vt

mi+d

informe de vigilancia tecnológica

serie
informes de tecnologías clave de la Comisión Europea

tecnología emergente en el contexto de seguridad

tecnología emergente en el contexto de seguridad

vt
CE
2

www.madrimasd.org

Acción Innovadora

mi+d

vt

mi+d

informe de vigilancia tecnológica

serie
informes de tecnologías clave de la Comisión Europea

tecnología emergente en el contexto de seguridad

www.madrimasd.org

Acción Innovadora

mi+d

Edición española coordinada por:

círculo de innovación cimtan en materiales, tecnología aeroespacial y nanotecnología

Revisado por: Carmen Rúa Morán
Carlos Prieto Saiz

Traducidos con el permiso de la CE.

índice

CAPÍTULO 1

Plano general

El 12 de diciembre de 2003, el Consejo Europeo adoptó una estrategia para la seguridad europea "Una Europa segura en un mundo mejor". Este documento proporciona el marco para la actividad europea concertada en el campo de la seguridad y, más específicamente, en actividades para anticiparse y solucionar con más eficacia las nuevas amenazas de la seguridad tales como el terrorismo, la proliferación de armas de destrucción masiva, estados que fracasan, conflictos locales y el crimen organizado.

La necesidad de emprender una acción en el terreno de la seguridad, se enfatizó con una serie de acontecimientos causados por la actividad terrorista en Madrid y en Londres o por desastres naturales con el maremoto conocido como Tsunami.

La comunidad de investigación europea respondió a esta necesidad. En marzo de 2004, la Comisión Europea lanzó su Acción Preparatoria para la Investigación de Seguridad (PASR) y el Grupo de Personalidades convocado en su informe "Investigación para una Europa Segura", la creación de un "Programa para la investigación de la Seguridad Europea" (ESRP).

De particular relevancia para preparar el contenido de este ESPR figuran las llamadas actividades de "road-mapping" (trazado de carreteras en mapas) (SeNTRE y ESSRT) que la Comisión Europea ha contratado bajo la primera llamada del PASR. Las actividades del "road-mapping" (SeNTRE y ESSRT), producirá un extenso análisis estratégico hacia donde las actividades de investigación deberían ser enfocadas prioritariamente.

CAPÍTULO 2

Retos socioeconómicos

2.1 Definición de seguridad

COM(2004) 72 define la seguridad como "un concepto en desarrollo" que "representa muchos retos para la UE-25 impactando sobre una amplia extensión de políticas existentes y emergentes en la UE, sobre las preocupaciones de los ciudadanos, incluyendo la protección de las amenazas del terrorismo, así como la adaptación de estructuras de gobierno para tratar con eficacia estas materias".

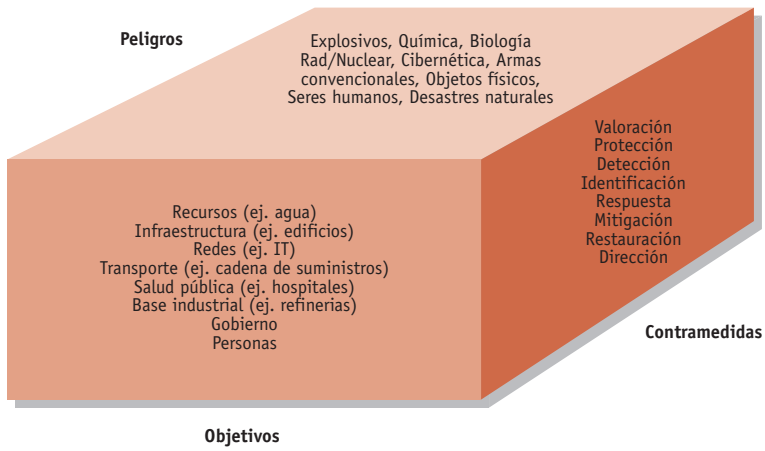
Ya que esta definición es más bien vaga y tiende a limitar el aspecto de seguridad a terrorismo y antiterrorismo, se sugiere adoptar, para el propósito de este informe, una definición que amplíe este ámbito, incluyendo también al crimen organizado como por ejemplo el tráfico ilegal, la inmigración ilegal, el contrabando, etc. Así como la necesidad de realzar las capacidades para combatir los desastres naturales tales como son las inundaciones, incendios forestales, etc.

El CEN BT/WG 161 sobre la Protección y Seguridad del Ciudadano adoptó la siguiente definición en Enero de 2005:

La seguridad es la condición (percibida o confirmada) de un individuo, una comunidad, una institución social, un estado y sus posesiones (tales como mercancías, infraestructuras) para ser protegida contra el peligro o amenazas como son la actividad criminal u otros actos deliberados u hostiles, así como desastres, ya sean naturales o provocados por la mano del hombre.

2.2 Modelo para la seguridad

La estructura para esta definición abajo mostrada se ilustra en el modelo de seguridad que figura a continuación y que fue presentado por el Grupo Consultivo sobre Seguridad ISO en el año 2004 (ISO/TMB AGS N 46, fechado el 6/1/2005) y adoptado por el CEN BT/WG 161.



El modelo proporciona un marco para clasificar aspectos de seguridad en tres dimensiones: ***objetivos***, ***peligros*** y ***contramedidas***.

Los ***objetivos*** son las entidades, incluyendo a las personas, las cosas y los procesos que son vulnerables a las amenazas y necesitan ser protegidas. Los objetivos pueden ser clasificados en varias categorías como queda reflejado en el modelo de seguridad arriba expuesto:

- *Recursos* comprende la calidad del agua, el terreno y el aire e incluye recursos energéticos naturales y la cadena de suministro de alimentos así como plantas y animales.
- *Infraestructuras* se refiere a construcciones de todo tipo, incluyendo pantanos de agua, y cubre las redes distribuidas tales como los sistemas de suministro de agua así como las redes de distribución de energía (ej. oleoductos de gas y petróleo). También considera el sistema de financiación.
- *Información*, *Ordenadores* y *Comunicación* incluye sistemas de información informáticos, sistemas para compartir información y redes de comunicación, pública (radiodifusión) así como comunicaciones de emergencia. También se refiere a los servicios postales.
- *Transporte* comprende redes de transporte por aire tierra y mar, y vehículos. También considera la cadena de suministro de transporte, incluyendo el transporte en contenedores.
- *Salud Pública / Seguridad* incluye todos los aspectos del sistema de la salud pública y los servicios de emergencia (ej. Bomberos, ambulancias, policía).

- *Base Industrial* comprende refinerías, centrales eléctricas, tanques de gas, plantas químicas, etc. y cualquier estructura que produzca, en potencia, materiales peligrosos. Pone especial atención en las instalaciones de proceso nuclear y la cadena de suministro de defensa.
- *Gobierno* (todos los niveles) se refiere a funciones de mando y control, servicios de inteligencia/información y continuidad de las operaciones.
- *Personas* incluye a todos los individuos, incluyendo sus propiedades así como sus derechos, ética, etc.

Peligros son los medios que pueden ser objeto de ataque y por lo tanto dañados. Los objetivos pueden ser clasificados dentro de varias categorías que a continuación se citan:

- *Explosivos*
- *Agentes Químicos*
- *Agentes Biológicos*
- *Material Nuclear radiológico*
- *Cibernética* incluye virus de ordenador, falta de servicio, "hacking" (daños producidos por intromisión de los conocidos "hackers", trucos, suplantación de identidad, etc.).
- *Armas convencionales* comprende armas ligeras, cuchillos, etc.
- *Objetos comunes utilizados en atentados* comprende el uso de un objeto o un vehículo, como pueden ser un avión o un camión, utilizados como arma (ej. el atentado con avión sobre las Torres Gemelas de Nueva York, al Pentágono).
- *Seres Humanos* incluye a grupos terroristas, criminales, etc.
- *Desastres Naturales* incluye terremotos, incendios, inundaciones, tormentas, etc.

Contramedidas son los sistemas, métodos y herramientas que se usan para impedir o responder las amenazas contra objetivos. Las contramedidas pueden ser clasificadas dentro de varias categorías que a continuación se citan:

- *Evaluación*.
- *Protección*.
- *Detección*.
- *Identificación*.
- *Respuesta*.
- *Mitigación*.
- *Restauración*.
- *Dirección*.

