

مقرر الجرائم السيبرانية

د. أسماء رويحي

المشرفة علي قسم ماجستير القانون الرقمي

LAW616

المحاضرة العاشرة

المسئولية الجنائية للوسطاء والتعاون الدولي
والشريعة الإسلامية في مواجهة الجرائم السيبرانية



ربط المحاضرات السابقة
بالمحاضرة الحالية

تمهيد وتقسيم :



محاور المحاضرة

المحور الثاني
الشريعة الإسلامية والتعاون الدولي
في مواجهة الجرائم السيبرانية

المحور الأول
المسئولية الجنائية للوسطاء في
الجريمة السيبرانية

عناصر المحاضرة :

المحور الأول:المسؤولية الجنائية للوسطاء في خدمات الإنترنت :

1. أولًا: تعريف وسطاء الانترنت:
- ثانيًا: أنواع وسطاء الإنترنت حسب التصنيف الوظيفي:
- ثالثًا: حالات اعفاء وسطاء الإنترنت من المسؤولية:
- رابعًا: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:
1. المسؤولية الجنائية لمقدم خدمة الحوسبة السحابية.
2. المسؤولية الجنائية لمقدم خدمة الاستضافة.
3. المسؤولية الجنائية لمقدم خدمة الاتصال بالإنترنت.



عناصر المحاضرة

المحور الثاني : موقف الشريعة الإسلامية والتعاون الدولي في مواجهة الجرائم السيبرانية:

- أولاً : موقف الشريعة الإسلامية في مواجهة الجرائم السيبرانية:
ثانياً : أهمية التعاون الدولي لمكافحة الجرائم السيبرانية:
ثالثاً : أنواع التعاون الدولي:
1. التعاون الدولي غير الرسمي:
 2. التعاون الدولي الرسمي:

عناصر المحاضرة

- رابعاً: جهود منظمة الأمم المتحدة في مواجهة الجرائم السيبرانية:
1. وثائق الجمعية العامة للأمم المتحدة بشأن الجرائم السيبرانية:
 2. قرارات المجلس الاقتصادي والاجتماعي:
 3. مؤتمر الأمم المتحدة الثامن لمنع الجريمة معاملة السجناء ... هافانا ١٩٩٠ بشأن الجرائم ذات الصلة بالكمبيوتر:
 4. إنشاء فريق من الخبراء الحكوميين المعنيين بالعمليات السيبرانية :

عناصر المحاضرة

خامسا : الاتفاقيات الدولية فى مجال مكافحة الجرائم السيبرانية:

1. معاهدة بودابست لمكافحة جرائم الإنترنت :

2. توصيات المجلس الأوروبي :

سادسا : جهود بعض المنظمات العالمية المتخصصة والتحالفات الدولية:

1. الاتحاد الدولي للاتصالات :

2. المنظمة العالمية للملكية الفكرية :

3. منظمة حلف شمال الأطلسي:

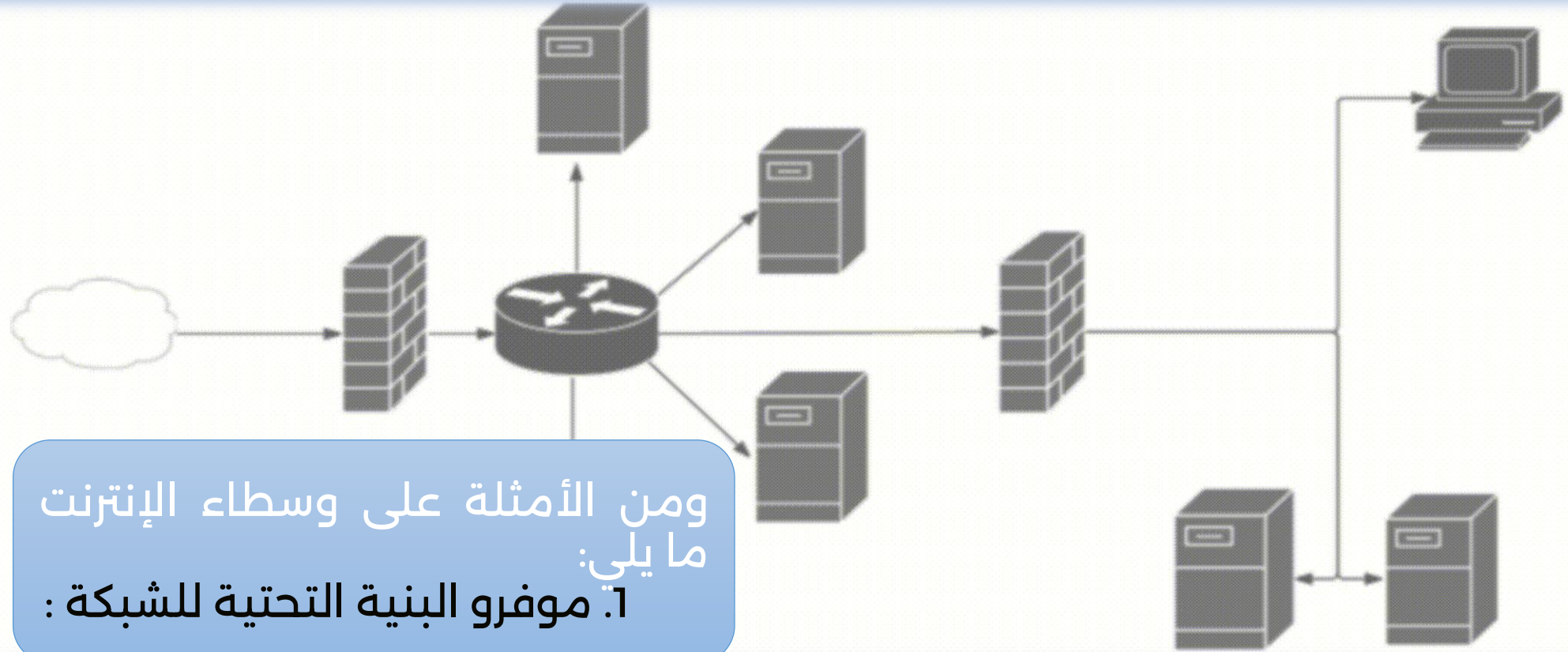
A hand is shown holding a glowing blue circuit board. A yellow oval is superimposed over the center of the image, containing Arabic text. The background is dark blue with a subtle pattern of white dots and lines.

المحور الأول المسئولية الجنائية للوسطاء في خدمات الإنترنت

أولاً: تعريف وسطاء الانترنت:



ثانياً: أنواع وسطاء الإنترنت حسب التصنيف الوظيفي:



ومن الأمثلة على وسطاء الإنترنت
ما يلي:
1. موفرو البنية التحتية للشبكة :

ومن الأمثلة على وسطاء الإنترنت ما يلي:
2. متعهد خدمات الوصول لشبكة الإنترنت:



ومن الأمثلة على وسطاء الإنترنت ما يلي:
3. مقدمو خدمات الإنترنت :



ومن الأمثلة على وسطاء الإنترنت ما يلي:
4. مقدموا خدمات الإستضافة :







ومن الأمثلة على وسطاء الإنترنت ما يلي:
6. الشبكات الإجتماعية:





ثالثاً: حالات اعفاء وسطاء الإنترنت من المسؤولية:



وهناك ثلاث أنواع من مقدمي الخدمات الوسيطة منحها التوجيه الأوروبي الاعفاء المشروط من المسؤولية وهم على وجه التحديد، إذا كان مقدم الخدمة:

1. ناقل للمعلومات أو مجرد قناة ناقلة للمعلومات.
2. يقوم بالتخزين المؤقت للمحتوي.
3. أو يقوم بالاستضافة.

رابعاً: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:

1. المسؤولية الجنائية لمقدم خدمة الحوسبة السحابية.
2. المسؤولية الجنائية لمقدم خدمة الاستضافة.
3. المسؤولية الجنائية لمقدم خدمة الاتصال بالإنترنت.



