ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Jefatura de Inteligencia Naval
Dirección Cibernética Naval

Teniente de Navío JUAN CARLOS CAMILO GARCIA RUIZ
18 de Mayo 2018

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Operaciones cibernéticas

Teniente de Navío JUAN CARLOS CAMILO GARCIA RUIZ
18 de Mayo 2018

Conceptos y Contexto

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

CIBERDEFENSA

Es la capacidad del Estado para **prevenir**, **detectar** y **neutralizar** toda amenaza o acto hostil de naturaleza **cibernética** que afecte la soberanía nacional, independencia, integridad y orden constitucional.

CIBERSEGURIDAD

Es la capacidad del Estado para **minimizar** el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Lineamientos Nacionales.

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

2011

Documento
Conpes 3701

Consejo Nacional de Política Económica y Social
República de Colombia
Departamento Nacional de Planeación

2016

LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA

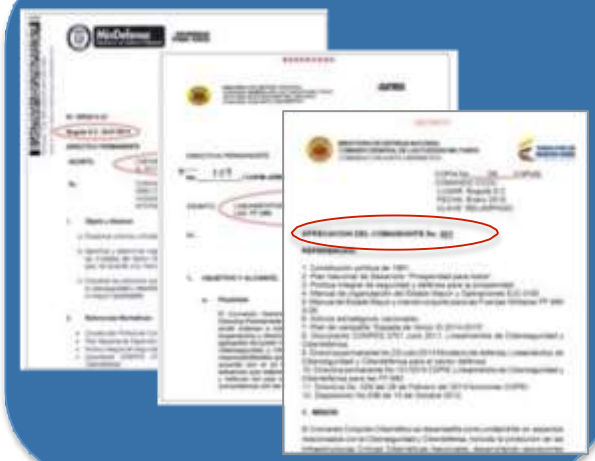
Documento CONPES 3854 de 2016

POLÍTICA NACIONAL DE SEGURIDAD DIGITAL DE COLOMBIA

Fundamento Legal

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Articulo 217 de la CPC



Institucionalidad

Funciones y Responsabilidades

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Implementar una Estrategia de Ciberdefensa para el país, basado en personas, tecnologías y procesos

(operaciones Militares en el Ciberespacio).

Desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional.

Ciberdefensa de la infraestructura crítica del País en el ámbito Cibernético, incluida la del Sector Defensa.

Unidades Militares Cibernéticas

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Unidad Cibernética Ejército Nacional

Unidad Cibernética Armada Nacional

Unidad Cibernética Fuerza Aérea

- Integración de capacidades de Ciberdefensa
- Operaciones Conjuntas en el Ciberespacio.
- Investigación, innovación y desarrollo en Ciberseguridad y Ciberdefensa.
- Ciberdefensa de la Infraestructura Critica Cibernética.

Protegemos el azul de la bandera

Contexto Internacional

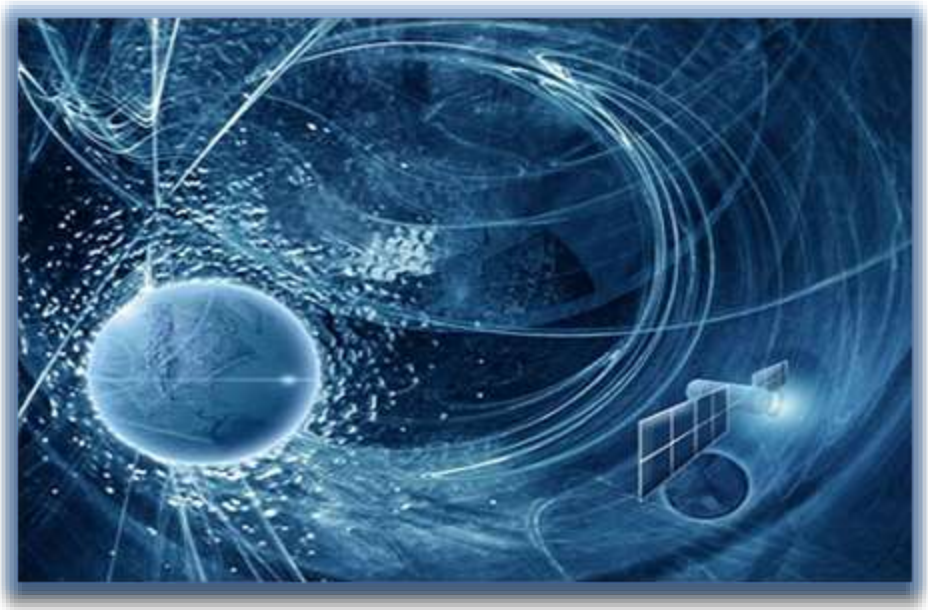
No.	PAÍS	SIGLA	NOMBRE
1	EE.UU	USCYBERCOM	UNITED STATES CYBER COMMAND
		FCC-C10F	US FLEET CYBER COMMAND
		ARCYBER	ARMY CYBER COMMAND
		AFCYBER	AIR FORCES CYBER/24TH AIR FORCE
2	COLOMBIA	CCOC	COMANDO CONJUNTO CIBERNÉTICO
		UCEJC	UNIDAD CIBERNÉTICA EJÉRCITO
		UCARC	UNIDAD CIBERNÉTICA ARMADA
		UCFAC	UNIDAD CIBERNÉTICA FUERZA AÉREA
3	ARGENTINA	EMCFFAA	COMANDO CONJUNTO CIBERDEFENSA
4	VENEZUELA	DICOCIBER	DIRECCIÓN CONJUNTA DE CIBERDEFENSA
5	ECUADOR	COCIBER	COMANDO DE CIBERDEFENSA (En Proceso de Activación)
6	PERÚ	CODEC	COMANDO OPERACIONAL DEL CIBERESPACIO (En Proceso de Activación)
7	URUGUAY	CERT-Militar	CENTRO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA MILITAR. (En Proceso de Activación)
8	BRAZIL	CDCIBER	CENTRO DE DEFENSA CIBERNÉTICA (EJÉRCITO)
9	MÉXICO	CCCC	CENTRO DE CONTROL DE CIBERDEFENSA Y CIBERSEGURIDAD (ARMADA - En Proceso de Activación)
10	CHILE	CIC	COMITÉ INTER MINISTERIAL DE CIBERSEGURIDAD
11	CANADA	CCIRC	CENTRO DE RESPUESTAS A INCIDENTES CIBERNÉTICOS
12	BOLIVIA	N/A	NO CUENTA CON CIBERCOMANDOS
13	PARAGUAY	N/A	

