



المحاضرة الرابعة

الأسباب الرئيسية لإرتكاب الجرائم السيرانية وخصائصها

تمهيد وتقسيم :

ومما لا شك فيه أن الجرائم السيرانية تختلف عن الجرائم التقليدية من ناحية الأفعال الإجرامية، ومن ثم ليس من المستغرب أن تختلف تلك الجرائم عن مثيلاتها من الجرائم التقليدية في بعض الخصائص التي تميزها عن غيرها، بخلاف الخصائص التي تطابق صفات الجرائم الأخرى.

فتتميز الجريمة السيرانية بصفة عامة عن الجريمة التقليدية في عدة نواح، سواء كان هذا التميز في السمات العامة لها، أو كان في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته. ونلاحظ أن أنماط مرتكبي أفعال الجرائم السيرانية، تختلف قليلا عن مرتكبي الأفعال الإجرامية التقليدية، ومن ثم فليس من المستغرب أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع إلى اقتراف الفعل غير المشروع.

وبالتأكيد فإن أمل الربح وروح الكسب هي من ضمن الأسباب التي تدفع إلى ارتكاب الجرائم السيرانية مع أسباب أخرى. ويمكن ملاحظة أن الإبداع اللانهائي لأفعال الجرائم السيرانية يستمر ويتطور بمعدل يفوق أسباب الحماية وجزاء المطبق.

ولذلك سوف نقسم المحاضرة بإذن الله تعالى إلى:

المحور الأول: الأسباب الرئيسية لارتكاب الجرائم السيرانية:

المحور الثاني: خصائص وسمات الجرائم السيرانية:

عناصر المحاضرة

المحور الأول: الأسباب الرئيسية لارتكاب الجريمة السيبرانية:

أولا : أسباب الجريمة السيبرانية على المستوى الفردي:

- ١ . الفرصة.
- ٢ . النشاط الروتيني.
- ٣ . الدوافع النفسية.
- ٤ . الدوافع العقائدية والسياسية والعنصرية.
- ٥ . الدوافع الشخصية.

ثانيا: أسباب الجريمة السيبرانية على المستوى المجتمعي:

- ١ . التحضر.
- ٢ . البطالة.
- ٣ . الضغوط العامة.
- ٤ . البحث عن الثراء السريع.
- ٥ . ضعف إنفاذ القانون وتطبيقه في الجريمة السيبرانية :

ثالثا: أسباب الجريمة السيبرانية على المستوى الكوني:

- ١ . التحول للمجتمع الرقمي.
- ٢ . العولمة.
- ٣ . إنكشاف البنية التحتية المعلوماتية الكونية.

رابعا: أسباب تتعلق بخصائص وسمات الجريمة السيبرانية:

وسوف نشرح هذه الاسباب بالتفصيل في المحور الثاني من المحاضرة من شرح خصائص وسمات الجرائم السيبرانية.

المحور الثاني : خصائص وسمات الجرائم السيبرانية:

١. سرعة التنفيذ.
٢. القيمة والديمومة.
٣. سرعة التطور في ارتكاب الجريمة السيبرانية.
٤. التنفيذ عن بعد.
٥. خفاء الجريمة.
٦. إحجام المجني عليهم عن الإبلاغ.
٧. جاذبية الجريمة السيبرانية والشغف بها.
٨. جرائم ناعمة.
٩. غياب المفهوم العام.
١٠. صعوبة إثباتها.
١١. التلوث الثقافي.
١٢. المؤثرات الخارجية.
١٣. التعاون والتواطؤ للإضرار بالغير.
١٤. أسباب خاصة بالمنشأة.
١٥. عالمية الجريمة السيبرانية.

المحور الأول

الأسباب الرئيسية لارتكاب الجريمة السيبرانية

هناك عدد من الأسباب لإرتكاب الجريمة السيبرانية، منها ما يقع على مستوى كوني، ومنها ما يقع على مستوى مجتمعي، ومنها ما يقع على مستوى فردي أو شخصي. كما ان أسباب الجريمة السيبرانية تتفاوت وفق نوعها ونوع المستهدف ونوع الجاني ومستوى تنفيذه (فردي، مجتمعي ، كوني). فجرائم الشباب والهواه والصغار تختلف عن أسباب جرائم المحترفين، وتختلف وفق هدفها سرقة أو معلومات أو تجارة بالمعلومات أو شخصية....الخ.

أولاً : أسباب الجريمة على المستوى الفردي:

١. الفرصة:

لقد وفرت التقنيات الحديثة والإنترنت فرصاً غير مسبقة لانتشار الجريمة السيبرانية، وأنَّ الفرصة تنتج الجريمة، وتلعب البيئة وترتيباتها دوراً كبيراً في إنتاج الجريمة، والخروج على قواعد الاجتماعية، فتوافر الانحراف عن قواعد الامتثال ليلاً ونهاراً وفي اي مكان، وعدم وجود رقابة في بيئة الإنترنت، كلها عوامل تزيد من فرصة ارتكاب الجريمة السيبرانية وقد تشكل المعلومات هدفاً سهل المنال، وتحقق المنفعة السريعة، وبالتالي يمكن سرقتها ، أو سرقة محتوياتها. فهي فرصة مربحة، وقليلة المخاطر، واحتمالية الكشف للفاعل فيها ضئيلة .

