## المحاضرة الخامسة– الفضاء السيبراني كمجال جديد للحروب والصراعات:

**مقدمة:**

اليوم سنتناول أحدا من أهم الموضوعات التي أصبحت في قلب العلاقات الدولية، وفي صميم التواصل التنظيمي داخل المؤسسات، الأمن السيبراني، لكن من زاوية دقيقة جدا، وهي تحول القضاء السيبراني إلى ميدان صراع وحروب شبيهة بالحروب التقليدية بل أخطر منها في بعض الأحيان.

لم يعد القضاء السيبراني مجرد قضاء رقمي للتواصل أو تخزين المعلومات، بل أصبح مجال استراتيجيا تمارس فيه الدول والشركات وحتى المجموعات غير التهامية عمليات تجسس، تخزين، ابتزاز، تضليل إعلامي، وشن هجمات يمكنها تشل دول بكامله.

- كيف يتحول القضاء السيبراني إلى ساحة حرب؟
- ما الفرق بين الحرب التقليدية والحرب السيبرانية؟
- ماهي الادوات التي تستخدم في هذه الحروب؟

**أولا– مفهوم الحرب السيبرانية وتطوراتها:**

**1– تعريف الحرب السيبرانية:** هي مجموعة من العمليات الهجومية أو الدفاعية التي تستخدم فيها وسائل تكنولوجية رقمية بهدف إلحاق الضرر بخصم معين، سواء كان دولة، مؤسسة أو بنية تحتية.

الحرب السيبرانية ليست خرقا تقنيا عابرا، بل هي نمط من الصراع المنظَّم، يهدف إلى الإرباك والتخريب والتجسس، وقد يصل إلى مستوى الشلل الكامل للبنية التحتية لدولة ما. وتتميز هذه الحرب بأنها تتيح للفاعل أن يضرب في العمق دون أن يتقدم بوصة واحدة داخل أراضي الخصم، ودون أن يُعرّف نفسه، أو أن يتحمّل الكلفة السياسية المباشرة لأي عدوان. ويُعد غموض الفاعل السيبراني، أو

ما يُعرف بـ"الإنكار المعقول"، أحد أقوى الأسلحة في هذا النوع من الحروب، لأنه يربك عملية الرد ويُعقّد الحسابات السياسية والدبلوماسية والعسكرية.

في حين أن الحروب التقليدية كانت تحتاج إلى إعلان نوايا واعتراف ضمني أو صريح من الطرفين المتحاربين، فإن الحرب السيبرانية تقوم على النفي والمراوغة، وتُدار بمنطق الهجوم من تحت العتبة، أي إن الطرف المعتدي يتعمّد البقاء تحت عتبة الردع العسكري التقليدي، كي يحقق أهدافه من دون أن يواجه برد مباشر. ولهذا فإن الحرب السيبرانية تخلخل مفهوم السيادة، لأنها تحاول أن تُظهر هشاشة الحدود الوطنية حين تُخترق البنية المعلوماتية، وتسيطر على الاتصالات، أو تُعطّل أنظمة البنوك، أو تُشوّه أنظمة المراقبة، وقد يصل الأمر إلى تسيير البنية التحتية الحيوية عن بُعد.

**2- لماذا تعتبر حربا؟:** لأنها منظمة ومخطط لها.

- تستهدف مصالح استراتيجية.
- تستخدم فيها "أسلحة" ذات تاثير مدمر مثل الفيروسات التخريبية، البرمجيات الخبيثة، الهجمات على الشبكات الصناعية .....

**3- أدوات الحرب السيبرانية:**

وتتعدد أدوات الحرب السيبرانية، من البرمجيات الخبيثة (malware) إلى هجمات حجب الخدمة (DDoS)، ومن التلاعب بالخوارزميات إلى سرقة قواعد البيانات، وصولا إلى التدمير الكامل للأنظمة التشغيلية كما في فيروس "ستاكس نت" الذي عُدّ أول سلاح سيبراني حقيقي استُخدم لتدمير المنشآت النووية في إيران. كما تشمل الحرب السيبرانية ما يُعرف بالحرب المعلوماتية، أي نشر الأخبار الكاذبة، وبث الإشاعات، وتفتيت الرأي العام في دولة الخصم من خلال حملات منسقة تُوظف الإعلام والمنصات الرقمية للتأثير على الوعي الجمعي. وهكذا لا تبقى الحرب السيبرانية مجرد مسألة أمن تقني، بل مسألة سيادة شاملة تتداخل فيها الأبعاد التقنية والنفسية والسياسية معا.

