



المحاضرة السادسة طرفا الجريمة السيبرانية

• تمهيد وتقسيم:

من المتعارف عليه دائما في العمل الإجرامي أن يكون لكل جريمة طرفان: الأول الجاني والذي نطلق عليه اسم المجرم السيبراني؛ لأن جريمتنا محل الدراسة هي الجريمة السيبرانية و الثاني هو المجني عليه وسنطلق عليه ذلك في الجريمة السيبرانية، وذلك على النحو التالي:

• عناصر المحاضرة:

المحور الأول : المجرم السيبراني:

أولا : سمات المجرم السيبراني:

1. السن.
2. الذكاء.
3. المهارة والمعرفة.
4. الميل إلى التقليد.
5. عائد إلى الإجرام.
6. الوسيلة و الوساطة.
7. الحرص الشديد وخشية الضبط واقتضاح الأمر .
8. يختفي مرتكب هذه النوعية من الجرائم تحت قناع فني يظهرهم من دولة إلى أخرى .

ونلاحظ أنه توجد سمات تتميز بها المجموعات في ارتكاب الجرائم السيبرانية وهي كالتالي:

1. التنظيم والتخطيط.
2. التكيف الاجتماعي و الروابط الدولية.
3. التطور في السلوك الإجرامي.

ثانيا : تصنيفات المجرم السيبراني .

التقسيم الأول : يمكن تصنيف الفاعل في الجريمة السيبرانية من حيث السن والخبرة:

1. الهواة والمبتدئون.
 2. صغار نوابغ السيبرانية.
 3. الأشخاص المحترفون في ارتكاب الجريمة السيبرانية.
- التقسيم الثاني: ينقسم الأفراد الذين يرتكبون تلك الجرائم بصفة عامة إلي:

1. أفراد من داخل المؤسسة.
2. أفراد من خارج المؤسسة وهم ثلاثة أنواع:
النوع الأول: المخترقون أو المتطفلون.

النوع الثاني: ناسخو البرامج.

النوع الثالث: صانعو الفيروسات.

التقسيم الثالث: يمكن تصنيف الفاعل في الجريمة السيبرانية من حيث الهدف أو الغاية إلي ثلاث فئات:

1. المتسللون.
2. المجرمون وتشمل فئة المجرمين:
أ. التجسس.
ب. الغرباء الذين ليس لهم حق استخدام النظام .

المحور الثاني : المجني عليه في الجرائم السيبرانية:

1. المنشآت المالية والقطاعات الحكومية.
2. المنشآت التجارية والصناعية.
3. المنشآت العسكرية.
4. الأشخاص الطبيعيون.

المحور الأول المجرم السيبراني

• تمهيد وتقسيم :

ينظر إلى الجريمة السيبرانية دائما أن مصدر ضعفها وانتهاكها هو الإنسان ذاته والذي غالبا ما يهيئ فرصة استغلال الوسيلة السيبرانية والتي أعدها سواء عن حسن أو سوء نية، ويرتبط جوهر المشكلة أذن بشخصيته ودوافعه، أي أن الإجراء السيبراني يرتبط ارتباطا وثيقا بشخصية المجرم.

ويترتب عليه أن تندرج الجرائم السيبرانية من الجرائم البسيطة إلى الجرائم الإرهابية وذلك تبعاً لشخصية المجرم السيبراني وبما لديه من خبرة في مجال تكنولوجيا المعلومات والوسائل التي يستخدمها والغرض من ارتكاب الجريمة. وهذا يؤدي إلى صعوبة تحديد صفات المجرم السيبراني وذلك لتعدد الجرائم السيبرانية وتنوعها، فهي تعطي صورا عديدة من الأنشطة الإجرامية .

ولكنه يلاحظ أن هناك مكاسب للمجرم السيبراني من الناحية الإعلامية، بحيث كان له القبول أكثر من المجرمين التقليديين، والقول بأن المجرم السيبراني أقل ضررا هو قول يتجاهل الدقة فالتهديد المعاصر يعد تهديدا حقيقيا. وليس ثمة أصدقاء في العالم الإلكتروني، وصغير المجرمين ككبيرهم، والمازح من بينهم كالحاقد، وضمان أمن المعلومات وضمان عدم التعرض للمسؤوليات يوجب التعامل مع الكل على أنهم مصدر للخطر، وليست المسألة إهدارا لفكرة حسن النية أو الثقة بالآخرين، بل إنها الضمان الوحيد للحماية من مصادر خطر بالغة قد تؤدي إلى مسؤوليات وخسائر لا يمكن تقديرها أو تجاوزها.

ويقول البعض إن المجرم السيبراني هو الذي لديه مهارات تقنية أو دراية بالتكنيك المستخدم في نظام الحاسوب والقادر على استخدام هذا التكنيك لاختراق الكود السري لتغيير المعلومات، أو لتقليد البرامج، أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه، أو عن طريق استخدام الحاسوب وشبكة الإنترنت وذلك من ناحية الاصطلاح القانوني.

إلا أننا لا نتفق مع الرأي المتقدم علي إطلاقه، فلقد ثبت عدم جدوى النظرة التقليدية للمجرم السيبراني التي سادت في كتابات الباحثين لفترة من الزمن، فمجرمو السيبرانية ليسوا دائما من النوابع الذين لا يمكن التنبؤ بهم أو معرفتهم، فإذا كان هذا النمط موجودا بالفعل إلا أنه يوجد أيضا المجرم الذي تربطه بالمجني عليه صلة ما والتي غالبا ما تكون صلة وظيفية أو أي علاقة أخرى مباشرة.

والاصطلاح الإلكتروني للمجرم السيبراني الذي يطلقه خبراء أمن المعلومات مصطلح "هاكرز"، وهو الإنسان الذي يقوم بعمليات الاختراق والتخريب عبر الإنترنت، وكما يطلقون مصطلح "هاكرز" علي

المتخصصين بفك شفرات البرامج وليس التخريب فهم نوع من الهاكرز المتخصص ، وفي اللغة العربية نظرا لعدم وجود ترجمة لكلمة "هاكرز" حتى الآن فتستخدم الكلمة كما هي مسجلة.