2.3 Modelos de seguridad

Tanto ISO/TMB AGS N 46 como CEN BT/WG 161 lanzaron inventarios sistemáticos sobre necesidades de capacidad por parte de los interesados en seguridad, con el objeto de identificar su uso en los modelos de seguridad y las preocupaciones con las tienen que hacer frente a este problema. El inventario es un continuo proceso y necesita sin falta ser puesto al día regularmente. Sin embargo, a continuación vemos reflejada una tendencia en el esquema que sigue:

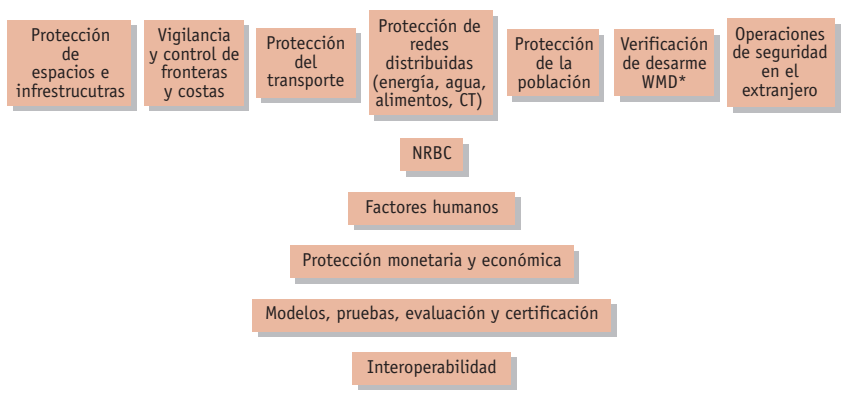
Aspecto general	*Detalles*	*Comentarios*
CBRN*	Prevención y contenido: "Antes, durante y después" enfoque de conjunto, incluyendo proceso de descontaminación para personas y lugares; Código de buena puesta en práctica para los primeros en reaccionar. Criterio de exposición para la población civil.	
Servicios de Emergencia	Equipo de emergencia, procedimientos de emergencia, servicios de post-trauma y formación (incluyendo traumas psíquicos)	
Seguridad de transporte	Calificación de Inteligencia sobre exportadores conocidos, evaluación de competencias para los agentes de seguridad, sellado/cierre y similares.	
Autentificación/ identificación	Protección del derecho de apropiación, lucha contra la suplantación de identidad; identificación de contenedores; firma digital para documentos legalmente obligatorios y cambio de datos.	
Información y comunicación	El Sistema de Dirección para la Seguridad de la Información (ISMS), la interoperabilidad de comunicaciones en las operaciones de protección civil.	ISMS
Seguridad física y servicios de seguridad.	Servicios de seguridad gestionados de forma privada. Evaluación de riesgos de armas ordinarias.	Actividad en CEN/BTTF 167. Servicios de seguridad
Seguridad de infraestructuras	Ej. Seguridad de los oleoductos para mercancía peligrosa, identificación de los puntos críticos en los locales y plantas. Evaluación de riesgo por medio de ordenador.	
Información de seguridad para público en general	"Antes, durante y después" enfoque de conjunto para asegurar mensajes claros y concisos	Prioridad menor
Obtención pública	"La mejor compra" especificación, interoperabilidad	Prioridad menor

* *CBRN*: Armas químicas, bacteriológicas, radiológicas y nucleares.

2.4 Misiones de seguridad

Respecto a objetivos sobre edificios, peligros y contramedidas, se puede desarrollar un enfoque de conjunto que identifique la seguridad y las actividades relacionadas con la seguridad, así como misiones y competencias necesarias para hacer frente a la protección, sostenibilidad y manejo de la que se observa como un medio ambiente seguro.

Misión de seguridad general



* *WMD*: Armas de destrucción masiva

La *protección de espacios e infraestructuras* comprende la protección de infraestructuras públicas, edificios gubernamentales, empresas de servicio público, puertos, aeropuertos, estaciones de ferrocarril y también se dirige hacia la protección de espacios de riesgo tales como factorías químicas, plantas nucleares, etc.

La *vigilancia y control de fronteras y costas* incluye la vigilancia y control de las fronteras azules y verdes así como la vigilancia del espacio aéreo. Comprende temas como el tráfico ilegal (ej. armas, drogas), emigración ilegal, falsificaciones, etc.

La *protección del transporte* se dirige hacia la protección de vehículos terrestres, marítimos y aéreos así como las infraestructuras de apoyo, incluyendo la polución. El transporte se considera como un objetivo posible pero también en el papel de posible arma.

La *protección de redes distribuidas* comprende redes que están extendidas (distribuidas) sobre grandes zonas geográficas, tales como las redes de suministro de energía (petróleo, gas, electricidad), los alimentos y la cadena de suministro de agua, etc. también incluye la protección de las redes de información y comunicación así como sus datos.

La *protección de la población* se dirige hacia las personas, ya sean como individuos o en grupos. Este tema cubre una amplia variedad de aspectos, que van desde vulnerabilidades específicas hasta el comportamiento humano en situaciones de crisis. Se prestará una atención específica a aquellas personas que tienen un papel crucial en la prevención y/o manejo de incidentes, crisis o desastres tales como las fuerzas de emergencia, los primeros en actuar y los que hacen cumplir la ley.

La *misión de verificación de desarme – armas de destrucción masiva* considera la capacidad necesaria para marcar y rastrear, y también incluye una vigilancia intensiva de los espacios.

Las *operaciones de seguridad en el extranjero* cubren los aspectos de operaciones humanitarias, apoyo en el manejo de crisis civiles, para conflictos en zonas fueras de la UE así como operaciones de evacuación.

Las cinco misiones horizontales son relevantes para las siete misiones verticales. Necesitan ser dirigidas sistemáticamente bajo cada una de las siete misiones verticales, ya que conciernen aspectos específicos de las capacidades requeridas para llevar a cabo las misiones verticales de un modo adecuado y global. Estas misiones horizontales son:

- *NBRC (prevención, detección, protección y descontaminación)*
- *Factores humanos*
- *Protección monetaria y económica*
- *Modelos, pruebas, evaluación y certificación*
- *Interoperabilidad*

CAPÍTULO 3

Análisis de SWOTS (puntos fuertes, puntos débiles, oportunidades y peligros)

3.1 Peligros

La comunidad de investigación e industria europea tiene una excelente habilidad para apoyar y desarrollar más allá su contribución para enfrentarse a los problemas diarios de seguridad, por ejemplo los sensores mundiales de todo tipo, las capacidades generadoras de redes (NEC), etc.

Esta sección proporciona una vista general sobre lo que son estas fuertes aptitudes y/o para que necesitarían ser desarrolladas. Al objeto de estructurar esta vista general, esta sección, para cada una de las misiones de seguridad y submisiones identificadas en la sección 2.4, dará una indicación de medidas de apoyo útil, describirá las tecnologías o herramientas de soporte requeridas así como ejemplos de integración y validación útiles.

El valor de simulación y de herramientas de formación se ilustrará en unos pocos ejemplos.

3.1.1 Protección de Espacios e Infraestructura

3.1.1.1 *Protección de Espacios*

Medidas de apoyo

- Trazado de los espacios críticos incluyendo la evaluación del medio ambiente, la situación actual y los riesgos en potencia.
- Arquitectura de sistemas incluyendo procedimientos de apoyo en caso de desastre (plan de emergencia).

Tecnologías o herramientas de apoyo

- Sensores:
  - Microtecnologías para sensores (vigilancia, rastreo y detección NRBC,...)
  - Sensores avanzados e ingeniosos de bajo coste y nuevas técnicas para vigilancia discreta
  - Cámara inteligente
  - Sensores autónomos y seguimiento automatizado en un campo
  - Red de sensores extendidos sobre el terreno en el aire o en el espacio
- Seguridad de red e integridad de datos entre los sensores distribuidos
- Enlaces de datos de banda ancha inalámbricos fijados para sistema informático fijo
- Comunicaciones fijas e interoperables (videoconferencias, teléfono móvil, WiFi): información personal y sistemas de comunicación con mayor realismo (“video, comunicaciones en Palm”)

- Protección de redes contra el medioambiente adverso (incluyendo armas de energía dirigida, láser, HPM,...)
- Modelo de reconocimiento: obtención de información de imágenes de baja calidad/sistemas artificiales de inteligencia
- Control de acceso no cooperativo
  - Puntos de revisión (característica de objeto y persona – imagen, rayos X, 3D, neutrón,... -, Bases de Datos)
  - Localización de compañeros civiles
- Materiales ligeros para protección humana y de espacios

Simulación y preparación

- Predicción de vulnerabilidad de estructuras después de las explosiones y soluciones estructurales
- Red de sensores existentes (bosque de sensores)
- Enlaces de datos de banda ancha inalámbricos (para bosque de sensores)
- Fusión de datos
- Interoperabilidad
- Clasificación industrial estándar personal con realidad aumentada
- Simulación de sensores
- Componentes y equipos de supervivencia
- Modelado y simulación avanzados del comportamiento humano:
  - Predicción del comportamiento en masa (con inmersión...)
  - Simulación para la toma de decisiones
- Cooperación de Video-Tag Biométrico

Integración y validación

- Video-demostrador de vigilancia avanzado (detección, rastreo, reconocimiento, identificación con cámaras móviles y fijas)
- Herramienta de simulación general para facilitar lo que se elige, de asistencia de procedimiento y asesoramiento de actuación
- Simulador de entrenamiento (métodos y herramientas para toma de decisiones antes y durante las operaciones)
- Proceso de datos y sensores y demostrador de fusión (para conseguir el Dibujo Global [Mundial] de Riesgos desde los datos del satélite a los micro UAVs [vehículos aéreos no tripulados] y rastreadores en el punto de comprobación...) para Vigilancia/Detección/Verificación...

3.1.1.2 *Infraestructuras públicas y protección de edificios públicos*

Medidas de apoyo

- Trazado en mapa de las instalaciones civiles europeas importantes (estacionesde metro y tren, estadios grandes, bancos, edificios gubernamentales, hospitales,...), evaluación de riesgo y peligro, prioridad contra aquello que se puede aportar

Tecnologías o herramientas de apoyo

- Sistemas de vigilancia y reconocimiento
- Nuevos materiales (vidrios,...)
- Localización y protección de NRBC, en particular la intoxicación y polución del aire
  - Sensores C de bajo coste
  - Sensores B
- Sistemas de advertencia a la población
- Conceptos de dirección de las consecuencias y evacuación

3.1.1.3 *Protección de empresas de servicio públicos*

Medidas de apoyo

- Trazado en mapas de las infraestructuras europeas para la alimentación, el agua, la agricultura, la energía (eléctrica, gas y petróleo, presas), telecomunicación, etc. y riesgo relacionado, así como la evaluación de peligros

Tecnologías o herramientas de apoyo

- Simulaciones (teorías del caos...)
- Protección del suministro de agua (localización de peligros poco corrientes y biológicos)
- Contaminación e intoxicación de la agricultura (lechos acuíferos, ríos, terreno, aire...). Virus en cosechas y en animales
- Control de alimentos
- Protección de las plantas de energía y redes de telecomunicación (vigilancia, sistemas de energía de apoyo [reserva]...)
- Sensores BC (capacidad del portador) para habitáculos públicos reducidos
- Materiales ligeros para la protección humana

Integración/validación

- Microvehículo demostrador aéreo no tripulado (micro-AV) con sensores BC en miniatura o sensores de vigilancia
- Personal nomade C2 con realidad aumentada

3.1.1.4 *Protección de espacios peligrosos*

Medidas de apoyo

- Construir y mantener una evaluación general de las infraestructuras europeas con un potencial de catástrofe (plantas de energía nuclear, instalaciones químicas, oleoductos, puertos, ...)

