هيئة التشريع والرأي القانوني
Legislation & Legal Opinion Commission

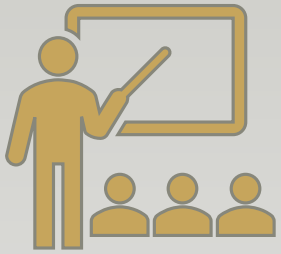
الاستجابة الجنائية للجرائم ذات الصلة بوسائل تقنية المعلومات وتأثيرها على الأمن السيبراني

الدكتورة نورة محمد الشملان
أستاذ القانون الجنائي المساعد
مدير تحرير مجلة الحقوق- جامعة البحرين

الأهمية؟

1. لهذه الجرائم أثر كبير وخطير على الأمن الوطني والنظام الاقتصادي والمالي، حيث اضرار هذا النوع من الجرائم تخرج عن إطار احداث الضرر للفرد ذاته فهي تمس المصلحة العامة وتكون عابرة للحدود.
2. سوق العمل يتطلب أن يكون هنالك باحثين في مجال الجرائم السبرانية التي لا يرتكبها المجرمين التقليدين وترتكب بالطرق الحديثة.
3. ينمي هذا الموضوع قدرة القانوني للتفكير خارج الصندوق من خلال التطرق الى نوع من الجرائم لم يعتادوا عليه.

بنهاية هذه المحاضرة سيتمكن المشاركين من:



- تحديد الاطار القانوني للجرائم المتعلقة بالأمن السيبراني بمملكة البحرين
- مناقشة المواجهة الجنائية للجرائم السيبرانية
- الربط بين أهم المعلومات الأساسية ذات العلاقة بالأمن السيبراني
- تقدير المسائل القانونية المستحدثة التي تتعلق بالأمن السيبراني

التقسيم

- أهم المفردات والمسائل المتعلقة بالأمن السيبراني
- طبيعة الجريمة السيبرانية
- الاطار التشريعي للمسائل السيبرانية بمملكة البحرين
- أهم المسائل المتعلقة بالامن السيبراني من ناحية قانونية
- الاستنتاجات والتوصيات

أهم المفردات والمسائل المتعلقة بالأمن السيبراني

Colonial Pipeline

جريمة معلوماتية　　جريمة سيبرانية　　بصمة برومـاتية

برمجيات خبيثة　　برامج الفدية　　هجوم انتحال الشخصية

قراصنة القبعة السوداء　　قراصنة القبعة الرمادية　　قراصنة القبعة البيضاء

هجمات الوسيط MitM　　التصيدPhishing

أمن معلومات/أمن سيبراني

الامن السيبراني

وسائل تمنع الاستخدام الغير مصرح به و سوء الاستغلال السيبراني بشكل يشمل جميع أشكال الأمن الرقمي (البيانات الرقمية أوالأنظمة الرقمية)

الولوج السرقة الضياع التجسس

السرية = امان النظام


حماية النظام والبيانات من التعديل أو المسح او الدخول
وقائية
علاجية

طبيعة الجريمة السيبرانية

تعريف الجريمة السيبرانية:

- تعتمد بالفعل على تكنولوجيا التواصل المعلوماتي بشكل أساسي الإنترنت، لارتكاب أفعال إجرامية ذات نطاق دولي.
- يشمل مجموعة أفعال مرتكبة ضد بيانات أو نظم حاسوبية أو باستخدامها.

"فعل ينتهك القانون يرتكب باستخدام تكنولوجيا المعلومات والاتصالات لاستهداف الشبكات والأنظمة والبيانات والمواقع الالكترونية، أو التكنولوجيا أو تسهيل ارتكاب الجريمة"

- تم النص على تعريف الجريمة الإلكترونية في القانون القطري والنظام السعودي الخاصيين بمكافحة جرائم المعلوماتية.