رابعاً: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:
1. المسؤولية الجنائية لمقدم خدمة الحوسبة السحابية:
أ. تعريف الحوسبة السحابية ومقدم خدمة الحوسبة السحابية:

رابعاً: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:
1. المسؤولية الجنائية لمقدم خدمة الحوسبة السحابية:
ب. التزامات مقدم خدمة الحوسبة السحابية:
- القانون الأمريكي:



رابعاً: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:
1. المسؤولية الجنائية لمقدم خدمة الحوسبة السحابية:
ب. التزامات مقدم خدمة الحوسبة السحابية:
- القانون السعودي:



رابعاً: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:
2. المسؤولية الجنائية لمقدم خدمة الإستضافة:





رابعاً: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:
2. المسؤولية الجنائية لمقدم خدمة الاستضافة:
أ. تعريف مقدم خدمة الاستضافة :

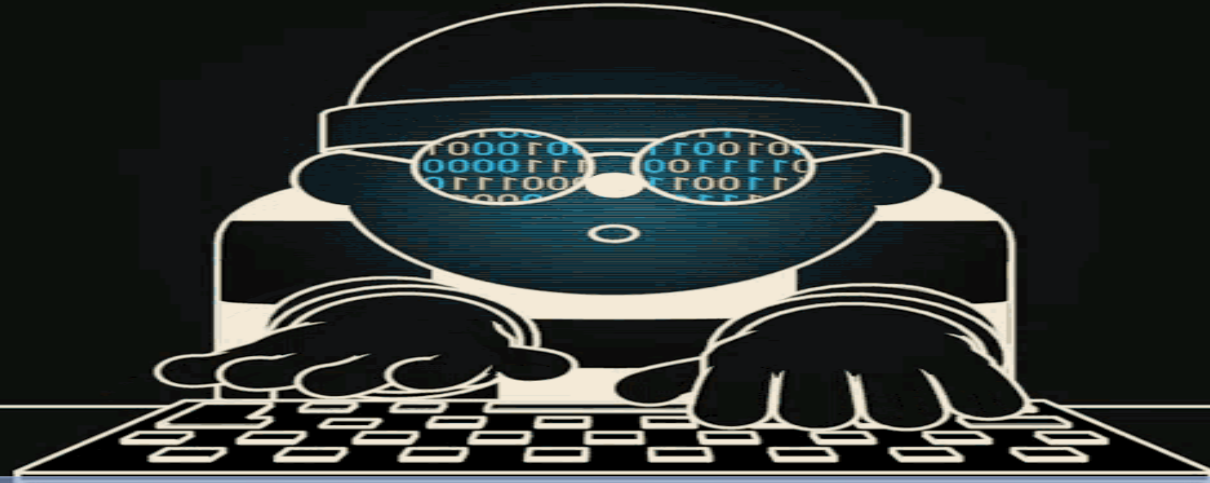


رابعاً: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:
2. المسؤولية الجنائية لمقدم خدمة الإستضافة:
ب. التزامات ومسؤولية مقدم خدمة الاستضافة:

رابعاً: مسؤولية وسطاء الإنترنت عن المحتوى الإلكتروني:
3. مقدم خدمة الإتصال بالإنترنت:



المحور الثاني الشريعة الإسلامية و التعاون الدولي في مواجهة الجرائم السيبرانية



تمهيد وتقسيم :



- أولا : موقف الشريعة الإسلامية في
مواجهة الجرائم السيبرانية:
ثانيا : أهمية التعاون الدولي لمكافحة
الجرائم السيبرانية:
ثالثا: أنواع التعاون الدولي:
1. التعاون الدولي غير الرسمي:
2. التعاون الدولي الرسمي:





رابعاً: جهود منظمة الأمم المتحدة في مواجهة الجرائم السيبرانية:

1. وثائق الجمعية العامة للأمم المتحدة بشأن الجرائم السيبرانية:
2. قرارات المجلس الاقتصادي والاجتماعي:
3. مؤتمر الأمم المتحدة الثامن لمنع الجريمة معاملة السجناء ... هافانا ١٩٩٠ بشأن الجرائم ذات الصلة بالكمبيوتر:
4. إنشاء فريق من الخبراء الحكوميين المعنيين بالعمليات السيبرانية :

خامسا : الاتفاقيات الدولية فى مجال مكافحة الجرائم
السيبرانية:

1. معاهدة بودابست لمكافحة جرائم الإنترنت :

2. توصيات المجلس الأوروبي :

سادسا : جهود بعض المنظمات العالمية المتخصصة
والتحالفات الدولية:

1. الاتحاد الدولي للاتصالات :

2. المنظمة العالمية للملكية الفكرية :

3. منظمة حلف شمال الأطلسي:



أولاً : موقف الشريعة الإسلامية في مواجهة الجرائم السيبرانية:



ثانيا : أهمية التعاون الدولي لمكافحة الجرائم السيبرانية:



ثانيا : أهمية التعاون الدولي لمكافحة الجرائم السيبرانية:



ثالثا : أنواع التعاون الدولي:



ثالثا : أنواع التعاون الدولي:
أ. التعاون الدولي غير الرسمي:



ثالثا : أنواع التعاون الدولي:
ب. التعاون الدولي الرسمي:



رابعاً: جهود منظمة الأمم المتحدة في مواجهة الجرائم السيبرانية:



رابعاً: جهود منظمة الأمم المتحدة في مواجهة الجرائم السيبرانية:
1. وثائق الجمعية العامة للأمم المتحدة بشأن الجرائم السيبرانية:



رابعاً: جهود منظمة الأمم المتحدة في مواجهة الجرائم السيبرانية:
2. قرارات المجلس الإقتصادي والإجتماعي:



رابعاً: جهود منظمة الأمم المتحدة في مواجهة الجرائم السيبرانية:
3. مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء ... هافانا ١٩٩٠
بشأن الجرائم ذات الصلة بالكمبيوتر:



رابعاً: جهود منظمة الأمم المتحدة في مواجهة الجرائم السيبرانية:
4. إنشاء فريق من الخبراء الحكوميين المعنيين بالعمليات السيبرانية :



خامسا : الاتفاقيات الدولية فى مجال مكافحة الجرائم السيبرانية:



خامسا : الاتفاقيات الدولية فى مجال مكافحة الجرائم السيبرانية:
1. معاهدة بودابست لمكافحة جرائم الإنترنت :



خامسا : الاتفاقيات الدولية فى مجال مكافحة الجرائم السيبرانية:
2. توصيات المجلس الأوروبي :



خامسا : الاتفاقيات الدولية في مجال مكافحة الجرائم السيبرانية:
3. إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية لعام 2025م:

A hand is shown reaching towards a digital globe. The globe is composed of a network of white dots connected by thin lines, creating a mesh-like structure. The background is a blurred cityscape at night with blue and white lights. The entire scene is framed within a blue-bordered box.

سادسا : جهود بعض المنظّمات العالمية المتخصصة والتحالّفات الدولية:

A hand is shown reaching towards a digital globe. The globe is composed of a network of white dots connected by thin lines, representing a global network or digital infrastructure. The background is a blurred cityscape at night with blue and white lights.

سادسا : جهود بعض المنظمات العالمية المتخصصة والتحالفات الدولية:
1. الإتحاد الدولي للإتصالات:

A hand is shown reaching towards a digital globe. The globe is composed of a network of white dots connected by thin lines, creating a mesh-like structure. The background is a blurred cityscape at night with blue and white lights. The entire scene is framed within a blue-bordered box.

سادسا : جهود بعض المنظمات العالمية المتخصصة والتحالفات الدولية:
2. المنظمة العالمية للملكية الفكرية:

سادسا : جهود بعض المنظمات العالمية المتخصصة والتحالفات الدولية:
3. منظمة حلف شمال الأطلسي:



<https://share.google/fqdaxnLY9Klv1fovK>

كيف نحمي أنفسنا من الجرائم السيبرانية التي تتم بواسطة برامج الذكاء الاصطناعي؟

يمكن للأفراد والعائلات تقليل مخاطر الذكاء الاصطناعي من خلال الآتي:

1. استخدام كلمات مرور قوية وفريدة :

الخطوة الأولى لحماية بياناتك هي استخدام كلمات مرور قوية وغير متكررة، بحيث تتضمن مزيجًا من الأحرف الكبيرة والصغيرة، الأرقام، والرموز الخاصة، ومن الأفضل تجنب استخدام كلمات المرور البسيطة أو تلك التي تعتمد على معلومات شخصية يمكن الوصول إليها بسهولة، مثل تاريخ الميلاد أو اسمك الكامل، كما يمكنك اللجوء إلى استخدام تطبيقات إدارة كلمات المرور التي تساعدك في توليد كلمات مرور قوية وتخزينها بشكل آمن.

