CIBERDEFENSA

NIVEL OPERACIONAL / GERENCIAL

ÁMBITO MILITAR

¿CÓMO ENFRENTAR ESTE NUEVO DOMINIO MILITAR?

OPERACIONES DEL CIBERESPACIO EN EL NIVEL OPERACIONAL

- Inserción de la Ciberdefensa en el proceso de planeamiento de nivel operacional.
- Influencia en el ciclo de reunión de información, inteligencia y contrainteligencia.
- Inserción de la Ciberdefensa en el proceso de toma de decisiones.

NIVELES DE LA GUERRA Y DE CONDUCCIÓN

- ESTRATÉGICO (**FINES**)
- **OPERACIONAL (MODOS)**
- TÁCTICO (**MEDIOS**)

TABLA 2: NIVELES DE LA GUERRA Y NIVELES DE CONDUCCIÓN[46]

NIVELES DE LA GUERRA	NIVELES DE CONDUCCIÓN	FINES	MEDIOS	ENFRENTAN (Método)
ESTRATÉGICO Poder	Político, Estratégico General o Nacional	Estado Final Estratégico	Todos los instrumentos del poder nacional	Voluntades (dialéctico)
	Estratégico Militar	Estado Final Estratégico Militar	Instrumento militar del poder nacional	
OPERACIONAL Poder y Fuerza	Operacional	Estado Final Operacional	Los medios militares asignados al TO	Maniobras Operacionales (heurístico)
TÁCTICO Fuerza	Táctico	Condiciones decisivas para lograr el EFO	Los medios enfrentados en cada operación militar	Maniobras Tácticas Medios de Combate (empírico)

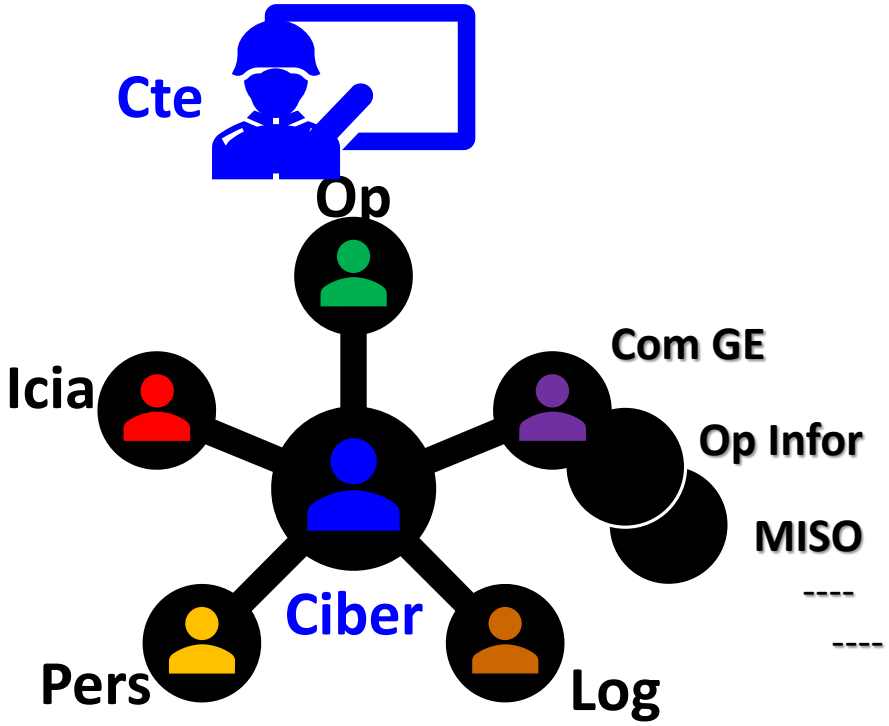
CA(R) Kenny A., CR(R) Locatelli O., TC Zarza, L. **ARTE Y DISEÑO OPERACIONAL**. 1a ed. Buenos Aires. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de la República Argentina, 2017.