COMANDOS CONJUNTOS

UNIDADES DE LAS FUERZAS

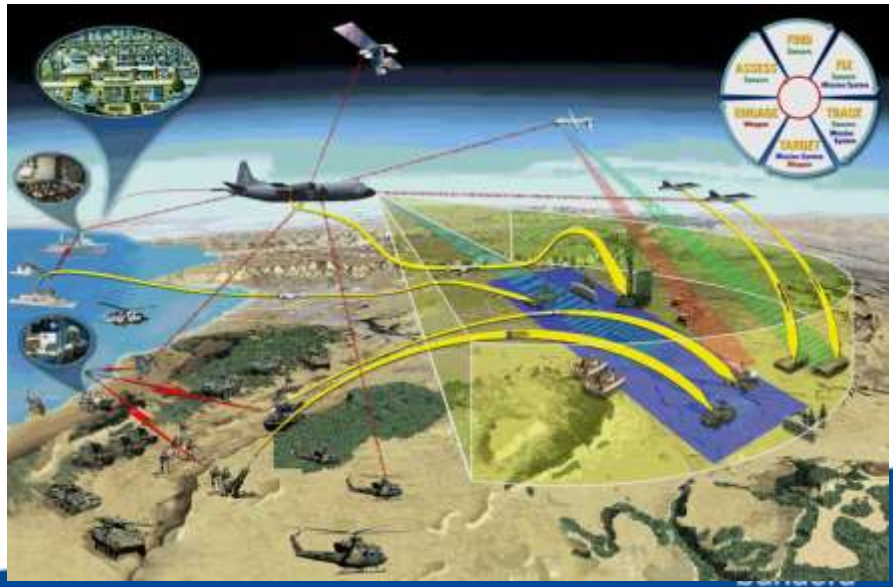
ORGANIZACIONES CIVILES

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA



Ciberespacio

¿nuevo campo de batalla?



Definición de Ciberespacio

REAL ACADEMIA ESPAÑOLA

Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización de la electrónica, la informática y la cibernética.(Academia de la Lengua Española)

NATO Cyber Defence Taxonomy and Definitions (2014):

- **Dominio global** formado por los sistemas TIC y otros sistemas electrónicos, su interacción y la información que es almacenada, procesada o transmitida por estos sistemas

