

الأمن السيبراني

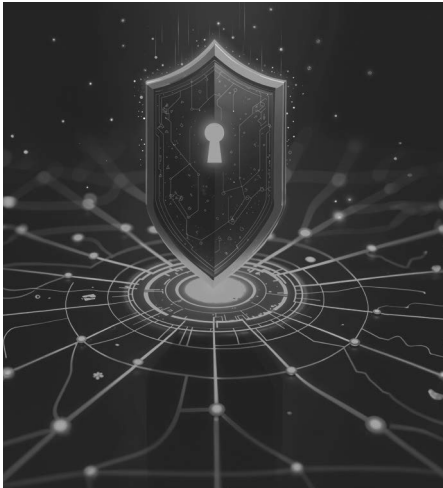
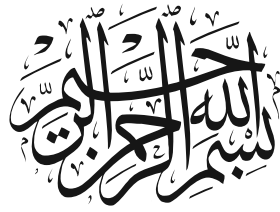
المفاهيم والتطبيقات والمخاطر الاجتماعية السيبرانية

CYBERSECURITY

Concepts, Applications & Cyber Social Risks

أ.د. ذياب البداينة





الأمن السيبراني

المفاهيم والتطبيقات والمخاطر الاجتماعية السيبرانية

CYBERSECURITY

Concepts, Applications & Cyber Social Risks

جميع الحقوق محفوظة. لا يسمح بإعادة إصدار هذا الكتاب أو أي جزء منه، أو تخزينه في نطاق استعادة المعلومات، أو نقله بأي شكل من الأشكال، دون إذن مسبق من الناشر.

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted in any form or by any means without prior written permission of the publisher.

DAR AL FIKER

جميع حقوق الطبع محفوظة ©



www.daralfiker.com

كتابي الصغير
للنشر والتوزيع



www.ketabi.jo

المملكة الأردنية الهاشمية - عمان
شارع رشيد المدفعي - بجانب المسجد الحسيني
وسط البلد (3د) عمارة الحجيري
هاتف: +962 6 4621938
ص.ب: 183520 عمان 1118 الأردن
بريد إلكتروني: info@daralfiker.com
بريد المبيعات: sales@daralfiker.com

التصنيف: 005.8

تأليف: دياب موسى فلاح البداينة
الأمن السيبراني المفاهيم والتطبيقات والمخاطر
الاجتماعية السيبرانية

رقم الإيداع: 2025/2/851

الواصفات: //الأمن السيبراني//أمن البرمجيات//
الجرائم الحاسوبية//الذكاء الاصطناعي//شبكات
المعلومات//الاتفاقيات الدولية//تكنولوجيا المعلومات

* أعدت دائرة المكتبة الوطنية بيانات الفهرسة والتصنيف الأولية
* يتحمل المؤلف كامل المسؤولية القانونية عن محتوى مصنفه ولا
يعبر هذا المصنف عن رأي دائرة المكتبة الوطنية أو أي جهة
حكومية أخرى.

الطبعة الأولى

1447- 2026

مواقع التواصل الاجتماعي



daralfiker1978@gmail.com



daralfiker/



dar_alfiker



dar al-fiker for publishing & distributing



pub/dar-alfiker

ISBN: 978-9957-92-319-8

الأمن السيبراني

المفاهيم والتطبيقات والمخاطر الاجتماعية السيبرانية

CYBERSECURITY

Concepts, Applications & Cyber Social Risks

أ. د. ذياب البداينة

كلية الدراسات العليا - أكاديمية الشرطة- قطر

الطبعة الأولى

1447- 2026

دار الفكر
ناشر وموزع



الفهرس موجز

الباب الأول: الفضاء السيبراني

17	الفصل 1 . الفضاء السيبراني.....
31	الفصل 2 . تكنولوجيا المعلومات والاتصالات ICT.....
51	الفصل 3 . التقنيات الناشئة.....
81	الفصل 4 . الذكاء الاصطناعي.....
119	الفصل 5 . الأمن السيبراني: التاريخ والمفاهيم الأساسية