CIBERDEFENSA EN EL PROCESO DE PLANEAMIENTO DE NIVEL OPERACIONAL

MÉTODO: DISEÑO OPERACIONAL

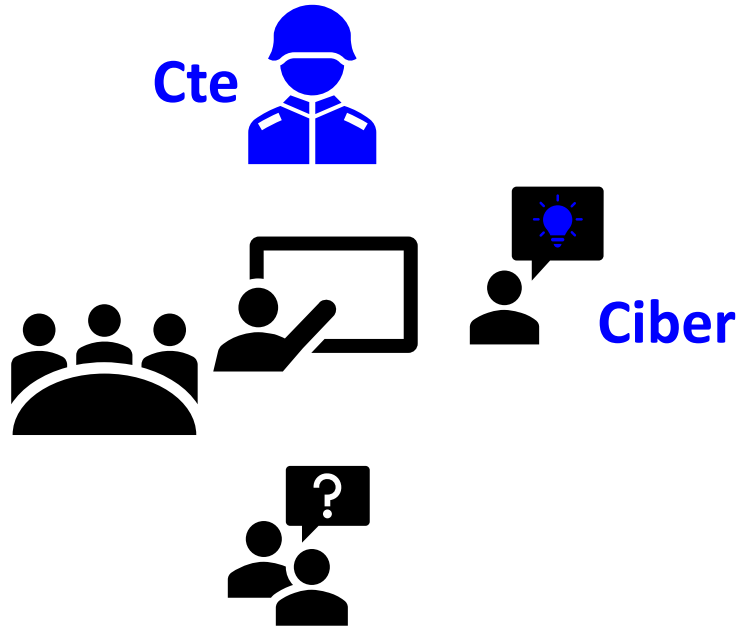
1. Identificación del problema.
2. Análisis del problema y enunciado de soluciones.
3. Confrontación.
4. Comparación.
5. Resolución del Comandante.

PLANEAMIENTO OFICIAL CIBER



DISEÑO OPERACIONAL Y PLANEAMIENTO CIBER

1. Identificación del problema.



A. Comprende el aspecto cibernético del problema:

- Ciberambiente de interés, limitaciones a las operaciones del ciberespacio, Fuerzas,actividades y aptitudes Ciber (Amigas y Enemigas), IICC, aspectos de SIGINT, Com GE.

Escenario Operacional (Ciber)

B. Estudia (preliminar) el Escenario Operacional:

- actores cooperadores y competidores; aspectos generales favorables, distintivos o limitantes de la Maniobra Estratégica; geolocalización del Ciberambiente de interés en la geometría del TO y su exterior; Restricciones a las Ops Ciber; Aspectos Políticos impuestos o supuestos; Aspectos Militares, Reglas de Empeñamiento Ciber (DICA en el ciberespacio)

Requerimientos de Información (EMC y nivel Estratégico)

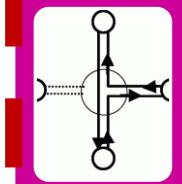
ANÁLISIS DEL CIBERAMBIENTE

Individuos / personas
Ciber-Personas

FUNCIÓN	RELACIÓN	CARACTERIZACIÓN
•Identidad •Roles / Perfiles •Privilegios	•Individuos •Grupos •Organizaciones	•Heterogénea •Global •Equilibrio Acceso / Seg

Información

FUNCIÓN	RELACIÓN	CARACTERIZACIÓN
• Comunicación, RRPP / Priv (Blogs, Plat Virt) • Educ, Difus (Youtube) • Conocimiento (Wikipedia), etc.	•Redes personales (I/O) •Redes grupales (horizontales) •Redes globales (entrópicas)	•Sin reglas •Diversidad de representación •Distribución de bajo costo



Lógica

APLICACIONES DE RED

SERVICIOS DE RED

ARQUITECTURA DE RED

CARACTERIZACIÓN

- Altamente elástica (Resiliencia)
- Recursiva (Jerarquía de sistemas)
- Límites fuertes

Física / Geoespacial

4G, MPLS, Ethernet, Fibra óptica, Wireless, WiFi, SCI / SCADA

SEGURIDAD FÍSICA

GEOLOCALIZACIÓN

CARACTERIZACIÓN

- Múltiples actores
- Interes económicos / Inversiones intensivas de capital
- Físicamente localizada

¿CÓMO ENFRENTAR ESTE NUEVO DOMINIO MILITAR?

ELEMENTOS DEL CIBERAMBIENTE

Sistemas del Sector Defensa:
- Industrias Militares
- Comando y Control
- Comunicaciones
- Armas
- Control
- Computarizados
- Tecnol Apy (PLC, E. Electr, Refrig, c/Incendio, etc)

Org(s) DC

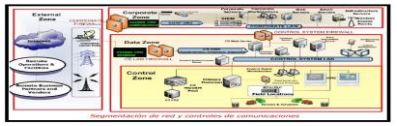
DC DC

Sistemas de los Sectores Estratégicos:
- **Gobierno y Administración Pública.**
- **Espacio.**
- **Transporte.**
- **Energía.**
- **Agua.**
- **Tecnologías de la Información y Comunicaciones.**
- **Industria nuclear.**
- **Industria química.**
- **Instalaciones de investigación.**
- **Salud.**
- **Alimentación.**
- **Sistema financiero y tributario.**

