الدبلوماسية السيبرانية وآليات التعاون الدولي لردع الهجمات الإلكترونية

تركيا - اسطنبول

13 – 17/ 12 / 2026

مقدمة:

في المشهد الجيوسياسي لعام 2026، لم تعد السفارات هي القنوات الوحيدة للدبلوماسية؛ فقد أصبح الفضاء السيبراني هو الجبهة الجديدة لتشكيل التحالفات وردع العدوان. إن الدبلوماسية السيبرانية هي "القوة الناعمة" التي تحمي "السيادة الصلبة" للدولة. يهدف هذا البرنامج إلى تمكين القادة من أدوات التفاوض الرقمي، وتوظيف الذكاء الاصطناعي لتصفير البيروقراطية في بروتوكولات التعاون الدولي، مع ضمان أعلى معايير النزاهة والشفافية في بناء جبهة عالمية موحدة ضد التهديدات العابرة للحدود، مما يعزز ريادة الدولة كلاعب استراتيجي في حوكمة الإنترنت العالمية.

أهداف الدورة:

- استيعاب مفاهيم "السيادة السيبرانية التساهمية" وعلاقتها بالأمن القومي وتصفير البيروقراطية.
- تطوير مهارات هندسة "التحالفات الرقمية" لردع الفاعلين من غير الدول والجهات المعادية.
- إتقان فن "الإسناد التقني (Attribution) "كأداة دبلوماسية للمحاسبة الدولية بنزاهة وشفافية.
- حوكمة ممارسات التعاون القضائي والأمني (MLAT) لتصفير زمن الاستجابة للهجمات الدولية.
- تعزيز السيادة المعلوماتية عبر المشاركة الفاعلة في صياغة المعايير الدولية.(UN Norms)
- تطبيق استراتيجيات القيادة في "الردع السيبراني" وضمان المصداقية والسمعة الدولية الشاملة.

محتويات الورشة:

اليوم الأول :

فلسفة الدبلوماسية السيبرانية والرشاقة في إدارة العلاقات الدولية

هندسة النفوذ الرقمي وتصفير البيروقراطية في القنوات الدبلوماسية

- مفهوم الدبلوماسية السيبرانية 2026 وأثرها على السيادة الوطنية وجودة الحياة والريادة والنمو.
- مواءمة استراتيجيات التعاون مع مبدأ تصفير البيروقراطية عبر "المنصات الدبلوماسية المشتركة."
- تحليل العلاقة بين "الالتزام بالمعايير الدولية" وبين بناء الثقة والمصداقية في النموذج الوطني.
- تمرين هندسة الاستباقية لتصميم بروتوكول تعاون يصفّر زمن التبليغ عن الثغرات بنزاهة وشفافية.

قيادة النزاهة في حوكمة "المسؤولية الدولية" والريادة الوطنية الشاملة

- تعزيز السيادة على المواقف الوطنية في المحافل الدولية لضمان استقلاليتها وتوافقها مع القيم.
- دور القائد في حماية صورة الدولة عبر ممارسات النزاهة في صياغة "معايير السلوك المسؤول."
- بناء ثقافة "الأمان الرقمي كمنفعة عالمية" وعلاقتها بالولاء المؤسسي والأمن القومي الشامل.
- صياغة ميثاق أخلاقيات الدبلوماسي السيبراني لدعم النزاهة والقدوة والتميز في كافة المستويات.

اليوم الثاني :

السيادة التقنية وهندسة القانون الدولي في الفضاء السيبراني

تصفير البيروقراطية في "التعاون القانوني المتبادل (MLAT) "والذكاء الاصطناعي

- توظيف الذكاء الاصطناعي في تحليل المعاهدات الدولية وتصفير زمن المواءمة التشريعية بنزاهة وشفافية.
- حماية "المواقف التفاوضية السيادية" عبر أنظمة تشفير وطنية لضمان سرية المداولات والنزاهة.
- تطبيق الهوية الرقمية للاتفاقيات لتصفير الهدر البيروقراطي في إجراءات المصادقة والتحقق والنمو.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي للالتزامات الدولية والسيادة.

حوكمة الأنظمة الخوارزمية والنزاهة في "إسناد الهجمات(Cyber Attribution) "

- إدارة المسؤولية البشرية القيادية عند استخدام الذكاء الاصطناعي في إصدار "قرارات الإسناد الفني."
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير الأخطار.
- ترسيخ مفهوم الأمانة في الأدلة الرقمية لضمان المصداقية أمام المحافل القضائية الدولية والسيادة.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الردع بنزاهة تامة والتميز.

اليوم الثالث :

استراتيجيات الردع والحياد في إدارة التحالفات والشمولية

هندسة الدفاع الجماعي وتصفير البيروقراطية في تبادل المعلومات الاستخباراتية

- بناء "شبكات الثقة (Trust Networks) "التي تصفّر زمن تبادل مؤشرات الاختراق بنزاهة وشفافية والتميز.
- تفعيل الرقابة الأخلاقية على منصات الدفاع المشترك لضمان حياد النظم الرقمية في توجيه الدعم.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات الرد السيبري التي قد تغفل البعد الإنساني.
- حساب معامل الثقة في مؤشرات الإنجاز الدبلوماسي لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية الشاملة