NATO OTAN

Capa Física

COMPONENTE GEOGRÁFICO

COMPONENTE DE RED FÍSICA

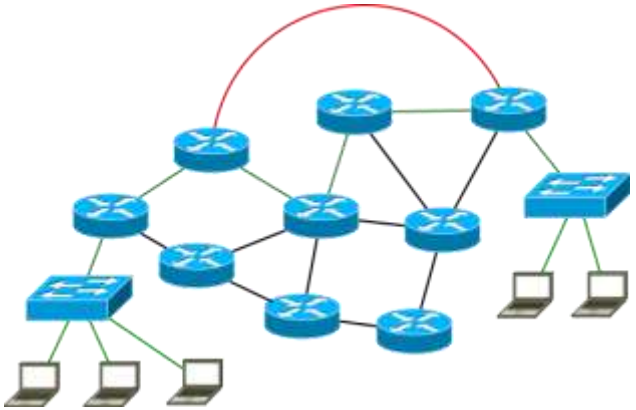
CAPA FÍSICA

Capa Lógica

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

CAPA LÓGICA

CAPA FÍSICA



CONEXIONES LÓGICAS

Capa Social

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

COMPONENTE CIBER PERSONAS

CAPA SOCIAL

CAPA LÓGICA

CAPA FÍSICA

COMPONENTE PERSONAS

Características del ciberespacio

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

- **Entorno virtual sin límites geográficos**
- **Escasa seguridad**
- **Delincuencia, terrorismo y espionaje**
- **Conflictos Armados**
- **No control armamentístico**
- **Se desarrollan actividades vitales para la sociedad -> hiperdependencia**
- **Anonimato vs Marco Legal**

¿EL CIBERESPACIO ES ALGO DAÑINO?

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Protegemos el azul de la bandera

Definitivamente

¿QUÉ ES UNA OPERACIÓN MILITAR?

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Protegemos el azul de la bandera

OPERACIÓN MILITAR MODERNA

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

DEFINICIÓN

"En el ámbito militar, el término operación designa aquella *incursión*, acción militar, que se llevará a cabo según un *plan establecido* de antemano y que tendrá la misión de cumplir determinados *objetivos militares*. O sea, a la operación militar le atañen cuestiones como el plan y la *movilización de las fuerzas* militares en cuestión y también se ocupará de recolectar aquella información implicada en la misma, como ser la *disposición de recursos, entrenamiento del personal* y todo aquello necesario para cumplir satisfactoriamente con la actividad".

http://www.definicionabc.com/general/operacion.php

¿SE PARECE A UNA OPERACIÓN MILITAR?

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Protegemos el azul de la bandera

EMPECEMOS

Ejes Fundamentales para el desarrollo de OpCyber

Amenazas Generales

AMENAZAS ESTRATÉGICAS CONTRA EL ESTADO

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

- HACKTIVISMO
- CIBERTERRORISMO
- CIBERCRIMEN
- CIBERESPIONAJE
- CIBERSABOTAJE

Protegemos el azul de la bandera

Amenazas Cibernéticas

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Estados:

- Amenaza más peligrosa: acceso a recursos, personal y tiempo.
- Conducen operaciones directamente o a través de terceros.

Soft power

Actores Transnacionales:

- Organizaciones formales o informales no ligadas a fronteras nacionales.
- Pueden ejercer “hacktivismo” o acciones terroristas haciendo uso del ciberespacio.

Amenazas *Cibernéticas*

Organizaciones criminales:

No sujetas a fronteras.

Objetivo: ganancia económica.