Tecnologías o herramientas de apoyo

- Sensores de largo alcance BC
- Protección EM
- Simulaciones (teorías del caos ...)
- Conceptos de análisis del impacto y reducción del mismo
- Sistemas de aviso a la población
- Evacuación y conceptos de dirección sobre las consecuencias
- Técnicas de descontaminación, primeros auxilios y su equipo de protección
- Supervivencia de componentes y de material.
- Predicción de la vulnerabilidad de las estructuras después de las explosiones y soluciones estructurales
- Protección y supervivencia de sistemas contra DEW (línea de aviso a distancia)(láser, HPM [material de producción peligroso])

Integración/validación

- Ruido electrónico
- Demostrador MAV para vigilancia
- Contenedores autoprotegidos (resistentes a explosión ...), con sensores químicos en un "chip"

3.1.1.5 *Protección de puertos*

Medidas de apoyo

- Estudios específicos para su utilización en tecnologías de defensa (capacidad)
- Protección en instalaciones a poca distancia de la costa (petróleo, molinos de energía eólica)
- "Puerto seguro" (estudio de viabilidad, evaluación del material más moderno, análisis del lugar de los hechos, definición de sistema)

Tecnologías o herramientas de apoyo

- Vigilancia a gran escala con multisensores
  - Sistemas de radar
  - Detectores ópticos, óptico-electrónicos, visión nocturna
  - Satélites
- Tecnología de defensa para
  - Sistemas de protección para minisubmarinos
  - Sistemas de vigilancia acústicos (para navegación ilegal)
- Vigilancia IR(infrarrojos)/óptica
- Vehículos submarinos no tripulados (UUVs)
- Refugios navales (con *chips*, estructura ligera antiexplosiva)

3.1.1.6 *Protección de aeropuertos*

Medidas de apoyo

- Estudios específicos para la utilización de las tecnologías de defensa (capacidad)
- Protección de las instalaciones cercanas a la costa (petróleo y molinos de energía eólica)
- «Puerto seguro» (estudio de viabilidad, evaluación del material más moderno, análisis del lugar de los hechos, definición de sistema)

Tecnologías o herramientas de apoyo

- Vigilancia a gran escala con multisensores, con el apoyo de satélites, etc.
- Sistemas de comunicación segura
- Arco de seguridad (para viajeros en correlación con equipaje verificado)
- Interoperabilidad segura con bases de datos para visados y otros instrumentos necesarios para el apoyo de la dirección de fronteras integradas

Integración/validación

- Contenedor inteligente
- Puerta de control integrada
- Endurecimiento contra el ruido electrónico
- Microaparato UAV de demostración para vigilancia, etc.

3.1.2 Dirección de fronteras integradas

3.1.2.1 *Vigilancia de fronteras*

Medidas de apoyo

- Vigilancia de fronteras a tiempo real, mando y control (inteligencia incluida)
- Control de acceso: control de entrada y salida «zona Schengen»

Tecnologías o herramientas de apoyo

- Observación/localización
  - Sensores autónomos y dependientes (aviso inmediato, terreno, globos,..., desde radar en tierra a vigilancia por video a rastreadores, sensores silenciosos)
  - Sensores óptico-electrónicos: de corto y largo alcance, en superficie y en aire, visión nocturna
  - Localización remota a través de sensores (lásers, UAVs [vehículos aéreos no tripulados],...)
  - Microsistemas/nanotecnologías...
  - Red de sensores pequeña, desechable y autoconfigurante
  - «Bosque de sensores» en tierra, aire y espacio
  - Materiales nuevos como sensores: reaccionan a las variaciones del medio ambiente (cambian de color...), defensas electromagnéticas, sensores sísmicos, vigilantes infrarrojos
- Comunicación y radiocomunicación
  - Teléfono móvil interoperable, WiFi, banda ancha (imagen de video/global, multisensores), distribuidos (entre 100.000 sensores... [tales como teléfonos móviles o PMR (comunicaciones móviles privados)] o satélites), protegidos (encriptados), análisis de espectro muy rápido (datos, voces), control GSM
- Identificación incluyendo biometría, localización rápida (tarjeta identificativa NRBC y pasaporte falsificado)
- Sistemas de control de acceso
  - Cooperativo y no cooperativo (cámara en un ordenador...), preautorización automática (niveles de espacio libre, pista rápida), puntos sobresalientes en el análisis de los datos en bruto
  - Localización de puestos de control (característica de objeto y persona): imagen, onda milimétrica, rayos X, 3D, neutrón), bases de datos
  - Intercambios de información y bases de datos interoperables paras lograr una valoración global

Integración/validación

- Aparato de demostración de vigilancia de fronteras que incluye, por lo menos, un puesto de control
- Microaparato UAV de demostración para control de fronteras

3.1.2.2 *Control de inmigración ilegal*

Medidas de apoyo

- Vigilancia estadística de fronteras (identificación de caminos,...)
- Sensores autónomos
- Instalaciones para inmigración y visados integradas e interconectadas
- Biometría
  - Permanente y no permanente: reconocimiento de rostro, cartografía térmica, huellas dactilares, iris/retina, forma de las manos, forma de las orejas
  - Comportamiento: voz, caligrafía, firma,
  - False Reject Ratio (se refiere a la probabilidad de rechazar como falsa una huella dactilar que debería ser aceptada como perteneciente al sujeto en verificación)

Integración/validación

- Aparato de demostración de puesto de control
- Verificación óptica y biológica con sistemas de sensores de reconocimiento

3.1.2.3 *Protección de costas y fronteras*

Medidas de apoyo

- Definición de un sistema factible para la realización de misiones de vigilancia costera (incluyendo misiones como tráfico de buques (rutas marítimas), búsqueda y rescate, asistencia a barcos, polución, lucha contra incendios, inmigración ilegal, contrabando de drogas en tiempo de paz así como aterrizajes terroristas y ataques en tiempo de "crisis de guerra") en una determinada zona (incluyendo puertos que constituyen HTV's (Objetivos de Máxima Importancia), estudios de intercambio comercial (eficacia, índice de localización, adaptabilidad, modulación ...)

Tecnologías y herramientas de apoyo

- Radares (para peligros en superficie y en el aire) : radar aéreo con imágenes (SAR e ISAR) radares costeros transportables
- Asentamientos de vigilancia de red (lugares fijos y movibles)
- Proceso de datos de imágenes, banda ancha, fusión de datos

- Sensores que incluyen EO activo (láser) y pasivo
- Integración de equipamiento
- Autonomía
- Sistemas sólidos de control de vuelos
- Certificación de sistemas (inclusión de UAVs [vehículos aéreos no tripulados] en dirección de tráfico aéreo civil)

Integración y validación

- Aparato de demostración de viabilidad avanzado para la vigilancia costera utilizando varios medios (UAVs [vehículos aéreos no tripulados], patrulla marítima aérea, helicópteros, comunicación por satélite, estación en tierra incluyendo móvil ...)

3.1.2.4 *Tráfico ilegal (drogas, armas, munición, explosivos)*

Medidas de apoyo

- Metodología de marcado y rastreo

Tecnología y herramientas de apoyo

- Detectores NRBC en puestos de control
- Labs on a chip (Se trata de una tecnología avanzada
- Identificación y rastreo de productos intermediarios
- Sensores químicos
- Sensores compactos con diodos láser ajustables para localización de mezcla de explosivos
- Etiquetas inteligentes
- Marcado duradero
- Marcado secreto

Integración/validación

- Disponibilidad de datos de base-redes mundial (estandarización/legal/política aceptable)

3.1.3 Protección de redes distribuidas

3.1.3.1 *Protección de la distribución y suministro de redes*

Medidas de apoyo

- Evaluación de riesgo IEM para redes de telecomunicación

Tecnologías o herramientas de apoyo

- Protección IEM
- Vigilancia de redes de petróleo/gas
  - Dentro de Europa: sensores miniaturizados, recopilación de datos, proceso
  - Fuera de Europa: a través del aire incluyendo observación

UAV/espacial (por radar principalmente)

- Distribución de agua
- Vigilancia de presas
  - Desde satélites a microsensores en el suministro de agua
  - Protección de suministro de agua (localización de peligros inusuales y biológicos)
  - Limpieza de aire/agua y sistemas de filtración

Integración/validación

- Redes civiles de comunicación habituales de bajo coste EM

3.1.3.2 *Información y protección de sistemas de información*

Medidas de apoyo

- Recopilación del servicio de información
- Algoritmos adaptables y pasivos para el proceso de datos/imágenes/señales

Tecnologías o herramientas de apoyo

- Técnicas de defensa y ataque eficaces EW/TW, medidas y contramedidas
- Seguridad cibernética incluyendo la propia disuasión cibernética
- Criptología y dirección clave
- Prevención e identificación de atentados
  - Web de servicio de información (colocación de minas con amplios datos)
  - Localización rápida desde sucesos poco reflejados en estadísticas
  - Técnicas no cooperativas IFF
- Protección de bases de datos y búsqueda dentro del contexto
- Redes y comunicaciones aseguradas independientes de protocolo. Sistemas sólidos de comunicación y multimodo. Comunicaciones movibles reconfigurables
- Acceso de banda ancha a usuarios movibles en situaciones dinámicas/lugares difíciles de tipo electromagnético.
- Localización de sistemas de comunicación “standard” para usuarios no cooperativos

- Penetración no cooperativa de sistemas electrónicos sospechosos
- Sistemas de muestra de factores en formato pequeño

Integración/validación

- Aparato de demostración C3 endurecido EM

3.1.4 Protección de transporte

3.1.4.1 *Protección de transporte terrestre*

Medidas de apoyo

- Trazado en mapas de zonas críticas en infraestructuras ferroviarias y de carreteras (conexiones a autopistas, puentes, túneles, etc.) y riesgo relacionado así como evaluación de peligros.