SIGN IN

☒

[forget your password?](#)

[Don't have an account? Sign up](#)

<https://share.google/s2cvNcJbFi5GCgfov>

2. تفعيل المصادقة الثنائية (2FA) :

المصادقة الثنائية هي طبقة إضافية من الأمان تتطلب خطوة ثانية لتأكيد هويتك عند تسجيل الدخول إلى الحسابات، تتضمن هذه الخطوة غالبًا إرسال رمز تحقق إلى هاتفك المحمول أو بريدك الإلكتروني، لذا ينصح بتفعيل المصادقة الثنائية في التطبيقات التي تدعم هذه الخاصية، مثل فيسبوك، جيميل، وإنستجرام، حيث تعتبر من الطرق الفعّالة لمنع المتسللين من الوصول إلى حساباتك حتى لو تمكنوا من معرفة كلمة المرور الخاصة بك.

3. التحقق من نظام الأذونات الخاص بك:

عندما تقوم بتنزيل تطبيق جديد، عادةً ما يطلب منك منح أذونات للوصول إلى بعض البيانات أو الوظائف في جهازك، مثل الكاميرا، الموقع الجغرافي، أو قائمة جهات الاتصال، من المهم التحقق بانتظام من الأذونات التي منحتها للتطبيقات، وحذف أو تعديل الأذونات التي تشعر بأنها غير ضرورية، كما يفضل تجنب تنزيل التطبيقات التي تطلب أذونات غير مرتبطة بوظائفها الأساسية.

إلغاء الاشتراك في التدريب: في تطبيقات الذكاء الاصطناعي مثل (ChatGPT) انتقل إلى الإعدادات وأوقف تشغيل "تحسين النموذج للجميع" أو خيارات مشاركة البيانات المماثلة.

4. استخدام شبكات VPN عند الاتصال بشبكات واي فاي عامة:

عند الاتصال بشبكات الواي فاي العامة، قد يكون من السهل على المتسللين اعتراض بياناتك، لذا يُفضل استخدام شبكة افتراضية خاصة (VPN) عند التصفح أو الوصول إلى حساباتك عبر شبكات الواي فاي العامة، حيث تقوم VPN بتشفير الاتصال وتأمين بياناتك، مما يقلل من خطر التهديدات السيبرانية أثناء استخدام الشبكات العامة.

الشبكة الافتراضية الخاصة (VPN) هي تقنية تُنشئ اتصالاً آمناً ومشفرًا بين جهازك والإنترنت، حيث تعمل كنفق خاص يُخفي عنوان الـ IP الفعلي، ويحمي بياناتك من التجسس والاختراق عبر الشبكات العامة. تُستخدم لتجاوز القيود الجغرافية، تأمين الاتصال، وتعزيز الخصوصية الرقمية.

أهم جوانب الـ VPN:

- التشفير والأمان: تقوم بتشفير حركة مرور البيانات بالكامل (Data Encryption)، مما يجعلها غير قابلة للقراءة من قبل مزودي خدمة الإنترنت أو المخترقين.
- إخفاء الهوية: تُبدل عنوان الـ IP الخاص بك بعنوان خادم الـ VPN، مما يخفي موقعك الجغرافي الفعلي وهويتك على الإنترنت.

أنواعها: قد تأتي كتطبيقات جاهزة للاستخدام الشخصي أو بروتوكولات مدمجة في أنظمة التشغيل

5. فكر في استخدام البريد الإلكتروني المجهول و أرقام هواتف مزيفة للتسجيل.
6. كن حذرًا من الإرشادات: لا تقم أبدًا بإدخال تفاصيل مالية أو عناوين شخصية .
7. عمل سرية في برامج الدردشة الآلية التي تعمل بالذكاء الاصطناعي.
8. حذف السجل: قم بمسح سجل المطالبات الخاص بك بانتظام لإزالة البيانات المخزنة.
9. مراجعة سياسات الخصوصية: تحقق من سياسات أمان بيانات الذكاء الاصطناعي لفهم كيفية استخدام بياناتك وتخزينها.
10. استخدم أدوات الذكاء الاصطناعي المحلية: عندما يكون ذلك ممكنًا، استخدم نماذج الذكاء الاصطناعي التي تعمل محليًا على جهازك بدلاً من السحابة، مما يقلل من نقل البيانات.