أن تكنولوجيا المعلومات والاتصالات والاستخدام المتزايد للأنترنت قد جعل هناك فرص جديدة للمجرمين وسهلت نمو الجريمة، أن جرائم الإنترنت تمثل شكلاً جديداً ومميزاً للجريمة، وقد خلقت تحديات لتوقع التطورات، والوقاية منها.

٢. النشاط الروتيني:

ويمكن تفسير زيادة ضحايا الجريمة السيبرانية من خلال التغيرات في أنشطة الناس الروتينية في الحياة اليومية، فمع ظهور شبكة الإنترنت فقد تغيرت طريقة الناس التي يتواصلون فيها أو يتفاعلون مع الآخرين في العلاقات الشخصية، والترفيه، والتجارة... الخ . وذلك من خلال استخدام النت وشبكات التفاعل الاجتماعي مثل الفيس بوك، والايمل والمواقع وغيرها قد خلقت فرصاً للجناة المتحفيين مع وجود أهداف قيمة وسهلة في الحيز الفضائي مع غياب الحراسة.

ويري بعض الفقهاء أنه من المرجح أن تحدث الجريمة عندما تتلاقى ثلاثة عوامل هي : وهذه العوامل هي: الجاني المتحفز، والهدف المناسب ، وغياب الحراسة. وأنه لا بد من توافر هذه العوامل الثلاثة من أجل أن تحدث الجريمة، وعدم وجود واحد من هذه العوامل هو "كافي لمنع حدوث ناجح لإكمال الاتصال المباشر، ويعطي اهتمام إلى التقارب في الزمان والمكان، وإن هذا التلاقي يمكن أن يؤدي إلى زيادة كبيرة في معدلات الجريمة. والمبدأ الأساسي هو أن التغييرات الهيكلية في النشاط الروتيني تؤثر على التقارب في العناصر الثلاثة من الناحية النظرية، وبالتالي تؤثر على معدل الجريمة .

٣. الدوافع النفسية:

هناك بعض الجرائم السيبرانية التي يرتكبها شباب طائش وصغار سن، وذلك من باب التحدي، وحب الظهور في الإعلام، وغالباً ما تتوقف هذه الفئة عن مثل هذه السلوكيات في عمر لاحق بعد سن العشرينيات. وتتمثل هذه الرغبة في إثبات الذات والتفوق على تعقيد وسائل التقنية، فالصورة الذهنية لمرتكبي الجرائم السيبرانية غالباً هي صورة البطل الذكي، الذي يستحق الإعجاب لا صورة المجرم السيبراني الذي يستوجب محاكمته، فمرتكبوا هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة فيحاولوا إيجاد الوسيلة إلى تحطيمها أو التفوق عليها.

ومن ناحية أخرى تنطلق دراسة ضبط الذات المنخفض من النظرية العامة في السلوك الطائش وتؤكد هذه النظرية أن احتمالية انخراط الأفراد في فعل إجرامي تحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض وقد عرف السلوك الطائش بأنه: كل فعل يقوم على القوة والخداع لتحقيق الرغبات الذاتية.

إن توفر صفة الضبط الذاتي المنخفض مع وجود الفرصة لارتكاب السلوك الطائش يعدان عاملين مؤثرين في ارتكاب السلوك الطائش، وأظهرت الدراسات أيضاً أن ضبط الذات المنخفض والاستعداد لتحمل المخاطر من أجل تحقيق مكاسب قصيرة الأجل، ينطبق على كثير من الأفعال التي يمكن إن تسهيل أو تعزز بواسطة وسائط الاتصالات الإلكترونية والإنترنت.

بالإضافة إلى ذلك، يتعرض الأفراد على الإنترنت لنماذج التعلم الإجرامي والأقران قد يكونون أكثر ميلاً للانخراط في الجريمة السيبرانية. ونظرية التعلم الاجتماعي - نظرية قد يكون لها تطبيق خاص عندما يتعلق الأمر بالجرائم السيبرانية- فالمجرمين وفقاً لهذه النظرية غالباً ما يحتاجون إلى تعلم تقنيات الكمبيوتر والإجراءات، فالنظرية التعلم الاجتماعي، ترى أن الأفراد يتصرفون في البيئة الافتراضية كما يتصرفون في العالم الحقيقي.

٤. الدوافع العقائدية والسياسية والعنصرية:

إن العقيدة من أقوى الدوافع والقوى المحركة للأشخاص، والتي يكون لدى الإنسان الاستعداد للتخلي الحياة بأسرها من أجل هذا الدافع ، فما هو الظن بما هو أيسر من ذلك، إذ أن كثيرا من الأشخاص يبررون محاولات اختراقاتهم لأجهزة الغير بتأويلات غريبة وأفكار سيئة، فمنهم من يحاول اختراق جهاز أو موقع بحجة أنه غير المذهب أو الطائفة الدينية أو بحجة تكفيره أو الإطلاع على أسرار له فضحه والتشهير به.

وإن كثير من الأشخاص التي تتبنى بعض الآراء و الأفكار السياسية وكذلك المنظمات في عصرنا الحالي ومن أجل الدافع عن هذه الآراء تقوم بأفعال إجرامية ضد معارضيها، ويتم عن طريق شبكة المعلومات، ذلك بالتشهير بهم، إذ أن هذا العصر الجديد للإرهاب تميز بالدور المركزي الذي تلعبه شبكة الأنترنت في تشكيلها ونقل الأفكار والخبرات عبرها، بين الجامعات والأفراد الذين يشكلونها.