ويطلق البعض " مصطلح المجرم الإلكتروني الرقمي " علي المجرم السيبراني؛ وذلك لأن تخزين البيانات في ذاكرة الحاسوب في شكل أرقام ، وإذا طلبت تخرج علي شاشة الحاسوب أو الطابعة في شكل مقروء حسب اللغة التي خزنت بها وليست كما في ذاكراته.

وعلي ذلك فالمجرم الإلكتروني الرقمي هو الذي لديه القدرة علي تحويل لغته إلي لغة رقمية و تخزينها واسترجاعها باستخدام الحاسوب الرقمي وملحقاته ووسائل الاتصال الرقمية، وذلك بأداء فعل أو الامتناع عنه مما يحدث اضطرابات في المجتمع الدولي والمحلي نتيجة لمخالفة قواعد الضبط الاجتماعي محليا أو دوليا. ولكنني مع الرأي بعدم الأفضلية لهذه التسمية، وذلك لأن مصطلح "المجرم السيبراني هو مصطلح أشمل وأعم، فليس المجرم السيبراني هو الذي لديه القدرة علي تحويل لغته إلي لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب وملحقاته فقط، فقد لا يتطلب الفعل الإجرامي المكون للجريمة هذه المعرفة، وقد يتطلبها.

وعلي سبيل المثال، إنه من الممكن الآن انتهاك حرمة الحياة الخاصة عن طريق جهاز الكمبيوتر والإنترنت، وذلك عن طريق طرق عديدة ، ومن هذه الطرق تحميل برنامج من الإنترنت وذلك لاختراق البريد الإلكتروني ، فيوجد أكثر من ٨٠ برنامج لاختراق البريد الإلكتروني علي شبكة الإنترنت ، ويتم تحميل هذه البرامج بسهولة وما عليك إلا اتباع المعلومات التي تظهر مع تحميل البرنامج ، وبعد تحميل البرنامج تستطيع أن ترتكب جريمة انتهاك حرمة الحياة الخاصة، من غير أن تكون قادرا علي أن تحول لغتك إلي لغة رقمية، فتستطيع أن تفعل ذلك من خلال معرفتك باستخدام الحاسوب والإنترنت والبريد الإلكتروني والحصول علي البرنامج المخصص لذلك.

وما من شك أن المدى الزمني لنشأة وتطور العلوم الجنائية، حمل معه نشوء وتطور واندثار نظريات عدة في مجال علم الإجرام، وفي مجال تصنيف المجرمين، وأسباب الجنوح والانحراف وأمكن في ظل هذه العلوم، وما نتج في نطاقها من دراسات في ميدان علم الإجرام تحديدا، بلورة سمات عامة للمجرم عموما وسمات خاصة يمكن استظهارها لطائفة معينة من المجرمين، تبعا للجرائم التي يرتكبونها، وبالتالي كان طبيعيا أن تحمل ظاهرة جرائم الحاسوب في جنباتها ولادة طائفة من المجرمين، هم مجرمو السيبرانية تتوافر فيهم سمات عامة بغض النظر عن الفعل المرتكب، وسمات خاصة تبعا للطبيعة المميزة لبعض جرائم السيبرانية، والأغراض المراد تحقيقها.

وقد أتاحت الثورة الرقمية للمجرم السيبراني تسخير الفضاء الكوني لتحقيق أغلب صور الاعتداء على الأشخاص من جنح بسيطة إلى جنايات كبرى والاختراقات لأغلب المواقع الهامة؛ حيث يكون ذلك إما كفاعل أصلي أو كفاعل معنوي وبأبسط الأساليب من خلال التلاعب ببرمجة البيانات عن بعد، وهنا تكون صورة الأذى المعنوي هي الأغلب في نطاق الإنترنت، إلا أن الأذى المادي يمكن تحقيق صورته كذلك إذا تم التلاعب بالبيانات.

ولعل **الصورة الغالبة** لتحقيق غاية المجرم السيبراني أو القراصنة في نطاق الإنترنت تتمثل في فعل الدخول غير المشروع على النظام السيبراني أو البقاء فيه بدون إذن ومن ثم قيام الجاني بارتكاب فعله الذي قد يكون مجرمًا بنصوص عقابية أو لا يكون كذلك، بل إنه ليس هناك أية مبالغة في القول بأن استخدام تقنية المعلومات في ارتكاب الجرائم هي وسيلة أكثر أمناً بالنسبة للجاني عن الوسائل التقليدية الأخرى.

وسوف نتعرض الآن لسمات وأنماط وتصنيفات المجرم السيبراني علي النحو التالي :

أولاً : سمات المجرم السيبراني.

ثانياً : تصنيفات المجرم السيبراني .

وذلك علي النحو التالي:

أولاً : سمات المجرم السيبراني:

لا يمكن لأي عقوبة أن تحقق هدفها سواء في مجال الردع العام أو الردع الخاص ما لم نضع في الاعتبار **شخصية المجرم مما لها صفات**، والذي ينبغي إعادة تأهيله اجتماعياً حتى يعود مرة أخرى مواطناً صالحاً للمجتمع.

والحقيقة أنه وحتى الآن لم تتضح الصورة جلية في شأن تحديد صفات مرتكبي الجرائم السيبرانية واستظهار سماتهم، نظراً لقلّة الدراسات الخاصة بالظاهرة برمتها من جهة، ونظراً لصعوبة الإلمام الحقيقي. ولا شك أن المجرم السيبراني قد تجاوز الطرق التقليدية بسمات وخصائص تميزه عن غيره، وذلك كانعكاس حتمي لما تتطلبه عمليات استخدام الإنترنت من قدرات تقنية وفنية، **بيد أن ذلك لا يعني حصر مرتكبي جرائم الإنترنت في طبقة أو فئة معينة أو جنس معين**، فمرتكب الجريمة قد يكون من البالغين أو الأحداث، والمتعلمين منهم أو من المثقفين، ومن الفقراء أو الأغنياء، ومن الرجال أو النساء.