وفي حين أن الحروب التقليدية كانت تحتاج إلى إعلان نوايا واعتراف ضمني أو صريح من الطرفين المتحاربين، فإن الحرب السيبرانية تقوم على النفي والمراوغة، وتُدار بمنطق الهجوم من تحت العتبة، أي إن الطرف المعتدي يتعمّد البقاء تحت عتبة الردع العسكري التقليدي، كي يحقق أهدافه من دون أن يواجه برد مباشر. ولهذا فإن الحرب السيبرانية تخلخل مفهوم السيادة، لأنها تحاول أن تُظهر هشاشة الحدود الوطنية حين تُخترق البنية المعلوماتية، وتسيطر على الاتصالات، أو تُعطّل أنظمة البنوك، أو تُشوّه أنظمة المراقبة، وقد يصل الأمر إلى تسيير البنية التحتية الحيوية عن بُعد.

**4- عوامل انتشار الحرب السيبرانية:**

- الاعتماد المتزايد على الانظمة الرقمية.
- قابلية البنى التحتية للاختراق (الطاقة، المياه، النقل،الاتصالات)
- انخفاض تكلفة الهجوم مقارنة بالحرب العسكرية.
- صعوبة تتبع الفاعلين، ما يسمح لدول كثيرة بالإنكار.

**5- مراحل تطور الحرب السيبراني**

أ- مرحلة التجسس الرقمي في بدايات الالفية.

ب-مرحلة الاستخدام العسكري المحدود.

ت-مرحلة الهجمات الواسعة المعطلة للقطاعات الحيوية.

ث-مرحلة الدمج بين العمليات السيبرانية والعمليات العسكرية الحقيقية (كما في النزاعات الحديثة).

**ثانيا- أدوات وتقنيات الهجوم والدفاع في الحرب:**

1. **الجدران النارية المقدمة:**تستخدم الذكاء الاصطناعي لصد الهجمات وتحليل حركة البيانات.
2. **أنظمة كشف التسلل:** تراقب الشبكات وتوقف الهجمات في وقتها.

3. **التشفير وحماية البيانات:** حماية الإتصالات والملفات الحساسة داخل المؤسسات.

4. **استراتيجية الاستجابة للحوادث:** ملفات جاهزة للتعامل مع الهجمات، تتضمن خطط طوارئ، فريق تدخل، أدوار محددة، خط اتصال إعلامي مؤسستي.

5. **التدرجات والمحاكاة:** خاصة في المؤسسات الحيوية والبنوك.

**ثالثا- الحرب السيبرانية بين الدول والشركات:**

**1- مستوى الدول:**

أ- **الهجمات بين القوى الكبرى:** أصبحت الدول تتبادل الهجمات مثل استهداف الانتخابات، تعطيل شبكات الطاقة، التجسس على المؤسسات الحكومية، اختراق مراكز أبحاث عسكرية.

**ب- حروب الظل:** حروب غير معلقة رسميا، تستخدم فيها مجموعات "هاكرز"، تابعة لدول ولكن بصورة غير مباشرة.

**ت- سياق التسلح السيبراني:** دول كثيرة أنشأت : وزارة الدفاع السيبراني، كتائب إلكترونية، وحدات هجومية داخل الجيوش.

**2- مستوى الشركات والمؤسسات:** لم تعد الشركات في مأمن ، استهداف بيانات الزبائن، ابتزاز المؤسسات ببرامج

الفدية.

**لماذاالشركات هدف؟** تمتلك حسابات حساسة، تعتمد على أنظمة رقمية، تمتلك أموالا يمكن ابتزازرها وإختراقها أسهل من اختراق الدول.

