تصميم استراتيجيات الأمن الوطني لمواجهة التهديدات الهجينة والناشئة

الإمارات العربية المتحدة - دبي

22 – 26/ 02 / 2026

مقدمة:

في المشهد الجيوسياسي المعقد لعام 2026، لم يعد الأمن الوطني يقتصر على حماية الحدود المادية، بل امتد ليشمل الفضاء السيبراني، والاقتصاد، والمعلومات، فيما يعرف بـ "التهديدات الهجينة". يهدف هذا البرنامج إلى تمكين القادة من هندسة استراتيجيات سيادية تصفّر البيروقراطية في اتخاذ القرار الأمني، وتوظف الذكاء الاصطناعي التنبؤي لضمان النزاهة والشفافية في مواجهة التهديدات الناشئة، مما يعزز ريادة الدولة كحصن أمني ذكي ومنيع يحقق أعلى جودة حياة لمواطنيها.

أهداف الدورة:

- استيعاب مفاهيم الأمن الوطني الشامل وعلاقتها بالسيادة الرقمية وتصفير البيروقراطية.
- تطوير مهارات هندسة "الاستراتيجيات المرنة" لمواجهة الحروب الهجينة والتضليل المعلوماتي.
- إتقان فن توظيف الذكاء الاصطناعي في محاكاة التهديدات الناشئة وبناء سيناريوهات الاستجابة.
- حوكمة ممارسات الأمن القومي لضمان التوازن بين الحماية المطلقة والنمو الاقتصادي السيادي.
- تعزيز السيادة المعلوماتية عبر بناء "منصات استراتيجية وطنية" محمية بتقنيات وطنية مستقلة.
- تطبيق استراتيجيات القيادة في إدارة "الأزمات المركبة" وضمان المصداقية والسمعة الدولية.

محتويات الورشة:

اليوم الأول :

فلسفة الأمن السيادي والرشاقة في مواجهة الحروب الهجينة

هندسة الحصانة الوطنية وتصفير البيروقراطية في التخطيط

- مفهوم التهديد الهجين وأثره على السيادة الرقمية والوطنية وجودة الحياة في عام 2026.
- مواءمة الاستراتيجيات الأمنية مع مبدأ تصفير البيروقراطية عبر أتمتة تدفق الاستخبارات الوطنية.
- تحليل العلاقة بين "الصمود المؤسسي" وبين بناء الثقة والمصداقية الدولية في النموذج الأمني للدولة.
- تمرين هندسة الاستباقية لتصميم دورة عمل تخطيطية تصفّر زمن تحديث العقيدة الأمنية بنزاهة.

اليوم الثاني :

السيادة التقنية وهندسة التنبؤ بالتهديدات الناشئة

تصفير مفاجآت المستقبل عبر الذكاء الاصطناعي والنمذجة التنبؤية

- توظيف الذكاء الاصطناعي في رصد الإشارات الضعيفة للتهديدات الناشئة وتصفير احتمالات المفاجأة.
- حماية "البيانات الاستراتيجية السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية النتائج والنزاهة.
- تطبيق الهوية الرقمية في توثيق تدفق المعلومات الاستراتيجية لتصفير الهدر البيروقراطي في التحقق.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي لمؤشرات الأمن القومي.

اليوم الثالث :

الحياد والعدالة في إدارة الأمن المجتمعي والشمولية

هندسة الحماية ضد التضليل والشمولية الرقمية في صون الهوية

- استخدام التحليلات الذكية لضمان عدالة حماية النسيج المجتمعي من حملات التضليل بنزاهة وشفافية.
- تفعيل الرقابة الأخلاقية على منصات رصد الرأي العام لضمان الشفافية وحياد النظم الرقمية.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات المواجهة التي قد تغفل البعد الإنساني.
- حساب معامل الثقة في مؤشرات الاستقرار المجتمعي لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة والنزاهة في الأزمات الهجينة

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل في الأزمات الهجينة المتسارعة والموازنة بين الإبهار والوقار السيادي الحكومي.
- الرقابة على البصمة الرقمية للالتزام بالمعايير وأثرها في تعزيز مصداقية القرار السيادي عالميًا.
- بناء أنظمة الإفصاح الاستباقي عن التهديدات المجهضة لضمان الشفافية وتصفير الشائعات المضللة.
- التدقيق الأخلاقي على سلاسل توريد التقنيات الأمنية لضمان خلوها من الممارسات الضارة والنزاهة.

اليوم الخامس :

هندسة الاستجابة الاستراتيجية وتصفير البيروقراطية في تصميم استراتيجيات الأمن الوطني والسيادة الشاملة

مختبر "العقيدة الرشيقة" وإدارة سيناريوهات التهديد الهجين والناشئ

- محاكاة "الهجوم الهجين المركب" والسيادة المعلوماتية: وضع القادة في سيناريو يحاكي تهديداً متعدد الأبعاد (سيبراني، اقتصادي، وتضليل إعلامي)، واختبار قدرتهم على استخدام "لوحات التحكم السيادية" لتوحيد الرؤية الاستراتيجية وتفعيل بروتوكول "الحصانة الوطنية" بنزاهة ووضوح تام لضمان صمود الأصول الحيوية.
- تصفير البيروقراطية في "هندسة تحديث العقيدة الأمنية": تطبيق مسار قرار صفري الإجراءات لتعديل الخطط الاستراتيجية وتخصيص الموارد الدفاعية بناءً على إشارات التهديد الناشئة، لضمان استباق الأزمات دون انتظار الدورات الإدارية التقليدية التي قد تمنح العدو فرصة للاختراق، مع الحفاظ على الحصانة القانونية والريادة العالمية الشاملة.
- هندسة "النزاهة الاستراتيجية" في مكافحة التضليل: اختبار مهارة القائد في الموازنة بين مخرجات أنظمة رصد الرأي العام المدعومة بالذكاء الاصطناعي وبين "الحكمة البشرية السيادية" لضمان عدالة الرد وصون الهوية الوطنية، ومنع أي انحيازات رقمية قد تمس النسيج المجتمعي، مما يعزز ريادة الدولة كبيئة أمنية فائقة الموثوقية والشفافية.
- ورشة "تفكيك صوامع الاستخبارات والربط السيادي": مراجعة فورية لنتائج المحاكاة باستخدام التحليلات التنبؤية لتحديد الفجوات في "منظومة الربط الاستراتيجي" بين القطاعات المختلفة، وتطوير حلول هندسية استباقية تمنع تضارب البيانات المعلوماتية، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار لبناء "رادار أمن وطني موحد".

المخرجات الرئيسية للدورة:

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

الفئة المستهدفة:

- القيادات العليا في وزارات الدفاع، والداخلية، والخارجية، والأجهزة الأمنية والسيادية.
- مسؤولو التخطيط الاستراتيجي والتميز المؤسسي وفرق تصفير البيروقراطية والتحول الرقمي.
- خبراء الحوكمة والنزاهة والرقابة الاستراتيجية المعنيون برسم السياسات الوطنية.
- رؤساء مراكز استشراف المستقبل ومحللو التهديدات الناشئة 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)