- حوكمة الشراكات مع المنظمات الدولية لضمان توافقها مع معايير جودة الحياة والسيادة والنزاهة والنمو.
- تطوير آليات رصد الأثر الاجتماعي والسياسي للهجمات العابرة للحدود لضمان النزاهة والعدالة والتميز.
- بناء سجلات نزاهة رقمية لكل "عملية ردع" كبرى لضمان الشفافية المطلقة والوضوح والريادة والسيادة.
- تمرين محاكاة لإدارة حوار دولي حول "السيادة السيبرانية وحقوق الإنسان" بأسلوب قيادي واثق وملهم.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في الأزمات الدولية

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية الشاملة

- أخلاقيات التواصل عند اتهام جهات خارجية والموازنة بين الإبهار والوقار السيادي والنزاهة والتميز.
- الرقابة على البصمة الرقمية للبعثات الدبلوماسية لتعزيز مصداقية القرار السيادي عالمياً والريادة والنمو.
- بناء أنظمة الإفصاح الاستباقي عن نجاحات "الدبلوماسية الوقائية" لتصفير فرص انتشار الشائعات والنزاهة.
- التدقيق الأخلاقي على سلاسل توريد المعلومات الدبلوماسية لضمان خلوها من الممارسات الضارة والسيادة.

حصانة المنظومة السيادية ضد الانتهاكات المعلوماتية والتلاعب بالنتائج

- المسؤولية القيادية في التبليغ عن الثغرات التي قد تهدد أمن بنك معلومات التعاون الدولي والسيادة.
- مهارات التواصل الأخلاقي عند حدوث خروقات في "اتفاقيات السرية" لضمان استعادة الثقة ببيانات صادقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل الرقمي والتميز.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج الرصد ضد التلاعب الممنهج بالبيانات والواقع الرقمي.

اليوم الخامس :

خارطة الطريق وصناعة القائد الرقمي "الدبلوماسي" القدوة: من التعاون البروتوكولي إلى هندسة الردع السيادي الشامل

هندسة "النبض الاستراتيجي" والرشاقة السيادية في الدبلوماسية السيبرانية

- مصفوفة "النبض اللحظي" للتحالفات الرقمية: تصميم نظام رصد سيادي يعتمد على الذكاء الاصطناعي لتحويل "مؤشرات الاختراق الدولية" إلى نبضات استراتيجية تظهر للقائد فوراً، مما يصفّر زمن التبليغ المتبادل ويضمن "الإسناد الفني" للهجمات بنزاهة ومصداقية تامة أمام المحافل الدولية.
- بروتوكول "الرشاقة السيادية" للردع الجماعي: هندسة مسار قرار "صفري الإجراءات" يسمح بتفعيل اتفاقيات التعاون الأمني والقضائي آلياً فور رصد النبضة الاستراتيجية لهجوم عابر للحدود، مما يضمن سرعة ملاحقة المهاجمين وتجميد أصولهم الرقمية دون قيود بيروقراطية أو مراسلات ورقية مجهدة تعطل العدالة الرقمية.
- حوكمة "المسؤولية الدولية" والنزاهة الدبلوماسية: وضع ضوابط أخلاقية تضمن "حياد الأدلة الرقمية" المقدمة للمنظمات الدولية، وتفعيل ميثاق "النزاهة في الإسناد السيبراني" لضمان استقلال الموقف الوطني والوضوح التام أمام المجتمع الدولي.
- مختبر "هندسة التفاوض تحت الأزمة": تمرين محاكاة متقدم لاختبار قدرة القائد على إدارة "نبضة أزمة سيبرانية دولية"، وكيفية صياغة بيان "إسناد فني" رصين يحمي السمعة الوطنية ويعزز قوة الردع السيادي.

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة دبلوماسية تضمن نزاهة التعامل مع التحالفات والبيانات الوطنية بنسبة 100.%
- القدرة على هندسة منظومات تعاون رشيقة وسيادية تتوافق مع متطلبات الريادة والتميز العالمية الشاملة.
- إتقان أدوات الرقابة الأخلاقية على الأنظمة الذكية لضمان الشفافية وتصفير مخاطر الانحياز الرقمي في النتائج.
- بناء سجل ممارسات فضلى في إدارة الذكاء الاستراتيجي الدولي يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا ومدراء الشؤون القانونية، والتحول الرقمي، وأمن المعلومات في الجهات الحكومية والسيادية.
- الدبلوماسيون والملحقون التقنيون في السفارات والبعثات الدولية وفرق التعاون الدولي.
- خبراء الحوكمة والنزاهة والرقابة التقنية المعنيون بضبط جودة الامتثال للاتفاقيات الدولية.
- رؤساء فرق المهام السيبرانية ومحللو السياسات الخارجية في الهيئات الاتحادية والمحلية.

أساليب التدريب:

يتم استخدام بعض من الأساليب التالية أو الكل حسب المتطلبات لكل تخصص :

- دراسة الحالة المعقدة (Complex Case Studies)
- المحاكاة والألعاب الاستراتيجية (Simulation and War Gaming)
- ورش العمل القائمة على التفكير التصميمي (Design Thinking Workshops)
- حلقات النقاش مع خبير من القطاعين العام أوالخاص.(Expert Panels)
- المختبرات التقنية التفاعلية (Interactive Technology Labs)
- التعلم من الأقران عبر الجهات الحكومية (Inter-Agency Peer Learning)
- نهج التعلم المدمج والمستمر (Blended & Continuous Learning Approach)