المحاضرة الثالثة–تفسير الأمن السيبراني في ضوء النظريات الأمنية:

مقدمة:

شهد العالم خلال العقود الأخيرة تحولات جذرية في طبيعة التهديدات الأمنية، حيث لم تعد مقتصرة على المجال العسكري التقليدي أو الحدود الجغرافية للدول، بل امتدت إلى الفضاء الرقمي الذي أصبح يشكل أحد أهم مجالات الصراع والتنافس، في هذا السياق برز الأمن السيبراني كأحد مفاهيم المركزية في الدراسات الأمنية المعاصرة لما له من ارتباط وثيق بحماية الدول، المؤسسات المنظمات وأفراد في بيئة رقمية معقدة ومتداخلة.

بالنسبة لطلبة الاتصال التنظيمي لا يفهم الأمن السيبراني فقط باعتباره مسألة تقنية بل لقضية اتصالية وتنظيمية وإستراتيجية تمس تدفق المعلومات داخل التنظيمات.

- حماية سمعة التنظيمية.
- الثقة الرقمية.
- استمرارية الاتصال المؤسسي

تهدف هذه المحاضرة إلى تفسير مفهوم الامن السيبراني انطلاقا من النظريات الأمنية الكبرى وبيان كيف ساهمت هذه النظريات في فهم طبيعة التهديدات السيبرانية مع ربط ذلك بسياق الاتصال التنظيمي.

أولا–الاطار المفاهيمي للأمن السيبراني.

1–تعريف الأمن السيبراني:

هو مجموعة السياسات، الإجراءات الممارسات والهياكل التنظيمية التي تهدف إلى حماية الفضاء السيبراني بما يشمل الشبكات، الأنظمة، البيانات، والاتصالات الرقمية من التهديدات والهجمات والاختراقات.

ويتميز الأمن السيبراني بعد خصائص:

- غير المرئي (INVISIBLE THREATS).
- عابر الحدود
- سريع التطور.
- متحرر الفاعليين (دول، منظمات، افراد، جماعات غير الرسمية)

2- الفضاء السيبراني كحقل امني جديد.

الفضاء السيبراني أصبح:

مجالا خامسا للامن إلى جانب البر، البحر، الجو، الفضاء الخارجي.

بيئة اتصالية مركزية ادارة التنظيميات.

ساعة للصراع المعلوماتي والحرب النفسية والتأثير الإتصالي.

ثانيا: مدخل عام إلى النظريات الأمنية.

النظريات الامنية هي أطر فكرية تسعى إلى

- تفسير طبيعة التهديدات.
- تحديد من هو الفاعل الأمني.
- بيان الوسائل المستخدمة لتحقيق الأمن

سنقوم بتفسير الأمن السيبراني من خلال أبرز هذه النظريات.

ثالثا: تفسير الأمن السيبراني في ظل النظرية الواقعية.

1- أسس النظرية الواقعية

تنطلق الواقعية من فرضيات أساسية

- الدولة هي الفاعل الأساسي في النظام الدولي.
- الأمن مرتبط بالقوة والسيادة.
- النظام الدولي فوضى
- الصراع أمر حتمي

2- الأمن السيبراني من منظور واقعي

ترى الواقعية أن

- الفضاء السيبراني مجال جديد للصراع بين الدول.
- الهجمات السيبرانية أداة من أدوات القوة.
- الأمن السيبراني جزء من الأمن القومي

في هذا السياق

- تطور قدرات هجومية ودفاعية سيبرانية.
- تستخدم الفضاء السيبراني لتحقيق الردع.

3- الانعكاسات على الاتصال التنظيمي.

- المؤسسات تعد أهدافا استراتيجية.
- الاتصال الداخلي قد يكون نقطة ضعف امنية.

- تسريب المعلومات ينظر إليه كتمديد سيادي.

رابعا: تفسير الأمن السيبراني في ضوء النظرية الليبرالية

1- أسس النظرية اللبيرالية.

تؤكد اللبيرالية على:

- التعاون الدولي
- دور المؤسسات والمنظمات.
- الاعتماد المتبادل.
- أهمية القواعد والمعايير.

2- الأمن السيبراني في منظور اللبيرالية.

وفق هذا التصور

- الامن السيبراني مسؤولية جماعية.
- لا يمكن لدولة واحدة تأمين الفضاء السيبراني.
- المنظمات الدولية والشركات التكنولوجية فاعلون أساسيون.

الامثلة:

- الاتفاقيات الدولية حول الجرائم الالكترونية.
- التعاون بين الدول والمؤسسات الخاصة.
- بناء الثقة الرقمية.

3- البعد الاتصالي والتنظيمي.

- أهمية سياسة الاتصال الأمني.
- الشفافية في غدارة الأزمات السيبرانية.
- التواصل مع الجمهور اثناء الهجمات الإلكترونية.

خامسا: تفسير الأمن السيبراني في ضوء البنائية.

1- اسس النظرية البنائية.

تركز البنائية على:

- الأفكار.
- القيم.
- الهوايات.
- الخطاب

وترى أن التهديدات ليست مادية فقط بل تبنى اجتماعيا.

2- الأمن السيبراني من المنظور البنائي.

من هذا المنظور

- التهديد السيبراني هو نتيجة إدراك جماعي.
- الخطاب الأمني يصنع الخوف أو الطمأنينة.
- وسائل الإعلام والاتصال تلعب دورا محوريا.

3- الامن السيبراني كبنية اتصالية.

- كيفية الحديث عن الاختراقات.
- إدارة السمعة الرقمية.

- الخطاب التنيظيمي أثناء الأزمات السيبرانية

سادسا: تفسير الأمن السيبراني في ضوء المقاربة الإنسانية للأمن

1- مفهوم الأمن الانساني.

يركز على:

- الفرد بدل الدولة.
- حماية الحقوق الرقمية.
- الخصوصية.
- الأمن النفسي والمعلوماتي.

2- الامن السيبراني كحماية للانسان.

- حماية البيانات الشخصية.
- محاربة الابتزاز الرقمي.
- الوقائة من العنف السيبراني.

3- دور الاتصال التنظيمي.

- التوعية الرقمية.
- بناء ثقافة أمن المعلومات داخل المؤسسة.
- تدين الموظفين على سلوك الاتصال الأمني.

سابعا: الأمن السيبراني والاتصال التنظيمي، مقاربة تكاملية.

من خلال النظريات الأمنية يتضح أن

- الامن السيبراني ليس تقنية فقط، بل هو سياسة، خطاب، وثقافة تنظيمية داخل التنظيمات.
- الاتصال غير الامني = التهديد السيبراني.
- ضعف الثقافة الاتصالية هشاشة أمنية.
- القيادة الاتصالية= عنصر الحماية.