الباب الثاني: الأمن السيبراني التشريعات والسياسات

159	الفصل 6 . المعايير العالمية للأمن السيبراني
177	الفصل 7 . المعاهدات الدولية في الأمن السيبراني

الباب الثالث: المخاطر السيبرانية الاجتماعية

199	الفصل 8 . التهديدات السيبرانية.....
221	الفصل 9 . الجرائم السيبرانية.....
261	الفصل 10 . الإرهاب السيبراني.....
297	الفصل 11 . الحرب السيبرانية.....
327	الفصل 12 . الضحية السيبرانية



الفهرس مفصل

الباب الأول: الفضاء السيبراني

المقدمة	13
الفصل 1. الفضاء السيبراني	17
تاريخ تطور مفهوم الفضاء السيبراني	18
لماذا سمي الفضاء السيبراني؟	20
الفضاء السيبراني : المكونات	20
طبقات الفضاء السيبراني	21
1. الطبقة المادية للفضاء السيبراني	21
2. طبقة المنطق	22
3. طبقة المعلومات	23
4. الطبقة الأعلى- الناس	24
الفصل 2. تكنولوجيا المعلومات والاتصالات	31
المقدمة	32
تأثير تكنولوجيا المعلومات والاتصالات	33
موجز عن تاريخ تكنولوجيا المعلومات والاتصالات	34
ما تكنولوجيا المعلومات والاتصالات ؟	36
مختصر تطور الإنترنت	37
مكونات نظام تكنولوجيا المعلومات والاتصالات	40

43.....	7 اختراعات جعلت من التسعينات زمن التكنولوجيا الذهبي.....
44.....	الاستفادة من تكنولوجيا المعلومات والاتصالات
51.....	الفصل 3. التقنيات الناشئة.....
52.....	التقنيات الناشئة
53.....	المقدمة
53.....	تاريخ التكنولوجيا
55.....	أهم التقنيات الناشئة
73.....	السياسة القطرية في مجال التقنيات الناشئة
81.....	الفصل 4. الذكاء الاصطناعي.....
82.....	الذكاء الاصطناعي
83.....	تاريخ الذكاء الاصطناعي؟
86.....	ما الذكاء الاصطناعي؟
88.....	الأنواع الأربعة للذكاء الاصطناعي.....
88.....	1. الذكاء الاصطناعي الارتكاسي (تفاعلي).....
88.....	2. آلات ذات ذاكرة محدودة
89.....	3. نظرية العقل
89.....	4. الذكاء الاصطناعي المدرك للذات
89.....	الذكاء المعزز مقابل الذكاء الاصطناعي
91.....	تعلم الآلة
92.....	حدود التعلم الآلي.....
93.....	أهمية الذكاء الاصطناعي
94.....	استخدامات الذكاء الاصطناعي.....
96.....	تطبيقات الذكاء الاصطناعي.....
97.....	بعض تقنيات الذكاء الاصطناعي
99.....	مكونات الاستخدام المسؤول للذكاء الاصطناعي
108.....	مزايا وعيوب الذكاء الاصطناعي
109.....	الذكاء الاصطناعي والأمن السيبراني
109.....	كيف يحسن الذكاء الاصطناعي الأمن السيبراني

111.....	التحديات الرئيسية التي يواجهها الأمن السيبراني
112.....	عيوب وقيود استخدام الذكاء الاصطناعي في الأمن السيبراني
119.....	الفصل 5. الأمن السيبراني: التاريخ والمفاهيم الأساسية
120.....	الأمن السيبراني: التعريف
123.....	أهمية الأمن السيبراني
123.....	الركائز الخمس لإطار ضمان المعلومات
124.....	الأمن السيبراني: التطور التاريخي
126.....	فجر الأمن السيبراني: السبعينات
128.....	الثمانينات: ظهور الإنترنت وبرامج مكافحة الفيروسات
130.....	العقد الأول من القرن الحادي والعشرين: عصر الحرب السيبرانية
131.....	2010: صعود شركات الأمن السيبراني
132.....	2020: مستقبل الأمن السيبراني
133.....	الأمن السيبراني: المفاهيم الأساسية
133.....	المفهوم الأساسي للأمن السيبراني
134.....	المصطلحات