ومن الدوافع أيضا الدوافع العنصرية والتي تميز بين شخص وآخر أو قبيلة أو عرق وبين آخرين، فبعض القبائل أو الأعراق لا يحبون القبيلة الأخرى أو العرق الآخر فتجد بعضهم يحاول عمل أعمال تخريبية من مشاكل على القبيلة أو العرق الآخر سواء باستخدام التدمير أو الإتلاف أو نشر الشائعات والأكاذيب أو غيره من طرق وأنواع الجرائم السيبرانية.

٥. الدوافع الشخصية :

قد يكون سلوك المجرم السيبراني المخادع بدافع من الإكراه أو الحقد، ويتمثل هذا الحقد على مكانة وظيفة معينة أو حقد مالي لعدم تمكنهم من القيام بالتزاماتهم المالية علي أكمل وجه، أو الانتقام من رب العمل وإلحاق الضرر به، أو قد يكون الشعور بالنقص .

فيعد الشعور بالنقص من العوامل المؤثرة في إقدام المجرم علي ارتكاب جريمته، وقد يكون هذا الشعور بالنقص سواء تعلق ذلك بالناحية النفسية أو العملية مما يؤدي إلى شعور الفرد بأنه أقل من مستوي الآخرين، مما يؤدي إلى إثبات ذاته والتغلب علي هذا النقص بإظهار تفوقه في مجال آخر تعويضا عن العجز الذي يملكه .

يعد دافع الانتقام من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة السيبرانية؛ لأن دافع الانتقام غالبا ما يصدر من شخص يملك معلومات كبيرة عن الشركة التي يعمل بها؛ لأنه غالبا ما يكون أحد موظفيها ويقوم بهذا الدافع نتيجة لفصله من العمل أو أي سبب آخر يجعله يقدم علي ارتكاب الجريمة، وقد يصدر التصرف بغرض الانتقام من دولة معادية أخرى.

ونلاحظ أن الفعل الواحد قد يعكس دوافع متعددة خاصة ما إذا اشترك فيه أكثر من شخص انطلق كل منهم من دوافع خاصة تختلف عن غيره.

ومثال هذه الدوافع في بعض مجالات الأعمال التجارية وعلى وجه الخصوص في نطاق المنافسة والتجسس، ودافع التهديد، ودافع الحاجة للمعلومات المتوافرة لدى الغير.

ثانيا: أسباب الجريمة السيرانية على المستوى المجتمعي:

١. التحضر:

يعد التحضر أحد أسباب الجريمة السيرانية عامة، حيث الهجرة الكبيرة من الريف إلى المدينة وإلى المناطق الحضرية والمدن الكبيرة. وعادة ما يهاجر الشباب غير المتمكنين من مواجهة متطلبات الحياة الحضرية، باهضه التكاليف، والتي تتطلب مهارات عالية أحيانا. مما يجعل شرائح كبيرة من المهاجرين غير قادرين على تلبية متطلبات الحياة الحضرية، مما يجعلهم يعيشون في مدن الصفيح والأحياء الطرفية والهامشية. وكنتيجة يجد الناس انفسهم في تنافس غير قادرين على مجاراته، مما يجعلهم يلتفتون إلى الاستثمار في الجريمة السيرانية حيث لا تتطلب راس مال كبير، فأن التحضر سبب رئيسي للجرائم السيرانية في نيجيريا، وكنتيجة لذلك فإن الصفوة بينهم قد وجدوا إن الاستثمار في الجريمة السيرانية مربح.

٢. البطالة:

ارتبطت الجريمة السيرانية شأنها شأن الجريمة التقليدية بالبطالة والظروف الاقتصادية الصعبة وتركز البطالة بين قطاعات كبيرة من الشباب.

٣. الضغوط العامة:

تعد الضغوط العامة التي يتعرض لها المجتمع من فقر وبطالة وأمية وظروف اقتصادية صعبة عوامل ضاغطة على المجتمع عامة وخاصة على قطاع الشباب، مما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد الظروف وضد المجتمع مما يدفعهم إلى أساليب تأقلم سلبية مع هذه الظروف منها الإتجار الإلكتروني بالبشر والجنس وغيرها من الجرائم السيرانية.

ترجع نظرية الضغوط العامة الانحراف وخرق القانون إلى دافع ناجم عن قوى البناء الاجتماعي أو استجاباته النفس اجتماعية للحوادث والظروف والتي تعمل كضغوطات عندما لا تتاح للأفراد الفرصة

لتحقيق أهدافهم المقبولة اجتماعياً ، وأن مصادر الضغوط لا تتوقف على الإحباط الذي يخبره الفرد عندما تسد الطرق لتحقيق هدف ما، وإنما يشمل المشاعر السلبية التي تحدث في المواقف الاجتماعية المتنوعة.

كما قد تلعب العوامل الاجتماعية والاقتصادية أيضاً دوراً هاماً في زيادة الجريمة السيبرانية، فعلى سبيل المثال الضغط على مؤسسات القطاع الخاص لخفض الإنفاق وخفض مستويات التوظيف يمكن أن يؤدي إلى تخفيضات في الأمن، وإلى فرص لاستغلال ثغرات وضعف تكنولوجيا المعلومات والاتصالات والشركات، مما يضطر لتوظيف المتعاقدين من الخارج أو المؤقتين، ففي هذه الحالة يصبح هناك موظفين ساخطين بسبب انخفاض الأجور والخوف من فقدان الوظيفة، والخطر يزداد من الأعمال الإجرامية والنفوذ من قبل منظمة إجرامية.

