

الأستاذ الدكتور ذياب البداينة

الأمن وحرب المعلومات



المحتويات

أ-ح	جدول المحتويات
ك	فهرس الجداول
ل	فهرس الأشكال
5	المقدمة

الجزء الأول: الأمن في المجتمع المعلوماتي

12	تمهيد
	الفصل الأول: الأمن الوطني في المجتمع المعلوماتي: المفهوم والتحديات والانكشافات
13	مقدمة
14	الأمن : المفهوم
21	الأمن من المنظور المعلوماتي
22	تحديات المجتمع المعلوماتي
23	الفصل الثاني: الثغرات الأمنية الجديدة والتهديدات المشتركة
29	مقدمة
31	التهديدات
33	الثغرات (الانكشافات) الجديدة
34	1- قطاع الاتصالات والمعلومات
37	2- قطاع التوزيع الفيزيقي
39	3- قطاع الطاقة
39	4- قطاع المال والبنوك
40	5- قطاع الخدمات الانسانية الحيوية
41	وسائل التعدي على البنية التحتية المعلوماتية
42	الفصل الثالث: خصائص المجتمع المعلوماتي
47	مقدمة
49	

57	معايير المجتمع المعلوماتي
58	خصائص مجتمع المعلومات:
71	أولاً: الخصائص التقنية
87	ثانياً: الخصائص الاجتماعية
93	ثالثاً: الخصائص الثقافية
96	رابعاً: الخصائص السياسية
101	خامساً: الخصائص الاقتصادية
105	سادساً: الخصائص الأمنية
	الأمن العربي في عصر المعلومات

الجزء الثاني: حرب المعلومات : التطور والنظرية

112	تمهيد
113	الفصل الرابع : تطور حرب المعلومات
114	مقدمة
115	تطور حرب المعلومات
126	المبادئ الجديدة للحرب في عصر المعلومات
128	مبادئ العدوان
130	مبادئ التفاعل
131	مبادئ السيطرة
132	مجالات حرب المعلومات:
132	أ- العبث (اللعب)
136	ب- الجريمة
140	ج- حقوق الفرد
141	د- الأمن الوطني
149	حرب المعلومات الاستراتيجية
145	خصائص حرب المعلومات الاستراتيجية
151	الفصل الخامس : حرب المعلومات : النظرية
153	مقدمة

153	مفهوم حرب المعلومات
164	نظرية حرب المعلومات :
164	أولاً: مصادر المعلومات
166	قيمة مصادر المعلومات
170	ثانياً: أطراف الصراع
174	ثالثاً: عمليات الهجوم
178	الاعداد والتصميم في حرب المعلومات
178	نمذجة حرب المعلومات
181	خطوات تنفيذ حرب المعلومات
185	الفصل السادس : حرب الخليج وأسلحة التخريب الشامل
187	مقدمة
188	1- تدمير البناء التحتي المعلوماتي
188	أ- تدمير نظم المعلومات
189	ب- شبكات الطاقة
190	ج- القنابل الكهرومغناطيسية
190	2- الوصول غير المصرح به للمعلومات
192	3- التجسس العسكري المعلوماتي
194	4- التجسس الالكتروني
196	5- زرع الفيروسات
197	6- العمليات النفسية
197	أ- التلفزيون والمحطات الفضائية
201	ب- الاذاعة
202	ج- الدعاية
203	د- المنشورات الورقية
207	هـ- الخداع
208	و- الخطابات
208	7- الرقابة الإعلامية

- أ. الانتقاء الإعلامي 208
 ب- المراقبة الاعلامية بالتأخير 210
 ج- التنصت 210

الجزء الثالث: حرب المعلومات الهجومية

- تمهيد 213
 الفصل السابع : المصادر المفتوحة 215
 مقدمة 217
 المصادر المفتوحة : 217
 1- استخبارات المصادر المفتوحة 217
 2- المتصفحات 218
 3- بروتوكول النص الفائق 218
 4- تحميل البرامج المجانية 219
 5- محركات البحث 219
 6- البريد الالكتروني 219
 7- بريد القمامة 219
 8- التجارة الالكترونية 219
 9- التفتيش في القمامة 220
 10- الشمشمة 221
 11- تصفح الوب 222
 12- استغلال الملكية الفكرية 222
 13- خرق الملكية الفكرية على الانترنت 223
 14- خرق حقوق النشر 223
 15- قرصنة البرامج 224
 16- خرق حماية الاتصالات والبيانات 227
 17- خرق الخصوصية 229
 18- الكعكات 229