(أي فعل يتضمن استخدام وسائل تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بشكل غير مشروعة، وفقا لما ورد في القانون)

- تشريعات كل من مملكة البحرين وسلطنة عمان ودولة الإمارات العربية المتحدة خالياً من النص على تعريف مصطلح الجريمة الالكترونية أو المعلوماتية لكن تم تسمية الافعال التي تم أعتبرها مجرمة وتم وضع العقوبات التي يراها المشرع مناسبة لها.

*الحاجة لتشريعات تعالج الجرائم السيبرانية **ILOVEYOU virus**

مسائل مهمة:

- عدم التوسع في تطبيق وتفسير القواعد الجزائية، كونها تنص على عقوبات وتدابير إكراهية تنال من (الحرية/المال/ التمتع بالحقوق)

X القياس أو التحليل = الخروج عن لا عقوبة ولا جريمة بدون نص

↓

عدم جواز تشويه الإرادة الفعلية للمشرع

- أهمية الصياغة: ثمة أنظمة قانونية قد تستخدم في صياغتها لوصف الفعل الجرمي عبارات أو ألفاظ قد تفتح المجال للتوسع في التفسير، مثاله: عبارة (آلي) في نص عقابي باللغة العربية فيشمل ذلك الأدوات المعلوماتية لأنها من الأدوات الآلية.
- تقدير التجريم والعقاب: يخضع لاعتبارات ثقافية واجتماعية واقتصاديات وضرورات
- العولمة أوجبت على المشرع اعتماد تعاريف ووصف متلائم مع القوانين العالمية.

السمات العامة (الخصائص)

أداة ارتكابها /الكيفية/ مرتكبيها /اثباتها/ معاينتها

- المستهدف بالجريمة السيبرانية في كثير من الحالات يكون غير ملموس
- طابع مائع لا تقليدي هرمي تتسم بالطابع الخدماتي
- عابرة للحدود
- تنطوي على مصالح القطاعيين العام والخاص
- اغلبها من جرائم ذوي الياقات البيضاء.

الاطار التشريعي للمسائل السيبرانية بمملكة البحرين

القوانين العامة

قانون العقوبات الصادر بالمرسوم بقانون رقم (١٥) لسنة ١٩٧٦ وتعديلاته

قانون الإجراءات الجنائية الصادر بالمرسوم بقانون رقم (٤٦) لسنة ٢٠٠٢ وتعديلاته

القوانين الخاصة

قانون رقم (٦٤) لسنة ٢٠٠٦ بإصدار قانون مصرف البحرين المركزي والمؤسسات المالية

قانون رقم (٣٥) لسنة ٢٠١٢ بشأن حماية المستهلك

قانون رقم (٦٠) لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات

قانون رقم (٢) لسنة ٢٠١٧ بالتصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

مرسوم بقانون رقم (٥٤) لسنة ٢٠١٨ بإصدار قانون الخطابات والمعاملات الإلكترونية

قانون حماية البيانات الشخصية، الصادر بالقانون رقم (٣٠) لسنة ٢٠١٨

تنقسم جريمة الفضاء السيبراني:

- النوع الأول هو الذي يكون فيه الحاسوب أداة تنفذ بواسطتها الجريمة كجرائم الاحتيال والأفعال الإباحية= جرائم عادية والحاسوب مجرد وسيلة.
- النوع الثاني هو الذي يكون فيه جهاز الحاسوب وشبكات الحواسيب وبرامجها موضوعاً للجريمة= كاختراق نظام أمان أو إرسال برنامج خبيث.

- جرائم التعدي على البيانات المعلوماتية
- جرائم التعدي على الأنظمة المعلوماتية
- إساءة استعمال الأجهزة أو البرامج
- الجرائم على الأموال
- جرائم الاستغلال الجنسي للقاصرين

الجرائم ذات الصلة بوسائل تقنية المعلومات

مادة (٧)

يعاقب بالسجن مدة لا تزيد على عشر سنين من قام بإدخال أو تعييب أو تعطيل أو إلغاء أو حذف أو تدمير أو تغيير أو تعديل أو تحريف أو حجب بيانات وسيلة تقنية المعلومات تخص إحدى المصالح الحكومية أو الجهات التي ورد ذكرها في المادة (١٠٧) من قانون العقوبات، على نحو من شأنه إظهار بيانات غير صحيحة على أنها صحيحة، بنية استعمالها كبيانات صحيحة، سواء كانت هذه البيانات مفهومة بشكل مباشر أو غير مباشر.