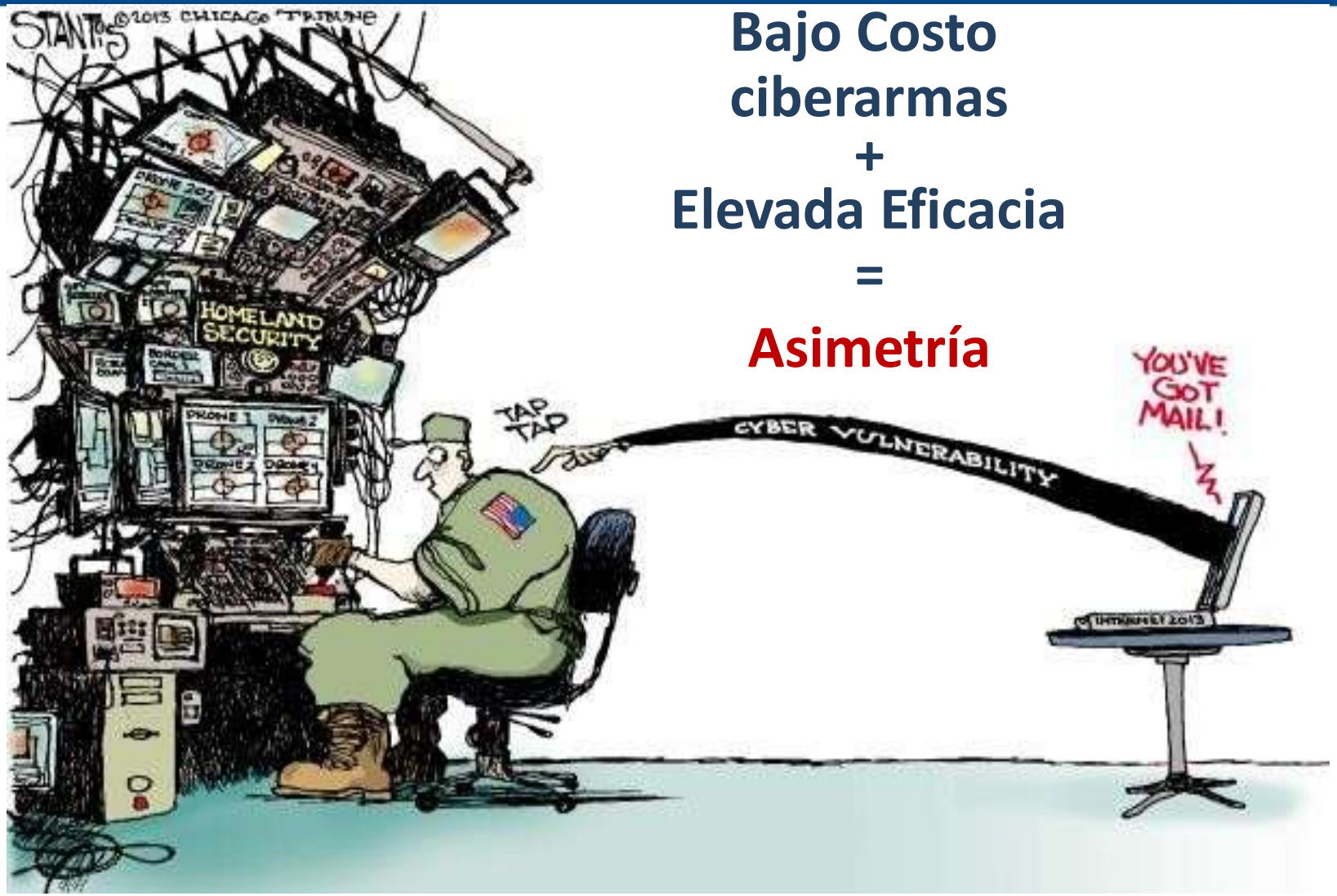
Pueden prestar servicios a estados o actores transnacionales.

Actores individuales o pequeños grupos:

Diversas motivaciones.

Pueden prestar servicios al resto de organizaciones.

