comparative Study]. Majallat Tatwir al-Adha’ al-Jami‘i, Mansoura University, 12(1), Egypt.

11. Al-Dalabih, A. A. A. (2021). Ta‘ziz al-amn al-saybiri dakhil al-dawla wa dawruhu fi al-hifaz ‘ala al-amn al-watani: Al-jil al-khamis min al-asliha [Enhancing Cybersecurity within the State and Its Role in Preserving National Security: The Fifth Generation of Weapons]. Unpublished Master's Thesis, Al al-Bayt University, Amman, Jordan.

12. Al-Samhan, M. A. (2020). Matalib tahqiq al-amn al-saybiri li-anzimat al-ma‘lumat al-idariyah fi Jami‘at al-Malik Saud [Cybersecurity Requirements for Management Information Systems at King Saud University]. Majallat Kulliyat al-Tarbiyah, Mansoura University, (111), Egypt.

13. Al-Shammari, M. I. S. (2021). Al-amn al-saybiri wa atharuhu fi al-amn al-watani al-‘Iraqi [Cybersecurity and Its Impact on Iraqi National Security]. Majallat al-‘Ulum al-Qanuniya wa al-Siyasiya, Diyala University, 10(1), Iraq.

14. Al-Ali, Z. A. (2019). Al-sira‘ wa al-amn al-jiyusaybiri fi al-siyasa al-dawliya: Dirasa fi istiratijiyat al-ishtibak al-raqmi [Conflict and Geocybersecurity in International Politics: A Study in Digital Engagement Strategies]. Amjad Publishing & Distribution, Amman, Jordan.

15. Al-‘Awadi, A. M. G. (2016). Al-amn al-ma‘lumati al-saybiri [Cyber Information Security]. Al-Bayan Center for Studies and Planning, Baghdad, Iraq.

16. Al-Faris, A. (2022). Ma yajibu ma‘rifatuhu ‘an takhassus al-amn al-saybiri fi al-Urdun [What You Need to Know About Cybersecurity as a Major in Jordan]. Retrieved October 3, 2022, from https://mawdoo3.com.

17. Al-Mubayidin, I. (2022). Ma hiya tahadiyat al-amn al-saybiri fi al-Urdun [What Are the Cybersecurity Challenges in Jordan?]. Retrieved October 3, 2022, from https://alghad.com.

18. Al-Malahi, F. (2015). Al-amn al-saybiri [Cybersecurity]. Majallat al-Doha, Ministry of Information, Doha, Qatar.

19. Al-Maqsudi, M. A. A. (2017). Al-jara’im al-ma‘lumatiya: Khasa’isuha wa kayfiyat muwajahatiha qanuniyan [Cyber Crimes: Their Characteristics and Legal Countermeasures]. Al-Majalla al-‘Arabiyya lil-Dirasat al-Amniya, Naif Arab University for Security Sciences, 33(70), Riyadh, Saudi Arabia.

20. Al-Yahya, R. M. (2013). Isra’il wa khutwat al-haymana ‘ala sahat al-fada’ al-saybiri fi al-Sharq al-Awsat [Israel and Its Steps to Dominate the Cyber Space in the Middle East]. Majallat Ru’a Istratijiya, 3(4), June 2013, pp. 68.

21. Ministry of Communications and Information Technology. (2018). Al-Istratijiya al-Wataniya lil-Amn al-Saybiri [The National Cybersecurity Strategy]. Amman, Jordan.

22. Bazzazou, I. (2020). Taqniyat al-robot al-raqmi fi sina‘at al-siyaha al-Urduniya [Digital Robot Technologies in the Jordanian Tourism Industry]. Al-Rai Newspaper, December 19, 2020, Amman, Jordan.

23. Jabbour, M. A. (2012). Al-amn al-saybiri: Al-tahadiyat wa mustalazimat al-muwajaha [Cybersecurity: Challenges and Requirements for Confrontation]. Arab League, Beirut, Lebanon.

24. Dahmani, S. (2018). Athar al-tahdidat al-saybiriya ‘ala al-amn al-qawmi: Wilayat al-Mutahida al-Amrikiyya namudhajan (2001–2017) [The Impact of Cyber Threats on National Security: The United States as a Model (2001–2017)]. Unpublished Master's

Cyber Attacks?]. Majallat Ittijahat al-Ahdath, (6).