وتكون العقوبة الحبس إذا ارتكبت الجريمة بشأن بيانات وسيلة تقنية المعلومات لا تخص إحدى المصالح أو الجهات المشار إليها في الفقرة السابقة إذا كان من شأن ذلك إحداث ضرر.

مادة (٨)

يعاقب بالحبس من توصل دون مسوغ قانوني إلى الاستيلاء على مال مملوك للغير أو حصل على أية مزية لنفسه أو لغيره أو إلى توقيع سند أو إلغائه أو إتلافه أو تعديله باتخاذ اسم كاذب أو صفة غير صحيحة أو بالاستعانة بطريقة احتيالية، وذلك من خلال أي فعل مما يلي:

أ) إدخال أو تعييب أو تعطيل أو إلغاء أو حذف أو تدمير أو تغيير أو تعديل أو تحريف أو حجب بيانات وسيلة تقنية المعلومات.

ب) القيام بأي تدخل في عمل نظام تقنية المعلومات.

ويسري بشأن هذه الجريمة الظرف المشدد المنصوص عليه في كل من المادتين (٣٩١) فقرة ثانية و(٣٩٢) فقرة ثانية من قانون العقوبات.

مادة (٩)

يعاقب بالحبس وبالغرامة التي لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من قام باستخدام التشفير في سبيل ارتكاب أو إخفاء أي من الجرائم المنصوص عليها في هذا القانون أو أي قانون آخر.

❖الركن المعنوي: جريمة عمدية يتخذ ركنها صورة القصد الجنائي القائم على العلم والإرادة.

مادة (٧)

يعاقب **بالسجن مدة لا تزيد على عشر سنين** من قام بإدخال أو تعييب أو تعطيل أو إلغاء أو حذف أو تدمير أو تغيير أو تعديل أو تحريف أو حجب **بيانات وسيلة تقنية المعلومات تخص إحدى المصالح الحكومية** أو الجهات التي ورد ذكرها في المادة (١٠٧) من قانون العقوبات، على نحو من شأنه إظهار بيانات غير صحيحة على أنها صحيحة، **بنية استعمالها كبيانات صحيحة**، سواء كانت هذه البيانات مفهومة بشكل مباشر أو غير مباشر.

وتكون العقوبة **الحبس** إذا ارتكبت الجريمة بشأن بيانات وسيلة تقنية المعلومات **لا تخص إحدى المصالح أو الجهات** المشار إليها في الفقرة السابقة إذا كان من شأن ذلك إحداث ضرر.

مادة (٨)

يعاقب بالحبس من توصل دون مسوغ قانوني إلى الاستيلاء على مال مملوك للغير أو حصل على أية مزية لنفسه أو لغيره أو إلى توقيع سند أو إلغائه أو إتلافه أو تعديله باتخاذ اسم كاذب أو صفة غير صحيحة أو بالاستعانة بطريقة احتيالية، وذلك من خلال أي فعل مما يلي:

أ) إدخال أو تعييب أو تعطيل أو إلغاء أو حذف أو تدمير أو تغيير أو تعديل أو تحريف أو حجب بيانات وسيلة تقنية المعلومات.

ب) القيام بأي تدخل في عمل نظام تقنية المعلومات.

ويسري بشأن هذه الجريمة الظرف المشدد المنصوص عليه في كل من المادتين (٣٩١) فقرة ثانية و(٣٩٢) فقرة ثانية من قانون العقوبات.

مادة (٩)

يعاقب بالحبس وبالغرامة التي لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من قام باستخدام التشفير في سبيل ارتكاب أو إخفاء أي من الجرائم المنصوص عليها في هذا القانون أو أي قانون آخر.