ولذلك نرى مع جانب من الفقه بأن المجرم السيبراني يمثل بالنسبة للمجموعات التقليدية للإجرام شخصية مستقلة بذاتها وإذا كان المجرم السيبراني يرتكب جرائمه وهو يمارس حياته الاجتماعية، فلا بد أن نقسم سمات المجرم السيبراني إلي سمات عامة للمجرم السيبراني الفرد والتي تتوافر لدي معظمهم والتي تميزهم عن غيرهم من المتورطين في أشكال الانحراف والإجرام الأخرى، و سمات أخرى و تتميز بها المجموعات في ارتكاب الجرائم السيبرانية وذلك علي النحو التالي :

أ. السمات العامة للمجرم السيبراني الفرد:

ومن أهم السمات العامة للمجرم السيبراني الفرد والتي تتوافر لدى معظمهم و التي تميزهم عن غيرهم من المتورطين في أشكال الانحراف والإجرام الأخرى هي :

1. السن:

حقيقة إن المتهمون بالإجرام السيبراني يبلغون ما بين ١٠ إلى ٦٠ من أعمارهم والمتوسط العمري ٢٥ سنة، كما أن مستوي مهاراتهم تتراوح بين مبتدئ (Novice) إلي محترف (Professional).

كما أن المجرم السيبراني هو في الغالب شخص عادي وليس محترف إجرام يحوز قدرات ومواهب فريدة فأى شخص أيا كان عمره مع قليل من المهارة ومدفوع بتحدي التكنولوجيا وإمكانية الربح وله سمعة سيئة أو روح الثأر أو له معتقدات يؤمن بها غير مشروعة يمكن أن يعد بها مجرما سيبرانيا.

2. الذكاء:

ومرة أخرى يختلف الإجرام السيبراني عن الإجرام التقليدي الذي يميل عادة إلي العنف، فيقال عادة إن الإجرام السيبراني هو إجرام الأذكاء بالمقارنة بالإجرام التقليدي الذي يميل إلي العنف .

فإذا كان من المتصور العنف في الإجرام الموجه ضد مكونات النظام المادية، فإنه لا يمكن تصور أن يكون هناك أي عنف في الإجرام الموجه ضد المكونات المنطقية والبيانات، وبالتالي يجب أن يكون المجرم علي دراية كافية بأنماط الجريمة.

3. المهارة والمعرفة:

تعد المهارة المطلوبة لتنفيذ النشاط الإجرامي من أبرز خصائص المجرم السيبراني، فينتمي مرتكبو هذه الجرائم عادة إلي الطبقة المتعلمة، ومعظمهم يكون من أصحاب التخصصات ومستخدمي الإنترنت، والذي يغريهم علي ارتكاب جرائمهم هو شعورهم بالأمن نتيجة الثقة الزائدة بالنفس، وجهل الكثير منهم بعلم وتقنيات الحاسوب، فيتملكهم الشعور بإمكانية ارتكاب الجريمة دون أن يتم اكتشافها، بحيث إذا كان الشخص مرتكب الجريمة علي قدر ضئيل من مستوي الخبرة، نجد أن الجرائم التي قد يرتكبها لا تتعدى الإتلاف المعلوماتي إما بالمحو أو بالإتلاف، وكذلك بنسخ البرامج و البيانات، واختراق البريد الإلكتروني.

إلا أن ذلك لا يعني ضرورة أن يكون المجرم السيبراني علي قدر كبير العلم في هذا المجال، أو أن تكون لديه خبرة كبيرة فيه، بل إن الواقع العملي قد أثبت أن بعض مجرمي السيبرانية لم يتلقوا المهارة اللازمة لإرتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

أما المعرفة فتتلخص في التعرف علي كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها و احتمالات فشلها. وتميز المعرفة بمفهومها السابق المجرم السبيرياني؛ حيث يستطيع أن يطبق جريمته علي أنظمة مماثلة لتلك التي يريد أن يستهدفها وذلك قبل تنفيذ جريمته.

4. الميل إلي التقليد:

يبلغ الميل إلي التقليد منتهاه حين يوجد الفرد وسط آخرين مجتمعين علي عمل معين إجرامي، إذ يكون عندئذ أسهل و أسرع انسياقا، ويظهر ذلك في مجال الجريمة السبيريانية؛ لأن أغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية التي لديه مما يؤدي به الأمر إلى ارتكاب الجرائم.

ولقد ساعد الإنترنت على تبادل الخبرات الإجرامية وتداولها، فكثير من المواقع تعرض البرامج التي تؤدي إلى اختراق البريد الإلكتروني مع شرح الكيفية التي تؤدي إلى ذلك، وكذلك كثير من المواقع تعرض البرامج المنسوخة، وما إلى ذلك .

5. عائد إلى الإجرام:

المجرم السبيرياني، مجرم عائد إلى الإجرام؛ حيث يعود كثير من مجرمي المعلومات إلى ارتكاب جرائمهم انطلاقا من الرغبة في سد الثغرات التي أدت إلي التعرف عليهم وعدم تقديمهم إلى المحاكمة مرة أخرى، ويؤدي ذلك إلي العود إلى الإجرام، وقد ينتهي بهم الأمر كذلك في المرة التالية إلي تقديمهم إلى المحاكمة.

6. الوسيلة و السلطة :

والوسيلة يراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته. والحقيقة أنه كلما كان نظام الحاسوب الذي يحتوي علي المعلومات المستهدفة غير مألوف كانت الوسائل المتطلبة أكثر صعوبة في الحصول عليها لاقتصارها علي عدد قليل من الأفراد هم عادة القائمون علي تشغيل النظام، وذلك علي عكس الأنظمة الشائعة الاستعمال.

أما السلطة فيقصد بها الحقوق والمزايا التي يتمتع بها المجرم السبيرياني والتي تمكنه من ارتكاب جريمته فكثير من مجرمي السبيريانية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة.

7. الحرص الشديد وخشية الضبط وافتضاح الأمر .

8. يختفي مرتكب هذه النوعية من الجرائم تحت قناع فني يظهرهم من دولة إلى أخرى .