Tecnologías y herramientas de apoyo

- Posicionamientos/puesta en práctica de rastreo (cf. Galileo)
    - Dirección de flota
    - Dirección integrada de recursos movibles
- Contenedores
    - Posicionamiento y rastreo
    - Contenedor autoprotegido (resistente a explosiones...) con sensores en un "chip"
    - Protección y supervivencia de sistemas contra DEW (línea de aviso a distancia) (láser, HPM [material de producción peligroso])
- Seguridad en terminales, almacenes y centros de distribución de materiales delicados (vigilancia con vídeo inalámbrico y vigilancia Opto)
- Protección de sistemas automatizados, procedimientos de documentación y tecnología de información para mando operacional y centros de control
- Protección de infraestructura ferroviaria y por carretera y localización de aspectos echados en falta.

Integración/validación

- Aparato de demostración de dirección de flota
- Aparato de demostración de recipiente "inteligente"

3.1.4.2 *Protección de transporte marítimo*

Tecnologías y herramientas de apoyo

- Navegación rastreo (incluso no cooperativo por recopilación de datos)
- Inspección regular de zonas marítimas y costeras críticas (espaciales y aéreas) para desechar signos falsos en momentos de crisis
- Localización de minas
- Protección de secuestro aéreo
- Simulación y modelos de polución (toxinas específicas / químicas ...., NRBC)
- Prevención de desastres producidos por la polución y equipamiento de dirección
- Recipientes autoprotegidos (resistentes a explosiones...) con sensores químicos en "chips"
- Predicción de vulnerabilidad en estructuras después de explosiones y soluciones estructurales
- Protección contra medio ambiente problemático EM
- Protección y supervivencia de sistemas contra DEW (línea de aviso a distancia) (láser, HPM[material de producción peligroso])

Integración/validación

- Aparato de demostración contenedor naval

3.1.4.3 *Peligros submarinos (minas marítimas incluidas)*

Medidas de apoyo

- Transferibles desde tecnologías de guerra submarina

Tecnologías y herramientas de apoyo

- Localización a distancia de minas (vuelo sobre el lugar)
  - Soluciones EM
  - Soluciones opticoelectrónicas con láser
- Minisubmarino de transporte
- Rastreadores de fondos
- Sonar de localización de submarinos
- Nuevas tecnologías de sensores de bajo coste para un impresionante conjunto submarino y magnético en caso de localización de amenaza pasiva y desarrollo de nuevas tecnologías de transformación tales como un micrófono o un motor eléctrico en otro tipo de energía , en caso de amenazas activas
- Innovador proceso de señales para la localización de objetos pequeños en un ambiente con reverberación

- Proceso innovador de clasificación y fusión de datos sobre los peligros acústicos y magnéticos detectados que están basados en una nueva metodología de inteligencia artificial
- Radar avanzado de baja energía de alta resolución e interceptación de pequeños objetivos en movimiento que están en desorden, asociados con una energía transmitida con un bajo pico de actuación al objeto de no dañar a las personas.
- Aparato de rayos infrarrojos con protección ocular e integración modular del sensor EO, con independencia de las características del terreno

3.1.4.4 *Protección del transporte aéreo*

Tecnologías y herramientas de apoyo

- Materiales ligeros para protección de aviones (blindaje ligero, etc.)
- Protección de SIC (clasificación industrial estándar)
- Comunicación en banda anc ha
- Detector electrónico de ruido

Simulación

- Simulación de sensores
- Componentes y equipo de supervivencia
- Predicción de la vulnerabilidad de las estructuras aéreas después de las explosiones y soluciones de estructura
- Protección y supervivencia de sistemas contra DEW (línea de aviso a distancia) como láser, HPM (material de producción peligrosa)

Integración/validación

- Sistemas de localización de sistemas BC (capacidad del portador) para aeropuertos
- Fuselaje con estructura NG, resistente a explosiones (después de predicción de vulnerabilidad y protección contra explosiones, también aplicable al uso de helicópteros para evacuación y protección de explosiones)
- Contenedor autoprotegido para aviones
- Sistemas de vigilancia de aparatos de demostración de contenedores (con “chips”)
- Protección para aviones civiles de atentados terroristas tales como Manpads (misiles antiaéreos portátiles) o rayo láser cegador: señuelos y contramedidas e infrarrojos
- Doseles endurecidos y muros de vidrio (contra láser, HPM)

3.1.4.5 *Armas no letales adaptadas al interior de aviones*

Información de apoyo

- Evaluación de riesgo del efecto LTLW en espacios cerrados
- Riesgo (lo que pueda ocurrir) en situaciones de despresurización

Tecnologías y herramientas de apoyo

- Marcado de aparatos
- Miniaturización
- Barreras de detención MFP
- Linterna láser para deslumbrar
- Lasers dolorosos
- Sonidos dirigidos de alta energía
- Lanzagranadas LTL
- Efectos LTLW a largo plazo – Antídoto
- Tecnologías de recuperación para aviones
- Simulación
- Comunicación segura con tierra
- Mini-robots

Integración/validación

- Tripulación/adiestramiento de personal de cabina y formación de usuarios

3.1.4.6 *Protección de transporte legal de mercancía delicada y peligrosa*

Información de apoyo

- Metodologías de rastreo y marcado/estudios de casos

Tecnologías y herramientas de apoyo

- Contenedores asegurados
- Posicionamiento integrado/localización/equipos de transmisión de datos
- Detectores de contenedores
- Marcado secreto
- Formación de modelos de empaquetamiento
- Materiales ligeros contra explosiones y ataque químico
- Responsabilidad de rastreo

Integración/validación

- Disponibilidad de red-bases de datos mundial (estandarización/legal/política aceptable)
- Aparato detector de demostración para ruidos electrónicos
- Aparato de demostración de contenedor asegurado

3.1.5 Protección de personas

3.1.5.1 *Protección de la población*

Medidas de apoyo

- Evaluación de riesgo en zonas públicas y urbanas

Tecnologías y herramientas de apoyo

- Formación / simulaciones (virtuales o de realidad aumentada)
- Modelado
    - Recopilación de datos reales
    - Fenómenos (propagación, efectos...)
    - Comportamiento de la población
    - Comportamiento individual / respuesta a los peligros (efectivo / físico y observado
- Seguridad personal
    - Protección contra virus / agentes biológicos / radioactividad
    - Vacunas / estudios inmunológicos
    - Materiales específicos / materiales compuestos / Filtros de inhalación de aire específicos
- Sensores BC de bajo coste y sistemas de alarma
- Percepción de seguridad (aspectos sociológicos)
- Vigilancia y reconocimiento en el medio ambiente urbano
- Sistemas de alerta para la población

Integración/validación

- Aparato de demostración de comunicaciones en el control de mando en crisis interoperables (C3) ("laboratorio de seguridad"), para elaboración de escenarios y formación de las fuerzas de emergencia
- Información personal y sistema de comunicaciones con realidad aumentada ("vídeo, comunicaciones en sistema Palm")

3.1.5.2 *Puesta en práctica del cumplimiento de la ley*

Información de apoyo

- Evaluación de riesgo técnico-operativo sobre uso no autorizado de armas de fuego o LTLW en dicha ley
- Evaluación de respuesta progresiva en proporción al peligro
- Control de multitudes (preparación, fase inicial – detención de vehículos, fase de transición- identificación de líderes de grupos, negociación – señalamiento de líderes, crisis – extracción de líderes, uso de medios correctivos. C3 específico)

Tecnologías y herramientas de apoyo

- Biometría
- Micropirotecnología
- Efectos fisiológicos

Integración/validación

- Concepto arquitectónico
- Eficacia táctico-operacional
- Responsabilidad legal – simulación de formación

3.1.5.3 *Protección de emergencia y otros servicios*

Medidas de apoyo

- Estudios de casos

Tecnologías y herramientas de apoyo

- Formación / simulaciones (virtuales o de realidad aumentada)
- Operaciones combinadas con robots, UAVs (vehículos aéreos no tripulados), etc.
- Visualizaciones/localización/mapas/ acceso a base de datos, etc. en terminales móviles
- Comunicaciones aseguradas
- Logística: intervenciones optimizadas
- Protección física del personal (detectores miniaturizados...)
- Técnicas de descontaminación
- Dirección del conocimiento, guardar y clasificar la experiencia adquirida para posteriores mejoras
- Puesta al día del modelado
- Compatibilidad del equipamiento para la puesta en práctica del cumplimiento de la ley

· Evaluación de daños

· Trazado automático en mapas

Integración/validación

· Simulador de dirección de crisis

3.1.6 Política de seguridad

3.1.6.1 *Evaluación de riesgo global*

Medidas de apoyo

· Análisis de datos disponibles (reservas, limitaciones, acceso...)