❖ **دور الإتصال التنظيمي:**

- صياغة خطة تواصل أثناء الكوارث السيبرانية.

- الحفاظ على سمعة المؤسسة.
- إدارة الأزمة أمام الجمهور.
- نشر ثقافة الوعي الرقمي بين الموظفين.
- التنسيق بين فرق الآمن المعلوماتي والإدارة العليا.

**1- مقارنة بين الحرب التقليدية والحرب السيبرانية.**

الحرب السيبرانية: فضاء إلكتروني رقمي (فيروس، كود، خوارزميات)، منخفضة نسبيا، دول، شركات، جماعات هاكر، لحظية وسريعة،رقمية، اقتصادية، نفسية.

الحرب التقليدية: أرضي، بحري، جوي، مادي(سلاح، دبابة)، تكلفة مرتفعة، دول وجيوش، طويلة ومستمرة، بشرية ومادية.

**دوافع لجوء الدول إلى الحروب السيبرانية**

- السيطرة على المعلومات.
- إضعاف الخصوم دون صدام مباشر.
- اختبار دفاعات العدو.
- توجيه رسائل سياسية خفية.
- الانتقام من عقوبات اقتصادية أو دبلوماسية

❖ **أدوات وتقنيات الحرب السيبرانية**

**الهجومية:**

أ- **البرمجيات الحبيثة:** تستخدم الاختراق الأنظمة وسرقة البيانات أو تدميرها، انواعها.

**ب-الفيروسات:** تلتصق بالملفات وتتكاثر.

**ت-الديدان (Worms)** : تنشر تلقائيا عبر الشبكات.

**ث-حصان طروادة:** يبدو بريئا لكنه يخفي برنامج تجسس.

**ج-برمجيات الفدية:** تشفر البيانات وتطلب مالا لفكها مثال: هجوم « Wanna Cny » عام 2017 أصاب أكثر من 200 ألف حاسوب من 150 دولة.

**ح- هجمات الحرمان من الخدمة:**هي أغراق موقع أو خادم بعدد هائل من الطلبات حتى يتوقف عن العمل، يستخدم كثيرا ضد المؤسسات الإعلامية والبنوك.

**خ- هجمات APT:** التهديدات المستمرة المتقدمة: هي عمليات اختراق طويلة الأمر تستهدف شبكات حساسة، وغالبا ما تكون برعاية دولية، الهدف منها ليس التخريب السريع بل التجسس الصامت.

**د- التلاعب بالمعلومات والحرب الإعلامية:** تستخدم شبكات التواصل كجبهة مثل بث إشاعات لتقسيم الرأي العام، نشر أخبار كاذبة أثناء الأزمات.

- استهداف السمعة المؤسسية أو الوطنية.
- مهما يصبح الأمن السيبراني متداخلا مع الاتصال الاستراتيجي.

**هـ- الهجمات على الانظمةالصناعية (SCADA/ICS):** أخطرها لانها تحدث أضرارا فيزيائية: كشل محطات الكهرباء، تعطيل شبكات المياه، التحكم عن بعد في المصانع أو الطائرات، أشهر مثال: فيروس STUSCENT (2010) الذي عطل أجهزة الطرد المركزي في إيران.

❖ **الادوات الدفاعية:**

أ- **الجدران النارية المتقدمة:** تعمل كدرع أولي يراقب البيانات ويفرز المسموح من المحظور.

**ب-انظمة كشف التسلل والاستجابة (IDS/IPS):** تكشف محاولات الاختراق وترد عليها لحظيا.

**ت-التشفير:** حماية البيانات الحساسة اثناء التنقل والتخزين.

**ث-خطط الاستجابة للازمات:** تحدد أدوار كل قسم أثناء الهجوم، الأمن المعلوماتي، الإتصال، الإدارة.

**ج-الوعي البشري:** 80%من الاختراقات سببها خطأ بشري (فتح رابط مجهول، استخدام كلمة مرور ضعيفة).

**I. المحور الرابع: الحرب السيبرانية من السياق الدولي والتنظيمي.**

**1-الحرب السيبرانية بين الدول:** أصبحت جزءا من العلاقات الدولية، بعض الأمثلة الشهيرة، الولايات المتحدة وروسيا تبادل الاتهامات بالختراق والتلاعب بالانتخابات.