ب. السمات التي تتميز بها المجموعات في ارتكاب الجرائم السيبرانية:

ونلاحظ أنه توجد سمات تتميز بها المجموعات في ارتكاب الجرائم السيبرانية وهي كالتالي:

1. التنظيم والتخطيط:

ترتكب أغلب الجرائم السيبرانية من مجموعة مكونة من عدة أشخاص، يحدد لكل شخص دور معين ويتم التخطيط والتنظيم السابق علي ارتكاب الجريمة، فمثلا تحتاج جريمة مثل نسخ برامج الحاسوب إلي شخص يقوم بنسخ تلك البرامج وقد يكونون مجموعة أشخاص وتحتاج أيضا إلي مجموعة تقوم بعملية البيع.

2. التكيف الاجتماعي و الروابط الدولية:

يختلف الإجرام السيبراني عن الإجرام التقليدي؛ حيث إن المجرم السيبراني في هذا الشأن يحيا وسط المجتمع، ويمارس عمله في المجال المعلوماتي أو غيره من المجالات الأخرى أي إنسان اجتماعي، فالمجرم السيبراني لا يضع نفسه في حالة عدااء سافر مع المجتمع الذي يحيط به، بل هو إنسان متكيف اجتماعيا. وتطبيقا لذلك فكثير من الجرائم السيبرانية ترتكب بدافع النصب، أو اللهو، أو لمجرد إظهار تفوقهم علي النظام المعلوماتي أو علي البرامج المتخصصة لأمن المعلومات.

وبالتالي فإنه في الغالب يكتفي بالتفاخر بين أقرانه ولكن لا نستخلص من ذلك، انعدام أي خطر اجتماعي للإجرام السيبراني. وليس السبب في ذلك عدم وجود نوايا أئمة ، ولكن أيضا للسلوك غير الواعي الذي يمكن أن يتسبب في أضرار جسيمة، حتى ولو لم يكشف عن أي عدااء للمجتمع وتعتبر هذه الخاصية امتدادا لسمة التخطيط والتنظيم؛ حيث إن التكيف الاجتماعي ينشأ بين مجموعة لها صفات مشتركة، فمثلا جماعة صغار النوايا المعلوماتية لا شك أنهم يتكيفون في أفكارهم فيما بينهم وتنشأ بالتالي صلات وروابط تساعد علي ارتكاب جرائمهم، وتتعدى بينهم تلك الروابط والصلات النطاق المحلي إلي المجال الدولي؛ بحيث تنشأ روابط دولية تتفق مع أفكارهم ومنهجهم في استثمار تلك المعرفة والتقدم العلمي. ولا شك أن إقامة المؤتمرات الدولية بين هؤلاء المجموعات خير دليل علي وجود تلك الصلات والروابط الدولية بينهم.

ولكل ما سبق فإنني لست مع الرأي القائل بأن (الشخص الذي يتمتع بذكاء شديد وتفوق في مجال الحاسبات والشبكة الدولية للمعلومات وما يتطلبه ذلك من استخدامه للحاسب الآلي لفترات طويلة جدا، يجعله بمعزل عن الآخرين عازفا عن مخالطة الناس وإنشاء علاقات معهم، نظرا لأنه يشعر أن العالم بين يديه، وأي

كانت احتياجاته ومتطلباته فهو يبحث عنها ويجدها في عالم تكنولوجيا المعلومات، فإذا أراد التحدث مع أحد فهناك مجموعات من النقاش المتواجدة دائما بالكثير من المواقع العالمية و المحلية، وإذا أراد البحث عن أي معلومة أو معرفة أي شيء فإن ذلك من أيسر الأمور في مجال الشبكة الدولية للمعلومات، ولذلك فإن احتياجه الاختلاط بالناس والتعامل معهم يقل تدريجيا حتى يجد نفسه معزولا عن الآخرين، مما يدفعه إلى ارتكاب جرائمه عبر الشبكة الدولية للمعلومات بدافع التحدي وإثبات الذات).

ولكني مع الفقهاء لا أتفق مع هذا الرأي السابق ويشوبه بعض التناقض؛ وذلك لأن الرأي السابق يجعلنا نطرح التساؤل التالي ، كيف يكون المجرم السيبراني الذي يدخل في مجموعات من النقاش المتواجدة دائما بالكثير من المواقع العالمية والمحلية بمنعزلا عن الحياة الاجتماعية، وهو يتعرف على كثير من الشخصيات في كثير من بلدان العالم، ويتبادلون فيما بينهم خبراتهم وثقافتهم المختلفة، بل نجدهم يتعاونون مع بعضهم البعض في كثير من الأحيان على ارتكاب جرائمهم المختلفة، أي أن الشخص عبر الإنترنت من الممكن أن يكون علاقات اجتماعية كثيرة، لا يستطيع أن يكونها بدون هذه الشبكة العالمية؟؟؟

3. التطور في السلوك الإجرامي :

والمقصود بذلك أن وجود الفرد في جماعة يشكل خطورة عليه؛ لأنه لا يكتسب المهارة التقنية والفنية فقط ولكن يزيد أيضا لديه الملكة الإجرامية، ومحاولة إثبات الذات والتفوق العلمي لديه مما يجعله يطور في أسلوب ارتكابه للجرائم.

ثانيا: تصنيفات المجرم السيبراني:

وعلى الرغم من أنه حتى الآن لم تتضح الصورة جليا في تحديد صفاتهم، واستظهار سماتهم وضبط دوافعهم نظرا لقلة الدراسات الخاصة بهذه الظاهرة من جهة ولصعوبة الإلمام بمداهها الحقيقي من جهة ثانية، بفعل الحجم الكبير من جرائمها غير المكتشف، أو غير المبلغ عن وقوعها، أو التي لم تتم بشأنها ملاحقة قضائية رغم اكتشافها، لصعوبة إثباتها، أو للنقص التشريعي الذي يحد من توفير الحماية الجنائية في مواجهتها. ومن جهة ثالثة فالمزيد من الوسائل والمخترعات يعني المزيد من التغير في أنماط الجريمة ووسائل الاعتداء، وهذا بدوره يساهم في إحداث تغير على السمات التي يتصف بها مجرمو الإنترنت .

وفي الواقع توجد العديد من التصنيفات للمجرم السيبراني، فلم يتم الاتفاق على تصنيف بعينه دون غيره، فكل يصنف على حسب النظرة التي ينظر إليها للمجرم السيبراني .