231	الفصل الثامن: العمليات النفسية وإدارة النفس والادراك
233	مقدمة
234	أنواع العمليات النفسية
235	مبادئ العمليات النفسية
236	إدارة النفس والادراك
238	وسائل الحرب النفسية المعلوماتية:
238	1- الكذب
238	2- التشويه
239	3- التحريف
239	4- الفسوق
240	5- الخداع
241	6- الهندسة الاجتماعية
244	7- الشجب
245	8- التحرش
246	9- الاعلان
246	10- الاحتيال المالي
247	11- بريد القمامة الالكتروني
247	12- الرقابة
248	13- التهديد الثقافي
249	14- التوهج
251	الفصل التاسع: الداخلون
253	مقدمة
253	1- الخونة والجواسيس
258	2- علاقات العمل
258	3- الزيارات والطلبات
259	4- الاحتيال والاختلاس
260	5- الصفقات المصطنعة

260	6- تعديل البيانات	285
260	7- التخريب الداخلي	285
261	8- الهجمات الفعلية	285
261	9- الهجمات البرمجية	285
261	10- انتحال صفة الآخرين	285
263	الفصل العاشر : مُصادرة الاشارات	
265	مقدمة	
265	اعتراض الاتصالات	
266	1- التلفون	285
267	2- خدمات الهاتف	285
267	3- الجوال والبيجر	285
269	4- تسجيل المكالمات	285
270	5- الفاكس	285
270	6- التلفون اللاسلكي	285
270	7- آلة الرد الصوتي	285
271	8- البريد الصوتي	285
271	9- اعتراض الاستخبارات الاجنبية	285
273	10- حل رموز الرسائل	285
274	11- الارسال بالستالايت	285
276	12- الفيديو	285
276	13- التنصت على المحادثات الهاتفية	285
277	الاحتيال في الاتصالات الهاتفية	
278	1- الاحتيال في البريد الصوتي	285
278	2- الاحتيال في بطاقات الاتصال	285
279	3- الاحتيال بالجوال والهواتف المقلدة	285
279	مراقبة شبكات الحاسب	
280	1- شمامو الخزم المعلوماتية	285

280	2- مراقبة ادخال المفاتيح
280	3 - تحليل المرور الالكتروني
281	4- كلمات الدخول
282	5- المودم
283	6- الحرمان من الخدمة
284	المراقبة البيئية
284	1- الكاميرات والفيديو
284	2- الستالايت
285	3- لاقطات فان إيك
285	4- المجسات الاخرى
286	5- المراقبة من الكتف
287	الفصل الحادي عشر: الاختراق
289	مقدمة
290	أدوات الحصول على الدخول غير المصرح به وأساليبها
290	1- ماسحات الشبكات
291	2- رزم الشم
291	3- مروجو كلمات المرور
291	4- الهندسة الاجتماعية
292	5- سرقة المعلومات
292	6- جمع التذكار
293	7- التأثير
293	8- تتبع الموقع على الشبكة
294	9- الغلق عن بعد
295	التخريب
295	1- التشويش
296	2- بنادق اتش أي آر آف
296	3- قنابل تحويل النبضات الكهرومغناطيسية

297	4- اسلحة ترددات الراديو	085
298	5- اسلحة الموجات القصيرة	085
299	الفصل الثاني عشر : التنكر والخفاء	
301	مقدمة	
301	سرقة البطاقة (الهوية)	
301	الرسائل والوثائق المزورة	
302	1- تزوير البريد الالكتروني	085
302	2- التزوير في البريد الدعائي	085
303	3- الفيضانات البريدية	085
303	4- تغير العنوان	085
304	5- التزييف	085
304	حصن طروادة	
305	1- برمجيات حصن طروادة	085
305	2- ركوب الوب	085
306	3- تتبع البريد الالكتروني	085
306	الفصل الثالث عشر : الوباء الالكتروني	
307	مقدمة	
309	الفيروسات	
309	1- فيروسات قطاع التشغيل	085
311	2- فيروسات الماكرو	085
312	3- الفيروسات الطفيلية	085
312	4- فيروسات البرامج	085
312	ديدان الانترنت	
313	حصن طروادة	
313	القنبلة المنطقية	
314		