OB

Elem(s)
Ciber
Elem(s) Com GE

Infraestructuras Críticas en la Z Interés



Icia EstrNac / FFSS / FFPP

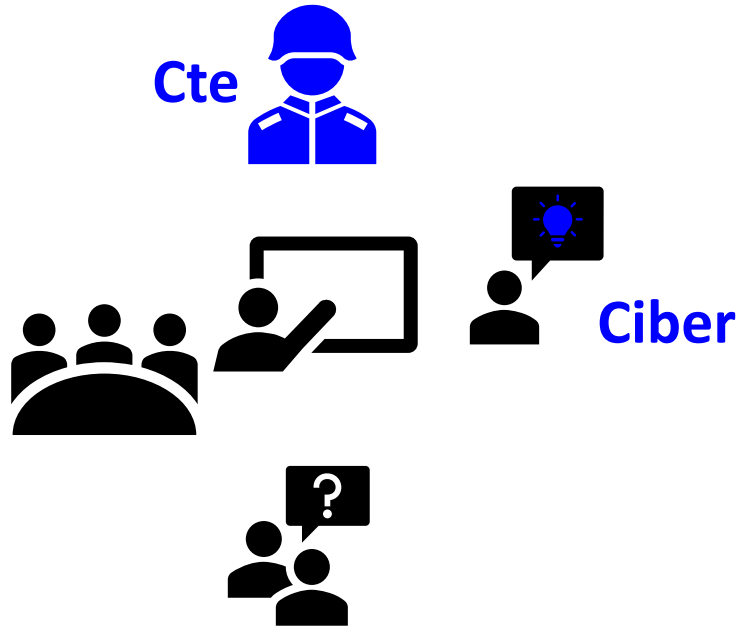
Ciber Terrorismo

Ciber Crimen

- Sist Ciberinteligencia / Contrainteligencia
- Aptitudes Operaciones de Información
- Redes Sociales / Redes de Hackers / Crackers / etc.
- Aptitudes Científicas y Tecnológicas

Diseño Operacional y Planeamiento Ciber

1. Identificación del problema.

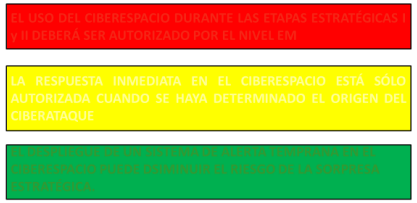


C. **Apreciación Preliminar del Oficial Ciber:**

- Aspectos generales del Escenario Operacional:
  - **POLÍTICA**
  - **MILITAR**
  - **ECONÓMICA**
  - **SOCIAL**

	POLÍTICA	MILITAR	ECONÓMICA	SOCIAL
ALFA		LAS OPERACIONES DEL CIBERESPACIO ANTES DE LA ACTIVACIÓN DEL TO DEBEN SER AUTORIZADAS POR EL NIVEL EM		
BETA	CAPACIDAD DE CIBERGUERRA CON HACKERS PATRIÓTICOS.	NO SE TIENE IDENTIFICADA Y LOCALIZADA LA CAPACIDAD CIBER (NO Y NEM)		POSEE HACKERS PATRIÓTICOS
GAMMA	APOYO CIBER A REQUERIMIENTO Y EN SECRETO.	CAPACIDAD DE CIBERATAQUE		
DELTA	APOYO A AMARILLO EN CSNU (LEGITIMIZACIÓN DEL USO DE LA FUERZA CIBER)			

- Restricciones
- Riesgos



¿CÓMO ENFRENTAR ESTE NUEVO DOMINIO MILITAR?

Diseño Operacional y Planeamiento Ciber

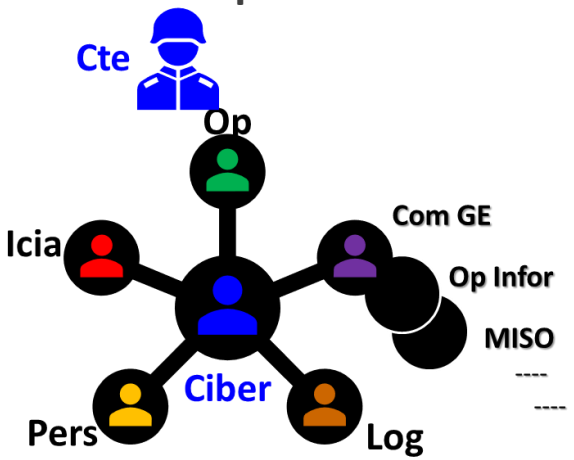
1.

2. Análisis del problema y enunciado de soluciones.
   - **Factores Operacionales (*Tempo*, Espacio, Fuerzas)**
   - **Requerimientos Operacionales Críticos**

3.

4.

5.



A. **Análisis de Factores Relativos al Ambiente Operacional, Poder de Combate Relativo, Factores de Fuerza y Debilidad:**
   - Objetivos de Valor Estratégicos (Propios y del Enemigo)
   - Infraestructuras Críticas que brindan servicios esenciales en el Nivel Estratégico y en el Nivel Operacional
   - Infraestructuras Críticas de Informaci en el Ciberambiente de interés.