فالبعض يصنف المجرم السيبراني على حسب سنه وخبرته بمجال تقنية المعلومات، والبعض الآخر يصنفه من حيث هدفه أو غايته من ارتكاب الجريمة، والبعض يصنف المجرم السيبراني من حيث وظيفته هل هو من داخل المؤسسة أو من خارجها؟

وسوف نعرض لأهم التصنيفات للمجرم السيبراني وذلك بغاية التعرف عليه لكي نتمكن من مواجهته وذلك على النحو التالي :

التقسيم الأول : يمكن تصنيف الفاعل في الجريمة السيبرانية من حيث السن والخبرة إلي :

1. الهواة والمبتدئون:

هم الذين يمارسون مواهبهم في استخدام الحاسوب فقط، أو الحاسوب والإنترنت أو كليهما معا بغرض اللهو أو الهواية، فهؤلاء الشباب تكون غايتهم في النهاية مجرد التسلية والملاحظة و ليس لديهم نية ارتكاب أفعال الجريمة السيبرانية .

ولذلك يري جانب من الفقه الجنائي أنه من الملائم ألا يصنف هؤلاء في طائفة أو أخرى من الطوائف الإجرامية؛ لأن لديهم ببساطة ميل للمغامرة وروح التحدي والرغبة في الاكتشاف ونادرا ما تكون أفعالهم غير شريفة، وهم لا يدركون ولا يقدرّون مطلقا النتائج المترتبة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة، ولكنني لست مع هذا الرأي لأن خطر انزلاق هذه الفئة إلى احتراف الأفعال غير المشروعة وارتكاب الجرائم السيبرانية هو احتمال قائم، فعادة ما يكونون مفتونين بهذه الأنشطة الإجرامية المبتكرة والمستحدثة، وعندئذ يتحول من مجرد هاو صغير للأفعال غير المشروعة إلي محترف لها.

2. صغار نوابغ السيبرانية:

وهم الذين يطلق عليهم أيضا مصطلح صغار مجرمي السيبرانية، وهذه الطبقة من الشباب لديها قدر لا بأس به من الخبرة المعلوماتية، وهم غالبا ما يكونون في مرحلة المراهقة، وعلى الرغم من صغر سنهم إلا أنهم قادرون علي اقتحام كافة أنواع الأنظمة البنكية والشركات، والمؤسسات المالية، وليس هناك حدود جغرافية لأفعالهم التي تصل إلي أنظمة ومراكز معلوماتية توجد علي بعد آلاف الكيلومترات من أماكن تواجدهم .

ويتميز هؤلاء المراهقون في أنهم لا يعتبرون أن ما يقومون به يعد جريمة؛ لأنهم يعتقدون أن النظام غير قادر علي حماية نفسه وليس من الخطأ اقتحامه، ولذلك فإنهم يعتبرون أنفسهم أبطالا لمساعدة المجتمع في تحديد نقاط الضعف الخاصة بالبرنامج الذي تم اقتحامه.

والذي ساعد علي تعزيز هذه الفكرة هو دور الإعلام بالنسبة لهذه الفئة من مرتكبي الجريمة السيبرانية؛ حيث تميل الصحافة لنشر هذه الأفعال وأحيانا تضخم هذه الظاهرة عن عمد، باعتبار أن العنوانين الجذابة هي أساس التسويق، وأن غالبية الأفراد عادة ما يكونون مفتونين بهذه الأنشطة الإجرامية المبتكرة والمستحدثة.

ويمكن لجماعات صغار نوابغ المعلوماتية أن تتحول إلى فئة القراصنة؛ لأنه عندما يصبحون علي درجة عالية وكبيرة من الخبرة والمهارة يتم استئجارهم واستغلالهم في أعمال ذات أهداف إجرامية.

3. الأشخاص المحترفون في ارتكاب الجريمة السيبرانية :

وهؤلاء الأشخاص الذين يحترفون ارتكاب الجريمة السيبرانية تتراوح أعمارهم بين ٢٥ إلى ٤٥ سنة أي أنه في هذه المرحلة قد تحول المجرم السيبراني من مرحلة الهواية إلى مرحلة الاحتراف في استخدام المعلوماتية من ناحية ، واحتراف ارتكاب الأفعال غير المشروعة للمعلوماتية من ناحية أخرى.

وتعد هذه الفئة من أخطر الفئات التي ترتكب الجرائم؛ لأن الهدف الذي تقوم عليه هذه الفئة ينحصر في نية الفعل الإجرامي، وهذا هو مصدر الخطورة؛ لأن المجرمين المحترفين يرتكبون أنواعا من الجرائم المختلفة وبأساليب مختلفة ؛ لأنهم يكونون علي درجة كبيرة من المهارة والإتقان والغرض دائما هو المكسب أو الحصول علي فائدة مادية أو معنوية.

ووفقا لمجموعة من الدراسات تشكل طائفة الموظفين أو المستخدمين التهديد الأكبر، وبالطبع فإن الجرائم السيبرانية غالبا ما تعد جرائم داخلية (Insider Crime)، ولقد قدرت دراسة واحدة أن 90% من جرائم الحاسوب الاقتصادية تم ارتكابها من قبل الموظفين أو المستخدمين العاملين لدي الضحايا في مؤسساتهم.

وقد أشار استبيان في شمال أمريكا وأوربا إلي أن مخاطر أمن الحاسوب كان مصدره داخليا وأن ٢٣% فقط كان مصدره خارجيا، ومثلما أن التطور مستمر لكي يصبح في إطار المعالجة عن بعد، فإن التهديد من مصادر خارجية سوف يتصاعد ، وذلك أنه مع تزايد الأنظمة غير المتصلة ماديا ببعضها ، وكذا إعداد متزايد لبرامج شبه مجانية، فإن المظهر الاجتماعي لمجرم السيبراني مصيره إلي التغيير.

