المحاضرة الحادية عشر–التعاون الدولي لمواجهة التهديدات السيبرانية:

مقدمة:

نبدأ هذه المحاضرة بتوضيح أن الأمن السيبراني تجاوز منذ سنوات حدود الدول، لأن الهجمات الالكترونية لا تعترف بالجغرافيا.

فالهجوم الذي يبدأ من دولة ما يمكن أن يستهدف عشرات الدول خلال ثوان فقط لذا أصبح التعاون الدولي ضرورة وليست خيارا.

أولا–طبيعة التهديدات السيبرانية العابرة للحدود:

1. خصائص الهجمات السيبرانية الدولية:

- ✓ انطلاقها من عدة دول في نفس الوقت.
- ✓ استخدام خوادم وسيطة لإخفاء المصدر الحقيقي.
- ✓ أحيانا تكون مدعومة من جهات دولية أو مجموعات منظمة.
- ✓ تستهدف بنى تحتية حيوية: كهرباء، صحة، طيران، مالية.....

2. التحديات التي تواجه الدول:

- ➢ نقص الخبرات التقنية.
- ➢ اختلاف التشريعات والأنظمة القانونية.
- ➢ الهجمات قد تنفذ من دول لا تملك قوانين لمكافحتها.

ثانيا–أشكال التعاون الدولي في مواجهة التهديدات السيبرانية:

أ– التعاون القانوني: ويتمثل أساسا في:

- اتفاقية بودابست لمكافحة الجريمة الالكترونية: وتعد أول إطار قانوني دولي لمواجهة الجرائم السيبرانية، يضع: تعريفات موحدة للهجمات.

  إجراءات التحقيق الرقمي، آليات تبادل الأدلة.

- اتفاقية تبادل المعلومات بين الدول: التعاون بين الشرطة الدولية (الإنتربول).

  تبادل بيانات المهاجمين والفيروسات الجديدة.

ب–التعاون الأمني–التقني:

- تبادل الخبرات بين فرق الاستجابة للطوارئ.
- إنشاء منصات دولية لتحليل البرمجيات الخبيثة.
- مشاركة بيانات الثغرات (CVEs).

3. التعاون السياسي–الدبلوماسي:

- ✓ الحوار بين الدول حول قواعد السلوك السيبراني المسؤول.
- ✓ وضع مبادئ تمنع الهجمات على البنى التحتية الحيوية.
- ✓ نقاشات الأمم المتحدة حول الأمن المعلوماتي.

4. التعاون الاقتصادي:

- دعم الدول النامية لبناء قدرات الأمن السيبراني.
- الاستثمار في بنى تحتية مشتركة للحماية.
- تعزيز الأمن السيبراني للتجارة الإلكترونية العالمية.

ثالثا- نماذج دولية رائدة في التعاون السيبراني:

1- الاتحاد الأوروبي: قام باستحداث مجموعة من الهيئات وهي:

- مبادرة NIS.
- الوكالة الأوروبية ENISA.
- برامج تبادل المعلومات الأعضاء.

2- الولايات المتحدة:

- التعاون بين NSAو Homeland Security.
- اتفاقيات ثنائية لملاحقة الجرائم السيبرانية.

3- آسيا: تمثلت مجهوداتها فيما يلي:

- شراكات الصين، كوريا واليابان.
- التركيز على حماية سلاسل التوريد التقنية.

4- دور الأنتربول:

- ✓ قواعد بيانات الجرائم الالكترونية.
- ✓ تدريب ضباط الأمن في عدة دول.
- ✓ تنسيق التحقيقات العابرة للخدود الوطنية.

رابعا-تحديات وأوجه قصور التعاون الدولي:

1- اختلاف السياسات والأولويات: ذلك أن بعض الدول تعتبر الفضاء الرقمي مجالا للصراع وليس للتعاون.

2- غياب الثقة بين الدول: حيث قد ترفض بعض الدول مشاركة بيانات حساسة.

3- بطء الاستجابة الدولية: وذلك أنها تحدث في أيام وأسابيع مقارنة بالهجمات الرقمية التي تستغرق لحظات.

4- تضارب القوانين: ليس هناك قواعد قانونية مشتركة بين الدول، ولا مفاهيم موحدة للجريمة السيبرانية، ولا للمسؤولية القانونية، وكذا العقوبات المقررة لمثل هذه الجرائم.

5- الفجوة الهائلة بين تطور الهجمات التقني السريع واستجابة القوانين الوضعية المجرمة لهذه الأفعال.

خامسا-مستقبل التعاون الدولي في المجال السيبراني:

يتضح مستقبل تعاون الدول من أجل مكافحة ظاهرة الجرائم السيبرانية المنتشرة بكثرة في الواقع الحالي في: الاتجاه نحو اتفاقيات دولية سيبرانية شاملة، وتوحيد الجهود عالميا من خلال إنشاء منظمة دولية للأمن السيبراني.

الاستعانة بالذكاء الاصطناعي للكشف عن الهجمات السيبرانية العالمية في وقتها الحقيقي، لتحقيق الأمن الجماعي، وكذا السعي لحماية الفضاء السيبراني العالمي.