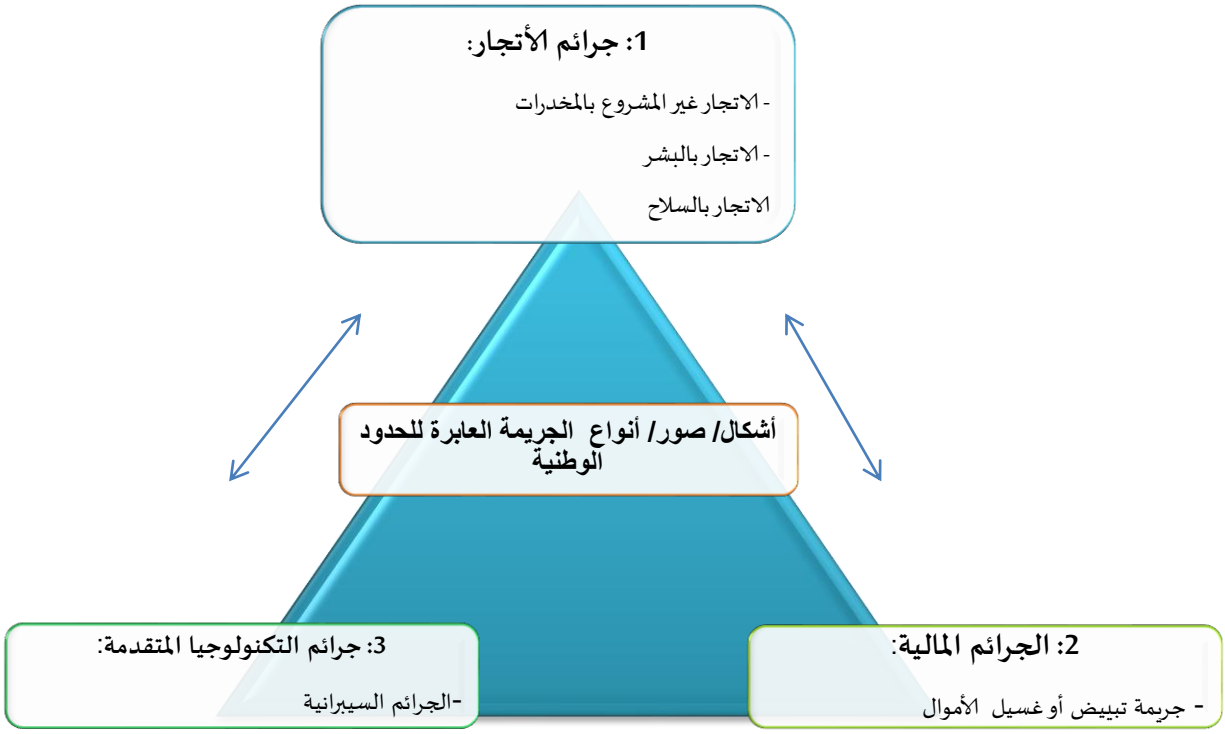
أشكال الجريمة العابرة للحدود الوطنية

تعد الجريمة المنظمة العابرة للحدود الوطنية من أكثر الظواهر الخطيرة التي تهدد الأمن الدولي في العصر الحالي، حيث تعمل الجماعات الإجرامية المنظمة على تنفيذ أنشطتها بشكل مخطط ومنظم وبطرق تفتقر إلى الأخلاق والقيم الإنسانية. وتستند تلك الجرائم على شبكات وعلاقات دولية تسهل عملها وتجعلها أكثر صعوبة في التصدي لها، وما زاد من خطورتها هو أن الجريمة المنظمة العابرة للحدود الوطنية تتضمن أنواع وصور متنوع من الجرائم وهذا ما حال دون قدرة الدول والمجتمع الدولي على مكافحتها، وفي ما يلي توضيح لأهم أشكال/ صور / أنواع الجريمة المنظمة العابرة للحدود الوطنية.



مخطط توضيحي لأشكال الجريمة المنظمة العابرة للحدود الوطنية

المحاضرة الرابعة

الجريمة الالكترونية "السيبرانية"

تمهيد:

ستهم التطور التكنولوجي والمعلوماتي في بروز نمط جديد من الجريمة المنظمة العابرة للحدود الوطنية وهي الجريمة الالكترونية أو السيبرانية الوجه المتطور من الجرائم التي تتميز بسرعة انتشارها وخطورتها على الأمن والاستقرار، فسابقا كانت الدول تسعى دائما لتوفير الأمن ضمن فضاءاتها التقليدية البر؛ البحر؛ الجو، لكن مع التطور الحاصل ضمن ما يعرف بالثورة المعلوماتية والتكنولوجية برز فضاء جديد وهو الفضاء السيبراني الذي يشكل تحدي أمني للدول إن لم تتمكن من مواجهة التهديدات المرتبطة به.