ونجد أن السبب في ذلك أنهم مسئولون عن أنظمة المعلوماتية، فهم يملكون المعرفة اللازمة والتقنية الكافية للتلاعب بالحاسوب، وعندئذ يقومون بتنفيذ أفعالهم غير المشروعة بأنفسهم، أو بمشاركة، أو مساعدة أشخاص آخرين، سواء كانوا فنيين أو مجرد وسطاء ، فهم يركزون قدراتهم نحو استقطاب صغار الموظفين وذوي القدرات الفنية، والذين هم علي مقربة من الأسرار المعلوماتية التي تساعد في تحقيق هدفهم، ومما يساعد علي نجاح عملياتهم غير المشروعة، وهنا يكمن الخطر الحقيقي، أنهم كثيرا ما ينظر إليهم بوصفهم مستخدمين مثاليين، والغالبية العظمي منهم يشغلون مراكز قيادية هامة ويتمتعون لذلك بثقة كبيرة في مجال عملهم و من الفئات الخطرة الجماعات الإرهابية التي أصبحت تستخدم أجهزة الكمبيوتر وشبكة الإنترنت في الاحتفاظ بالمعلومات وفي تلقي الأوامر من الجهات الخارجية التي تقود تلك الجماعات من الخارج وبالتالي يحقق لهم الحاسوب وسيلة مهمة للاختباء .

ومن الفئات الخطرة أيضا فئة ذوي الياقات البيضاء؛ وهم هؤلاء الذين يقومون بارتكاب جرائمهم عن طريق استخدام التكنولوجيا الحديثة، فلم يعد هناك مقتضي لإراقة الدماء أو استخدام أسلحة قاتلة للسرقة؛ لأن هذه الفئة تقوم بتحويل ملايين الجنيهات باستخدام أزرار الكمبيوتر من خلال الدخول علي أنظمة أحد البنوك حيث يقومون بارتكاب جرائم السرقة والنصب والاحتيال من بعد باستخدام شبكات الحاسوب في تحويل مبالغ مالية من أي جهة وبدأت سائر المنظمات الإجرامية في ارتكاب الأنواع المختلفة من الجرائم باستخدام الحاسوب، ومن هؤلاء مرتكبو جرائم المخدرات في عملية تبادل المعلومات وتحديد الأسعار، حيث لا تتم المقابلة إلا عند التسليم فقط .

ويضمن بالتالي هؤلاء المجرمون تحقيق أعلى معدلات التأمين لاسيما إذا استخدموا جميعاً أنظمة التشفير في عملية الاتصال حتى يظلوا دائما بعيدين عن أعين رجال الأمن.

التقسيم الثاني: ينقسم الأفراد الذين يرتكبون تلك الجرائم بصفة عامة إلي:

1. أفراد من داخل المؤسسة :

وهم الأخطر؛ لمعرفتهم بنظام المؤسسة وتشغيل النظام، والعبث به، ومعرفة نقاط الضعف والقوة بذلك النظام.

والحل الوحيد لمواجهة هذا النوع من المجرمين هو أن تحسن الشركات التعامل مع الموظفين، وإنهاء خدماتهم فقط عند الضرورة القصوى، وبصورة ودية، ومجزية ليس بدافع الخوف، وإنما لتحسن تعامل الشركة مع كل الموظفين الحاليين والذين يصبحون من السابقين.

2. أفراد من خارج المؤسسة وهم ثلاثة أنواع :

النوع الأول: المخترقون أو المتطفلون:

وهم الأشخاص الذين يخترقون شبكات الحاسوب مستعينين بما لديهم من قدرات متميزة ورغبات جامحة وينقسم الهاكرز إلى **فئتين** :

الأولي: المحترفون الذين يعملون في إطار عمل منظم لتحقيق أهداف معينة غالباً ما تهدف إلي الكسب غير المشروع من خلال اختراق حسابات البنوك أو الشركات الاستثمارية.

الثانية: **المعتمدون علي قدراتهم لإشباع الفضول وإثبات الذات**، وهؤلاء عندما يصلون إلى غايتهم يتركون الشبكة دون العبث في بياناتها وملفاتها ولا يعودون لاختراقها ثانيا إلا بعد تطوير طرق الحماية فيها مما يبعث فيهم روح التحدي للأخلاقي للاختراق. وهؤلاء من مرتكبي هذه الجرائم يكون هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول علي مكاسب مادية من ضمن هذه الأهداف.

النوع الثاني: ناسخو البرامج:

وفي الاصطلاح الإلكتروني **"قراصنة البرامج"** أو **"الكرakers"** ويطلق هذا اللفظ علي الشخص المقتحم الخبير في مجال المعلومات واستخدام الحاسوب، ويعتمد علي كسر الحماية الموجودة حول الشبكات وأجهزة الكمبيوتر ولذلك فإن الكراكر يستطيع اختراق الشبكات واقتحام البرامج، وينقسمون إلى فئتين :

الأولي: تقوم بهذه العملية أحيانا لاستخدام البرنامج استخداما شخصيا وليس تجاريا.
أما الثانية: فتقوم بهذه العملية بغرض الاستنساخ وتحقيق كسب مادي غير مشروع.

النوع الثالث: صانعو الفيروسات:

ويتمتع هؤلاء بمهارات مبرمجة وباستطاعتهم **الاختراق**. والقيام بعمليات حسابية معينة لا تنتهي فيستمر الحاسوب بالتنفيذ والحساب حتى يستنفذ كل مصادره من ذاكرة رئيسية وثنائية مما يؤدي لانهايار النظام ونلاحظ أن تطور الفيروسات والآليات المشابهة تعد تهديدا جديدا وواضحا فالفيروسات والوسائل المعقدة مثل القنابل المنطقية (Logic bombs) ، وحصان طروادة (Trojan Horse) يمكنها جميعا أن تستهدف موضوعات محددة، وبحيث ينتج عنها جرائم متنوعة ذات طابع تقليدي أكثر من مجرد إيذاء. وعلاوة علي ذلك فإن هذه الجرائم يمكن أن ترتكب حالا أو يمكن أن يتم الإعداد لها لكي ترتكب مستقبلا.