· Modelos y metodologías para evaluación proactiva y de riesgo así como alerta rápida

  · Para prevención de actos de terrorismo

  · Para control de la estabilidad global

Tecnologías y herramientas de apoyo

· Evaluación y modelos de consideración de riesgos y bases de datos

· Uso informático de red

· Extracción de datos heterogéneo y avanzado / repaso de información sensible

· Análisis multivariable

· Inteligencia aplicable para la prevención de actos de terrorismo

· Análisis de comportamiento para la seguridad

  · Manejo incierto, métodos de optimización

  · Sistemas de opinión

· Evaluación de riesgos en objetivos potenciales de terrorismo

  · Bases de datos culturales

  · Traductores universales

Integración/validación

· "Browser" fuente abierta específica ("seguridad Google")

3.1.6.2 *Ayuda humanitaria (trabajos Petersberg)*

Medidas de apoyo

- Definición de capacidad de dirección de análisis en una crisis europea

Tecnología o herramientas de apoyo

- Para todas las misiones:
  - Observación, control y supervisión, a través del espacio, aire, Humint (inteligencia humana), etc... adquisición de datos, recopilación, procesos (extracción de datos, fusión de datos, modelado...)
  - Comunicaciones/posicionamiento asegurado (anti-interferencias por radio, comunicaciones por el espacio...)
  - C4ISR de seguridad avanzado incluyendo lo relativo a infraestructura movible y de despliegue (posible artículo 169)
  - Apoyo logístico: medios avanzados incluyendo simulaciones y formación
- Operaciones humanitarias y de evacuación
  - Logística para helicópteros de transporte y médicos
  - Instalaciones médicas móviles incluyendo telemedicina

Integración/validación

- Aparato demostrador para plataforma en dirección de crisis incluyendo logística, C3, planes, etc... así como aplicación de despliegue
- Fuselaje con estructura compuesta de nueva generación, resistente a explosiones (después de predicción de vulnerabilidad y de protección contra explosiones) (aplicable también a helicópteros de evacuación o de operaciones humanitarias)
- Dirección de alta calidad y de bajo coste para helicópteros (para operaciones de evacuación)
- Sistema fiable de detección de minas de tierra de bajo coste

3.1.6.3 *Contraproliferación – verificación de armamento y desarme*

Medidas de apoyo

- Evaluación y predicción de amenaza balística

Tecnología o herramientas de apoyo

- Bases de datos e inteligencia:
  - Identificación de componentes únicos y fáciles de encontrar, movimientos/compras
  - Chips en aparatos peligrosos

- Espacios vulnerables y localización de “tracks” (rastros)
- “Labs on a chip” (Se trata de una tecnología avanzada que integra un sistema de microfluidos en un “chip” a microescala; se puede decir que se logra introducir un minúsculo laboratorio “lab” en un “chip”)
- “Conjuntos de verificación incluyendo acceso remoto a bases de datos”

- Apoyo a deshechos nucleares/plantas térmicas/”limpieza” de submarinos nucleares: es decir, con Rusia y Ucrania
  - Control de vegetación y medio ambiente
  - Control de posición
- Tráfico ilegal:
  - Vigilancia de fronteras (caminos, carreteras...) por aire, espacio, cámaras
  - Detectores de bajo coste – Marcado y rastreo de armas y munición

Integración/validación

- Sistemas de vigilancia con aparatos de demostración de contenedores (con “chips”) (marcado y rastreo)

3.1.6.4 *Sistemas de dirección de crisis incluyendo cuarteles generales en despliegue*

Medidas de apoyo

- Fuentes de datos disponibles, enlaces, etc... en la Unión Europea
- Características de candidatos

Tecnología o herramientas de apoyo

- Despliegue rápido/movilidad/sostenibilidad
- Multimedia/integración con fuentes múltiples en vídeo
- Interacción
- Inmersión
- Entrega de gran veracidad
- Características del multiusuario: dirección y configuración de datos
- Preparación del escenario: Inteligencia artificial, simulación de sistema imaginario
- Análisis de resultados: dirección de conocimiento, muestra visual...
- Interfaces multimodales: de voz, PC móvil, inalámbrico, PDA (asistente digital personal)
- Fusión de datos / “Datos bajo demanda”
- Red informática / acceso en tiempo real
- Extracción de datos (agrupamiento, pruebas automáticas..., tiempo real...)

- Factores humanos (estrés...) en procesos de decisión
- Comportamiento bajo estrés (especialmente en ambientes de movimiento...)
- Endurecimiento del EM (Movimiento Europeo) para sistemas de despliegue

Integración/validación

- Simulador central en análisis de crisis/logística de formación (laboratorio de seguridad)
- Cuartel general de despliegue móvil

3.1.7 Misiones horizontales

3.1.7.1 *Localización NRBC, protección y descontaminación*

Medidas de apoyo

- Creación de modelos para evaluación de peligro e impacto
- Definición de asistencia a equipamiento

Tecnología o herramientas de apoyo

- Localización
  - Sistemas de alerta lejanos y en el lugar, detectores miniaturizados...
  - Vigilancia de amplia escala (productor de imágenes de máximo espectro, IR infrarrojos 8-12µ, fluorescencia inducida por láser, neutrón...), aparatos de identificación
  - Sensores de láser "Terahertz" para localización tipo B
  - Detector nuclear basado en sensores de despliegue para:
    - Localización en primer plano de la tasa de dosis de los rayos gamma y radio nucleido gamma
    - Control de contaminación radioactiva
- Protección de la población
  - Filtros NRBC, sistemas de cierre de aire
  - Materiales específicos y compuestos
  - Protección especial contra virus, agentes biológicos, radioactividad...
  - Vacunas, antídotos, estudios inmunológicos
- Técnicas de descontaminación
  - Duchas específicas
  - Nuevos materiales activos, cuadros...

Integración/validación

- Localización NRBC integrada/sistema de protección para instalaciones públicas (aeropuertos, estaciones de ferrocarril)

3.1.7.2 *Operaciones de sistema integrado ("Operaciones Centrales de red")*

Información de apoyo

- Evaluación de los sistemas militares y civiles existentes en la UE
- Interoperabilidad de los sistemas de comunicaciones civiles y de seguridad
- Estudio de estructura de sistema basado exigencias de misión ("sistema de sistemas")

Tecnología y herramientas de apoyo

- Conocimiento de situación aumentado y ayudas de apoyo en decisiones
  - Redes de sensores inteligentes y móviles
  - Comunicaciones fiables y seguras para y desde plataformas (control de espectro, interceptación de comunicación) incluyendo puesta en práctica de las mismas en una zona particular, resistente a un medio hostil
  - Técnicas de fusión de datos e información
  - Datos bajo demanda > red informática / tiempo de acceso real
  - Proceso de información distribuida
- Interoperabilidad de componentes incluyendo comunicaciones aseguradas
  - Sistemas modulares integrados (integradores, interoperadores, adaptables...)
  - Centros de llamadas

Integración/validación

- Aparato demostrador de forma de infraestructura para información común
- Información "Nomade" y sistema de comunicación con realidad aumentada en un Palm
- Red de ordenadores personales "Nomade" y CIS

3.2 Puntos fuertes

3.2.1 Necesidad para un posterior desarrollo específicos de competencias tecnológicas

Los recientes acontecimientos terroristas y grandes desastres muestran que, a pesar de la buena ciencia interior europea, las competencias de investigación y tecnología no proporcionan adecuadamente y con eficacia la prevención de estosterribles atentados para que dejen de ocurrir así como la protección de seres humanos y sus propiedades y activos contra los efectos catastróficos que ellos producen.

Al objeto de realzar una capacidad total y absoluta para responder adecuadamente, es necesario un progreso significativo en un desarrollo más pronunciado de las tecnologías individuales y combinadas mostradas en la sección 3.1.

3.2.2 Necesidad de un método integrado

Las actuales misiones de seguridad y manejo de crisis civiles requieren unos conceptos que a continuación se exponen:

- Que tengan capacidad de respuesta y que sean adaptables, de modo que puedan contestar a necesidades de cambio en la situación que se plantee y que a su vez puedan ser adaptadas y reconducidas basándose en la experiencia aprendida en este terreno.
- Sólidas y fuertes, de modo que resulten efectivas durante toda la operación.
- Interoperables, de modo que puedan operar en todos los niveles, en acciones integradas incluyendo todos los servicios nacionales e internacionales.
- Amplias, de modo que puedan actuar en un amplio margen de situaciones.

Al objeto de conseguirlo, es necesario en todo momento tener una vista general de lo que está ocurriendo en este campo. De modo que, se necesitan capacidades para ser desarrolladas con especial método en:

- Disponibilidad de información completa, proporcionando al usuario en todo momento, información y capacitándole en la búsqueda e intercambio de la misma que haya sido recogida por todas las fuentes internas y externas en este campo.
- Apercibimiento de la situación, proporcionando un entendimiento compartido e interpretación de la situación, la planificación de la misión, las potenciales fuentes de acción, etc...
- Sistemas flexibles y modulares, permitiendo medios para rápidamente cambiar las necesidades de la misión.

- Apoyo de red integrado, permitiendo el uso e integración de las capacidades del servicio público, ONGs, industria, etc... y cuando sea necesario servicios militares para apoyar las operaciones.