٤. البحث عن الثراء السريع :

يسعى الإنسان إلى المتعة ويتجنب الألم هكذا تقول النظرية العامة في الجريمة ويسعى بعض الناس إلى الوسائل غير المقبولة اجتماعياً لتحقيق أهداف مقبولة اجتماعياً.

والمال هو عصب الحياة، وهو ما يدفع الفرد للقرصنة أو السرقة أو الاختلاس عن طريق الحاسوب للحصول على المال لتلبية حاجاته الأساسية والرغبة في الثراء السريع الغير المكلف.

فالرغبة في الثراء يواجهها صعوبات بالغة في تحقيقه بالطرق المقبولة اجتماعياً والقانونية، ولذا يلجأ بعض الناس إلى الجرائم السيبرانية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة وضعف إنفاذ القانون وتطبيقه في الجريمة السيبرانية.

و الرغبة في تحقيق الثراء الشخصي هي الدافع إلى الإجرام المعلوماتي الأكثر انتشاراً، فهو أهم البواعث على ارتكاب وانتشار الجرائم السيبرانية لما تحققه من ثراء فاحش وسريع.

٥. ضعف إنفاذ القانون وتطبيقه في الجريمة السيبرانية :

القوانين التقليدية السائدة لم تعد قادرة على مواكبة هذه السرعة الهائلة في تكنولوجيا المعلومات والتي أدت إلى تطور الجريمة من خلالها، وظهور جرائم لم تكن موجودة في السابق وباتت القوانين التقليدية عاجزة عن مواجهة هذه الجرائم مما يوجب تدخل المشرع في بعض الدول إلى سن تشريعات

حديثاً لمواجهة الجرائم السيبرانية، وأن عقاب الجرائم السيبرانية مازال محدوداً حتى الآن بالرغم مما صدر من تشريعات .

وهذا لا يتوقف عند تطور التشريعات وإنما يشمل الشرطة والتحقيق والقضاء، وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني، كما هو الحال على المستوى الدولي. فمما يشعل الجريمة السيبرانية غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية والقضائية في محاكمة والتحقيق في الجرائم السيبرانية.

ثالثاً: أسباب الجريمة السيبرانية على المستوى الكوني:

١. التحول للمجتمع الرقمي :

إن من أهم سمات عصر المعلومات السمات الثلاثة الرئيسة :

أ. تغيرات كمية في مقدار المعلومات المتدفقة ونوعيتها: فبفعل تكنولوجيا الاتصالات والمواصلات فإن الصور والمعلومات تغطي كافة المعمورة بسرعة ودقة.

ب. إرسال المعلومات إلى العديد من الأطراف (البشر والمعدات) : فالمعلومات توجه الصاروخ والصحفي يرسل التقرير، والبث المباشر من مكان الحدث.

ت. وجود الشبكات : حيث يتم تداول المعلومات بين جميع الأطراف مثل البريد الإلكتروني، الجوال،... الخ . ففي الفضاء الافتراضي، تكونت التفاعلات الافتراضية وحلت محل التفاعل وجها لوجه وتكونت السلوكيات الافتراضية والشخصية الافتراضية والمجتمع المحلي الافتراضي.

لقد دخلنا عصر المعلوماتية الجديدة (أي الفضاء الإلكتروني أو العالم الافتراضي)، فالناس يقضون جزءاً من حياتهم اليومية في الفضاء الإلكتروني، ينشؤون الشبكات والمواقع ويتمتعون بأنواع جديدة من العلاقات الاجتماعية، وهم على تواصل مع ما يجري في العالم الخارجي، والقيام ببعض الأعمال، بالإضافة إلى أننا نرى الآن أن الكثير من الحكومات تتحول إلى حكومات رقمية، كل من هذه الأنشطة - التي يقوم بها الأفراد وأيضاً الحكومات - قد جعلت للجميع أن يمارسها بوجود جهاز كمبيوتر أو مودوم مع معرفة التقنية القليلة.

٢. العولمة:

أن ظهور الفضاء الإلكتروني يخلق ظواهر جديدة متميزة عن وجود أنظمة الكمبيوتر أنفسها، والفرص المباشرة للجريمة والتي وفرتها أجهزة الكمبيوتر الآن ضمن الفضاء الإلكتروني، قد يظهر الأشخاص الفروق في امتثالهم الخاص (القانوني) وعدم الامتثال (غير القانوني) مقارنة مع سلوكهم في العالم المادي. فالأشخاص، على سبيل المثال، قد يرتكبون جرائم في الفضاء السيبراني لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم بالإضافة إلى ذلك، فمرونة الهوية، وعدم ظهور الهوية وضعف عوامل الردع تحفز السلوك الإجرامي في العالم الافتراضي .

هذا العصر يتطلب مؤسسات أمنية مصممة للتعامل مع التغير السريع، تركز على الإبداع والشفافية وإرضاء العملاء والمجتمع بأسره، مؤسسات ذات سرعة عالية في نشر المعلومات وأعلام الجمهور، مؤسسات قادرة على إعادة تصميم ذاتها لمواجهة المستجدات السريعة والسريعة التغير في عالم الجريمة السيبرانية.