B. **Análisis de actividades críticas y áreas funcionales prioritarias en relación a la Misión**

C. **Determinación de Capacidades, Requerimientos y Vulnerabilidades Críticas en el Ciberambiente de interés**

CAPACIDADES, REQUERIMIENTOS Y VULNERABILIDADES CRÍTICAS

Ciber Centro de Gravedad	Capacidades críticas (CC)
Sistemas e infraestructura de sistemas de información militar.	Implementar ciberataques contra los sistemas e infraestructura de sistemas de información por medios manuales (contratar a una persona para el uso de *malware* o utilizar un disco duro infectado con gusanos en esos sistemas).
	Infectar los sistemas de información militar del enemigo con virus informáticos, gusanos o *malware* para robar o reunir información (capturas de pantalla, pulsaciones de teclas y archivos) por infiltración en los sistemas o *spear fishing* mediante el uso de las redes sociales, fuentes abiertas de inteligencia (OSINT) e ingeniería social
	Implementar un *"Zero Day"* para explorar una base de datos, email y servidores conectados en Internet.
	Implementar ataques DDOS.

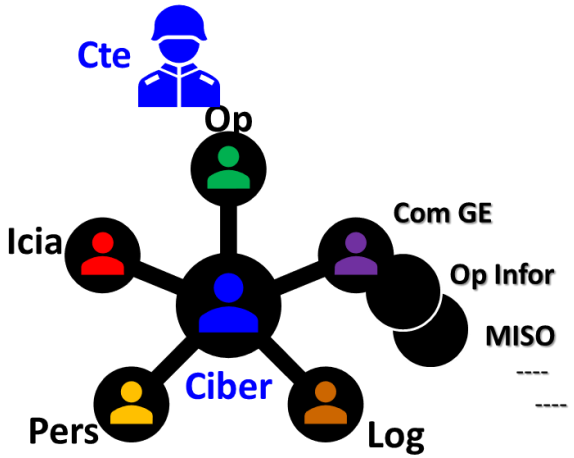
Vulnerabilidades críticas (VC)	Requerimientos críticos (RC)
Uso limitado de actividades de ciber inteligencia.	Reunir OSINT sobre sistemas e infraestructura de sistemas de información militar y sus requisitos del sistema mediante redes TOR o direcciones IP falsificadas.
Desafíos legales nacionales e internacionales (¿Es un acto de Guerra o no? Ambigüedad de las leyes y Reglas de Empeñamiento).	Elaborar un documento jurídico marco donde se definan claramente las actividades, tareas y funciones cibernéticas.
Falta de especialistas cibernéticos talentosos y especialistas en los ámbitos de planificación de las organizaciones militares.	Revertir la ingeniería y múltiples criterios de análisis de algunos conocidos *malware* dirigidos a recopilar información de los sistemas que infectan.
Falta de una clara definición de las tareas que deben realizar las instituciones al respecto de las actividades cibernéticas.	Formar un equipo de redes sociales que trabaje permanentemente en Facebook, Twitter, LinkedIn, Instagram y otras.

GD(R) de Vergara E., CA(R) Trama, G. **OPERACIONES MILITARES CIBERNÉTICAS. Planeamiento y Ejecución en el Nivel Operacional** .1a ed. Buenos Aires. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de la República Argentina, 2017.

¿CÓMO ENFRENTAR ESTE NUEVO DOMINIO MILITAR?

Diseño Operacional y Planeamiento Ciber

1.
2.
3. Confrontación.
4.
5.