- **التقسيم الثالث يمكن تصنيف الفاعل في الجريمة السيبرانية من حيث الهدف أو الغاية إلي ثلاث فئات:**

1. المتسللون:

والدافع لهم العبور للنظام أو البيانات والمتسلل شخص يخترق الإجراءات الأمنية لنظام الحاسوب والحصول علي دخول غير مصرح به، والهدف قد يكون الحصول علي معلومات بطريقة غير قانونية من الحاسوب أو استخدام مصادر الحاسوب من أجل اكتساب خبرة، أو بدافع الفضول، أو لمجرد رد إثبات القدرة علي اختراق هذه الأنظمة .

2. المجرمون وتشمل فئة المجرمين:

أ. التجسس:

يستخدم الحاسوب في العالم اليوم العديد من المهام الحساسة والمتعلقة بكافة نشاطات المجتمع الاقتصادية والعسكرية والوطنية.... إلخ، وتنقل مثل هذه المعلومات لدول أخرى أو بالتعاون معها. وتمثل هذه الفئة خطورة عظمى وهي احتضان منظمات أو أفراد غير شرفاء لهؤلاء الشباب، واستغلالهم في ارتكاب العديد من الجرائم والملاحظ أن الجرائم التي ترتكب بمثل هذه التقنية تلاقي صعوبة أساسية في اكتشافها.

ب. الاحتيال وسوء الاستخدام والإهمال:

يعد الاحتيال وسوء الاستخدام والإهمال في الحاسوب من الجرائم المتزايدة :

بالنسبة للاحتيال فقد انتقلت غالبية الجماعات المنظمة المحلية والدولية إلى جرائم السيبرانية يبتغون من وراء نشاطهم الإجرامي تحقيق الربح المادي بطريقة غير مشروعة.

وأما سوء الاستخدام والإهمال لا شك أنه قد يترتب عليهما نتائج خطيرة، قد تؤدي إلى حد إزهاق الروح والتدخل في شؤون الحياة الخاصة للأفراد وما إلى ذلك.

ونلاحظ أن الجامع بين محترفي جرائم نظم المعلومات تمتعهم بقدرة عالية من الذكاء، وإلمامهم الجيد بالتقنية العالية واكتسابهم معارف علمية وعملية وانتماؤهم إلى التخصصات المتصلة بالحاسوب والإنترنت من الناحية الوظيفية.

ثالثا : العابثون:

إن فئة العابثين هم الذين يتعدون علي الملكيات العامة والخاصة. فغالبية هذه الفئة غاضبة من مكان عملهم أو من الحياة بشكل عام، ويمكن تقسيمهم إلى مجموعتين:

1. المستخدمون الذين لهم حق استخدام النظام ويتعاملون مع النظام الذي يخترقونه أو يسيئون استخدامه.
2. الغرباء: الذين ليس لهم حق استخدام النظام.

ويتجه الباحثون مؤخرا إلى الإقرار بأن أفضل تقسيم للمجرم السيبراني هو التصنيف القائم على أساس أغراض الاعتداء، وليس على أساس التقنية الفنية المرتكبة في الاعتداء، أو على أساس الوسائط محل الاعتداء، أو المستخدمة في تنفيذه أو غير ذلك من التصنيفات.

وختاما فإننا نؤكد على أنه ما من معيار ثابت ومحدد نستطيع من خلاله وضع تصنيف واحد لمجرمي الجرائم السيبرانية ولا يعني ذلك بطبيعة الحال أن كل مجرم يندرج تحت طائفة محددة دون غيرها، بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة، إلا أن الشيء الثابت هو أن هؤلاء المجرمين وإن تميزوا ببعض السمات والصفات الخاصة بهم يبقى في النهاية أنهم مجرمون ارتكبوا فعلا إجراميا وبالتالي فلا مناص من توقيع العقاب عليهم .

المحور الثاني

المجني عليه في الجرائم السيبرانية

تشير الإحصائيات النادرة في هذا المجال إلى إنه عملا، إن جميع الأنشطة التي تستخدم الحاسوب تكون عرضة لخطر الإضرار السيبراني، فأى قطاع من الأنشطة ليس بمنأى عن ذلك. ويبدو بجلاء أن انتهاك هذه الأنظمة المعلوماتية هو الأكثر توفيرا بالنسبة للمحتالين .

ومن المتصور أن يقع ضحية هذه الجرائم جميع الأشخاص سواء الطبيعية منها، أو المعنوية، أو العامة، أو الخاصة، وذلك يرجع إلى أن هؤلاء الضحايا لا يعلمون شيئا عنها إلا بعد أن تقع بالفعل.

ويميل الغالبية العظمى من ضحايا الإضرار السيبراني الحفاظ على سمعتهم التجارية ومكانتهم المرموقة، والقليل منهم هو الذي يكشف عن أفعال الإضرار السيبراني التي وقعوا ضحية لها ويعترفون بنتائجها، ويتحملون النتائج المترتبة على ذلك .

وغالبا ما يشغل مرتكبو أفعال الإضرار السيبراني مركز المسؤولية، ويحتلون مراتب عليا في التدرج الوظيفي بالمنشآت التي يعملون بها، وهذا ما يدفع مديرو هذه المنشآت إلى التستر على المسألة وحل المشكلة داخل المنشأة.

ويمكن تعريف المجني عليه بأنه الشخص الطبيعي أو المعنوي صاحب الحق أو المصلحة المشمولان بالحماية الجنائية، واللذان أضرت بهما الجريمة أو عرضتهما للخطر .

تتنوع القطاعات المستهدفة من قبل مرتكبي هذه الجرائم تبعا لأهمية المنشأة والتي تحتوي على الأموال أو المعلومات، وتبعا لدرجة كفاءة مرتكب تلك الجرائم ومقدرته على ارتكابها ويرتبط هذا النوع من الجرائم بالنواحي المالية و التجارية والصناعية والعسكرية والشخصية، ويتخذ المجنى عليهم الأنماط الآتية:

1. المنشآت المالية والقطاعات الحكومية :

حيث تمس هذه الجرائم **المركز الحسابي والإداري والمالي**، والاستثمارات في المنشآت العامة أو الخاصة، وهي أكثر الأماكن المستهدفة من مرتكبي جرائم السرقة والنصب والاحتيال.