1: التعريف الجريمة السيبرانية:

في إطار تحديد المقصود بالجريمة السيبرانية أو الإلكترونية، اتضح أنه لا يوجد إطار نظري عام منسق في تقديم تعريف موحد وشامل لهذا النوع من الجرائم، وذلك لاختلاف تسميتها عبر مراحل تاريخية مختلفة، حيث تم استخدام مصطلح الجريمة الحاسوبية، ثم جريمة إساءة استخدام الحاسوب، ثم الجريمة المعلوماتية والجريمة التقنية ومن ثم الجريمة الالكترونية أو السيبرانية وهو الأكثر تداولا في الوقت الحالي، وفي ما يلي أهم التعريفات:

- تعريف منظمة التعاون الاقتصادي والتنمية 1983:" **كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية لبيانات ونقلها**"
- تعريف المؤتمر 10 للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين:" **أي جريمة يمكن ارتكابها بواسطة نظام حاسبي أو شبكة حاسبة وتشمل كل الجرائم التي تكون في البيئة الإلكترونية**".
- **الجريمة السيبرانية** هي أي نشاط إجرامي يتم باستخدام شبكة الإنترنت أو تقنيات الحوسبة الحديثة لارتكاب فعل غير قانوني. تشمل هذه الجرائم مجموعة متنوعة من الأفعال التي تستهدف الأفراد، الشركات، أو الحكومات، مثل السرقة، الاحتيال، التخريب، أو التهديد عبر الفضاء الإلكتروني.

تشير الجريمة السيبرانية أو الجريمة الإلكترونية إلى الأنشطة الإجرامية التي تتم عبر الإنترنت أو باستخدام أجهزة الكمبيوتر والشبكات الرقمية. تتنوع هذه الجرائم بشكل كبير، ولكنها تشترك في أنها تُنفذ باستخدام التكنولوجيا الحديثة.

2: أشكال الجريمة السيبرانية

3: خصائص الجريمة السيبرانية:

- **جريمة عالمية**: جريمة لا تعرف الحدود لأن الفضاء الذي تمارس فيه الجريمة نشاطها هو فضاء بلا حدود مادية.
- **جريمة سهلة الانتشار**: انتقال الناس من العالم الواقعي إلى العالم الافتراضي " خلف بيئة جديدة لتكوين عدد أكبر من الضحايا".
- **جريمة يصعب اثباتها**: غياب الأثر المادي التقليدي بالإضافة إلى سهولة مسح الدليل.
- **جريمة ناعمة**: لا تتطلب استخدام العنف المادي.
- **جريمة فنية تقنية**: تتطلب الدقة والمهارة والمعرفة التكنولوجية.
- **نوعية المجرم المنفذ**: مجرم الكتروني يتوفر على مهارة عالية في مجال المعلوماتية والقدرة على الاختراق بسرعة وسرية.
- **جريمة ذات تكلفة عالية، جريمة تمتاز بغياب التشريعات والأطر القانونية المنظمة**

4: أركان الجريمة السيبرانية

الركن المادي	الركن المعنوي	الركن الشرعي
يتطلب وجود بيئة رقمية والتي يقصد بها مجموعة المواد والنصوص والصور والفيديوهات والمخزنة بطريقة رقمية. كما يتطلب السلوك المادي معرفة بداية النشاط والشروع فيه فمجرد الدخول غير القانوني يعتبر جريمة يعاقب عليها القانون.	على الرغم من عدم ارتكاب هذه الجريمة في العالم المادي بل الافتراضي ، إلا أنه من الضروري توفر الركن المعنوي، بحيث يجب أن يكون الجاني على علم بأن الفعل غير قانوني مع وجود قصد للقيام بهذا الفعل وهنا تصبح جريمة عمدية. وقد تكون جريمة سيبرانية غير عمدية إذا كان الجاني قصده فقط ارتكاب السلوك دون ارادة تحقيق النتيجة، مثال: موظف استخدم قرص مرن لنقل المعلومات إلى حساب المؤسسة دون علمه بأنه يحتوي على فيروسات التي أدت إلى تدمير كلي أو جزئي للمعلومات الخاصة بالمؤسسة.	يشمل كل الأطر القانونية التي تسعى لمكافحة هذا النوع من الجرائم والتي أغلبها عبارة عن اتفاقيات، لأن التشريعات الوطنية لا تزال ضعيفة على مستوى هذا النوع من الجرائم.

5: أسباب الانتشار؛ المخاطر، المكافحة

أسباب الانتشار	المخاطر	المكافحةأو الاعتداء
- التطور التكنولوجي السريع - ظهور التقنيات الحديثة مثل **الذكاء الاصطناعي**. - سهولة الوصول إلى الأدوات السيبرانية. - الانتشار الواسع للأجهزة الرقمية - النمو الأنشطة الاقتصادية الإلكترونية. - الضعف الأمن المعلوماتي.	- انتهاك سيادة الدول وتجاوز حدودها الاقليمية . - اهتزاز ثقة الأفراد والمؤسسات في الدور الايجابي لتكنولوجيا. - تهديد الأمن الشخصي للأفراد من خلال انتهاك خصوصيتهم والتعدي على اسرارهم. - تهديد أمن واستقرار الدول وتهديد البنى الاقتصادية.	-**اتفاقية بودباست 2001**:" اتفاقية الجريمة عبر العالم السيبراني"، حددت الاتفاقية الأطر القانونية العامة للجرائم المعلوماتية والتي أدت على أن الدخول غير المشروع والاعتداء على سلامة البيانات يعتبر جريمة معاقب عليهاّ، كما نصت على ضرورة التزام الدول عند سن التشريعات الوطنية حول هذه الجريمة مراعاة الاتفاقيات الدولية لحقوق الانسان. -**شرطة الويب الدولية 1986**: تهدف لملاحقة الجناة والقراصنة. - نشاء مراكز لمكافحة الجرائم السيبرانية مثل **مراكز الاستجابة للحوادث الأمنية** لتنسيق الجهود بين الحكومات والشركات في التصدي للهجمات. -وضع خطط استجابة سريعة للحوادث السيبرانية، تتضمن إجراءات فورية للكشف عن الهجوم، تقييم الأضرار، ومن ثم التصدي للهجوم