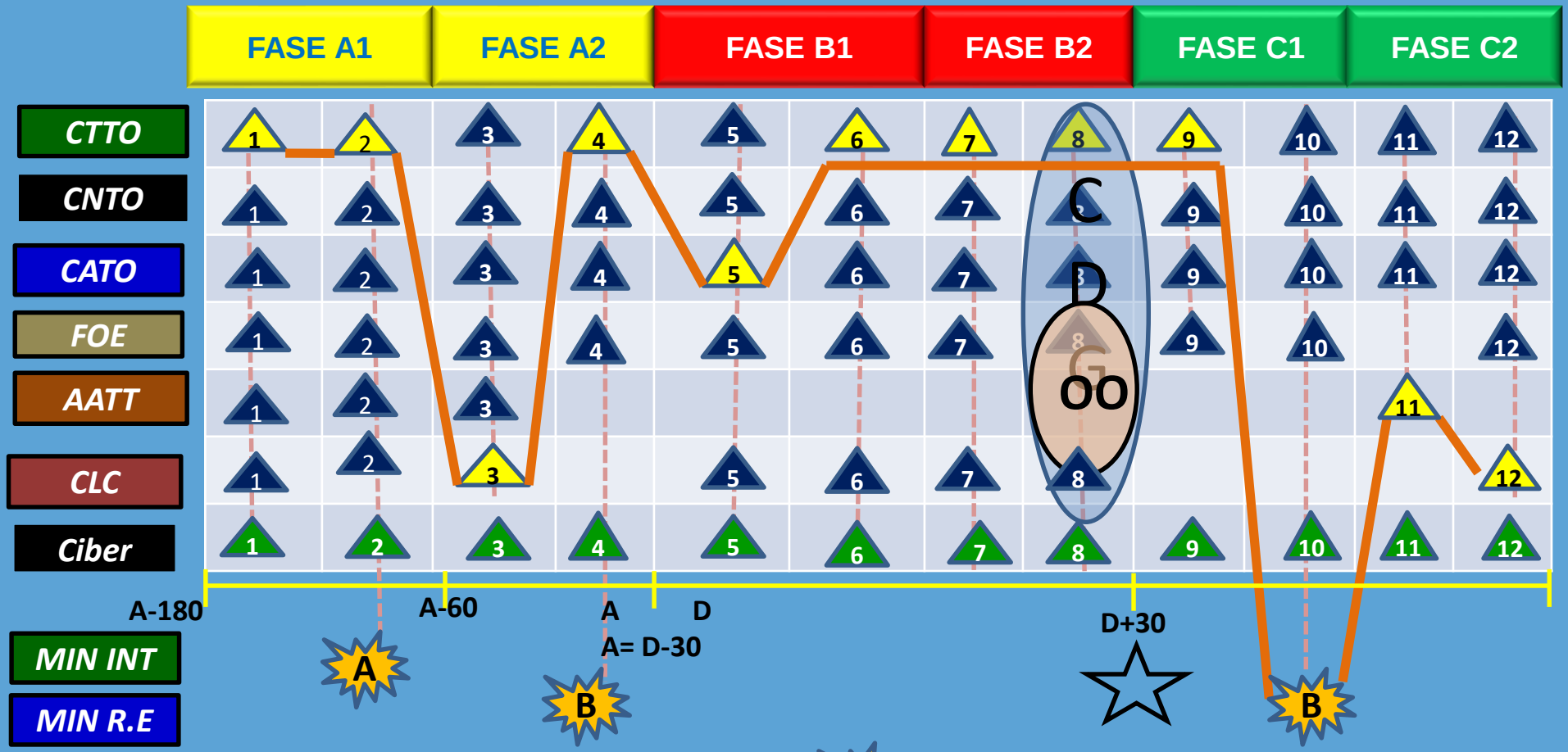
A. **Determinación de los agentes intervinientes (MILITARES o CIVILES), a disposición (GOBIERNO, SECTORES ECONÓMICOS Y DE SERVICIOS) y de aquellos necesarios fuera del nivel operacional (ESTRATÉGICOS NACIONALES o INTERNACIONALES).**

C. **Determinación de las LLO para cada tipo de Agencia (MILITAR, GOBIERNO y SECTORES ESTRATÉGICOS), la sucesión de Puntos Decisivos y criterios de finalización.**

D. **Análisis de los Modos de Acción (MA) y las tareas Ciber vinculadas**

E. **Determinación de la factibilidad y aceptabilidad del MA**

Línea de Operación CIBER



A Estabilización de la región lograda

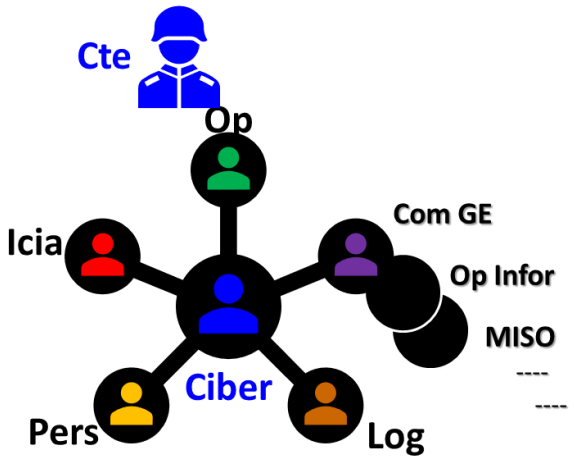
1. **SIST ALER TEMPR** desplegado.
2. **INFILTRACIÓN e INCUSIÓN CIBERNÉTICA** realizada.
3. **VELO Y ENGAÑO CIBERNÉTICO** completado.
4. **MANIPULACIONES CIBERNÉTICAS** completadas.
5. **INFRAESTRUCTURAS CRÍTICAS** protegidas.
6. **CIBERATAQUES a IICC** bloqueados.

B Maniobra política de disuasión finalizada

7. **ALTERNATIVAS ESCAL PRIVILEGIO** creadas
8. **ASALTO CIBERNÉTICO** ejecutado
9. **SIST ALER TEMPR** reconfigurado.
10. **CREDENCIALES DE ACCESO A OO CIBER** aseguradas.
11. **INFRAESTRUCTURAS CRÍTICAS** organizadas
12. **SIST COORD CIBER INTERAGENCIAL** establecido.

Diseño Operacional y Planeamiento Ciber

1.
2.
3.
4. Comparación.
5.