Asimetría de actores



Bajo Costo
ciberarmas
+
Elevada Eficacia
=
Asimetría

Capacidades de las FFAA

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

DEFENSA
PREVENTIVA
PROACTIVA
REACTIVA

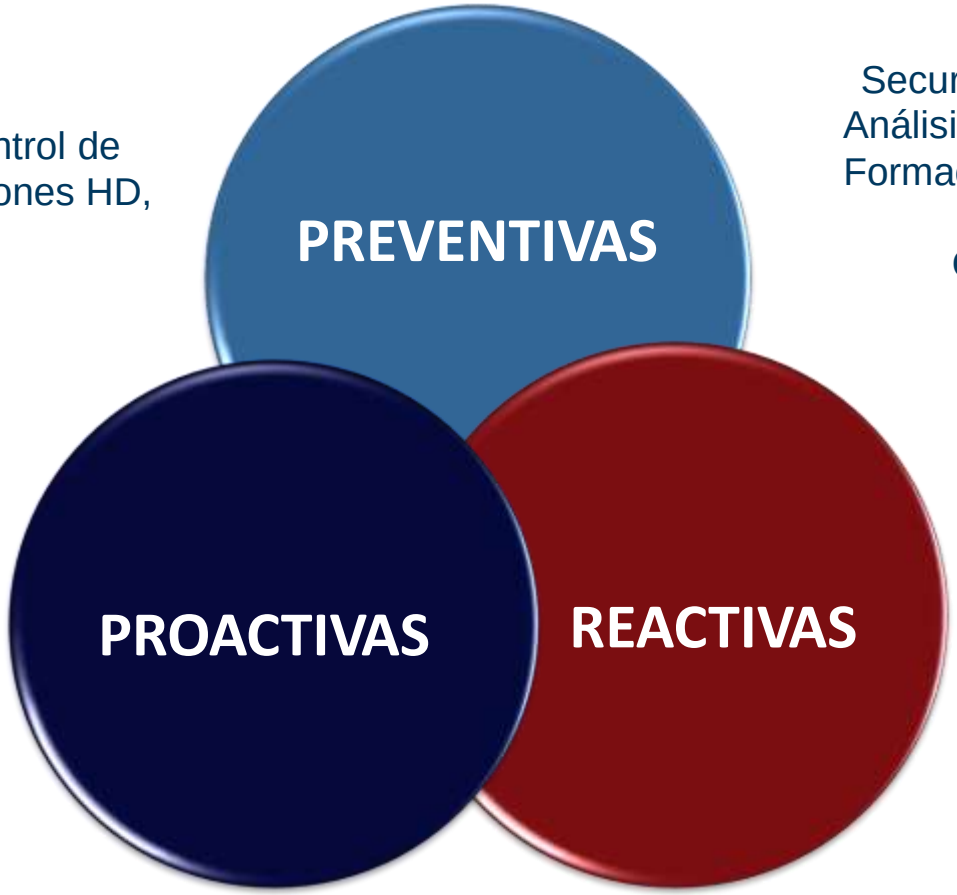
EXPLOTACIÓN
CONOCIMIENTO SITUACION
INTELIGENCIA
ALERTA TEMPRANA

RESPUESTA
LEGÍTIMA
OPORTUNA
PROPORCIONADA

Capacidades de defensa

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Seguridad física
Control de accesos Control de emanaciones Actualizaciones HD, SO, SO, SW, AV



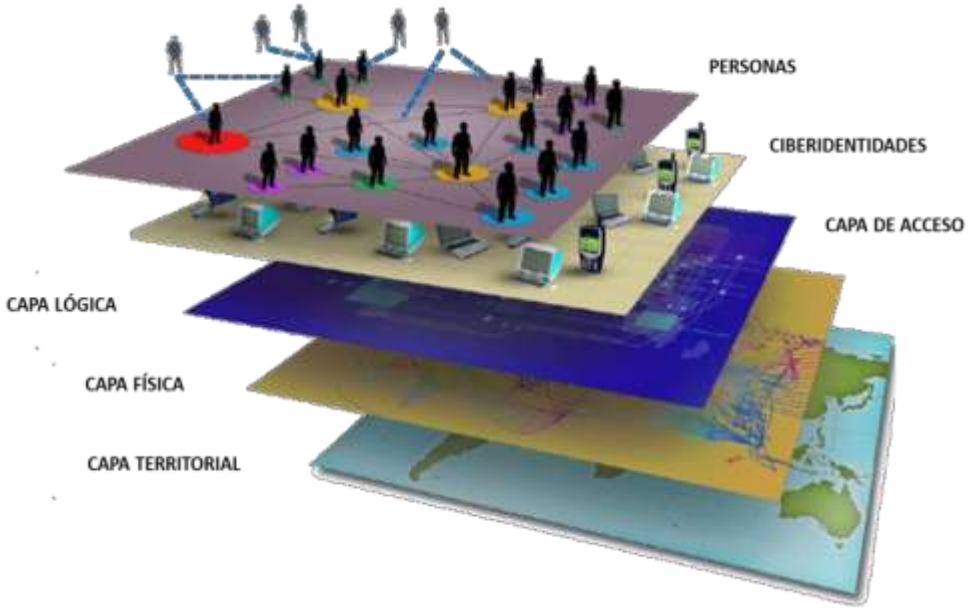
Securización de sistemas
Análisis de vulnerabilidades
Formación y Adiestramiento
Alertas
Concienciación

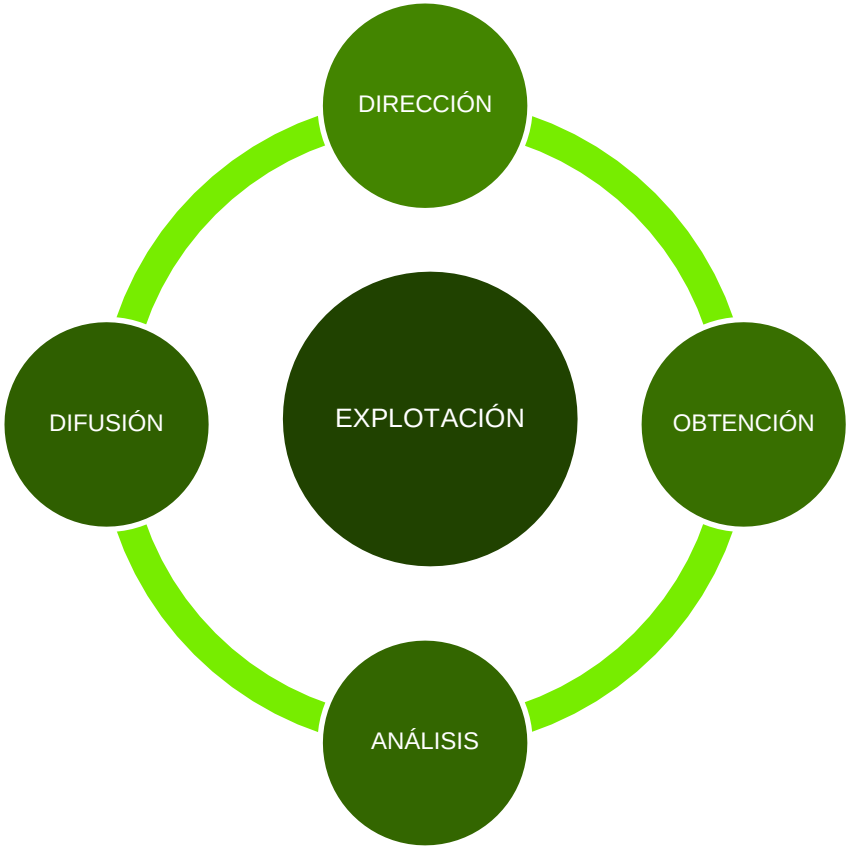
Inspecciones y Auditorías
Monitorización
Tests de penetración