La Unión Europea tiene al día de hoy 25 estados miembro, cada uno de estos estados con diferentes sistemas, con diferentes protocolos, con formas de tomas de decisión, etc... Es más, la seguridad es una actividad de servicio múltiple que incluye personal para una variedad de funciones. Por ejemplo, control y dirección de fronteras incluyen guardas, cumplimiento de la ley, aduanas, oficinas de inmigración ilegal, etc. Para semejante medio fragmentado y heterogéneo, puede que no resulte adecuado un concepto doctrinal integrado de "uno para todos puede que no sea el mejor método. Se sugiere que se siga y desarrolle el concepto de capacidades de red que permitan la acción pertinente (NEC) que están mucho más involucradas en una capacidad de desarrollo uniendo a aquellos que tomas las decisiones, así como a sensores y otros sistemas, permitiéndoles reunir su información utilizando el sistema de redes al objeto de lograr una capacidad sobresaliente. En NEC, la palabra clave es interoperabilidad.

Un método integrado requiere interoperabilidad en el aspecto técnico así como en el nivel humano y de datos. La interoperabilidad técnica relaciona los aspectos técnicos mencionados con la interconexión de los diferentes sistemas y sus equipamientos, de modo que el intercambio de información entre estos diferentes sistemas y equipamientos lo convierta en técnicamente posible. La interoperabilidad de datos trata de la incompatibilidad de data y juegos de datos, y ve el proceso de extracción y de fusión de datos, con el objetivo de lograr que la información correcta llegue a la persona adecuada, al lugar preciso, en el tiempo correcto, de modo que esta persona tome a su vez, la decisión correcta y/o lleve a cabo la acción adecuada (llamada "compartimiento de información sin fisuras".

Sin embargo, los desafíos más grandes de interoperabilidad están en el nivel operativo humano. Los problemas necesitan, en particular, ser superados a través de multiagencia, multiservicio, comunicación y colaboración cultural.

- Diferentes procesos y comportamientos cognitivos
- Diferentes formas de acopio, compartimiento y reutilización de conocimientos (basados en aprendizaje que supone la experiencia)
- Diferentes estructuras de organización y procesos de decisión
- Diferente comprensión del impacto y costes
- Diferentes formas del apercibimiento de la situación del equipo, así como de la situación que comparte en ese momento.
- Diferentes procedimientos de información
- Necesidad para modelos y protocolos de agencia transversal

3.2.3 Necesidad de un método variado

Un paso más en el proceso hacia la total integración, es el llamado proceso de las tecnologías convergentes. Este proceso se combina y se construye sobre las sinergias y la fertilización cruzada de cuatro diferentes áreas tecnológicas:

- La nanociencia y la nanotecnología
- La biotecnología y la biomedicina
- El proceso de información, incluyendo informática y comunicaciones avanzadas
- La ciencia cognitiva, incluyendo neurociencia cognitiva.

Cada una de las tecnologías mencionadas está a un gran paso del desarrollo, y se pueden incluir como ejemplos de momentos decisivos: cambios revolucionarios, técnicas de comunicación altamente efic aces, mejora individual y creatividad de grupo, el punto común entre el perfeccionamiento de hombre- máquina, etc.

Para la clarificación de propósitos, el potencial de las tecnologías convergentes se ilustra por medio de un ejemplo práctico, es decir, educación y formación.

El objetivo es crear un medio de formación virtual y real, que esté adaptada a las formas de aprendizaje del individuo, usando los contextos que estimulen al mismo y que reduzcan cualquier situación embarazosa producida por algún error. El intercambio de información por medio del ordenador puede ser totalmente interactivo (hablado, de visión y de movimiento).

En el ejemplo anterior, los *nano-aparatos* será esenciales para almacenar la variedad de información o imágenes necesarias y para procesar dicha información en la interacción a tiempo real.

La *biotecnología* es importante para proporcionar una "retroalimentación" (feedback) en el estado de precisión y retención del individuo.

La *tecnología de información* debe desarrollar el "software" que permita un procesado y muestra de información mucho más rápido. Ya que, por ejemplo, la formación para la emergencia o dirección de fronteras integrada deben incluir relaciones en equipo, el "software" finalmente debe proporcionar interacción entre las diferentes partes. También se necesitan las innovaciones que proporcionen manuales de realidad aumentada donde los individuos pudieran tener muestras a tiempo real de información para las acciones de reparación y mantenimiento.

El aprendizaje efectivo debe comenzar con un entendimiento del proceso *cognitivo*. Las personas tienen unas formas diferentes de aprender (orales, visuales, táctiles). Responden a diferentes formas de motivación y a diferentes contextos. La memoria

humana y los procesos de toma de decisiones dependen de procesos bioquímicos. Un mejor entendimiento de estos procesos puede conducir a unos mejores estados de precisión y retención.

3.2.4 Necesidad de una nueva prueba y procedimiento de evaluación y certificación.

La integración de sistemas tiene un gran impacto sobre la actual forma de comprobación, evaluación y certificación. No sólo es suficiente probar, evaluar y certificar individualmente el equipamiento, sino que es esencial que los sistemas integrados sean examinados, evaluados y certificados también en la interacción del mencionado equipamiento en el medio integrado. Físicamente será imposible de examinar para la mayoría de combinaciones adecuadas de integración de sistemas. Se necesitará explorar una nueva prueba y herramientas de evaluación.

3.3 Oportunidades

3.3.1 Investigación basada en la capacidad

La capacidad es un ambiente muy complejo con una gran variedad de escenarios, misiones/tareas, integrantes e intereses del usuario. Cada una de las misiones específicas requiere las capacidades para actuar con eficacia en los problemas del día a día que se les presentan a los guardas de fronteras, el personal de emergencia, los servicios de aduanas, etc. En este contexto, la ciencia, la investigación y el desarrollo técnico para la seguridad, tiene otra dimensión. Las citadas ciencia, investigación y desarrollo tecnológico para la seguridad es una *investigación basada en la capacidad*. Es acometida para apoyar y facilitar el trabajo diario de las personas involucradas en las actividades relacionadas con la seguridad. En términos prácticos, temas que necesitan ser definidos como:

- Es una tecnología, no para reemplazar a la acción humana sino para completar y apoyar.
- Una tecnología, no para ofrecer soluciones autónomas introducidas en la cadena de operaciones.
- Tecnología para ofrecer soluciones complejas e integradas y para que permanezcan en un tono amigable y fácil de actuar.
- Tecnología para que resalte el nivel de seguridad pero que no intervenga en la intimidad y libertad individual.
- Tecnología para intensificar el control pero no para aumentar el nivel de falsas alarmas o la duración del proceso.
- Etcétera

La investigación basada en la capacidad no es un concepto completamente nuevo. Al tiempo que puede ser un nuevo método para los programas de investigación civil de la comunidad, también existe una significativa habilidad en el terreno militar. Pero tenemos que pensar que el ambiente de seguridad es muy diferente del ambiente militar. La mayor diferencia es la gran extensión de la comunidad del usuario, dando como resultado una gran variedad de necesidades del usuario así como capacidades que se necesitan. De modo que, aunque el terreno militar procura un buen punto de inicio, es necesario adaptarlo significativamente al fin de dirigir adecuadamente el punto específico del sector de seguridad.

3.3.2 Nuevos avances tecnológicos

La sección 3.1 proporciona un buen plano general sobre qué tipo de evoluciones tecnológicas podrían realzar significativamente las competencia s de conjunto para responder a los nuevos retos de seguridad adecuadamente.

En resumen, las siguientes partes sobre tecnología necesitan ser más desarrolladas al nivel de las tecnologías individuales.

3.3.2.1 *Tecnologías de sensores y radares*

El campo sobre tecnologías de sensores y radares cubre los retos relacionados de nuevos y avanzados sensores que tratan del espectro de frecuencia total, es decir, tecnologías de sensores RF, tecnologías de sensores de onda micromilimétrica, nanotecnologías para sensores, tecnologías para sensores electromagnéticos, aparatos electroópticos y optrónicos, tecnologías de láser, tecnologías de sensores IR (infrarrojos), de sensores de onda UV/visible, de sensores térmicos, de sensores NRBC (nuclear, radiológica, biológica, química), en particular para la localización de amenaza biológica y química, etc.

Este campo también se refiere a procesos avanzados en la tecnología radar, incluyendo tecnologías relacionadas con el diseño del receptor y el transmisor, proceso y programación de tiempo real digital, proceso de algoritmos y control, el ambiente electromagnético, etc.

3.3.2.2 *Tecnologías de comunicación*

El campo de las tecnologías de la comunicación abarca conceptos para la comunicación asegurada, incluyendo comunicaciones aseguradas independientes de red y protocolo, comunicaciones aseguradas multimodo, comunicaciones reconfigurables, comunicaciones aseguradas móviles, tecnologías innovadoras relacionadas con la protección de redes de comunicación contra un ambiente hostil, etc.

3.3.2.3 *Tecnologías de la sociedad de la comunicación*

El campo de las tecnologías de la sociedad de información cubre conceptos para la información y los sistemas de datos, incluyendo reconocimiento de normas, recopilación de datos innovadores, clasificación de datos así como técnica de fusión de datos, manejo del conocimiento, proceso de datos y señales innovadoras, informática de red, inteligencia "web" (extracción de grandes datos), técnicas de búsqueda en el contexto, inteligencia accionable, etc.

También se refiere a temas de guerra de información, tales como seguridad cibernética, incluyendo cibernética disuasoria, criptología y dirección clave, técnicas de localización rápida, técnicas no cooperativas IFF (Identification Friend or Foe) (Identificación amigo o enemigo), introducción no cooperativa de sistemas electrónicos sospechosos, tecnologías de interferencias y antiinterferencias, etc.

3.3.2.4 *Tecnologías de materiales*

El campo de materiales cubre el desarrollo de materiales nuevos ligeros y fuertes, cubrimientos, etc., incluyendo materiales para la protección humana, materiales ligeros para la protección de espacios, tecnología de materiales resistentes a explosiones y autoprotectores, tecnología de materiales protectores NRBC, etc.