A. Estudio de las Ventajas y Desventajas de cada Modo de Acción

B. Conclusiones del Apoyo Cibernético al Modo de Acción Retenido:

- Listado de **Tareas y Efectos deseados** para el Modo de Acción Retenido
- Noción de Apoyo Cibernético

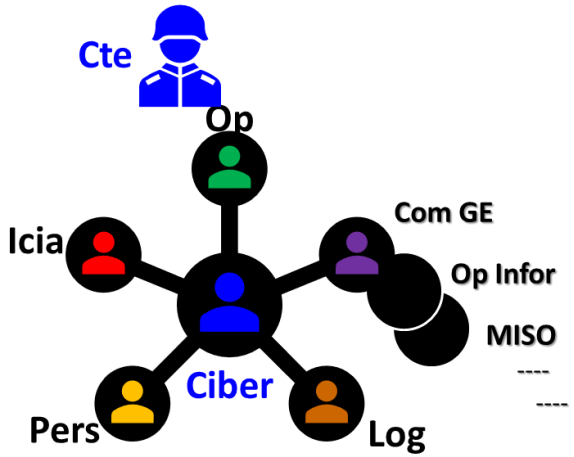
Tareas y Efectos

Cte	JEM	C I	C II	C III	C IV	C V	C VI	CIBER

- **Fase A1:**
  - Crear un órgano coordinador entre la Ciberseguridad Nacional y la Ciberdefensa Militar para planificar acciones interagenciales.
- **Fase A2:**
  - Incrementar las acciones de Ciberdefensa y Guerra Electrónica para apoyar el esfuerzo principal.
- **Fase B1:**
  - Ejecutar tareas de Ciberdefensa Activa, VyE Cibe, Guerra Electrónica y COMINT para proteger el Sist C2 y IICC de los OOVE.
- **Fase B2:**
  - Realizar Ciberataques, tareas de Guerra Electrónica y COMINT para neutralizar la capacidad de C2 del Enemigo.
- **Fases C1 y C2:**
  - Mantener el sistema de Alerta Temprana de el Ciberespacio.

Diseño Operacional y Planeamiento Ciber

1.
2.
3.
4.
5. Resolución del Comandante.



A. Diseño del Concepto de Apoyo Cibernético

B. Concepto de Apoyo Cibernético a la Campaña

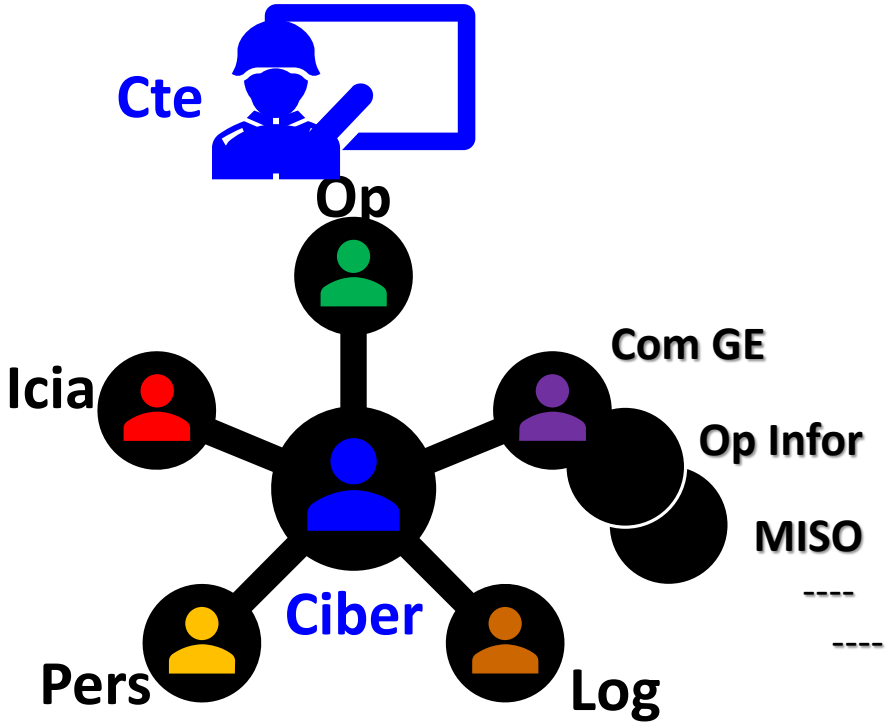
- Organización para el Combate
- Enunciado del Concepto de Apoyo

