توظيف الأنظمة المستقلة والذكاء الاصطناعي في العمليات الأمنية

الإمارات العربية المتحدة - دبي

24 – 28/ 05 / 2026

مقدمة:

تمثل الممرات البحرية والمجال الجوي الشرايين الحيوية للتجارة العالمية والأمن القومي، وحمايتها في عام 2026 تتطلب تجاوز الأساليب التقليدية نحو "السيادة الرقمية" الكاملة. يهدف هذا البرنامج إلى تمكين القادة من أدوات الرصد الذكي وتوظيف التقنيات المتقدمة لتصفير البيروقراطية في إدارة المنافذ السيادية، مع ضمان أعلى معايير النزاهة والشفافية في تأمين سلاسل التوريد وحماية الأجواء، مما يعزز ريادة الدولة كمركز عالمي آمن ومبتكر.

أهداف الدورة:

- استيعاب مفاهيم "الوعي بالمجال البحري والجوي (MDA/ADA) "وعلاقتها بالسيادة الرقمية الوطنية.
- تطوير مهارات هندسة منظومات الرقابة الذكية لتصفير البيروقراطية في إدارة حركة المرور الدولية.
- إتقان فن توظيف الدرونات والأنظمة المستقلة والذكاء الاصطناعي في تأمين الممرات الاستراتيجية.
- حوكمة العمليات الأمنية لضمان التوازن بين انسيابية الحركة وبين المتطلبات السيادية الصارمة.
- تعزيز السيادة المعلوماتية عبر بناء قواعد بيانات وطنية محمية بأنظمة تشفير سيادية متطورة.
- تطبيق استراتيجيات القيادة في إدارة الأزمات العابرة للحدود وضمان المصداقية والنزاهة في التقارير.

محتويات الورشة:

اليوم الأول :

فلسفة السيادة في الأجواء والبحار والرشاقة الأمنية

هندسة الأمن القومي وتصفير البيروقراطية في إدارة المنافذ

- مفهوم السيادة الرقمية كدرع لحماية الممرات الملاحية والمجال الجوي الوطني من التهديدات الهجينة.
- مواءمة استراتيجيات الرصد مع مبدأ تصفير البيروقراطية عبر أتمتة تصاريح العبور والتدقيق اللحظي.
- تحليل العلاقة بين "الأمن الذكي" وبين بناء الثقة والمصداقية الدولية في النموذج اللوجستي للدولة.
- تمرين هندسة الاستجابة الاستباقية لتصميم دورة عمل أمنية تصفّر زمن اتخاذ القرار بنزاهة وشفافية.

قيادة النزاهة في حوكمة الأصول السيادية والريادة العالمية

- تعزيز السيادة على الأنظمة التقنية للرصد لضمان استقلاليتها وتوافقها مع القيم والهوية الوطنية.
- دور القائد في حماية صورة الدولة عبر ممارسات النزاهة في تأمين ممرات التجارة العالمية.
- بناء ثقافة "الأمن المسهل للازدهار" وعلاقتها بجودة الحياة والنمو الاقتصادي السيادي والوطني الشامل.
- صياغة ميثاق أخلاقيات قائد المنافذ السيادية لدعم النزاهة والتميز في كافة المستويات القيادية.

اليوم الثاني :

السيادة التقنية وهندسة الأنظمة المستقلة والذكاء الاصطناعي

تصفير مخاطر الاختراق عبر الدرونات والتوائم الرقمية

- توظيف الدرونات (UAVs) والزوارق غير المأهولة (USVs) في الرصد المستمر وتصفير الفجوات الأمنية.
- حماية "البيانات الملاحية السيادية" عبر أنظمة تشفير وطنية لضمان موثوقية المعلومات والنزاهة.
- تطبيق الهوية الرقمية للمركبات (Digital ID) لتصفير الهدر البيروقراطي في إجراءات التعرف والتعقب.
- تطوير لوحات تحكم سيادية (Sovereignty Dashboards) للرصد اللحظي للمجال الجوي والبحري.

حوكمة الأنظمة الخوارزمية والنزاهة في الرصد الجوي والبحري

- إدارة المسؤولية البشرية القيادية عند استخدام أنظمة التحليل الآلي في تحديد الأهداف المشبوهة.
- حوكمة مخرجات أنظمة التنبؤ لضمان الحياد الأخلاقي وتصحيح الانحيازات الرقمية في تقدير المخاطر.
- ترسيخ مفهوم الأمانة في البيانات المستقاة من الأقمار الصناعية لضمان المصداقية أمام صانع القرار.
- ورشة عمل حول ضوابط استخدام البيانات الضخمة في تحسين جودة قرارات الأمن السيادي بنزاهة تامة.

اليوم الثالث :

الحياد والعدالة في إدارة الممرات الدولية والشمولية

هندسة الحماية الشاملة والشمولية الرقمية في إدارة الملاحة

- استخدام التحليلات الذكية لضمان عدالة تقديم خدمات الملاحة لجميع الشركاء بنزاهة وشفافية مطلقة.
- تفعيل الرقابة الأخلاقية على منصات إدارة المرور لضمان الشفافية وحياد البيانات الرقمية في النتائج.
- تطبيق قاعدة الإرادة البشرية القيادية للتدخل وتعديل مسارات الأمن التي قد تغفل البعد الإنساني أو الهوية.
- حساب معامل الثقة في مؤشرات الإنجاز الأمني للممرات لتقليل احتمالات الخطأ الناتج عن الفجوات التقنية.

