سنة ثانية إعلام

مقياس قضايا دولية معاصرة

المحاضرة رقم 06: الجريمة السيبرانية

الأهداف التدريسية للمحاضرة:

في نهاية المحاضرة المندرجة تحت عنوان" الجريمة السيبرانية" يكون الطالب قادرا على:

- أن يعرّف مفهوم الجريمة السيبرانية وخصائصها.
- أن يذكر أنواع الجرائم السيبرانية وتصنيفاتها.
- أن يناقش دور وسائل الإعلام في التوعية بمخاطر الجرائم السيبرانية.
- أن يحلّل طريقة تناول وسائل الإعلام لقضايا الجريمة السيبرانية.
- أن يقارن بين الإعلام التقليدي والإعلام الرقمي في معالجة هذه الجرائم.

أولا– مفهوم الجريمة السيبرانية

يستخدم مصطلح الجريمة السيبرانية للإشارة إلى جرائم الانترنت التي تشمل أي فعل متعمد يتعلق بالاستخدام غير المشروع لتكنولوجيا المعلومات بهدف الاعتداء على الممتلكات المادية أو المعنوية أو انتهاك خصوصية الأفراد.

وتتضمن الجرائم السيبرانية أيضا الاعتداء على الأنظمة المعلوماتية مثل الدخول غير المشروع إلى نظام معلوماتي أو البقاء فيه بهدف الوصول إلى البيانات الحساسة، كما تشمل تعطيل العمل المعلوماتي بشكل متعمد، ويقصد بها أيضا تلك الجرائم التي يستخدم فيها النظام المعلوماتي كوسيلة لارتكاب جرائم تقليدية سواء أكانت ضد الممتلكات مثل التحويل غير المشروع للأموال الكترونيا، أو ضد الأفراد مثل التشهير أو السب أو القذف عبر الأنترنت.

وعليه يمكن القول أن الجريمة السيبرانية هي أي نشاط غير قانوني يستخدم الكمبيوتر، الشبكات، أو الأجهزة الرقمية كأداة أو هدف مثل الاختراق، الاحتيال، أو سرقة البيانات

ثانيا– خصائص الجريمة السيبرانية:

- جريمة عابرة للحدود الجغرافية
- جريمة سريعة التنفيذ
- تتم باستخدام الحاسب الآلي والأنترنت كأداة لارتكاب الجريمة،
- جرائم تستدعي إلمام مرتكبيها بالمعرفة التقنية والخبرة الفائقة في مجال الإعلام الآلي.
- جرائم لا تمتاز بالعنف، لا تستوجب استخدام مرتكبيها للقوة الجسدية أو العضلية للقيام بالجريمة
- يصعب إثباتها بسبب غياب الدليل المرئي

ثالثا– أنواع الجرائم السيبرانية

يمكن تقسيم الجريمة السيبرانية إلى فئتين:

– الجرائم السيبرانية التي تستهدف أجهزة الكمبيوتر: تمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر، منها: القرصنة، الفيروسات والبرامج الضارة، استغلال الثغرات الأمنية،

– الجرائم السيبرانية التي تستخدم فيها أجهزة الكمبيوتر كأدوات لارتكاب الجرائم الالكترونية: سرقة الهوية، التصيد الاحتيالي، المطاردة السيبرانية، سرقة الملكية الفكرية، الابتزاز والتجسس الإلكتروني، بيع الأصناف غير القانونية كالمخدرات، توزيع محتوى غير قانوني كالمحتويات الإباحية، الإرهاب الإلكتروني.

ربعا– أليات مكافحة الجرائم السيبرانية

فيما يلي أليات مواجهة الجرائم السيبرانية:

1 .الآليات التقنية: وتتمثل في

– جدران الحماية :(Firewalls) مراقبة حركة الشبكة ومنع الوصول غير المصرح به.

– استخدام برامج مكافحة الفيروسات(Antivirus) للكشف عن البرمجيات الخبيثة وإزالتها.

– تحديث أنظمة الأمان.

– التشفي لحماية البيانات من السرقة أو التلف

– التوثيق الثنائي: تعزيز أمان الحسابات الشخصية والمؤسساتية .

2– الأليات القانونية والتشريعية: وتشمل:

– سن تشريعات خاصة أو تحديث القوانين لتشمل جرائم الإنترنت، مثل قوانين مكافحة جرائم المعلوماتية.

– تدريب الشرطة القضائية: تأهيل فرق متخصصة في تحليل الأدلة الرقمية.

إجراءات التحقيق الرقمي: التفتيش، الحجز الرقمي، ومراقبة الاتصالات لجمع الأدلة

3 .الآليات الدولية والتعاونية:

– الانضمام للاتفاقيات الدولية مثل "اتفاقية بودابست" لمكافحة الجرائم السيبرانية.

– التعاون القضائي والأمني لأجل تبادل المعلومات والخبرات بين الدول، وملاحقة المجرمين عبر "الإنتربول ."

4 .الآليات التوعوية: وتتمثل في:

– تنظيم حملات لتثقيف الأفراد حول طرق الاحتيال والابتزاز الإلكتروني.

– تكوين الموظفين في أساسيات الأمن السيبراني.