Este campo también abarca tecnología de materiales opticoelectrónicos y el análisis de los efectos estructurales, considerando, por ejemplo, tecnología de materiales de fibra óptica, de detectores UV/IR (ultravioleta/infrarrojo), de materiales ópticos no lineales, tecnología de cerámica y vidrio, de materiales compuestos, etc.

También se deben considerar en este contexto, más desarrollos en el terreno de los materiales energéticos y de tecnología de plasma, abarcando temas tales como la micro-pirotecnología, técnicas de localización de explosivos, etc.

3.3.2.5 *Ciencias humanas*

El campo de las ciencias humanas se refiere a los aspectos del análisis y modelado del comportamiento humano y, en particular, también considera el comportamiento individual, el de la población, la predicción del comportamiento en masa, proceso de la información humana, trabajo en equipo, organizaciones y culturas, formación (individual y en equipo) y técnicas de la misma, formación colectiva, realce del modo de actuar humano, modelado del análisis de funciones, etc.

Este campo también abarca los factores humanos, incluyendo la supervivencia, los efectos de protección y estrés, modelado de la forma de actuar humana y el estrés así como de la fatiga, factores humanos en la fabricación, sistemas referentes al manejo de la duda y la opinión, factores humanos en el proceso de decisión, etc.

3.3.2.6 *Ciencias sociales*

El campo de las ciencias sociales abarca los desarrollos políticos (nacionales, europeos e internacionales), multiculturalismo y diversidad, ética y derechos humanos, temas

sociales y de medio ambiente, bienestar y sostenimiento del mismo, orientaciones religiosas, papel de la sociedad en la investigación, etc.

3.3.2.7 *Biotecnología*

El campo de la biotecnología se dirige al desarrollo de tecnologías biológicas, abarcando las relacionadas con biomateriales y nanofabricación y materiales biocompatibles.

También se consideran las tecnologías biomédicas, en particular los análisis rápidos de agentes biológicos y de susceptibilidad humana a enfermedades y tóxicos, diagnóstico rápido de enfermedades infecciosas, telemedicina (diagnóstico y cirugía), antivíricos novedosos, antibióticos, vacunas, y desarrollo de fármacos, etc.

Además, el campo de la biotecnología cubre biotecnología agroalimentarias, incluyendo la contaminación e intoxicación de la agricultura, ("water beddings", ríos, terreno, aire, etc.), cosechas y virus en animales, etc., y también se refiere a técnicas de descontaminación.

3.3.3 Integración de sistemas, datos y servicios

Como ya se ha indicado en el sección 3.2.2, aunque los avances en las tecnologías individuales se necesitan mucho más, las misiones de seguridad moderna y la gestión de crisis civil requieren urgentemente un fuerte planteamiento en los conceptos integrados y todo esto en el nivel de sistemas, datos y servicios.

La sección 3.1 proporciona una buena vista general sobre que tipo de evoluciones tecnológicas podrían significativamente realzar la competencia de conjunto para responder más adecuadamente a los nuevos desafíos en la seguridad.

En resumen, las siguientes áreas de tecnología necesitan desarrollarse más a nivel de los planteamientos integrados:

3.3.3.1 *Tecnologías de radar y sensores*

El campo de las tecnologías de radar y sensores incluye los retos relacionados con la integración de las diferentes tecno logías de sensores, en sensores que permitirían la localización de diferentes tipos de sustancias (biológicas, químicas y/u otros materiales o agentes) simultáneamente usando diferentes técnicas de búsqueda por medio de estos aparatos. Esta parte incluye conceptos como bosque de sensores, centro de red de sensores existentes, vigilancia de multisensores de alargo alcance y amplia escala, de autonomía, de automatización, compacto, sensores reconfigurables

y móviles, sensores en un "chip", técnicas innovadoras para vigilancia discreta, técnicas de de imágenes y trazado en mapas relacionados con estos sensores.

3.3.3.2 *Tecnologías de comunicación*

El área de las tecnologías de comunicación se refiere a las tecnologías en apoyo de la comunicación interoperativa como son los enlaces de datos de banda ancha inalámbricos para comunicaciones aseguradas, acceso de banda ancha para usuarios móviles en situaciones dinámicas, escenarios difíciles en el plano electromagnético, técnicas de alerta a la población, etc.

3.3.3.3 *Tecnologías de la sociedad de la información*

El campo de las tecnologías de la sociedad de la información abarca redes y estructuras, incluyendo el desarrollo de conceptos tales como enlaces de datos de banda ancha inalámbricos y asegurados para la informática distribuida y asegurada, seguridad de red e integridad de datos entre los sensores distribuidos, intercambios de información y bases de datos interoperables, etc.

3.3.3.4 *Tecnología de sistemas integrados*

El campo de las tecnologías de sistemas integrados considera el diseño de sistemas integrados, integración del equipamiento, interoperabilidad, fiabilidad y mantenimiento de los sistemas, conceptos de control de sistema de salud, etc. Se necesita prestar una atención específica a la certificación de estos sistemas, ya que los métodos actuales de valoración, evaluación y certificación no están adaptados para realizar todas estas funciones en sistemas integrados complejos. Este tema se relaciona con el problema indicado en la sección 3.2.4 y se comentará más adelante en la 3.3.4.

3.3.3.5 *Simulación*

El campo de la simulación se refiere a las técnicas de simulación del equipamiento, cubriendo aspectos la predicción de vulnerabilidad de soluciones expuestas y estructurales, centro de red de sensores existentes, estimulación de los mismos, cooperación a través vídeo-tag-biométrica, supervivencia de los componentes y equipamiento, realidad virtual y aumentada, formación del equipamiento, etc.

También comprende las técnicas de la situación previsible, en particular la simulación y modelado avanzado del comportamiento humano, simulación para la toma de

decisiones, de misiones, técnicas de gestión de las consecuencias derivadas, teoría del caos, conceptos de análisis de impacto y reducción del mismo, modelado de polución, prevención de vulnerabilidad de estructuras, etc.

3.3.3.6 *Ciencias humanas*

El campo de las ciencias humanas cubre coordinación interorganizativa y comunicación, incluyendo la coordinación de acuerdo con las estructuras de organización, sus papeles y medios, comunicaciones de situaciones críticas con relación a sectores externos (medios de información, agencias gubernamentales, etc.), posibles participantes y público en general, sala de control colectivo, etc.

También se refiere a interoperabilidad humana, que incluye la necesidad una mejor comprensión de las partes específicas y características de los servicios individuales, incluyendo su proceso de decisión y medio operativo y comprende el desarrollo de un planteamiento común en relación a las operaciones combinadas.

3.3.4 Nuevos conceptos para ensayos, evaluaciones y certificaciones

Como se ha descrito en la sección 3.2.4, la integración de los sistemas tiene un gran impacto en el modo actual de comprobación, evaluación y certificación. Nuevas herramientas de examen y evaluación necesitan ser exploradas, en particular, el uso de la estimulación en los ensayos y también en el nivel de (pre) certificación

Por ejemplo, un aspecto clave en la dirección de fronteras integradas es la colocación de líneas verdes entre los puestos de control. En términos prácticos podría ser difícil evaluar la función de las herramientas para control de fronteras en todas las posibles situaciones medioambientales, así como en todas las situaciones climáticas posibles. Por lo tanto, se propone utilizar simuladores en su lugar. Estos simuladores necesitarían comprender e integrar:

- Todos los criterios de datos genéricos que caracterizan la variedad del paisaje/ medioambiente/condiciones geográficas de los puntos o zonas de cruce de la frontera verde y azul europea
- Todos los criterios de datos genéricos que caracterizan las posibles situaciones climáticas

Estos datos tienen que ser integrados al objeto de proporcionar una plataforma adecuada para examinar y evaluar según las especificaciones y características técnicas de los sistemas integrados en un medioambiente simulado.

3.4 Amenazas

3.4.1 Tecnologías de sistemas contra tecnologías de capacitación

El riesgo de la investigación basada en la capacidad y un enfoque integrado es el énfasis exagerado de las tecnologías de sistemas y, consecuentemente, la falta de enfoque en capacitar o apuntalar tecnologías o investigación básica.

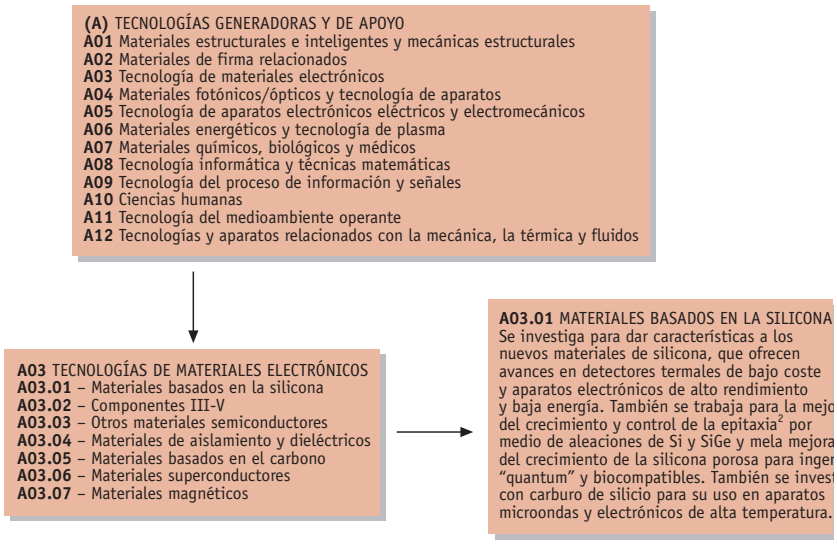
Este peligro de tecnología de sistema sobreenfatizado, no solamente es real para las actividades de investigación relacionadas con la seguridad. También constituye un problema muy destacado en las actividades de investigación relacionadas con la defensa, e incluso para las últimas evoluciones en las actividades de investigación relacionadas con el aspecto civil.