الجزء الرابع : حرب المعلومات الدفاعية

317	تمهيد
321	الفصل الرابع عشر : سد الثغرات والانكشافات
323	مقدمة
323	مراقبة الانكشافات
324	انواع التهديدات
325	ايجاد الثغرات في الحاسب والشبكات
326	مراقبة المنشورات الأمنية
327	بناء النظم الآمنة
328	الوعي الأمني والتدريب
328	تجنب الانهيار الكلي
329	إدارة الخطورة
329	1- تحليل الخطورة
330	2- تحديد التهديدات
332	3- تقدير الخطورة
332	الدفاع عن المجتمع المعلوماتي
332	البناء الوطني المعلوماتي
334	حماية البنية التحتية الوطنية المعلوماتية
335	1- المبادئ العامة
337	2- الهيئة الرئاسية
342	سياسة التشفير
343	أ- صنع الترميز
343	ب- فك التشفير
344	ج- فحص التشفير وقوته
344	السياسة الدولية في التشفير
345	التهديدات الخارجية

347	مقدمة
349	1- الحماية الفيزيكية
349	وسائل الحماية الفيزيكية
350	أ- العوائق
350	1- المفاتيح والاقفال
350	2- الحماية من الكوارث الطبقية
351	3- الحماية من التهديدات البيئية
351	ب- ضبط الدخول
351	ج- المراقبة
352	1- التفتيش المنتظم
352	2- التفتيش العشوائي
352	3- اختبارات الدخول غير المصرح بها
353	انموذج للحماية الفيزيكية للمعلومات
353	2- التشفير (التعمية)
354	نظام التشفير الرقمي
356	فك الشفرة
357	توليد وتوزيع المفاتيح
357	تشفير المفتاح العام أ ر اس ايه
359	1- التشفير بالمفتاح العام
359	2- طريقة أ ر اس ايه
360	3- توزيع المفاتيح العامة
361	4- التشفير بالمفتاح السري
362	نظام المفتاح الخاص
363	رقيقة كليبر
365	قصور التشفير
365	المخابئ

366	المجهولية
367	الترشيح
368	6- التخلص من النفايات المعلوماتية
368	7- درع المعلومات
371	الفصل السادس عشر: نقاء المعلومات
373	مقدمة
373	1- التحقق من الأمن الفيزيقي
374	2- وسائل الكشف والاثبات البيولوجية الاحصائية
375	3- قياسي التكاملية
375	4- التوقيع الرقمي
375	5- كلمات المرور والمتعلقات السرية الأخرى
376	6- إدارة المفاتيح العامة والشهادات
376	7- العلامات المائية
377	8- الاتصال الراجع والاتصال بالمنزل
377	9- التحقق بناءً على الموقع
378	10- الشارات والبطاقات
379	الفصل السابع عشر: حراسة المعلومات ورقابتها
381	مقدمة
381	1- التحكم بالدخول للأصول المعلوماتية
381	أ- سياسات السماح بالدخول
384	ب- رقباء التحكم في الدخول
387	2- ترشيح المعلومات
387	أ- جدران الحماية
388	ب- مرشحات البريد غير المرغوب
389	ج- مرشحات الشبكة
390	3- اكتشاف التطفل وسوء الاستخدام

391	أ- الرقابة في مكان العمل	المراجع
392	ب- الكشف التلقائي	
392	ج- خرق الحاسب وكشف سوء الاستخدام	
395	أ- العربية	
395	ب- الانجليزية	
402	الملاحق	
463		

351	ب- ضبط الدخول	372
352	ج- المراقبة	372
352	1- التفتيش المنظم	372
352	2- التفتيش العشوائي	370
353	3- اختبارات الدخول غير المصرح بها	370
353	الحماية الفيزيائية للمعلومات	372
354	2- التشفير (التعمية)	372
356	مفاتيح التشفير الرقمية	372
	لبنان	372
357	وتوزيع المفاتيح	184
359	تفسير المفتاح العام أو سر آيه	184
359	1- التشفير بالمفتاح العام	184
360	2- طريقة آر إس آيه	184
361	3- توزيع المفاتيح العامة	384
362	4- التشفير بالمفتاح السري	384
363	نظام المفاتيح الخاصة	884
363	خاتمة كبرى	984
365	مفاتيح التشفير	994
365	المفاتيح	