Gestión de incidentes
Restauración de sistemas
Análisis forense
Atribución
Acciones legales

Capacidades de Explotación

- Inteligencia de ciberamenazas.
- Alerta temprana ante posibles ataques.
- Apoyo al Planeamiento de Operaciones.





Capacidades de Respuesta

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Acciones contra potenciales adversarios o agentes hostiles que afecten a la integridad y disponibilidad de sus sistemas de información y telecomunicaciones, así como a la información que éstos manejan.

DEFINICIONES

- **Operación Militar en el Ciberespacio:**
  - Es una operación en la que se emplean capacidades "ciber" con el objetivo principal de alcanzar objetivos militares en el ciberespacio o a través de él.

- **Ataque Armado en el Ciberespacio:**
  - Es una acción originada en el ciberespacio en la que se producen daños a personas u objetos.

- **Efectos en el Ciberespacio:**
  - Efectos producidos sobre los sistemas de información que afectan a la Confidencialidad, Integridad o Disponibilidad de la información contenida en ellos.

PLANEAMIENTO DE OPERACIONES EN EL CIBERESPACIO

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

- Las operaciones en el ciberespacio se planean igual que en el resto de dominios.

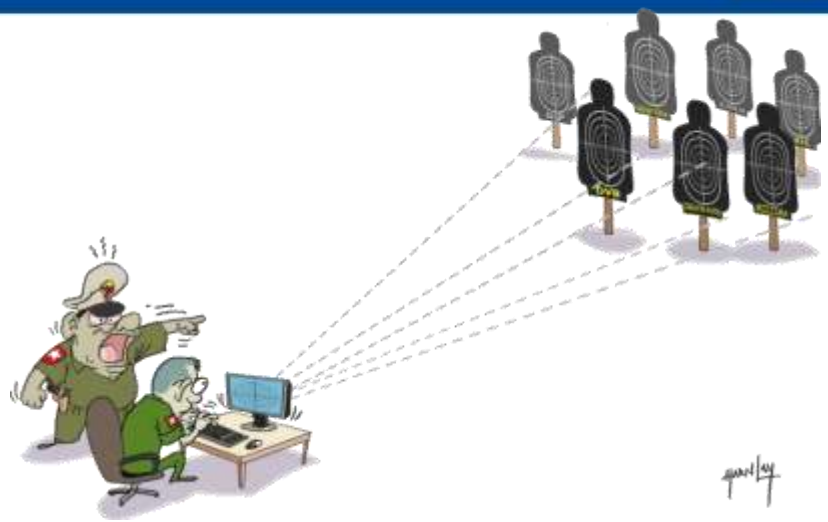
- Las acciones en el ciberespacio se deben integrar en todas las operaciones a nivel táctico, operacional y estratégico.

PLANEAMIENTO DE OPERACIONES EN EL CIBERESPACIO

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

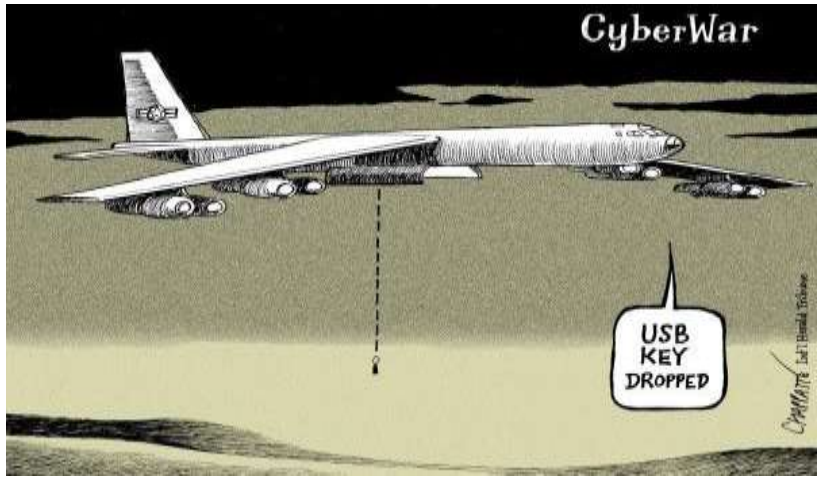
Cyber Targeting

Proceso de selección y priorización de objetivos en el ciberespacio, así como los efectos a producir sobre ellos.



