JORNADA DE SEGURIDAD Y DEFENSA

EL CIBERESPACIO COMO NUEVO ESCENARIO DEL CONFLICTO

Hace veinte años, podría haber sido el argumento de un thriller de aeropuerto de mala calidad. Hoy en día, es una rutina. El pasado 7 de mayo, los ciberdelincuentes cerraron el oleoducto que suministraba casi la mitad del petróleo a la costa este de Estados Unidos. Para que volviera a fluir, pidieron un rescate de 4,3 millones de dólares a Colonial Pipeline Company, la propietaria. Días después, un ataque similar con petición de rescate paralizó la mayoría de los hospitales de Irlanda.

La ciberseguridad es también una cuestión de geopolítica. En la guerra convencional y en la delincuencia transfronteriza existen normas de comportamiento que ayudan a contener los riesgos. En el ámbito cibernético reinan la novedad y la confusión. ¿Un ciberataque de delincuentes tolerados por un adversario extranjero justifica las represalias? ¿Cuándo una intromisión virtual requiere una respuesta en el mundo real?

En algunos países se están formando unidades que integran organizaciones de inteligencia con unidades militares de inteligencia bajo la dirección de la agencia de inteligencia. Ejemplo es la Fuerza Cibernética Nacional del Reino Unido. Aunque se siguen creando unidades y capacidades centradas en la cibernética, siguen existiendo problemas para generar un número adecuado de personal, así como las carencias de la capacidad industrial de defensa.

La integración efectiva de las operaciones cibernéticas defensivas y ofensivas con la ciberinteligencia, la vigilancia y el reconocimiento, así como con las capacidades de ataque cinético, impone la necesidad de contar con sofisticados sistemas de gestión de la batalla.

El ciberespacio es a la vez un integrador clave y un vector de ataque para el concepto de operaciones multidominio (MDO) que sustentará algunos esfuerzos de modernización militar durante la próxima década. Estados Unidos

está trabajando en un concepto de lucha conjunta para las operaciones en todos los dominios, basado en las MDO

Los activos espaciales son esenciales para las operaciones militares en el ciberespacio. Los satélites dependen del ciberespacio para el flujo de datos que enlazan sistemas de mando, control, comunicaciones, ordenadores e inteligencia, vigilancia y reconocimiento (C4ISR).

La Fuerza Espacial estadounidense está explorando soluciones de ciberdefensa, ya que los activos espaciales son vulnerables a los ataques de denegación de servicio distribuidos o a la suplantación o captura a través del ciberespacio. Los activos basados en el espacio, como los satélites, no solo proporcionan una ciber ISR crucial, sino que también son capaces de efectos cibernéticos ofensivos.

Varios países están experimentando con la integración de la capacidad de guerra cibernética y electromagnética. El ejército estadounidense ha creado un nuevo batallón de Inteligencia, Operaciones de Información, Ciberespacio, Guerra Electrónica y Operaciones Espaciales como como parte de su concepto de Fuerza de Tarea Multidominio. El Reino Unido ha dicho que las actividades cibernéticas y electromagnéticas son interdependientes.

Para la seguridad de la OTAN, las amenazas cibernéticas son complejas, destructivas, coercitivas y cada vez más frecuentes. Así lo han demostrado recientemente incidentes pidiendo rescate y otras actividades cibernéticas maliciosas dirigidas a infraestructuras críticas e instituciones democráticas de la Alianza, que pueden tener efectos sistémicos y causar daños importantes.

Para hacer frente a este desafío en evolución, la Alianza ha aprobado en la Cumbre de Bruselas del 14 de junio, la Política Global de Ciberdefensa de la OTAN, que apoyará sus tres tareas fundamentales y la postura general de disuasión y defensa, y mejorará aún más su capacidad de recuperación.

A mayor abundamiento, la Alianza está decidida a emplear en todo momento toda la gama de capacidades para disuadir, defender y contrarrestar activamente todo el espectro de amenazas cibernéticas, incluidas las que se llevan a cabo como parte de campañas híbridas, de acuerdo con el derecho internacional.

Por otra parte, la Alianza se reafirma en que la decisión sobre cuándo un ciberataque daría lugar a la invocación del Artículo 5 sería tomada por el Consejo del Atlántico Norte caso por caso. Los aliados reconocen que el impacto de las actividades cibernéticas acumulativas maliciosas significativas podría, en determinadas circunstancias, considerarse como un ataque armado.

Asimismo, la Alianza siempre está comprometida a actuar de acuerdo con el derecho internacional, incluida la Carta de las Naciones Unidas, el derecho internacional humanitario y el derecho internacional de los derechos humanos, según corresponda. Su intención es promover un ciberespacio libre, abierto, pacífico y seguro, al mismo tiempo que se esforzará por mejorar la estabilidad y

reducir el riesgo de conflicto apoyando el derecho internacional y las normas voluntarias de comportamiento estatal responsable en el ciberespacio.

Por último, la OTAN, como organización, seguirá adaptando y mejorando sus ciberdefensas. Cinco años después de la adopción de su Compromiso de Ciberdefensa, sigue comprometida con el mantenimiento de unas ciberdefensas nacionales sólidas con carácter prioritario, al mismo tiempo que continúa implementando el ciberespacio como dominio de operaciones.

Objeto

Realizar unas Jornadas de Seguridad y Defensa en el que se debata entre calificados expertos y analistas representantes de varios segmentos e instituciones de la sociedad española sobre *el ciberespacio como nuevo escenario del conflicto* teniendo presente el gran protagonismo global que está adquiriendo la dimensión del ciberespacio en el campo económico, tecnológico, diplomático, en el de las empresas digitales o en el militar ante el cambio de era que se avecina en el entorno del primer tercio del siglo XXI así como cuál es el efecto que puede producir en el sistema geopolítico de seguridad y estabilidad internacional.

Lugar, Hora y Fecha

Lugar
Salón de ISDEFE
C/Beatriz de Bobadilla 3
28040 MADRID

Fecha y hora
9 de febrero de 2022
De 17.00 h a 19.30 h

Programa de la Jornada

17.00 h

Inauguración

Jesús Alonso. Representante de ISDEFE

Antonio Núñez García-Saúco. Embajador de España. Presidente del Instituto Europeo de Estudios Internacionales (IEEI)

David Santos. Presidente de la Asociación de Alumnos de Altos Estudios de la Defensa (ADALEDE)

Jesús Argumosa Pila. General de División (R). Presidente de la Asociación Española de Militares Escritores (AEME).

17,15 h

Conferencia inaugural: *La geopolítica del ciberespacio*, a cargo de **Shaun Riordan**. Director Cátedra Diplomacia y Ciberespacio del IEEI.

17.45 h.

Mesa Redonda: *El ciberespacio como nuevo escenario del conflicto*

Moderador

Almirante (R) Juan Rodríguez Garat. Ex Almirante de la FLOTA (ALFLOT). Asociado de AEME.

Ponentes

GD. Rafael García Hernández. General Director del Mando Conjunto del Ciberespacio

Las operaciones militares en el ciberespacio

TG (R) Rubén García Servet. Ex Jefe del Centro de Operaciones Combinadas de la OTAN (CAOC) de Torrejón. Miembro de ADALEDE

El ciberespacio en la OTAN

César Ramos. Director General de TEDAE

Impacto del ciberespacio en la industria y tecnología de Defensa

19.00 h

Coloquio

19.30 h

CLAUSURA

TG. Fernando García González-Valerio. Jefe del Estado Mayor Conjunto (JEMACON).

Madrid, 17 de enero de 2022