Por ejemplo, el concepto de Proyectos Integrados (FPVI): *Los Proyectos Integrados están basados en un "sistema de programa" que trata con diferentes temas. Normalmente están compuestos por varios componentes, que abarcan a investigación, demostración, adiestramiento, etc. Se espera que reúnan la necesaria masa crítica de actividades, de habilidades y recursos para objetivos ambiciosos (investigación dirigida hacia el objetivo)*[1].

Aunque sus actividades de investigación puedan cubrir todo el espectro de la misma desde la investigación básica a la empleada, la tendencia es que estos IP (Proyectos Integrados) evolucionen desde una investigación dirigida hacia el objetivo a una investigación dirigida hacia el sistema, en particular en aquellos IP, las actividades de demostración son parte del proyecto.

[1] Comisión Europea – Clasificación de los instrumentos FP6 – Descripción detallada.

Las tecnologías generadoras y de apoyo son aquellas que son fundamentales y necesarias para la construcción de sistemas. La taxonomía UK MOD identifica las citadas tecnologías como sigue:



3.4.2 La seguridad contra los principios legales y éticos

Uno de los temas "políticos" clave en el contexto ESRP es cómo reforzar la seguridad sin infringir la intimidad o libertad del individuo. No es la intención del ERSP crear un gran ambiente de hermandad, sino que debería actuar dentro de un marco de equilibrio entre la seguridad, la justicia y la libertad.

Hay una fina línea de equilibrio entre la seguridad, la libertad y la justicia y esta línea está sujeta a la fluctuación dependiendo de la situación política y el ambiente social.

Las recientes recomendaciones del Consejo Europeo a partir de los atentados terroristas en Londres, apoyaron el principio de la retención de datos. Este principio requiere empresas de telecomunicación y servidores de Internet para guardar las comunicaciones por teléfono y por "web" durante, al menos, un año. El contenido de las llamadas y correos electrónicos no deberían ser guardados, pero los detalles del remitente, del destinatario, hora, duración y localidad deberían ser retenidos. Merece la pena reseñar que en una reciente propuesta sobre este asunto por parte del Reino Unido y Francia, las empresas de telecomunicación y el Parlamento Europeo presentaron una gran oposición ya que se consideró que se infringía la llamada privacidad. Se presentará ahora una propuesta de la Comisión por parte de un directivo.

[2] Epitaxia: operación consistente en favorecer el desarrollo de una capa de material semiconductor sobre un sustrato, teniendo esta capa la misma orientación que el sustrato.

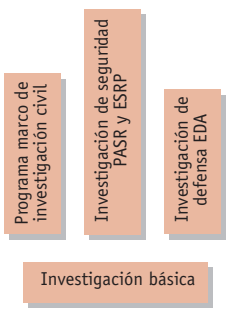
También son muy populares los temas de la privacidad en el terreno de la biométrica. La biométrica es una técnica que se usa como forma segura de identificación de un individuo dentro de una variedad de aplicaciones de carácter mundial. También se está utilizando para la mejora de la seguridad, como asegurarse que sólo gente autorizada tenga acceso a instalaciones e información al objeto de impedir robos o fraudes (tales como la usurpación de identidad y fraude con tarjetas de crédito). También hay una forma de identificar a las personas que pueden estar reclamadas por las autoridades. La mayoría de los medios biométricos trabajan para conseguir información a través de una foto o una grabación, por ejemplo de, una huella dactilar, una cara o una voz. Esta información es, entonces, almacenada para posteriormente confrontarla para verificar la identidad de las personas.

Si la biométrica se pone en marcha, inmediatamente la buena voluntad del público para usar la biométrica necesita ser considerada también, así como un número de preguntas relevantes: ¿Qué datos se almacenan, dónde estos datos almacenados, quién tiene acceso a estos datos, para qué pueden ser usados esta datos, etc.?

3.5 Soluciones

3.5.1 Un programa común para la investigación básica

Con objeto de enfocar el programa la creciente necesidad para dar prioridad a la capacidad así como a la investigación orientada en sistema, se sugiere que el establecimiento de un programa de investigación europeo básico, del cual su aplicación y dichos programas (FP "Parte Fija", PASR "Acción Preparatoria sobre Investigación de Seguridad, ESRP "Programa Europeo de Investigación de Seguridad" e investigación de defensa) puedan tirar de las tecnologías generadoras más importantes, como se ilustra en el esquema:



Semejante planteamiento permitiría prestar una atención específica a las tecnologías generadoras y de apoyo, cuyos ejemplos han sido descritos en la sección 3.4.

Sin embargo, es necesario, dentro de este contexto, refe rirse a los mecanismos de fondos de este programa. En la investigación básica debería de haber oportunidades para explorar nuevas áreas tecnológicas, incluyendo tecnologías que puedan dar como resultado grandes oportunid ades de aplicación, así como tecnologías con un alto riesgo potencial o con poca visión de, cómo estas oportunidades de aplicación podrían ser en el futuro a largo plazo. Un mecanismo de fondos que requiera un 50% de esos fondos, no anima a este último tipo de investigación, dejando, de este modo, huecos importantes en la capacidad de acción dicha tecnología.

3.5.2 Tecnología de observación y supervisión

Se reconoce a este tipo de tecnología como una actividad crucial para el logro y mantenimiento de posiciones competitivas en ambiente de comercial que se desarrolla con rapidez. Sirve para el propósito de identificación y evaluación de avances tecnológicos críticos para la competencia y la innovación, así como de detección de cambios y falta de continuidad en tecnologías existentes. En este contexto, sería digno de tener en cuenta, el comienzo de un debate sobre "un mecanismo o proceso común para la observación de la tecnología aplicado a la comunidad civil, de seguridad y de defensa.

CAPÍTULO 4

Temas de corte transversal

La investigación basada en la seguridad está a su vez basada en la capacidad y orientada hacia los diferentes cometidos. Sus aspectos clave de investigación se refieren a diferentes tecnologías integradas, de interoperabilidad y convergentes. El resto de informes sobre tecnología clave son de un gran relieve para el informe relacionado con la seguridad: biotecnología, nanotecnología, investigación sobre el sector de servicios, complejidad y sistemas, ciencias sociales y humanidades, ciencia cognitiva, tecnologías agroalimentarias y medioambientales, de energía, ICT (Tecnologías de la Información y la Comunicación), tecnologías de manufacturación y actividades de investigación relacionadas con el transporte, estudiadas como individuales pero incluso más, como integradas.

CAPÍTULO 5

Conclusiones y recomendaciones

La ciencia, la investigación y el desarrollo tecnológico para la seguridad es ***seguridad basada en la capacidad***. Se emprende para apoyar y facilitar el trabajo diario de las personas involucradas en las actividades relacionadas con la seguridad.

Aunque la industria europea y la comunidad de la investigación tienes excelentes habilidades para apoyar y desarrollar su contribución para los problemas de seguridad diarios, los recientes acontecimientos terroristas y desastres a gran escala, muestran que estas habilidades no son suficientes para impedir que ocurran, adecuada y eficazmente, dichos acontecimientos terribles y para proteger a los seres humanos y sus propiedades contra los efectos catastróficos. Se necesita llevar a cabo ***un desarrollo superior en un amplio conjunto de tecnologías***.

Aunque se necesitan mucho más las tecnologías individuales, las misiones de seguridad actuales y la dirección de momentos críticos civiles requieren urgentemente ***centrarse con decisión en los conceptos integrados***. Se sugiere seguir y desarrollar el concepto de capacidades generadoras de redes (NEC), las cuales está mucho más preocupadas de la capacidad de evolución reuniendo a aquellos que toman las decisiones, sensores u otros sistemas o equipamiento, permitiéndoles que reunir su información, trabajando en la red al objeto de logra una capacidad mayor. En NEC, la palabra clave es interoperabilidad y esto, al nivel de los respectivos servicios (***interoperabilidad humana***), sistemas (***interoperabilidad técnica***) e información (***interoperabilidad de datos***). ***Las tecnologías convergentes*** son una zona clave a explorar.

La integración de sistemas tiene un gran impacto en el modo actual de examen, evaluación y certificación. ***Nuevas herramientas de examen, evaluación y certificación*** necesitan ser estudiadas, en particular, el uso de la estimulación en el examen, evaluación y también en el nivel de (pre-) certificación.

Al objeto de dirigir el riesgo de información basada en la capacidad y un enfoque integrado para resaltar en gran medida las tecnologías de sistemas y, de ese modo, no prestar la suficiente atención a tecnologías generadoras y de apoyo, así como la investigación básica, se recomienda considerar el establecimiento del ***programa de investigación básico europeo***, desde el cual los programas de investigación de sistema orientados y de aplicación (FP "Parte Fija", PASR "Acción Preparatoria sobre Investigación en Seguridad", ESRP "Programa Europeo de Investigación en Seguridad" e investigación de defensa) podrían extraer las tecnologías generadoras más importantes.

Se necesitan ser estudiados nuevos mecanismos de fondos.

Con el propósito de identificar y evaluar avances tecnológicos importantes para la competitividad y la innovación y detectar cambios y discontinuidades en tecnologías existentes, se recomienda entablar un debate sobre ***un mecanismo o proceso común para la observación de la tecnología*** para la comunidad de defensa, de seguridad y civil.