الباب الثاني: الأمن السيبراني التشريعات والسياسات

159.....	الفصل 5. المعايير العالمية للأمن السيبراني
160.....	القانون الدولي في الفضاء السيبراني؟
161.....	المعايير السيبرانية في الأمم المتحدة
162.....	تاريخ تشريعات الأمن السيبراني في الأمم المتحدة
163.....	مؤشر الأمن السيبراني العالمي
165.....	الولايات المتحدة
167.....	الاتحاد الأوروبي
167.....	المملكة المتحدة
168.....	الآسيان / أوقيانوسيا
168.....	في أستراليا
168.....	السلوك المسؤول للدولة في الفضاء السيبراني

المسؤولية الأخلاقية في العالم الرقمي: الوثيقة القطرية.....	169
دليل المسؤولية الأخلاقية في العالم الرقمي.....	170
الفصل 7. المعاهدات الدولية في الأمن السيبراني.....	
موجز تمهيدي عن القانون الدولي والفضاء السيبراني	178
اللاعبون	178
القضايا الرئيسية	178
معاهدة الأمم المتحدة لمكافحة الجرائم السيبرانية	180
تحديات الأمن السيبراني في القانون الدولي	182
اللوائح السيبرانية العالمية	182
المعاهدات الدولية في الأمن السيبراني	182
القانون الدولي القابل للتطبيق في الفضاء السيبراني (كندا)	184
التطبيق العام للقانون الدولي	185
السيادة	185
تحديات السيادة السيبرانية:	187
عدم التدخل	187
إجراءات تحقق المتطلبات	188
مسؤولية الدولة	
القانون الدولي لحقوق الإنسان	189
التهديد أو استخدام القوة	189
الدفاع عن النفس ضد الهجوم المسلح	190
القانون الدولي الإنساني	190
الإجراءات القانونية: التخطيط للتدخلات المستقبلية	190

الباب الثالث: المخاطر السيبرانية الاجتماعية

الفصل 8. التهديدات السيبرانية.....	
المقدمة	200
التهديد السيبراني	201
مصادر التهديدات السيبرانية	201

201.....	الدول المعادية
202.....	الجماعات الإرهابية
202.....	جواسيس الشركات ومنظمات الجريمة المنظمة
202.....	المتسللون
202.....	المطلعون (الداخليون) الساطون
202.....	القرصنة
203.....	الكوارث الطبيعية
203.....	الإجراءات العرضية للمستخدمين المصرح لهم
203.....	أمثلة على التهديدات السيبرانية
206.....	التهديدات السيبرانية في عام 2022
208.....	الحماية من التهديدات السيبرانية
209.....	الدفاع ضد التهديدات السيبرانية: ذكاء التهديد السيبراني
210.....	ذكاء التهديد السيبراني والأنواع الأخرى من الذكاء السيبراني
210.....	أهمية ذكاء التهديد السيبراني
213.....	دورة حياة ذكاء التهديد السيبراني
215.....	أهمية ذكاء التهديد السيبراني
221.....	الفصل 9. الجرائم السيبرانية
222.....	الجريمة السيبرانية
222.....	مصطلح «الجريمة السيبرانية»
223.....	تعريفات مصطلح «الجرائم السيبرانية»
227.....	تصنيفات تعريف «الجرائم السيبرانية»
229.....	تصنيف الجرائم السيبرانية
240.....	التاريخ المختصر للجرائم السيبرانية
246.....	نظريات الجريمة السيبرانية
246.....	علم الجريمة السيبراني
248.....	نظرية النشاط الروتيني
249.....	نظرية التعلم الاجتماعي
249.....	نظرية انتقال الفضاء
250.....	نظرية سقوط الضحايا
250.....	نظرية الضغوط العامة