- الصين والولايات المتحدة: صراع اقتصادي وتجسس صناعي.
- إسرائيل وإيران: هجمات متبادلة على البنى التحتية.
- كوريا الشمالية: متهمة بهجمات على بنوك عاملية لتمويل برامجها النووية.

ما يميز هذه الحروب:

- تدار في الخفاء.
- يصعب إثبات مصدرها القانوني.
- تستخدم جماعات هاكرز، وكلاء غير رسميين.

- **الحرب السيبرانية بين الشركات والمؤسسات:** ما يميز هذه الحروب
  - تدار في الخفاء.

- يصعب إثبات مصدرها القانوني.
- تستخدم جماعات هاكرز، وكلاء غير رسميين.

**II. المحور الخامس: الأبعاد القانونية الأخلاقية للحروب السيبرانية.**

1- **الإشكال القانوني الدولي:** القانون الدولي لم يحدد قواعد واضحة لهذه الحروب.

2- **الاتفاقيات والمبادرات الدولية:** اتفاقية بوداست (2001) لمكافحة الجريمة السيبرانية، مبادرات الامم المتحدة لتطوير قواعد سلوك رقمية للدول.

لكن تطبيق ما يزال محدودا بسبب اختلاف المصالح السياسية.

3- **الأبعاد الأخلاقية:** استهداف المدنيين والمؤسسات الصحية مخالف لأخلاقيات الحرب

- التجسس على المواطن يشكل انتهاكا للخصوصية.
- نشر المعلومات المظللة ينقص الثقة العامة.

يجب أن تفرق بين الأمن السيبراني كحماية والحرب السيبرانية كاعتداء

✓ **الحماية السيبرانية:** هي مجموعة من الممرسات والتقنيات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات الرقمية تشمل هذه الحماية تأمين أجهزة الكمبيوتر والشبكات والبيانات من الهجمات الرقمية، تشمل هذه الحماية تامين اجهزة الكمبيوتر والشبكات والبرامج والبيانات الحساسة من الوصول غير المصرح بهوالقلق والتعطيل بهدف الامن السيبراني إلى الحفاظ على سرية وسلامة وتوافر المعلومات، وهو امر حيوي للأفراد والشركات والحكومات في العصر الرقمي.

أهدافها: **حماية البيانات:** منع الوصول غير المصرح به إلى المعلومات الحساسة مثل البيانات الشخصية أو المالية.

- **ضمان استمرارية العمل:** منع تعطيل العمليات التجارية بسبب هجمات الشبكة.
- **ضمان سلامة البيانات:** منع تغيير البيانات أو تدميرها.
- **توفير الثقة:** بناء ثقة العملاء من خلال التامين.

✓ **مكونات الحماية**

**البرامج والتقنيات:** استخدام برامج مكافحة الفيروسات، جدران الحماية، التشفير، ادوات التحقق من الهوية.

**السياسات والاجراءات:** وضع سياسات امنية وإجراءات لضمان سلامة المعلومات.

**الاستجابة للحوادث:** تطوير استراتيجيات للاستجابة للهجمات واكتشافها والتحقق من آثارها.

**امثلة على اجراءات الحماية السيبرانية الفردية.**

- **استخدام كلمات مرور قوية وفريدة:** لكل حساب، ويفضل استخدام برامج إدارة كلمات المرو.
- **تامين الأجهزة الشخصية:** إعداد الهاتف الذكي لتقفل تلقائيا مع استخدام بصمة الأصبع أو الوجه لفتحه.
- **الحذر عند استخدام منافذ الشحن العامة:** تجنب استخدامها قدر الإمكان، وعدم رفض طلبات نقل البيانات أثناء الشحن.
- **مراجعة أذونات التطبيقات:** التحقق من الاذونات التي تطلبها التطبيقات ومنحها فقط للملفات الضرورية.