CIBERDEFENSA EN EL PROCESO DE PLANEAMIENTO DE NIVEL OPERACIONAL

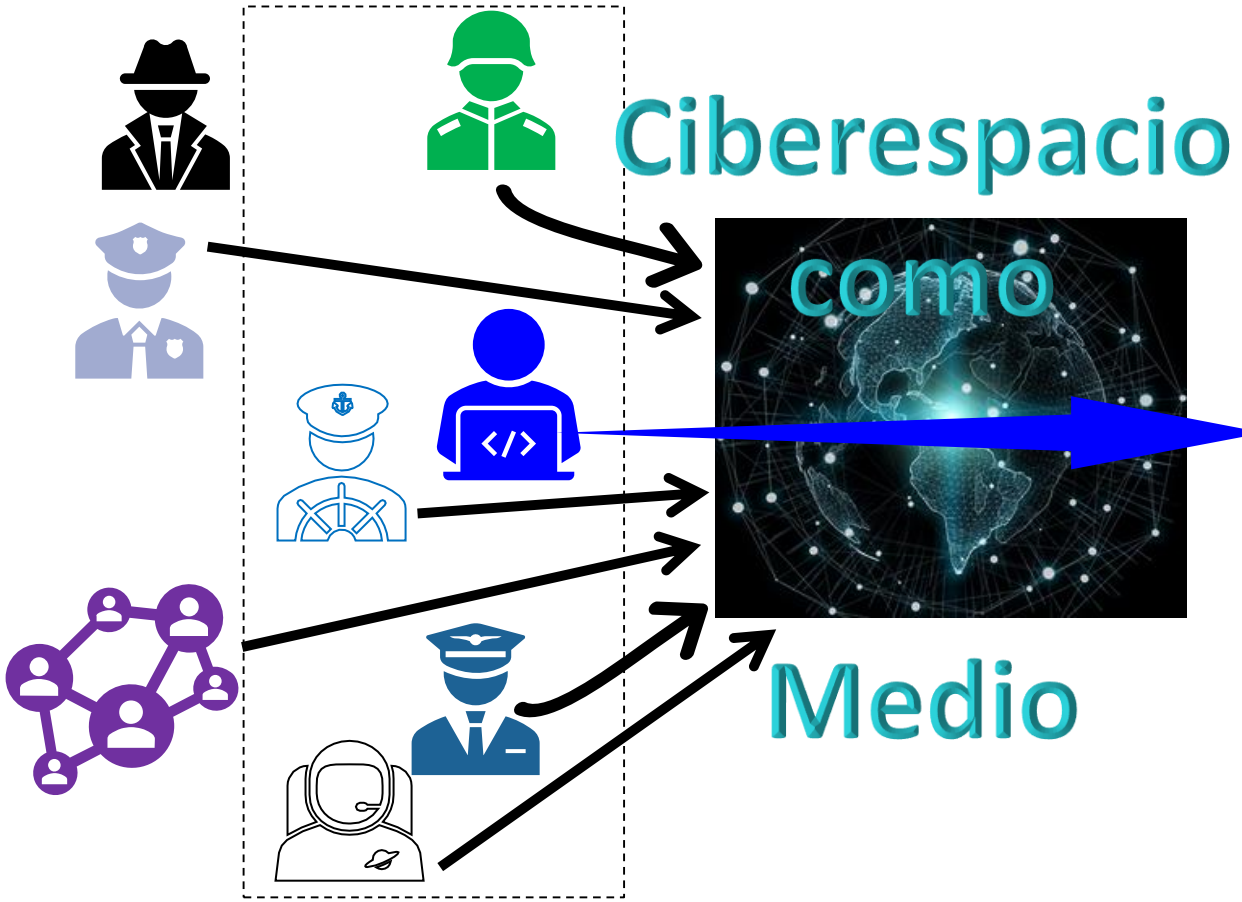
MÉTODO: DISEÑO OPERACIONAL

1. Identificación del problema.
2. Análisis del problema y enunciado de soluciones.
3. Confrontación.
4. Comparación.
5. Resolución del Comandante.

PLANEAMIENTO OFICIAL CIBER



INFLUENCIA EN EL CICLO DE REUNIÓN DE INFORMACIÓN, INTELIGENCIA Y CONTRAINTELIGENCIA



- **Operaciones Militares Cibernéticas**
- Operaciones de Apoyo de información a las Op Mil (MISO)
- Guerra Electrónica
- Engaño Militar
- de Inteligencia (Recol Infor, sabotaje, descifrado criptográfico, afectar Ciberpers,…)
- Contrainteligencia (MSCI, “tiempo real”, Secreto, Desinformación, Redes Sociales, *Fake News*, Log Ciber)