251.....	أنواع الجرائم السيبرانية
252.....	البرامج غير المرغوب فيها
253.....	كيفية مكافحة الجرائم السيبرانية

261..... **الفصل 10. الإرهاب السيبراني**

262.....	الإرهاب السيبراني
264.....	الإرهاب السيبراني : التعريف
270.....	الذنب المنفرد السيبراني
271.....	لماذا الإرهاب السيبراني.....
272.....	خصائص الهجوم السيبراني
274.....	أهداف الإرهاب السيبراني ودوافعه
275.....	تاريخ الإرهاب السيبراني
277.....	حوادث سيبرانية مهمة منذ عام 2006
279.....	أساطير الإرهاب المادي والسيبراني
281.....	الحرب السيبرانية والإرهاب السيبراني
282.....	التقنيات الناشئة والإرهاب السيبراني
282.....	الذكاء الاصطناعي والإرهاب السيبراني
285.....	ذكاء التهديد السيبراني والإرهاب السيبراني
285.....	إنترنت الأشياء والإرهاب السيبراني
286.....	إنترنت كل شيء والإرهاب السيبراني
287.....	الطائرات دون طيار والإرهاب السيبراني
288.....	إنترنت الأجسام
288.....	الإرهاب السيبراني والتقنيات الناشئة: تحديات الأمن الوطني والسيادة الوطنية
290.....	السيادة القومية السيبرانية والإرهاب السيبراني
292.....	المضامين الأمنية للتقنيات الناشئة والفضاء السيبراني

297..... **الفصل 11. الحرب السيبرانية**

298.....	المقدمة
302.....	الحرب السيبرانية
302.....	أمثلة على عمليات الحرب السيبرانية
307.....	أهداف الحرب السيبرانية

307.....	أنواع هجمات الحرب السيبرانية
308.....	أنواع هجمات الحرب السيبرانية
310.....	الحرب السيبرانية واستخدام القوة.....
310.....	دليل تالين
311.....	الدفاع ضد الحرب السيبرانية
312.....	الردع السيبراني
312.....	أمثلة تاريخية لهجمات الحرب السيبرانية
314.....	مكافحة الحرب السيبرانية
314.....	كيفية مكافحة الحرب السيبرانية
314.....	إجراء تقييمات المخاطر باستخدام مناورات الحرب السيبرانية
315.....	أهمية الدفاع متعدد الطبقات
315.....	تأمين القطاع الخاص
316.....	القوة السيبرانية
317.....	وصف القوة السيبرانية
318.....	الحياد السيبراني والحرب السيبرانية
318.....	القانون الدولي والحرب السيبرانية
319.....	المتحاربون والحياد السيبراني
319.....	إجراءات تحقق المتطلبات
320.....	التدابير المضادة
327.....	الفصل 12. الضحية السيبرانية
329.....	الضحايا
329.....	لماذا يصبح الشخص ضحية؟
329.....	دور الضحية في الجريمة
330.....	ثنائي الضحية المجرم: هانز فون هينتيغ
331.....	تصنيف الضحايا والمسؤولية
332.....	تصنيف الضحايا والمسؤولية: ستيفن شيفر
332.....	نظريات الضحية السيبرانية
332.....	نظريات ضحايا الجرائم السيبرانية
333.....	نظرية المكان المنحرف

333.....	نظرية غط الحياة
335.....	نظرية سقوط الضحايا
336.....	نظرية الأنشطة الروتينية
337.....	أمثلة على الضحايا
345.....	الأمن السيبراني: الواقع والتحديات (نحو أنموذج جديد في الأمن)
349.....	المراجع
373.....	حول المؤلف