❖ الركن المادي: يتكون أولا من عنصر الفعل الجرمي، والذي هو ارتكاب سلوك يحظره المشرع من قبيل الجرائم

- (القواعد العامة) تختلف الدول معظمها ظاهريا في بيان وسائله، فمنها اكتفت بذكر استعمال طرق احتيالية ومنها أيضا أدرجت ضمن الأفعال الاحتيالية الاستفادة من غلط وقع فيه المجني عليه كالقانون البولوني

أما العنصر الثاني ألا وهي النتيجة الجرمية متمثلة في تسليم المال باختيار وطواعية للجاني فتكون إرادة المجني عليه معيبة عند التسليم؛ والعنصر الثالث هي العلاقة السببية وهي الرابطة بين الفعل الاجرامي والنتيجة السابق ذكرهما، فتتمثل فيما يصدر من الجاني من كذبٍ مدعمٍ بإحدى وسائل الاحتيال والتي تقود المجني عليه للتسليم لوقوعه في الغلط

(سبرانيا) يختلف من حيث تسخير تقنية المعلومات لإحداث الأفعال من إدخال أو تحريف وغيرها ببيانات وسيلة تقنية المعلومات أو أن يتمثل الفعل بالتدخل في نظام تقنية المعلومات وكانت الوسيلة تم استخدامها بالطرق الآتية: اتخاذ اسم كاذب/ صفة غير صحيحة/ الاستعانة بطريقة احتيالية

تقوم الجريمة إذا كان الفعل الجرمي في الركن المادي أتخذ صورة الحصول بشكل غير قانوني على: الاستيلاء على مال مملوك للغير/الحصول على أية مزية لنفسه أو لغيره/ توقيع سند أو إلغائه أو إتلافه أو تعديله

هل مجرد استخدام الشبكة العنكبوتية يجعل الجريمة احتيالا سبرانيا/ إلكترونيا/ برقيا؟

UNITED STATES v. SELBY

"تم إدانة جين سيلبي المسؤولة السابقة في إدارة الطاقة في بونفيل (BPA) عن عدد من التهم من بينها الاحتيال البرقي؛ ذلك إن جين سيلبي قامت بإعادة إرسال بريد إلكتروني داخلي حول مداولات الوكالة إلى زوجها سكوت الذي يعمل في Knowmadic والذي له مصلحة مالية في ذلك، مما لعب دورا كبيرا في المبلغ الذي حصلت عليه Knowmadic في التسوية بين BPA و Knowmadic والتي أسفرت على دفع مبلغ حوالي ١،٣٠٠،٠٠٠ دولار أمريكي ل Knowmadic حصل بموجبها زوجها سكوت سيلبي على عمولة قدرها ١٠،٤٩٣,٥٢ دولارًا أمريكيًا. بناءً عليه قررت هيئة المحلفين ادانتها عن الاحتيال البريدي بانتهائها إلى أنه لا يلزم أن يكون استخدام البرق عنصرًا أساسيًا في عملية الاحتيال حيث يكفي أن يستخدم البرق في مواصلة الاحتيال فإرسال البريد الإلكتروني كافٍ لتحديد عنصر استخدام البرق للاحتيال، وبالتالي كافٍ لتحقق القصد الجنائي اللازم للإدانة وكالة اتحادية تنتج وتنقل الطاقة في جميع أنحاء شمال غرب المحيط الهادئ."

- أوجد المشرع الحماية الخاصة بأن وضع نصا عاماً لجميع الجرائم التي ترتكب بموجب قانون تقنية المعلومات أو أي قانون آخر بأن جرم من قام باستخدام التشفير لإخفاء الجرائم.
- جريمة الاحتيال عن طريق وسيلة أو نظام تقنية المعلومات مصحوبة بارتكاب جرائم أخرى؛ مثاله ارتكاب الجرائم المتعلقة بالتوقيع الالكتروني و المنصوص عليها في المادة ٢٦ من قانون الخطابات والمعاملات الإلكترونية.
- تم تجريم الشروع على ارتكاب هذه الجرائم وقيام المسؤولية للشخص الاعتباري عن جرائم تقنية المعلومات.