وتعد القطاعات الحكومية هي الهدف الذي يقصده الجواسيس، ويستهدف أيضا مرتكبو هذه الجرائم القطاعات الخاصة؛ حيث يعتمد أصحاب الشركات إلى التجسس على الشركات المنافسة لمعرفة حجم المبيعات وغيرها من المعلومات التي قد تساهم في تقليل الفرص على الشركات الأخرى للمنافسة في الإنتاج.

2. المنشآت التجارية والصناعية:

وتمس هذه الجرائم **الدراسات الخاصة بالأسواق ومشروعات الاستثمار والتصنيع والإنتاج والتجارة والتوزيع، والأسعار، ومراكز البيع، والقطاع الصناعي للإنتاج.**

3. المنشآت العسكرية:

والتي تتمثل **الاعتداءات فيها على أسرار الدولة**، والمنشآت النووية، والتصنيع الحديث للأسلحة. ويظهر هذا بصورة أكبر في القطاعات الخاصة بالقوات المسلحة؛ نظرا لطبيعة وأهمية المعلومات التي تحتويها تلك القطاعات .

حيث أصبحت الدولة التي تمتلك المعلومات هي الدولة الأقوى، ولذلك بدأ الاهتمام ينصب على الجاسوسية العسكرية، وأصبح إطلاق الأقمار الصناعية من الجهات العسكرية هو المحور الذي يقوم عليه الاتجاه في تطوير الأجهزة والمعدات العسكرية، مما استتبع ظهور حروب جديدة تسمى بحرب المعلومات بين الدول، وتعتمد آليات هذه الحرب على شبكات الحاسوب في نقل المعلومات عن طريق الشبكات ومن خلال الأقمار الصناعية.

4. الأشخاص الطبيعيون :

إن كثيرا من الأشخاص يتعرضون لجرائم النصب، والسرقة، والإتلاف، ومن الطبيعي أن يكون الإنترنت المجال الخصب لارتكاب تلك الجرائم.

وتعتبر جرائم الإتلاف عن طريق الفيروسات أو جرائم انتهاك الحق في حرمة الحياة الخاصة هي من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون وخصوصا عبر البريد الإلكتروني؛ لأن هذا البريد الإلكتروني يعتبر من أهم البوابات التي يقفز منها القراصنة إلى أجهزة الأشخاص . وأيضا الاعتداءات تقع فيها علي المعلومات الشخصية المخزنة في ذاكرات الأنظمة المعلوماتية لدي البنوك وشركات التأمين، والمحامين، والمستشفيات، وأقسام الشرطة، والأحزاب..... الخ.

وخلاصة القول:

يوما بعد يوم تزداد مخاطر الجرائم السيبرانية وتتوسع دائرتها لتشمل كافة مرافق الحياة العامة، وتهدد الحقوق والحريات، وخطر ما في الأمر أن أغلب مرتكبي هذه الجرائم يبقون مجهولي الهوية، وهذا الأمر يتيح لهم الاستمرار والتفنن بطرق التلاعب بموارد الآخرين عن طريق السيطرة على أنظمتهم الإلكترونية.

المراجع

• الكتب:

1. د. أحمد خليفة الملط ، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي / الأسكندرية، سنة 2005.
2. د. أيمن عبد الحفيظ: { الاتجاهات الفنية والأمنية لمواجهة جرائم المعلوماتية } - بدون دار نشر - الطبعة الأولى - سنة 2005 م .
3. 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 .
4. د. عبد الفتاح بيومي حجازي : { مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت } - دار الفكر الجامعي - الطبعة الأولى - سنة ٢٠٠٦ م .
5. د. محمد علي العريان : [الجرائم المعلوماتية] - الدار الجامعية الجديدة للنشر الإلكتروني - الطبعة الأولى - سنة 2004م.
6. د. محمد سامي الشوا : [ثورة المعلومات وإنعكاستها علي قانون العقوبات] - دار النهضة العربية - الطبعة الأولى - سنة 1994م.
7. د. مصطفى محمد موسى، (أساليب إجرامية بالتقنية الرقمية - ما هيئتها - مكافحتها) - سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية - الطبعة الأولى - مطابع الشرطة للطباعة والنشر والتوزيع - القاهرة - سنة 2003م.

• الرسائل:

8. د. أسماء رويحي : [الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية]، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة ، سنة 2013م.
9. د. أيمن عبد الحفيظ عبد الحميد سليمان، الأحكام الموضوعية للقانون الجنائي والجرائم المعلوماتية، رسالة ماجستير - كلية الحقوق - جامعة القاهرة - 2010 .
10. د. أيمن عبد الله فكري، جرائم نظم المعلومات، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، سنة 2005.
11. د. نائلة عادل محمد فريد قورة : [جرائم الحاسب الإقتصادية] - رسالة دكتوراة - جامعة القاهرة - 2003م.
12. د. منى فتحي أحمد عبد الكريم : (الجريمة عبر الشبكة الدولية للمعلومات صورها ومشاكل إثباتها) - رسالة دكتوراة - كلية الحقوق - جامعة القاهرة - 2008 .

• الدوريات والمؤتمرات:

13. د. ذياب البداينة: { 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 والدولية خلال الفترة من 2 - 4 / 9 / 2014 م - عمان - الأردن.

• موقع إلكتروني:

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

www.eastlaws.com

15. الدكتور حسين بن سعيد بن سيف الغافري: { أثر شبكة الإنترنت علي حرمة الحياة الخاصة } - بحث منشور علي موقع

<http://www.atsdp.com>

16. ضياء هاشم: { قرصنة الإلكترونيّة عصر جديد من الجرائم } - مقال منشور علي موقع

<http://www.elaphblog.com>

• مرجع مترجم:

17. ملخص الترجمة العربية لمرشد الأمم المتحدة لعام 1999م، (التحكم في جرائم الحاسوب وردعها – المراقبة الدولية للسياسة الجنائية) ، ترجمة وعرض د. عمر محمد بن يونس – دار النهضة العربية – الطبعة الأولى – سنة 2005م.

تم بحمد الله

الإنهاء من شرح المحاضرة السادسة

مع تمنياتي بالتوفيق د. أسماء رويحي