٣. انكشاف البنية التحتية المعلوماتية الكونية:

تتفاوت البنى التحتية المعلوماتية بدرجة انكشافها إلى الكوارث الطبيعية والإهمال البشري، وسوء التصرف الإنساني، وحدد التقرير الرئاسي الأمريكي بخصوص حماية البنية التحتية الحساسة خمسة قطاعات بناءً على الخصائص المشتركة لها ، وهذه القطاعات هي :

أ. قطاع الاتصالات والمعلومات:

وتشمل شبكات الاتصالات العامة، والإنترنت، والحاسبات في المنازل والاستخدام الأكاديمي، والحكومي، والتجاري.

ب. قطاع التوزيع المادي (الفيزيقي):

ويشمل الطرق السريعة للمواصلات، وخطوط السكك الحديدية، والموانئ وخطوط المياه، والمطارات، وشركات النقل، وخدمات الشحن التي تسهل انتقال الأفراد والبضائع.

ث. قطاع الطاقة:

وتشمل الصناعات التي تنتج الطاقة، وتوزع الطاقة الكهربائية، والبتترول، والغاز الطبيعي.

ج. قطاع المال والبنوك :

وتشمل البنوك ، وشركات الخدمات المالية من غير البنوك، ونظم الرواتب، وشركات الاستثمار ، والقروض المتبادلة، والتبادلات الأمنية والمادية.

د. قطاع الخدمات الإنسانية الحيوية:

وتشمل نظم التزويد بالمياه وخدمات الطوارئ والخدمات الحكومية (البطالة والضمان الإجتماعي والتعويض والإعاقات وإدارة سجلات المواليد إلخ).

من الصعب ربط التهديدات الإلكترونية بمكان أو زمان ، أو جماعة، فقد تصدر من هاو أو من طفل أو محترف، أو جماعة إرهابية، أو جماعة تنافسية، أو استخبارات أجنبية .

وأصبح الإرهاب وثيق الصلة بالتكنولوجيا لدرجة أنه يمكن معه القول أن بث الإرهاب عبر الأنترنت أصبح من سمات الألفية الثالثة، حيث يتميز الإرهاب الإلكتروني عن الإرهاب التقليدي بالطريقة العصرية المتمثلة في استخدام المواد المعلوماتية والوسائل الإلكترونية التي جلبتها تقنية عصر المعلومات، ولذلك نجد أن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين.

فخطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة التي تضار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية مما يجعلها هدفا سهلا للمال.

فبدلا من استخدام المتفجرات تستطيع الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية وإغلاق المواقع الحيوية مثل أنظمة القيادة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية أو شل محطات إمداد الطاقة والماء، أو إختراق النظام المصرفي مما يضر بأعمال البنوك والأوراق المالية العالمية.

رابعا: أسباب تتعلق بخصائص وسمات الجرائم السيبرانية:

وسوف نشرح بالتفصيل في المحور الثاني من المحاضرة هذه الخصائص بالتفصيل وذلك علي النحو التالي:

المحور الثاني : خصائص وسمات الجرائم السيبرانية:

فيما يلي مجموعة من خصائص الجرائم السيبرانية والتي تؤدي إلى ارتكاب الجريمة السيبرانية منها:

١. سرعة التنفيذ :

وخطورة هذه الظاهرة الإجرامية المستحدثة أن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، وأحيانا تتم في بضع ثوان، فلا يتطلب تنفيذ الجريمة الوقت الكبير ، وبضغطة واحدة علي لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلي آخر، وهذا لا ينفي أنها تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة .

٢. القيمة والديمومة:

معلومات بطاقات الائتمان والحسابات المصرفية والتصاميم... ذات قيمة عالية، والديمومة هي من صفات المعدات والبرامج المسروقة يمكن أن تستخدم لفترة طويلة.

٣. سرعة التطور في ارتكاب الجريمة السيبرانية :

التطور السريع الذي تشهده تكنولوجيا المعلومات أرخي بظلاله علي الجرائم السيبرانية؛ حيث إن أساليب ارتكابها في تطور مستمر، وأن المجرمين في مختلف أنحاء العالم يستفيدون من الشبكة في تبادل الأفكار والخبرات الإجرامية فيما بينهم .

٤. التنفيذ عن بعد :

لا تتطلب الجرائم السيبرانية في أغلبها (إلا جرائم سرقة الحاسوب) وجود الفاعل في مكان الجريمة، بل يمكن للفاعل تنفيذ جريمته وهو في دولة بعيدة كل البعد عن مكان الجريمة، سواء كان من خلال الدخول للشبكة المعنية، أو اعتراض عملية تحويل مالية، أو سرقة معلومات هامة سواء كانت معلومات شخصية أو عامة، أو تخريب..... الخ.

٥. خفاء الجريمة :

الجرائم السيبرانية، في أكثر صورها مستترة خفية لا يلحظها المجني عليه غالباً، مع أنها قد تقع أثناء استخدامه للإنترنت، ولكنه لا يكون عالماً بها ولا ينتبه إليها إلا بعد فترة من وقوعها وفي بعض الأحيان لا يكتشف أمرها، ويعود ذلك إلى تعامل الجاني مع نبضات إلكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسوب، كما أنه في بعض الجرائم فإن توافر المعرفة والخبرة لدى الجاني في هذا المجال يؤدي إلى صعوبة اكتشاف جريمته، وذلك باتباعه لطرق وأساليب لا يفطن إليها المستخدم العادي للإنترنت.