العلة التشريعية؟

الجرائم ذات الصلة بوسائل تقنية المعلومات

مادة (٧)

يعاقب بالسجن مدة لا تزيد على عشر سنين من قام بإدخال أو تعييب أو تعطيل أو إلغاء أو حذف أو تدمير أو تغيير أو تعديل أو تحريف أو حجب بيانات وسيلة تقنية المعلومات تخص إحدى المصالح الحكومية أو الجهات التي ورد ذكرها في المادة (١٠٧) من قانون العقوبات، على نحو من شأنه إظهار بيانات غير صحيحة على أنها صحيحة، بنية استعمالها كبيانات صحيحة، سواء كانت هذه البيانات مفهومة بشكل مباشر أو غير مباشر.

وتكون العقوبة الحبس إذا ارتكبت الجريمة بشأن بيانات وسيلة تقنية المعلومات لا تخص إحدى المصالح أو الجهات المشار إليها في الفقرة السابقة إذا كان من شأن ذلك إحداث ضرر.

مادة (٨)

يعاقب بالحبس من توصل دون مسوغ قانوني إلى الاستيلاء على مال مملوك للغير أو حصل على أية مزية لنفسه أو لغيره أو إلى توقيع سند أو إلغائه أو إتلافه أو تعديله باتخاذ اسم كاذب أو صفة غير صحيحة أو بالاستعانة بطريقة احتيالية، وذلك من خلال أي فعل مما يلي:

أ) إدخال أو تعييب أو تعطيل أو إلغاء أو حذف أو تدمير أو تغيير أو تعديل أو تحريف أو حجب بيانات وسيلة تقنية المعلومات.

ب) القيام بأي تدخل في عمل نظام تقنية المعلومات.

ويسري بشأن هذه الجريمة الظرف المشدد المنصوص عليه في كل من المادتين (٣٩١) فقرة ثانية و(٣٩٢) فقرة ثانية من قانون العقوبات.

مادة (٩)

يعاقب بالحبس وبالغرامة التي لا تجاوز مائة ألف دينار أو بإحدى هاتين العقوبتين كل من قام باستخدام التشفير في سبيل ارتكاب أو إخفاء أي من الجرائم المنصوص عليها في هذا القانون أو أي قانون آخر.

أهم المسائل المتعلقة بالأمن السيبراني من ناحية قانونية

أغراض العقوبة

- الردع
  - العام
  - الخاص
- الاعجاز/التعطيل
- إعادة التأهيل
- القصاص والعدالة
- التعويض/الرد

هل جميعها نحتاجها في كل أنواع الجزاءات؟

كيفية تصميم العقوبة في الأنظمة العقابية الحديثة؟

الشروط الواجب توافرها في العقوبة:

- القانونية
- المساواة
- الشخصية

❖العوامل المؤثرة في اختيار الجزاء

السياسة التشريعية الاجرائية

- الاجراءات الخاصة بأوامر التحفظ والمنع

بالولايات المتحدة تستطيع الشرطة وكذلك الادعاء العام وضع منع على الحسابات في حالة هناك عمليات مشبوهة، مثاله خرق للمعلومات أو انتحال شخصية.

هل السلطات مبينه بشكل دقيق؟

- الاشتراطات الخاصة بمعالجة البيانات الشخصية الحساسة

إمكانية استخدامها؟ حدوث خروقات؟

هل هذا يعرض المؤسسة للمسؤولية؟

كفاية التشريعات؟

تفتيش وضبط البيانات المتعلقة بهجوم سان برناردينو ٢٠١٥ –The 2016 Apple Case

- موازنة الحقوق
- حرية التعبير
- طبيعة الطلب

مادة (١٥)

١) للنيابة العامة أن تصدر أمراً مسبباً بالدخول إلى ما يلي وتفتيشه:

أ) نظام تقنية المعلومات المتصل بالجريمة أو أي جزء منه وأية بيانات لوسيلة تقنية المعلومات مخزنة فيه.