المقدمة

في الفضاء السيبراني المترابط اليوم، أصبح الأمن السيبراني حجر الزاوية للمجتمع الحديث. من حماية البيانات الشخصية إلى تأمين البنية التحتية الحيوية، يمتد نطاق الأمن السيبراني إلى ما هو أبعد من التحديات التقنية البحتة إلى التحديات الاجتماعية السيبرانية حيث يمثل السلوك الإنساني السيبراني أهم المخاطر الأمنية السيبرانية - فهو يشمل الأبعاد الاقتصادية والاجتماعية والأخلاقية. تم تأليف هذا الكتاب **المدخل إلى الأمن السيبراني: المفاهيم والتطبيقات والمخاطر الاجتماعية السيبرانية** لتوفير معرفة شاملة وعامة في مجال الأمن السيبراني، بما في ذلك تقديم المفاهيم الأساسية، بينما تستعرض أيضاً التطبيقات الواقعية في الصناعات مثل التمويل والرعاية الصحية والحكومة. برز الأمن السيبراني كواحد من أكثر التحديات إلحاحاً في عصرنا. من الأجهزة الشخصية إلى البنية التحتية الوطنية، يعد النظام البيئي الرقمي معجزة من الإبداع وهدفًا ضعيفًا للاستغلال. الأمن السيبراني، الذي كان ذات يوم اهتمامًا خاصًا بالمتخصصين، أصبح الآن أولوية عالمية تتطلب اهتمام الأفراد والشركات والحكومات على حد سواء. يتناول هذا الكتاب موضع الأمن السيبراني من منظور علم الجريمة، وبعيداً عن المجال الفني، يتناول الكتاب أيضاً التفاعل الحاسم بين الأمن السيبراني والمجتمع، ويلقي الضوء على قضايا مثل المعلومات المضللة عبر الإنترنت، ومخاوف الخصوصية، والأخلاق الرقمية، والعوامل البشرية التي تؤثر على نقاط الضعف السيبرانية.

يشمل **الباب الأول من الكتاب** خمسة فصول هي: **الفصل 1** ويتناول موضوع **الفضاء السيبراني**، حيث الفضاء السيبراني هو نظام هجين وفريد من نوعه في الخصائص المادية والافتراضية، والأجهزة والبرامج، وهو جميع شبكات الكمبيوتر في العالم بما في ذلك الإنترنت وكذلك الشبكات الأخرى المنفصلة وغير المرتبطة بالإنترنت. ويتناول **الفصل 2** موضوع **تكنولوجيا المعلومات والاتصالات**، تُعد تكنولوجيا المعلومات والاتصالات (ICT) من أبرز التطورات التي شهدتها العالم في العقود الأخيرة، حيث أصبحت أساساً جوهرياً لتقدم المجتمعات وتطورها. تشتمل تكنولوجيا المعلومات والاتصالات على مجموعة واسعة من الأدوات والتطبيقات التي تهدف إلى إدارة المعلومات ومعالجتها وتبادلها بطرق أكثر كفاءة وفعالية. كما يتناول **الفصل 3** موضوع **الفضاء التقنيات الناشئة**، حيث تمثل تقنيات جديدة وحديثة أو لا تزال في طور التطوير والتطبيق، مثل التطبيقات المختلفة للتكنولوجيا الحيوية بما في ذلك العلاج الجيني أنها «تقنية متطورة جذرية وسريعة النمو نسبياً تتميز بدرجة معينة من الترابط المستمر مع الوقت. يتناول **الفصل 4** موضوع **الذكاء الاصطناعي**، الذكاء الاصطناعي ثورة تقنية واجتماعية ويهتم بتطوير أنظمة الكمبيوتر التي تحاكي التفكير البشري عندما تكون كذلك وتطبق في مجال المعرفة العقلانية.. واخيراً يتناول **الفصل 5** موضوع **الأمن السيبراني: المفهوم والتطور**، حيث يستعرض التطور التاريخي وأهم المصطلحات الرئيسية. فالأمن السيبراني معني بالتدابير المتخذة لحماية الكمبيوتر أو نظام الكمبيوتر (كما هو الحال على الإنترنت) ضد الوصول أو الهجوم غير

المصرح به وهو مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمانات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول التنظيم والمستخدم» ضمن بؤر الأمن السيبراني لأهداف السرية والتوافر والنزاهة.