Cyber Weaponeering

Proceso para determinar la cantidad y tipo de ciberarmamento necesario para producir los efectos deseados sobre un objetivo.



TIPOS DE OPERACIONES EN EL CIBERESPACIO

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

- **Operaciones Defensivas:**
  - Su objetivo es mantener la libertad de acción, evitando que se vea afectada la Confidencialidad, Integridad o Disponibilidad de la información.
  - Comprenden acciones para proteger, monitorizar, analizar, detectar y responder a actividades no autorizadas en sistemas de información propios.

  - Dos tipos:
    - Las realizadas permanentemente en los sistemas del Ministerio de Defensa (medidas de protección).
    - Las realizadas con misión de proteger un sistema específico contra una amenaza definida.

TIPOS DE OPERACIONES EN EL CIBERESPACIO

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

- **Operaciones de Explotación:**
  - Obtención de información de los sistemas adversarios designados como objetivos susceptibles de ser atacados.
  - Obtención de información del origen de ataques a sistemas propios.
  - Tipos:

    - Inteligencia de fuentes abiertas (OSINT): información DNS, Google hacking, sitios web y metadatos de archivos.
    - Reconocimiento pasivo: enumeración de dispositivos, escaneo de puertos activos (protocolos y servicios), identificación de SO,s y evaluación de vulnerabilidades.
    - Amenaza Persistente Avanzada (APT): exfiltración constante de información del objetivo mediante la penetración en sus sistemas.

TIPOS DE OPERACIONES EN EL CIBERESPACIO

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

- **Operaciones Ofensivas:**
  - Acciones realizadas en el ciberespacio para degradar, interrumpir, denegar o destruir sistemas de información o la propia información que estos almacenan.

  - Sincronizadas con acciones en otros dominios para alcanzar los objetivos militares asignados.
  - Requieren previamente de Operaciones de Explotación para la obtención de información.

Entorno Operacional

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

DÓNDE

NIVEL FÍSICO:

- **Geográfico:** ubicación geográfica tridimensional.
- **Red física:** servidores, terminales, electrónica de red, cableado, etc.

CÓMO, CUÁNDO

NIVEL LÓGICO:

- **Software**: sistemas operativos, programas, protocolos de comunicaciones, servicios, etc.
- **Normativa**: procedimientos, políticas, estructura organizativa, etc.

QUIÉN

NIVEL SOCIAL:

- **Persona lógica**: identidad digital, perfiles, avatares, etc.
- **Persona física**: individuo, organización, estado, etc.

ESTRATEGIA DE PROTECCIÓN Y DEFENSA A LA ICCN

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Mecanismos de coordinación
para la infraestructura críAca cibernéAca

Centro Operaciones Cibernéticas Conjunto

Políticas Nacionales
CONPES 3701 y CONPES 3854
Comisión Nacional Digital

Formación CiberComandos

Convenios y Planes Interinstitucionales

Proyecto: Centro nacional para la Protección y defensa de la IC en Colombia

Iniciativa de Ley para Asuntos del Ciberespacio

Ejercicios de Simulación y Entrenamiento

Actualización Periódica
Catálogo de ICCN

Plan Nacional para Protección y Defensa de la ICCN

Operaciones Conocidas

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

ELECCIONES 2018

CENSO NACIONAL DE POBLACIÓN Y VIVIENDA 2018 · COLOMBIA

▶ Noticias

Bogotá , lunes, 22 de enero de 2018 Foto: Juan David Tena - SIG

Se activa puesto de mando unificado para enfrentar amenazas de seguridad digital durante elecciones del 2018

Apoyo a la Gestión ante incidentes Cibernéticos
Censo Virtual y elecciones 2018

Cyber.CO 2017

CyberEX 2016

1 PUESTO – TEAM COLOMBIA

Protegemos el azul de la bandera

GUERRA CIBERNÉTICA

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Es el componente que extiende el poder cibernético detrás de los límites defensivos de las redes amistosas, para detectar, determinar, denegar el uso del ciberespacio y derrotar a los adversarios.

Protegemos el azul de la bandera

Fuera De Los Límites Defensivos

¿Cómo Nos Movilizamos Fuera De Los Límites Defensivos?

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Protegemos el azul de la bandera

Consideraciones Previas

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Si haces que los adversarios no sepan el lugar y la fecha de la batalla, siempre puedes vencer.

Solo los gobernantes iluminados y los generales sabios usan la mayor inteligencia del ejército para espiar, y por tanto consiguen grandes resultados.