مخرجات المقرر

1. المعرفة والفهم النقدي لتطور الجريمة إلى أن تصبح جرائم السيبرانية و معرفة المصطلحات المرتبطة بهذه الجرائم .
2. معرفة وفهم الأعمال النظرية الرئيسية المتعلقة بالجرائم السيبرانية.
3. استخدام مفاهيم إجرامية مجردة ذات الصلة بالجرائم السيبرانية.
4. تحليل و تقييم للتشريعات في مواجهة الجرائم السيبرانية.

المراجع

• الكتب:

1. د. أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، دراسة تحليلية تأصيلية مقارنة، الطبعة الأولى، سنة 2017.

• الرسائل:

2. د. أحمد طلعت عبد الحكيم عبد الحكيم عبد الرحمن، السياسة الجنائية في مواجهة جرائم تقنية المعلومات في ضوء القانون المصري رقم 175 لسنة 2018، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، 2022.

3. د. محمد خالد إبراهيم، الجوانب الموضوعية لجرائم تقنية المعلومات، دراسة مقارنة، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، سنة 2023.

• المواقع الإلكترونية:

4. د. هاني محمد إبراهيم خليل، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، بحث منشور علي موقع:

<https://espesl.journals.ekb.eg.pdf>

المراجع الأجنبية:

1. Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, 2, 100034.
<https://doi.org/10.1016/j.jeconc.2023.100034>
2. Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences*, 2(2), 379-398.
<https://doi.org/10.3390/forensicsci2020028>
3. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., ... & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, 10 (1), 1-10.
<https://doi.org/10.1057/s41599-023-01560-x>
- Chawki, M.**, & Abraham, A., (2025), *Cybercrime Unveiled: Technologies for Analysing Legal Complexity*, Springer International Publishing AG.
<https://link.springer.com/book/10.1007/978-3-031-80557-8>
- Lukings, M.** & Lashkari, A. (2026), *Understanding Cybercrime Victim Services, Challenges, Risks, Strategies, and Trends*, Springer International Publishing AG.
<https://link.springer.com/book/10.1007/978-3-032-13273-4>
- Sibe, R. T.**, & Kaunert, C. (2024). *Cybercrime, digital forensic readiness, and financial crime investigation in Nigeria*, Springer International Publishing AG.
<https://link.springer.com/book/10.1007/978-3-031-54089-9>
- Yiu, L.**, & Lau, C. (2025). *Cybercrime in Asia Policing, Technological Environment, and Cyber-Governance in China and Vietnam*, Springer International Publishing AG.
<https://link.springer.com/series/10634>

1. <http://www.indianmediacouncil.in>
3. <https://www.linkedin.com/pulse/scattered-spider-profiling-financially-motivated-group-kotha-xujrc/>.
5. <https://blog.avast.com/who-and-what-are-cybercriminals-avast>
6. <https://tenor.com/view/hacking-gif-20202201>
- 9:11 <https://www.coe.int/fr/web/freedom-expression/internet-intermediaries>
12. <https://blog.cloudflare.com/fr-fr/magic-transit-fr-fr>
13. <https://www.stor.fr/top-9-des-raisons-dexternaliser-ses-donnees-dans-le-cloud-a-la-reunion/>
<https://www.immo974.com/fournisseurs-dacces-a-reunion.html>
14. <https://sosp.name/choisir-fournisseur-dacces-a-internet-fai-thierry/>
15. <https://softflow.ca/fr/services/>
16. <https://fr.equinix.ch/products/data-center-services/colocation>
17. <https://www.blogdumoderateur.com/chiffres-reseaux-sociaux/>
21. <https://www.azinformatique.ch/>
33. https://gifer.com/en/72uZ#google_vignette
34. <https://www.cimtl.org/cyberattaque-wannacry-securite-internationale-et-cooperation-internationale-les-nouveaux-enjeux-de-la-generation-2-0/>
39. <https://siecledigital.fr/2023/10/04/cooperation-internationale-cle-de-voute-pour-affronter-cybermenaces/>
44. <https://www.zdnet.fr/actualites/comment-l-interieur-se-reorganise-pour-mieux-lutter-contre-la-cybercriminalite-39962634.htm>
47. <https://www.coe.int/fr/web/cybercrime/webinars>
51. <https://www.pinterest.com/pin/687995280571275766/>

تم بحمد الله
الإنهاء من شرح المحاضرة العاشرة
مع تمنياتي بالتوفيق د. أسماء رويحي



Thank You