٦. إحجام المجني عليهم عن الإبلاغ :

نجد إحجام بعض المجني عليهم سواء كانوا أشخاصاً طبيعيين أو معنويين - مثل الشركات والمؤسسات - في مجتمع الأعمال عن الإبلاغ عما يرتكب داخلها من جرائم تجنباً للإساءة إلى السمعة والمكانة التي يتمتعون بها، وهز الثقة فيها، وللرغبة في استقرار حركة التعامل ومحاوله إخفاء أسلوب ارتكاب الجريمة حتى لا يتم تقليدها من جانب الآخرين.

وتؤدي كل هذه الأفعال السابق ذكرها إلى ترتيب نتائج عكسية تؤدي إلى تشجيع الجناة على ارتكاب مزيد من الجرائم، وخلق مجالات إجرامية جديدة وانتشار واتساع للقرصنة المعلوماتية، بل إنه تستخدم بعض الحكومات وعصابات الجريمة المنظمة والجماعات الإرهابية إمكانيات الجريمة السيبرانية لتحقيق أغراضها، ومن المتوقع أن تحدث تغيرات في نوعية المجني عليهم في هذه الجرائم نظراً لتزايد استخدامات الأنظمة المعلوماتية وشبكات المعلومات، ومنافذ بطاقات الائتمان، والبريد الإلكتروني، والتجارة الإلكترونية.

٧. جاذبية الجريمة السيبرانية والشغف بها:

نظراً لما تمثله سوق المعلومات و الحاسوب والإنترنت من ثورة كبيرة للمجرمين أو للإجرام، فقد غدت أكثر جاذباً لاستثمار الأموال وغسيلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول إلى الشبكات وسرقة المعلومات وبيعها، أو سرقة البنوك، أو اعتراض العمليات المالية وتحويل مسارها، أو استخدام بطاقات الائتمان.... الخ.

ونلاحظ أنه يميل مرتكبو أفعال الإجرام المعلوماتي إلى إظهار تفوقهم ومستوي ارتقاء براعتهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي أفعال الإجرام المعلوماتي الذين لديهم شغف بالآلة، يحاولون إيجاد الوسيلة إلى تحطيمها وغالباً ما يجدون ذلك ويتزايد شيوخ هذا الدافع لدى فئة الشباب أو المعرفين باسم صغار النوابغ المعلوماتية، الذين يمضون وقتاً طويلاً أمام حواسيبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات، ولإظهار تفوقهم على وسائل التقنية.

وغالبا ما يكون الدافع هو إثبات الذات وتحقيق الانتصار على تقنية الأنظمة المعلوماتية، ويرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمنشئي برامج النظام المعلوماتي لارتكاب تلك الجرائم.

والبعض يرتكب تلك الجرائم بدافع المزاح والدعابة، فيقوم الشخص بتصرفات وإن كان لا يقصد من ورائها إحداث جرائم، وإنما بغرض المزاح فقط ولكن هذه التصرفات قد ترقى إلى مستوى الجريمة وذلك إن كان هناك قانون يجرم مثل هذا الفعل.

وقد يتولد لدى طائفة من المجرمين صفة الغرور والمتعة؛ بحيث يقدم المجرم على ارتكاب الجريمة من أجل التعالي و التفاخر بقدرته على إحداث الآثار المترتبة.

ويمكن التمييز بين الشخص المغرور و الشخص الذي يكون هدفه إثبات التفوق العلمي في أن الشخص المغرور قد لا يكون على درجة علمية كبيرة، هذا بعكس الشخص الذي يسعى إلى إبراز كفاءته أمام الغير بما لديه من معلومات؛ لأنه لا يقصد من وراء هذا السعي التفاخر أو الغرور بل قد يكون ذلك كنوع من التحدي مع النفس لإثبات قدرته العلمية فقط.

٨. جرائم ناعمة:

تتطلب الجريمة التقليدية استخدام الأدوات والعنف أحيانا كما في جرائم الإرهاب والمخدرات، والسرقة والسطو المسلح إلا أن الجرائم المتصلة بالحاسوب تمتاز بأنها جرائم ناعمة لا تتطلب عنفا، أو مجهودا كبيرا في تنفيذها، وإنما تنفذ بأقل جهد ممكن يقوم به الجاني فنقل البيانات من حاسوب إلى آخر للاعتداء على حرمة الحياة الخاصة لا يتطلب أي عنف، أو السطو الإلكتروني على أرصدة بنك أيضا لا يتطلب أي عنف على عكس تبادل إطلاق النار مع رجال الأمن.

إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية (FBI) نظرا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف.

٩. غياب المفهوم العام:

غياب مفهوم عام متفق عليه بين الدول حول نماذج النشاط المكون للجريمة السيبرانية، وغياب - أيضا - الاتفاق حول التعريف القانوني للنشاط الإجرامي المتعلق بهذا النوع من الإجرام.

١٠. صعوبة إثباتها :

يصعب إثبات الجريمة السيبرانية للأسباب الآتية :

أ. سرعة غياب الدليل المرئي:

إن محو آثار الجريمة وإتلاف أدلتها غالبا ما يلجأ إليه الجاني عقب ارتكابه للجريمة، إذ يستطيع المجرم السيبراني في أقل من ثانية أن يمحو، أو يحرف، أو يغير البيانات والمعلومات الموجودة في الكمبيوتر، لذا فإن المصادفة وسوء الحظ للمجرم المعلوماتي لهما دور في اكتشاف الجريمة السيبرانية يفوق دور أساليب التدقيق والمراقبة؛ وذلك لأن ما يتطلب من فحص دقيق لموقع الجريمة من قبل المتخصصين في هذا المجال للوقوف على دليل ضد الجاني، وما يتبع ذلك من فحص الكم الهائل من الوثائق والمعلومات والبيانات المخزنة، فضلا عما يتطلبه ذلك من تكلفة اقتصادية عالية.