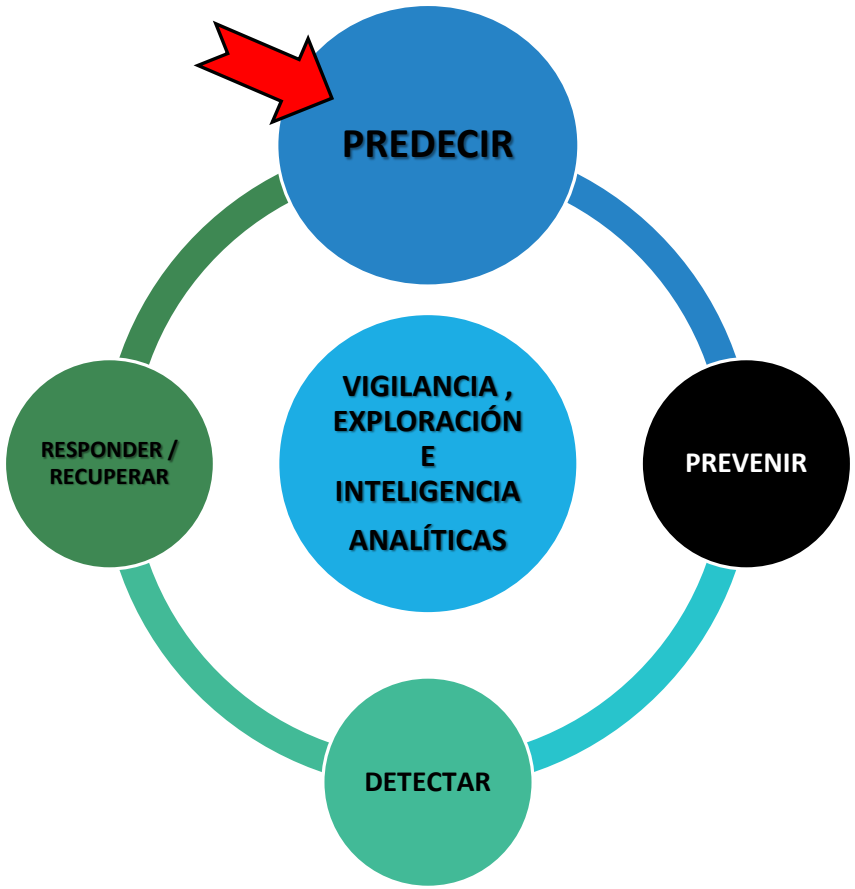
❖ **Vulnerabilidades en los Sist Mil e IICC (OE) >> Oponentes + Gpos Hackers, Cibercriminales,…**

- Prep Log
- Lib Mbra
- Obj Mil

Operaciones de Información

¿CÓMO ENFRENTAR ESTE NUEVO DOMINIO MILITAR?

INSERCIÓN DE LA CIBERDEFENSA EN EL PROCESO DE TOMA DE DECISIONES



PROCESO	ACTIVIDAD	TECNOLOGÍAS
PREDECIR	• ANÁLISIS PROACTIVO DE LA EXPOSICIÓN Y DEL RIESGO • PREDICCIÓN DE CIBERATAQUES • ANÁLISIS DE TENDENCIAS, TTP DE AMENAZAS Y VULNERABILIDADES (LÍNEA BASE DE SISTEMAS TIC)	• TECNOLOGÍAS BI • TECNOLOGÍAS AI / ML • HERRAMIENTAS ANALÍTICAS (HA) • SOFTWARE DE GESTIÓN DE VULNERABILIDADES Y AMENAZAS (SGVA)
PREVENIR	• ROBUSTECIMIENTO, SEGMENTACIÓN Y AISLAMIENTO DE SISTEMAS CRÍTICOS • VELO Y ENGAÑO DE ATACANTES • PREVENCIÓN DE INCIDENTES (ENSAYOS Y SIMULACIÓN)	• SGVA • SISTEMAS DE AUTOMATIZACIÓN DE LAS OP SEG (SAOS) • HERRAMIENTAS DE VIRTUALIZACIÓN Y SIMULACIÓN • TECNOLOGÍAS AI / ML
DETECTAR	• DETECCIÓN DE INCIDENTES • CONFIRMACIÓN Y PRIORIZACIÓN DEL IMPACTO • CONTENCIÓN DE INCIDENTES	• HA • SGVA y SIEM • SAOS • ML
RESPONDER / RECUPERAR	• SOLUCIÓN / IMPLEMENTACIÓN DE CAMBIOS DE SEGURIDAD • MODELADO / DISEÑO DE NUEVOS PROCEDIMIENTOS Y CONTROLES • INVESTICACIÓN INFORMÁTICA FORENSE	• SAOS • HA • SGVA y SIEM

¿CÓMO ENFRENTAR ESTE NUEVO DOMINIO MILITAR?

OPERACIONES DEL CIBERESPACIO EN EL NIVEL OPERACIONAL

- Inserción de la Ciberdefensa en el proceso de planeamiento de nivel operacional.
- Influencia en el ciclo de reunión de información, inteligencia y contrainteligencia.
- Inserción de la Ciberdefensa en el proceso de toma de decisiones.

¿CÓMO ENFRENTAR ESTE NUEVO DOMINIO MILITAR?

¡Muchas gracias!

CDCICERCHIA@FIE.UNDEF.EDU.AR