تتنوع تقنيات وادوات الحماية في الأمن السيبراني لتستعمل حلولا متعددة مثل جدران الجماية، وانظمة كشف ومنع التسلل وبرامج مكافحة البرمجيات الخبيثة،وادوات التشفير، وانظمة إدارة

المعلومات والأحداث الأمنية (SIEM) تهدف هذه التقنيات إلى تأمين الشبكات والأجهزة والبيانات عبر التحصين ضد الهجومات، ومراقبة الأنشطة المشبوهة أو الاستجابة للحوادث بفاعلية.

❖ **تقنيات وادوات الحماية:**

1- **جدران الحماية (Firevells):** تعمل كحزام دفاع أول للشبكات، حيث تراقب وتتحكم في حركة مرور البيانات الواردة والصادرة، تتطور إلأى جدران الحماية من الجيل التالي(NGFU) التي تفحص محتوى التطبيقات والأجهزة بدقة أكبر.

2- **برامج مكافحة الفيروسات والبرمجيات الخبيثة (Antivirus/ Antimaluvare).**

تقوم بفحص الأجهزة وحمايتها من البرامج الضارة، ويجب تحديثها باستمرار.

3- **انظمة كشف ومنع التسلل (IDS/IPS):** تراقب حركة مرور الشبكة بحثا عن الانشطة الضارة وتحظر الهجمات المحتملة.

4- **ادوات إدارة المعلومات والاحداث الامنية (SIEM):** قمع وتحلل السجلات من مختلف المصادر لتقدير رؤية شاملة للأمن السيبراني، وتساعد في الكشف عن التهديدات والاستجابة لها.

5- **ادوات التشفير:** تحمي البيانات الحساسة أثناء نقلها أة تخزينها مما يجعلها غير قابلة للقراءة بدون مفتاح فك التشفير المناسب من أمثلتها أدوات مثل Veragypt و Bitlokor و TLS.

6- **أدوات اختبار الاختراق:**تستخدم لمحاكاة الهجمات المعروفة في الانظمة قبل أن يستغلها المهاجرون.

7- **ماسحات الثغرات الامنية:** تقوم بفحص الانظمة بحثا عن الثغرات الامنية المعروفة.

8- **أدوات منع فقدانالبيانات (DLP):** تساعد فيمنع تسرب البيانات الحساسة خارج المؤسسة.

❖ **التقنيات المتقدمة والمستقبلية**

1- **الذكاء الاصطناعي والتعلم الآلي: (AI/MC):** تستخدم للتنبؤ بالهجمات واكتشاف الأنماط المشبوهة، وتحسين سرعة الاستجابة للحوادث الامنية.

2- **البلوكيشن:** تستخدم لتامين البيانات عبر سلسلة اللامركزية، مما يجعل من الصعب التلاعب بها.

❖ **أدوات اخرى اساسية**

1- **التوثيق الثنائي:** يضيف طبقة أمان إضافية للحسابات الرقمية عن طريق طلب رمز تأكيد بالإضافة إلى كلمة المرور.

2- **برامج التحقق من الروابط (LINK SCANNERS):** تساعد في تحديد الروابط المشبوهة التي قد تؤدي إلى مواقع تصيد أو برمجيات خبيثة قبل التعرف عليها.

إن أخطر ما في الحرب السيبرانية أنها تعيد تعريف مفهوم القوة. فلم تعد القوة فقط هي القدرة على الردع التقليدي، بل أصبحت مرتبطة بالتحكم في المعلومات، والقدرة على الحماية، والمرونة أثناء الصدمة، والقدرة على الانتعاش السريع بعد الهجوم. وفي هذا السياق، فإن الدول التي لا تملك سيادة رقمية، أي لا تتحكم في أنظمتها وبنيتها التحتية السيبرانية، تصبح مكشوفة أمام خصومها، بل وتتحوّل إلى رهينة لموازين قوى لا تُدركها إلا بعد فوات الأوان.