يشمل الباب الثاني فصلين هما: الفصل 6 ويناول موضوع المعايير العالمية للأمن السيبراني، حيث تولي الدول اهتماماً متزايداً لحوكمة الفضاء السيبراني (الهندسة التقنية التي تسمح للإنترنت العالمي بالعمل) والحوكمة في (كيف يمكن للدول والصناعة والمستخدمين استخدام ذلك التكنولوجي). في حين يتناول الفصل 7 موضوع القانون السيبراني والسيادة الوطنية السيبرانية، على عكس العديد من القضايا الدولية الأخرى، لم تنشأ حوكمة الفضاء السيبراني مع الدول، ولكن مع المؤسسات الأكاديمية والجهات الفاعلة الخاصة التي قامت ببناء الإنترنت (وإن كان ذلك بتمويل حكومي). مع تسويق الإنترنت، ظهرت شركات تكنولوجيا المعلومات والاتصالات.

يشمل الباب الثالث خمسة فصول هي: يتناول الفصل 8 : التهديدات السيبرانية. تشير التهديدات السيبرانية الاجتماعية إلى الممارسات الضارة في سياقات الإنترنت، والتي يتم تصنيف بعضها على أنها سلوك إجرامي، والتي يتم تمكينها أو تسهيلها بواسطة وسائل التواصل الاجتماعي ومنصات الألعاب عبر الإنترنت، ويتناول الفصل 9 : الجرائم السيبرانية يشمل تصنيف الجريمة السيبرانية من (1) العبور السيبراني، و(2) الخداع السيبراني والسرقة و(3) الإباحية السيبرانية والفحش، و(4) العنف السيبراني.. لا يوجد تعريف مقبول عالمياً للجريمة السيبرانية. يتمثل النهج الشائع في تعريفها إلى فئتين: الجرائم السيبرانية المعتمدة على الإنترنت والجرائم السيبرانية الممكنة عبر الإنترنت. كما يتناول الفصل 10: الإرهاب السيبراني الفضاء السيبراني ليس بلا جانب مظلم، فقد أُستغل من قبل الإرهابيين كأداة اتصال بين المجموعات الإرهابية وأداة تجنيد وتنفيذ، كما استخدم هذا الفضاء كأداة تدمير وتعطيل لبنية التحتية وحرمان من الخدمة. كما إنه يشكل حيزاً ووسيطاً لتوزيع الرسائل والمعلومات الإرهابية ومع انتشار التقنيات الناشئة مثل الذكاء الاصطناعي وانترنت الأشياء والاجسام وذكاء التهديد السيبراني ومع وجود الذئب المنفرد السيبراني جنباً إلى جنب مع الخصائص المسهلة للإرهاب في البيئة السيبرانية. ويتناول الفصل 11: الحرب السيبرانية يشير مصطلح «الحرب السيبرانية» إلى الحرب التي تجري في الفضاء السيبراني من خلال الوسائل والأساليب السيبرانية.. تتضمن الحرب السيبرانية هجمات سيبرانية متعددة من قبل دولة واحدة أو أكثر ضد أخرى؛ أبعد من ذلك، غالباً ما يختلف خبراء الأمن والمسؤولون الحكوميون والقادة العسكريون حول أنواع الجرائم السيبرانية التي ينبغي أن تعد أعمال حرب سيبرانية وأخيراً يتناول الفصل 12: الضحية السيبرانية يتناول دراسة الضحايا. يشمل علم الضحايا، إذن، دراسة مسببات (أو أسباب) الضحايا وعواقبها، وكيفية تعامل نظام العدالة الجنائية مع الضحايا ومساعدتهم، وكيفية تعامل عناصر المجتمع الأخرى مثل وسائل الإعلام مع ضحايا الجريمة.

البروفيسور ذياب البدينة