33. Mansour, A. M. (2021). Ta'thir al-amn al-saybiri 'ala al-raqaba al-dakhiliya wa in'ikasatuha 'ala al-wahda al-iqtisadiya: Dirasa istitla'iya [The Impact of Cybersecurity on Internal Auditing and Its Reflection on the Economic Unit: An Exploratory Study]. Majallat al-Idara wa al-Iqtisad, Al-Mustansiriya University, (127), Iraq.

34. Yahya, R. M. (2013). Isra'il wa khutwat al-haymana 'ala sahat al-fada' al-saybiri fi al-Sharq al-Awsat: Dirasa hawl isti'dadat wa mahawir 'amal al-dawla al-'ibriya fi 'asr al-internet (2002–2013) [Israel and Its Steps to Dominate the Cyber Space in the Middle East: A Study on the Preparations and Action Axes of the Hebrew State in the Internet Era (2002–2013)]. Majallat Ru'a Istratijiya, 3(4), June 2013, p. 68.

35. Ministry of Communications and Information Technology. (2018). Al-istratijiya al-wataniya lil-amn al-saybiri [The National Cybersecurity Strategy]. Amman, Jordan.

36. Amoroso, E. (2007): Cyber Security, Silicon Press.

37. Bazazo, I; Al-Orainat, L; Abuizhery, F; & Al-Dhoun, R.A. (2019): Cyber Security Applications in the Modern Tourism Industry. Journal of Tourism, Hospitality and Sport, Vo.43.

38. Jain, J. & Pal, P. (2017): A Recent Study Over Cyber Security and its Elements, International Journal of Advanced Research in Computer Science (India: Rajasthan, Janardan Rai Nagar Rajasthan Vidyapeeth, Vol.8, No. 3

39. Nye, J.R. (2010): Cyber Power, Harvard Kennedy School.

40. Shabani, N., & Munir, A. (2020, July). A Review of Cyber Security Issues in Hospitality Industry. In Science and Information Conference (pp. 482-493). Springer, Cham.

41. World Economic Forum (2009-2022): The Travel & Tourism Competitiveness Reports 2011-2021, Geneva, Switzerland

Thesis, Faculty of Law and Political Science, Mohamed Boudiaf University, Algeria.

25. Raqouli, K., & Lakhder, N. (2019). Al-amn al-saybiri al-mutawassiti bayn al-waqi' wa al-rahanat al-amniya [Mediterranean Cybersecurity: Between Reality and Security Stakes]. Majallat Tabna lil-Dirasat al-'Ilmiya al-Akademiya, (3), Algeria.

26. Samir, B. (2017). Al-amn al-saybiri fi al-Jaza'ir: Al-siyasat wa al-mu'assasat [Cybersecurity in Algeria: Policies and Institutions]. Al-Majalla al-Jaza'iriyya lil-Amn al-Insani, (4), Algeria.

27. Shafiq, N. (2014). Athar al-tahdidat al-elektruniya 'ala al-'alaqat al-dawliya: Dirasa fi ab'ad al-amn al-elektruni [The Impact of Electronic Threats on International Relations: A Study in the Dimensions of Cybersecurity]. Arab Office for Knowledge, Cairo, Egypt.

28. Asiri, F. M. (2020). Al-amn al-saybiri wa hifaz amn al-ma'lumat [Cybersecurity and Information Security Protection]. Riyadh, Saudi Arabia.

29. Gharib, H., & Meziani, S. (2020). Tahdid al-irhab fi al-fada' al-saybiri: Nahwa rasm muqaraba ma'rifiya lil-tahdid al-nashi' [The Threat of Terrorism in Cyberspace: Towards a Cognitive Approach to Emerging Threats]. Majallat al-Dirasat al-Istratijiya wa al-'Askariya, Arab Democratic Center, 2(7), Berlin, Germany.

30. Qadir, I. (2016). Idarat al-hurub al-nafsiyah fi al-fada' al-elektruni: Al-istratijiya al-Amrikiyya al-jadida fi al-Sharq al-Awsat [Managing Psychological Warfare in Cyberspace: The New American Strategy in the Middle East]. Scientific Symposium on the Globalization of Political Media and National Security Challenges in Developing Countries, University of Algeria.

31. Mashoush, M. (2018). Al-juhud al-dawliya li-mukafahat al-ijram al-saybiri [International Efforts to Combat Cybercrime]. Faculty of Legal, Economic, and Social Sciences, Hassan I University, Morocco.

32. Mukhtar, M. (2015). Hal yumkin an tatajanab al-duwal makhater al-hajamat al-elektruniya? [Can States Avoid the Risks of