ونلاحظ أن مرتكبي هذه الجرائم، وبالذات في مجال الجريمة المنظمة يلجئون إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية في أنظمة إلكترونية، مع استخدام شفرات أو رموز سرية لإخفائها عن أعين أجهزة العدالة، كما أن أنواع العناوين الإلكترونية والبيانات التي تخزن في ذاكرة النظام الحاسوبي لمدة قصيرة ولا تخزن بشكل دائم، مما يثير مشكلات كبيرة في جمع الأدلة الجنائية وإثبات هذه الجرائم قبلهم.

ب. انعدام الآثار التقليدية للجريمة :

تتميز الجريمة السيبرانية بقلة عدد الحالات التي تم اكتشافها بالفعل، إذا ما قارنا ذلك في ضوء ما يتم اكتشافه من الجرائم التقليدية.

الجريمة التقليدية نجد أن أغلب المجرمين يتركون أثرا يؤدي إلى اكتشافهم و التوصل إليهم ولو بعد فترة من الزمن، أما في حالة الجرائم السيبرانية فلا توجد في أغلب الأحيان آثار خارجية أو مادية تدل على مرتكب الجريمة .

ولذلك فهي جرائم تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية غير المرئية ولا توجد مستندات ورقية فهي جرائم مخفية لا تترك أثرا بعد ارتكابها فيصعب الاحتفاظ الفني بآثارها إن وجدت ويصعب أيضاً تتبع مرتكبيها، فمن السهولة إخفاء معالم الجريمة السيبرانية، فأدلة الإدانة فيها غير كافية إلا في حدود ٢٠%.

ج. تشتيت جهود التحري فيها :

الكم الهائل للبيانات والمعلومات التي يجري تداولها في الأنظمة المعلوماتية، يشكل أحد مصادر الصعوبات التي تؤدي إلى تشتيت جهود التحري فيها، آية ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسوب متوسط الأهمية يتطلب مئات الآلاف من الصفحات التي لا تثبت كلها تقريباً شيئاً على الإطلاق.

كما يلعب البعد الزمني (اختلاف المواقيت بين الدول)، والمكاني (إمكانية تنفيذ الجريمة عن بعد)، والقانوني (أي قانون يطبق ؟) دوراً مهماً في تشتيت جهود التحري و التنسيق الدولي لتعقب مثل هذه الجرائم.

د. إعاقة الوصول إلى الدليل الرقمي بوسائل الحماية الفنية في الجرائم السيبرانية:

المجرم في الجرائم السيبرانية يحاول قدر الإمكان إعاقة الوصول إليه بشتى الطرق، فهو بعد ارتكاب جريمته يقوم بدس برامج، أو وضع كلمات سرية و رموز تعوق الوصول إلى دليل أو ليلجأ إلى تشفير التعليمات مما يصعب الوصول إلى دليل يدينه.

ولجوء مرتكبي الجرائم السيبرانية إلى إستخدام وسائل وأساليب متجددة تتميز بالطابع التقني والفني المعقد، والتي يصعب على أفراد الأجهزة الأمنية التعامل معها مثل جرائم الأعتداء بواسطة شبكة البوت نت، وتنشأ الشبكة بزرع برنامج خبيث في الحاسوب المخترق والذي يسمى بوت ويتم توصيله أو إدراجه فيما بعد ضمن شبكة من الحواسيب المخترقة، ويقدر عدد الأجهزة الموجودة بكل شبكة متفرقة لأغراض مختلفة مثل قطع الخدمة، وسرقة معلومات مهمة ونشر برامج خبيثة، حيث يمكن مخترق التحكم في مجموعة كبيرة من الحواسيب المخترقة الموجودة على أحدي شبكات البوت نت.

هـ. نقص الخبرة لدى الأجهزة الأمنية و القضائية:

اكتشاف الجرائم السيبرانية يتطلب إلماماً بالأمر الفنية والتقنية لدى أجهزة الشرطة، والنيابة العامة، والقضاء؛ وذلك للتوصل إلى مرتكبي هذه الجرائم وإثباتها ويتطلب أسلوباً خاصاً في التحقيق والتعامل مع مثل هذه الجرائم ذات الطبيعة التقنية المتطورة والأساليب المعقدة .

ولذلك نري ضرورة عقد دورات تدريبية، مشتركة بين رجال القضاء والنيابة العامة ورجال الشرطة، والخبراء الفنيين مجتمعين معا، وذلك بغرض معرفة كل جهة بطبيعة عمل الجهة الأخرى مما يحقق معه التعاون بين هذه الجهات وصولا إلي أنسب الطرق القانونية لمكافحة الجرائم السيبرانية.