المسؤولية المهنية وحماية مكتسبات المجتمع والريادة الوطنية

- حوكمة الشراكات مع المنظمات الدولية (IMO/ICAO) لضمان توافق الأنظمة مع معايير السيادة والنزاهة.
- تطوير آليات رصد الأثر البيئي والاجتماعي للعمليات الأمنية لضمان النزاهة والعدالة في تقديم الخدمة.
- بناء سجلات نزاهة رقمية لكل عملية تأمين كبرى لضمان الشفافية المطلقة والوضوح التام والتميز.
- تمرين محاكاة لإدارة حوار أمني حول "حرية الملاحة والسيادة" بأسلوب قيادي واثق وملهم للشركاء.

اليوم الرابع :

المسؤولية المهنية وإدارة السمعة في الأزمات العابرة للحدود

القيادة الاتصالية وحماية السمعة الرقمية للجاهزية الوطنية

- أخلاقيات التواصل في الأزمات البحرية والجوية المتسارعة والموازنة بين الإبهار والوقار السيادي.
- الرقابة على البصمة الرقمية للالتزام الأمني وأثرها في تعزيز مصداقية القرار السيادي عالمياً والريادة.
- بناء أنظمة الإفصاح الاستباقي عن التهديدات المجهضة لضمان الشفافية وتصفير الشائعات الرقمية.
- التدقيق الأخلاقي على سلاسل توريد التقنيات الأمنية لضمان خلوها من الممارسات الضارة أو التجسسية.

حصانة الأنظمة السيادية ضد الانتهاكات المعلوماتية والتلاعب

- المسؤولية القيادية في التبليغ عن الثغرات التقنية التي قد تهدد أمن بنك المعلومات الملاحي السيادي.
- مهارات التواصل الأخلاقي عند حدوث تداخل في الترددات أو إشارات الرادار لضمان استعادة الثقة.
- إدارة التعافي المؤسسي وإعادة بناء الصورة الذهنية بعد رصد أي انحراف في قيم العمل الرقمي والمهني.
- بناء خطة الحصانة المنظومية الشاملة لتحصين نتائج العمل الأمني ضد التلاعب الممنهج بالبيانات.

اليوم الخامس :

هندسة الاستجابة السيادية وتصفير البيروقراطية في العمليات الأمنية المستقلة والذكاء الاصطناعي

مختبر "المحيط الذكي" وإدارة الجاهزية اللوجستية تحت محاكاة التهديدات العابرة للحدود

- محاكاة "الاختراق الهجين" والسيادة المعلوماتية: وضع القادة في سيناريو يحاكي محاولة اختراق لممر ملاحي أو مجال جوي سيادي عبر طائرات بدون طيار أو زوارق مسيرة معادية، واختبار قدرتهم على استخدام "لوحات التحكم السيادية" لتفعيل بروتوكول "التحييد التلقائي" بنزاهة ووضوح تام لضمان حماية الممرات الاستراتيجية دون تعطيل حركة التجارة العالمية.
- تصفير البيروقراطية في "هندسة قرار العبور": تطبيق مسار قرار صفري الإجراءات لمنح تصاريح العبور اللحظية أو اعتراض الأهداف المشبوهة بناءً على "الهوية الرقمية للمركبات" (Digital ID)، لضمان انسيابية الحركة اللوجستية في الزمن الحقيقي دون انتظار الموافقات الإدارية التقليدية التي قد تمنح التهديد فرصة للتملص، مع الحفاظ على الحصانة الرقمية والريادة العالمية.
- هندسة "النزاهة والحياد" في الرصد الجوي والبحري: اختبار مهارة القائد في الموازنة بين مخرجات أنظمة "التحليل الآلي للأهداف" وبين "الحكمة البشرية السيادية" لضمان عدالة قرارات الاعتراض، ومنع أي انحيازات خوارزمية قد تسبب أزمات ديبلوماسية أو اقتصادية، مما يعزز ريادة الدولة كمركز عالمي آمن يتسم بالشفافية المطلقة والمصداقية الدولية.
- ورشة "تفكيك صوامع البيانات الملاحية والربط السيادي": مراجعة فورية لنتائج المحاكاة باستخدام التحليلات التنبؤية لتحديد الفجوات في "منظومة الرقابة الموحدة"، وتطوير حلول هندسية استباقية تمنع تضارب البيانات بين الأقمار الصناعية والأنظمة الأرضية، مما يحقق التميز في الأداء الوطني والوضوح التام أمام صانع القرار لبناء "رادار حماية سيادي معصوم".

المخرجات الرئيسية للدورة:

- امتلاك استراتيجية حصانة سيادية تضمن نزاهة التعامل مع البيانات والمشاريع الوطنية بنسبة %.100
- القدرة على هندسة منظومات رصد 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 الأمني الاستراتيجي يدعم اتخاذ القرار القيادي الآمن والمستدام.

الفئة المستهدفة:

- القيادات العليا في القوات البحرية، الجوية، وخفر السواحل، وهيئات الطيران المدني والموانئ.
- مسؤولو التخطيط الاستراتيجي والتميز المؤسسي وفرق تصفير البيروقراطية في القطاعات الأمنية واللوجستية.
- خبراء التحول الرقمي والحوكمة والنزاهة المعنيون بتطوير أنظمة الرصد والمراقبة الذكية.
- رؤساء غرف العمليات والسيطرة والمهندسون الاستراتيجيون في البنية التحتية للمنافذ السيادية.

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)