ب) أي من وسائط تخزين بيانات وسيلة تقنية المعلومات التي من المحتمل أن يكون مخزناً عليها بيانات متصلة بالجريمة.

٢) إذا قامت لدى النيابة العامة أثناء تنفيذ الأمر المشار إليه في البند (أ) من الفقرة (١) من هذه المادة أمارات قوية بأن البيانات المتصلة بالجريمة مخزنة في نظام تقنية المعلومات آخر أو في جزء منه، وكانت هذه البيانات قابلة لأن يتم الدخول إليها من خلال نظام تقنية المعلومات الأول أو متاحة من خلاله على نحو مشروع، فإن للنيابة العامة أن تصدر أمراً مسبباً بمد الدخول والتفتيش إلى النظام الآخر

السياسة الجنائية هي الأساليب التي يتبناها المشرع لمكافحة الجريمة بشكل عام، يجب أن تقوم على وضع نهج لمكافحة السلوك الشاذ لتوفير الأمن السيبراني والحفاظ عليه سواء من خلال تبني مبادرات وخطط تؤدي لسن تشريعات توائم أهداف الدولة وواقعها الاقتصادي والسياسي بشكل خاص وكونها جزء من العالم بشكل عام.

X

- وجود معلومات رسمية كافية ودقيقة حول واقع الأمن السيبراني والتهديدات المتوقعة.
- يسمح لصحاب الاختصاص والمهنيين من تقديم اقتراحات وحلول عملية.
- أهمية تمكين شركات الامن السيبراني.
- جدية التعاون الاقليمي والدولي فيما يخص تبادل المعلومات والخبرات.

النتائج

- أهمية المعرفة والاطلاع بالمجال السيبراني.
- أنواع الجرائم السبرانية وطبيعتها ومايترتب على ذلك من اختلاف في المعاملة التشريعية.
- تكامل المنظومة التشريعية.
- نقص المعلومات حول واقع الأمن السيبراني والتهديدات المتوقعة.

التوصيات

- التخصص القضائي
- التفصيل في وضع التشريع
- السياسة الجنائية
- التشريع والفقه والقضاء المقارن
- الدراسات البينية/ تكامل العلوم
- الانفاق في مجال الأمن السيبراني

المصادر:

- Lubin, Asaf (2023) "Cyber Plungers: Colonial Pipeline and the Case for an Omnibus Cybersecurity Legislation," Georgia Law Review: Vol. 57: No. 4, Article 4.
- ماينو، جيلالي وعروس، كوثر-الجريمة السيبرانية في صورها المستحدثة- مجلة القانون والتنمية- كلية الحقوق والعلوم السياسية، جامعة طاهري محمد- بشار،المجلد٤، العدد١،جويلية ٢٠٢٢
- الشملان، نورة- الاحتيال كجريمة من جرائم ذوي الياقات البيضاء (الاحتيال البرقي أنموذجا) العدد٥٣- السنة الرابعة عشرة- أبريل ٢٠٢١
- AlShamlan, Noora"SEARCHING AND SEIZING DATA THAT RELATED TO A CRIME: A Case Study of the 2015 San Bernardino Attack" Volume 39, Issue2, December 2016, the Journal of Legal Studies, Assiut University, Egypt
- حلقة العمل ٣: تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة، مثل الجرائم الإلكترونية (السيبرانية) والاتجار بالممتلكات الثقافية، بما في ذلك الدروس المستفادة والتعاون الدولي -مؤتمر الأمم المتحدة الثالث عشرلمنع الجريمة والعدالة الجنائية الدوحة، ١٢-١٩ نيسان/أبريل ٢٠١٥
- Prosecuting Computer Crimes- Office of Legal Education for United States Attorneys (2010)

شكرا جزيلا...