Las operaciones secretas son esenciales en la guerra; a través de ellas se basa el ejército para hacer todos sus movimientos.

Sun Tzu (544 a. C. – 496 a. C.)

Pensemos

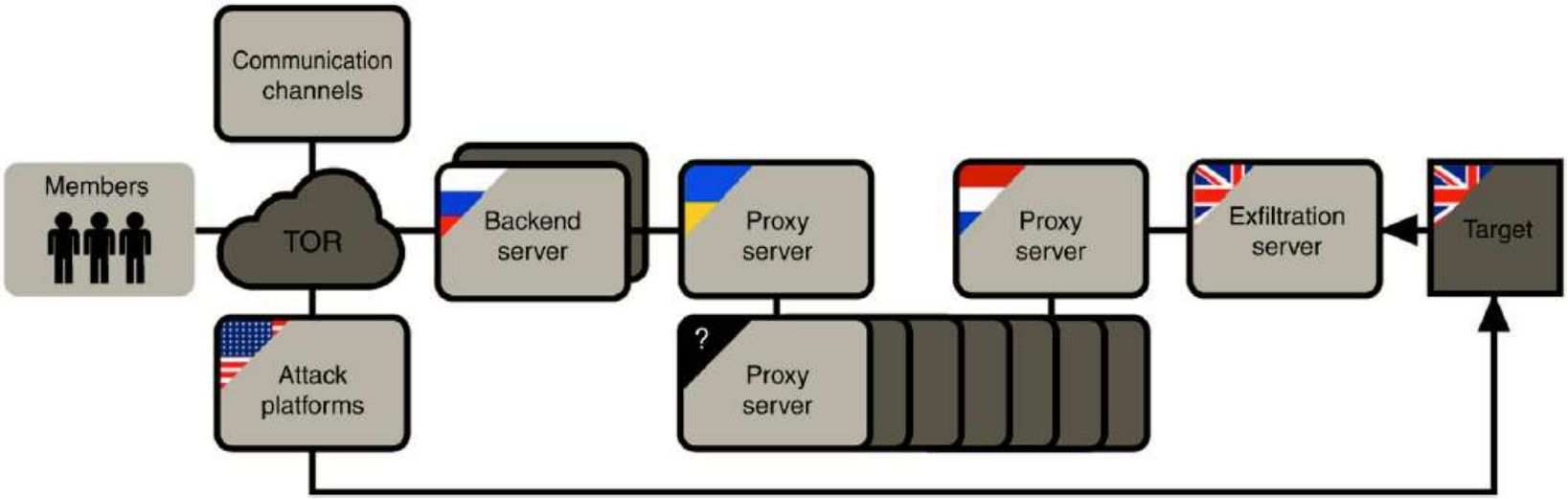
¿Cuál es la mejor forma de "movilizarnos" en el ciberespacio aprovechando sus bondades?

¿Cuál Podría Ser Una Bondad Relevante Del Ciberespacio?

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Protegemos el azul de la bandera

¿Cómo Es La Forma Más Adecuada De Salir De Los Límites Defensivos?



■ FIGURE 2.2 Example of an infrastructure configuration required for operations.

Los Servidores Virtuales Privados Juegan Un Papel Importante

MANIPULACIÓN DE INFORMACIÓN

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

Se desata una tormenta internacional para Facebook tras fuga de datos

Gobiernos del mundo piden explicaciones e investigan el escándalo que rodea a la red social.

Cambridge Analytica

El escándalo que hizo perder millones a Facebook en un día

Cambridge Analytica es acusada de robo de datos, interferencia política y chantajes con prostitutas.

MUNDO

El jefe de Facebook continúa su mea culpa ante el Congreso de EE. UU.

Mark Zuckerberg enfrenta este martes una sesión conjunta de dos comisiones del Congreso estadounidense en medio del espectacular escándalo por las fallas de seguridad de la gigante red social sobre la privacidad de sus usuarios.

El jefe de Facebook continúa su mea culpa ante el Congreso de EE. UU. Foto: AFP

QUE RECOLECTA GOOGLE

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

He mirado todos los datos que Google tiene sobre mí, y confirmo que es el Gran Hermano definitivo

Google registra cuándo y a qué hora utilizas cada app de tu móvil Android.

Google mantiene los datos aunque borres el historial de tu navegador

Un perfil con todos tus intereses

Protegemos el azul de la bandera

GOOGLE

https://takeout.google.com/settings/takeout?pli=1

TU ERES EL ESLABON MAS DEBIL POR ESO

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Protegemos el azul de la bandera

Preguntas

Referencias

- INCIBE
- Mando Conjunto de Ciberdefensa España.
- Comando Conjunto Cibernético Colombia.
- Profesor maestría TN Aponte Julián.
- OTAN