قد بات واضحا أن القوى الكبرى تعتبر الحرب السيبرانية جزءا لا يتجزأ من منظومتها الدفاعية والهجومية. لذا طورت وحدات سيبرانية عسكرية متخصصة، تعمل على مدار الساعة لحماية المصالح الحيوية وشن هجمات استباقية عند الحاجة. كما أن التحالفات الدفاعية التقليدية، مثل حلف "الناتو"، بدأت تعترف رسميا بالهجوم السيبراني باعتباره سببا كافيا لتفعيل المادة الخامسة، أي اعتباره هجوما على كل دول الحلف.

لكن التحدي الأكبر في هذه الحرب هو غياب الإطار القانوني الدولي الصارم. فالقانون الدولي لم ينجح حتى الآن في وضع تعريف جامع للهجوم السيبراني، ولا في تحديد المسؤولية القانونية عن الأفعال التخريبية، ولا في فرض قواعد ملزمة على الدول. وهذا يفتح المجال أمام فوضى استراتيجية، تُستغل فيها الحرب السيبرانية لتصفية الحسابات، أو اختبار قدرات الخصم، أو حتى التأثير على نتائج الانتخابات واستقرار المجتمعات.

لذلك، فإن الحرب السيبرانية تفرض اليوم على الدول أن تعيد رسم أولوياتها الأمنية، وأن تتعامل مع السيادة الرقمية كقضية مصيرية، إذ إنها ليست ترفا تقنيا. وهذا يشمل بناء بنية تحتية مؤمّنة، وتطوير كفاءات وطنية للاعتماد عليها، وتعزيز أنظمة الردع الرقمي، وتوطين البرمجيات، وتقليص الاعتماد على الأنظمة المستوردة التي قد تحتوي على أبواب خلفية. كما ينبغي خلق ثقافة رقمية مجتمعية، تعزز من وعي الأفراد تجاه التهديدات السيبرانية، وتمنع تحويل المواطنين إلى نقاط ضعف في شبكة الأمن الوطني.

القدرات الوطنية السيبرانية تمثّل العمود الفقري لأي استراتيجية أمنية معاصرة، إذ تتيح للدولة الدفاع عن بنيتها التحتية الرقمية والرد على التهديدات الخفية بفعالية. وتشمل هذه القدرات الكفاءات البشرية، والتقنيات المؤمّنة، والسيطرة على شبكات الاتصال والبيانات. من دون تطوير ذاتي لهذه القدرات، تبقى الدولة عرضة للاعتماد على الخارج، مما يعرّضها للاختراق أو الابتزاز. كما أن امتلاك قدرات هجومية موثوقة يمنح الدولة قوة ردع حقيقية، ويُعيد التوازن في بيئة استراتيجية لم تعد تعترف بالحدود التقليدية.

باختصار، الحرب السيبرانية لم تعد خيارا مستقبليا يُنتظر، بل واقع يومي يتسلل بصمت إلى كل بيت ومؤسسة ودولة. وهي حرب لا تُخاض بجيوش نظامية، بل بخوارزميات ومهارات بشرية

خفية، ومراكز عمليات افتراضية. ومن لا يملك فيها دفاعا وهجوما، يصبح مهددا ليس بالخسارة فحسب، بل بالانكشاف الكامل، وربما التلاشي الصامت في خريطة النفوذ العالمي.

في عصر لم تعد فيه الحدود تُخترق بالدبابات بل بالشيفرات، تُعيد الحرب السيبرانية تعريف السيادة والردع والمعنى الكامل للقوة. فهي تُمكّن الدول والفاعلين من شن هجمات دون إعلان، وتخريب البنى التحتية دون تحمّل التبعات، وزعزعة المجتمعات من الداخل عبر المعلومة لا السلاح. وبينما تزداد أدوات الهجوم تطورا وانخفاضا في الكلفة، يبقى الدفاع السيبراني هشا ومعقّدا وباهظا. ولهذا، فإن مستقبل الأمن الوطني مرهون اليوم بالسيادة الرقمية، والجاهزية الأخلاقية، والقدرة على الرؤية الاستراتيجية في ميدان لا يُرى.