٦. التلوث الثقافي:

لا يتوقف تأثير الجرائم السيبرانية عند الأثر المادي الناجم عنها، وإنما يتعدي ذلك ليهدد نظام القيم والأخلاق خاصة في المجتمعات المحافظة والمغلقة، فنشر المواد الإباحية والأخلاقية التي تمثل محرمات في بعض المجتمعات من شأنها أن تؤدي إلي جرائم في القيم وتلويث في ثقافة هذه المجتمعات كما قد تؤدي إلي التفسخ الاجتماعي، ويمكن ذلك نظرا لتشعب الشبكة وإمكانية الدخول إليها من أي مكان.

٧. المؤثرات الخارجية:

نجد أن الإنسان مخلوق هش من الناحية السيكلوجية، حيث يمكن في بعض المواقف أن يستسلم للمؤثرات الخارجية، فتمارس أفعال الإجرام المعلوماتي والتي تنفذ تحت تأثير تهديد أو ضغط من الغير.

٨. التعاون والتواطؤ للإضرار بالغير :

يمكن أن يتعاون أكثر من شخص أو جهة علي إرتكاب الجريمة السيبرانية للإضرار بالمجني عليه، وقد يكون إشتراكا سلبيا يترجم بصمت من يعلم بوقوع الجريمة، في محاولة منه في تسهيل إتمامها، وقد يكون إشتراكا إيجابيا يتمثل غالبا في مساعدة تقنية أو فنية.

٩. أسباب خاصة بالمنشأة :

لاشك أن الشخص المسئول عن المركز المعلوماتي، هو بدون منازع في وضع يمكنه من استغلال - إذا ما شاء ولمصلحته - نقاط الضعف المحتملة لمركز المعالجة. وتعد الألفة المتبادلة بينه وبين الأنشطة التي يزاولها ، ومركز الثقة الذي يحوزه أفضل أسلحة له لارتكاب أفعال الإجرام المعلوماتي .

المراجع

• الكتب:

١. د. أحمد خليفة الملط ، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي / الأسكندرية، سنة ٢٠٠٥.
٢. د. أيمن عبد الحفيظ: { الاتجاهات الفنية والأمنية لمواجهة جرائم المعلوماتية } - بدون دار نشر - الطبعة الأولى - سنة ٢٠٠٥ م .
٣. د. جميل عبد الباقي الصغير : { القانون الجنائي و التكنولوجيا الحديثة - الجرائم الناشئة عن استخدام الحاسب الآلي - الكتاب الأول - دار النهضة العربية - الطبعة الأولى - سنة ٢٠١٢.
٤. د. عبد الفتاح بيومي حجازي : { مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت } - دار الفكر الجامعي - الطبعة الأولى - سنة ٢٠٠٦ م .
٥. د. محمد علي العريان : [الجرائم المعلوماتية] - الدار الجامعية الجديدة للنشر الإلكتروني - الطبعة الأولى - سنة ٢٠٠٤م.
٦. د. محمد سامي الشوا : [ثورة المعلومات وإنعكاستها علي قانون العقوبات] - دار النهضة العربية - الطبعة الأولى - سنة ١٩٩٤م.

• الرسائل:

٧. د. أسماء روبيعي : [الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية]، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة ، سنة ٢٠١٣م.
٨. د. عيبر فؤاد عبد العزيز : { الحماية الجنائية لبرامج الحاسب الآلي } - رسالة ماجستير - جامعة القاهرة - كلية الحقوق - سنة ٢٠٠٧م.
٩. د. فهد سلطان محمد أحمد : [مواجهة جرائم الإنترنت] - رسالة ماجستير - كلية الحقوق - جامعة القاهرة - سنة ٢٠٠٤م.
١٠. د. محمد عبيد الكعبي : [الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت] - رسالة ماجستير - كلية الحقوق - جامعة القاهرة - ٢٠٠٤م.
١١. د. نائلة عادل محمد فريد قورة : [جرائم الحاسب الإقتصادية] - رسالة دكتوراة - جامعة القاهرة - ٢٠٠٣م.

• الدوريات والمؤتمرات:

١٢. أسامة محمد عبد الله، عيبر مجلى أبو ديه " الجرائم الإلكترونية " الملتقى الخامس للرابطة العلمية للبحث العلمي وعلوم الإتصال بعنوان " إشكالية المصطلح في علوم الإعلام والإتصال في العالم العربي " بيروت من ٢٩ نوفمبر إلي ١ ديسمبر ٢٠١٨.
١٣. د. ذياب البدينة: { أمن المعلومات } - مجلة دراسات مستقبلية - السنة السادسة - العدد الثامن يوليو ٢٠٠٣ م .
[الجرائم الإلكترونية : المفهوم والأسباب] - ورقة علمية مقدمة في الملتقى العلمي بعنوان الجرائم المستحدثة في ظل المتغيرات والتحويلات الإقليمية و الدولية خلال الفترة من ٢ - ٤ / ٩ / ٢٠١٤ م - عمان - الأردن.
١٤. د. محمد أبو العلا عقيدة : { التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية }، ورقة عمل مقدمة للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية - منظم المؤتمر: إكاديمية شرطة دبي ، مركز البحوث والدراسات، تاريخ الانعقاد : من ٢٦ إلي ٢٨ نيسان ٢٠٠٣م - الدولة : دبي الإمارات العربية المتحدة.

• مواقع إلكترونية:

١٥. محمد محمد صالح الألفي : [أنماط جرائم الإنترنت] – بحث منشور علي موقع

www.eastlaws.com

تم بحمد الله الإنتهاء من شرح المحاضرة الرابعة
مع تمنياتي بالتوفيق د. أسماء رويحي