



مجموعة المالكي للتدريب والتطوير

تقدم

الورشة التدريبية بعنوان

التعاون الدولي في مكافحة الجرائم الإلكترونية

مكان الإنعقاد : الإمارات العربية المتحدة - دبي

تاريخ الإنعقاد : 18 - 22 / 5 / 2025.





مقدمة :

مع التوسع الكبير في استخدام التكنولوجيا عبر الحدود الوطنية، أصبحت الجرائم الإلكترونية تشكل تهديدًا عالميًا يتطلب جهودًا مشتركة من الحكومات والمنظمات الدولية. لم تعد هذه الجرائم مقتصرًا على دولة بعينها، بل أصبحت تتجاوز الحدود الجغرافية، مما يجعل التعاون الدولي أمرًا ضروريًا لمكافحتها. يتطلب النجاح في هذا المجال التنسيق بين الجهات المعنية على المستوى الدولي، تبادل المعلومات والخبرات، وتطبيق القوانين والتشريعات المتوافقة مع المعايير العالمية. يهدف برنامج "التعاون الدولي في مكافحة الجرائم الإلكترونية" إلى تزويد المشاركين بالمعرفة والأدوات اللازمة لتعزيز الجهود الدولية لمكافحة الجرائم الإلكترونية، من خلال استراتيجيات حديثة وتطبيقات فعالة.

أهداف الورشة:

- فهم طبيعة الجرائم الإلكترونية وتأثيرها على الأمن الوطني والدولي.
- التعرف على الإطار القانوني الدولي لمكافحة الجرائم الإلكترونية.
- تحليل التحديات التي تواجه التعاون الدولي في مكافحة الجرائم الإلكترونية.
- تطوير استراتيجيات فعالة للتعاون الدولي في مجال الأمن السيبراني.
- بناء قدرات المؤسسات الحكومية على التعاون وتبادل المعلومات في مجال مكافحة الجرائم الإلكترونية.
- تعزيز التعاون بين القطاعين العام والخاص في مكافحة الجرائم الإلكترونية.
- تطبيق المعرفة المكتسبة في تطوير مبادرات للتعاون الدولي في مجال الأمن السيبراني.

محتويات الورشة:

اليوم التدريبي الأول:

الجرائم الإلكترونية والإطار القانوني الدولي

- أنواع الجرائم الإلكترونية (مثل الاحتيال، القرصنة، التجسس، الإرهاب الإلكتروني، غسيل الأموال الإلكتروني).
- تأثير الجرائم الإلكترونية على الأمن الوطني والدولي.
- الاتفاقيات والمعاهدات الدولية المتعلقة بمكافحة الجرائم الإلكترونية (مثل اتفاقية بودابست، اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية).
- التشريعات الوطنية ذات الصلة ومواءمتها مع المعايير الدولية.
- ورشة عمل: تحليل حالة جريمة إلكترونية دولية وتطبيق الإطار القانوني الدولي.



اليوم التدريبي الثاني:

تحديات التعاون الدولي

- التحديات القانونية (مثل الاختلافات في التشريعات الوطنية، قضايا الاختصاص القضائي، تسليم المجرمين).
- التحديات التقنية (مثل تحديد هوية المجرمين، جمع الأدلة الرقمية، التعاون في التحقيقات الفنية).
- التحديات السياسية (مثل التعاون بين الدول ذات المصالح المتباينة، قضايا السيادة الوطنية).
- ورشة عمل: تحليل حالة تعاون دولي فاشلة في مكافحة جريمة إلكترونية وتحديد أسباب الفشل.

اليوم التدريبي الثالث:

استراتيجيات التعاون الدولي

- بناء الثقة والتعاون بين الدول من خلال الاتفاقيات الثنائية ومتعددة الأطراف.
- تبادل المعلومات والخبرات وأفضل الممارسات في مجال مكافحة الجرائم الإلكترونية.
- تنسيق الجهود على المستوى الدولي والإقليمي من خلال المنظمات الدولية ومجموعات العمل المشتركة.
- بناء القدرات وتدريب الكوادر على أحدث التقنيات والأساليب في مكافحة الجرائم الإلكترونية.
- ورشة عمل: تطوير استراتيجية للتعاون الدولي في مجال محدد من مجالات الأمن السيبراني (مثل مكافحة الجرائم المالية الإلكترونية).

اليوم التدريبي الرابع:

التعاون بين القطاعين العام والخاص

- أهمية الشراكة بين القطاعين العام والخاص في مكافحة الجرائم الإلكترونية.
- تبادل المعلومات والخبرات بين القطاعين.
- المشاركة في تطوير وتنفيذ استراتيجيات الأمن السيبراني.
- دور القطاع الخاص في توفير التقنيات والحلول الأمنية.
- ورشة عمل: تصميم نموذج لشراكة بين القطاعين العام والخاص في مجال الأمن السيبراني.



اليوم التدريبي الخامس:

أفضل الممارسات والتطبيق العملي

- أفضل الممارسات في التعاون الدولي لمكافحة الجرائم الإلكترونية.
- دراسة حالات نجاح في التعاون الدولي في مكافحة الجرائم الإلكترونية.
- استعراض أحدث التقنيات والأدوات المستخدمة في التعاون الدولي.
- تقييم البرنامج التدريبي وحلقة نقاش مفتوحة.
- إعداد خطط عمل فردية لتطبيق المعرفة المكتسبة في بيئة العمل.

أساليب التدريب :

- نقاشات مفتوحة لتحليل وجهات النظر.
- دراسة حالات.
- قصص وأمثلة واقعية .
- التمارين واختبارات الشخصية.
- العصف الذهني.
- تكليف المتدربين بمشروعات جماعية أو فردية.
- ربط المحتوى بتجارب مألوفة.