SEMINARIO

"LAS GUERRAS DE CUARTA GENERACIÓN Y LOS DESAFÍOS DE LA CIBER GUERRA Y CIBERSEGURIDAD"

Seminario Ciber Guerra

Enfocado en la guerra del futuro 4GW, la acciones de la ciber guerra como una de las amenazas no convencionales propias de este escenario y protección de ciberseguridad.

Agenda del Seminario

- **Introducción** al tema Ciber Guerra
- **Presentación** de los expositores
- **Desarrollo** de las exposiciones
- **Foro** con los expositores
- **Cierre** del seminario

regto.sangabriel. jesoto21@gmail.com

Integrantes del Panel y Temas

- Moderador: May (IPM)Julio Vásquez Méndez
- Tema 1: Guerra del Futuro 4GW CRL Julio Soto Silva
- Tema 2:Ciber Guerra GDB René Leiva Villagra
- Tema 3: Ciber Seguridad Srta Fernanda Mattar Catalán

Introducción Ciber Guerra

- Ciber => cibernético, relacionados con el mundo de las plataformas informaticas ,Sw , App y de la realidad virtual: emergen el ciberespacio, cibernauta, ciberguerra , ciberseguridad , ciberataque, cibercrimen, etc.

- La ciberguerra, es un conflicto armado cuyo campo de batalla es el ciberespacio. Se basa en ataques digitales para dañar los sistemas informáticos que permiten a las Instituciones y organizaciones de un país realizar tareas esenciales.

Ciberguerra: el campo de batalla es digital

- La ciberguerra emplea **armas tecnológicas** que afectan la estabilidad y la seguridad de los países. Las batallas son digitales y los ataques se planean detrás de una pantalla.

- Pero **¿en realidad sabemos qué es la ciberguerra y cuáles son sus armas?** Para entender mejor a qué peligros nos enfrentamos, se definen los tipos de guerras cibernéticas.

¿Por qué surgen las ciberguerras?

- Tipos de guerras cibernéticas
  - 1. Sabotaje informático
  - 2. Terrorismo cibernético
  - 3. Espionaje Cibernético
  - 4. Activismo civil (hacktivismo)
- ¿Qué motivaciones hay detrás?
  - Deseo de desestabilizar un gobierno hasta el control de sus recursos estratégicos.
- No existen acciones ni Instituciones aisladas la conectividad del mundo es clave IoE .

Cuantas Generacion de Guerras existen

- La Guerra de primera generación 1GW la asociamos a las luchas con armas de fuego y la lucha por el poder.
- La segunda G2W comenzaría con la revolución industrial.
- La tercera G3W se podría situar durante la segunda guerra mundial
- Cuarta Guerra G4W se visualiza como una hipótesis de conflicto emergente de la pos-Guerra Fría.

¿Que Generación de la Guerra estamos?

- En nuestra época, ya podemos afirmar que nos encontramos ante la denominada Guerra de Cuarta Generación, un término usado por expertos analistas y expertos para hacer referencia a los diversos conflictos que derivan de las nuevas tecnologías e interacciones globalizadas y que por ende se hace necesario innovadoras estrategias.
- Guerra de cuarta generación es una denominación dentro de la doctrina militar estadounidense que comprende a la guerra de guerrillas, la guerra asimétrica, la guerra de baja intensidad, hibrida , la guerra sucia, el terrorismo de estado u operaciones similares y encubiertas, la guerra popular, la guerra civil, desinformación.

Escenario de la Ciber Guerra es el Ciberespacio

- El ciberespacio es un ámbito artificial que fusiona las redes de comunicación, datos e información en un entorno digital, en el cual interactúan las personas con su contenido, pasando del mundo real al mundo virtual.
- En una línea similar, la International Organization for Standardization (ISO) define al ciberespacio como un complejo entorno resultado de la interacción de personas, software y servicios en internet, apoyado en tecnologías de la información y las comunicaciones físicas distribuidas en todo el mundo (ISO, 2012)

Escenario de la Ciberguerra es el CIBERESPACIO

El ciberespacio constituye un **escenario táctico, estratégico y operativo diferente** de los espacios **terrestre, marítimo, aéreo y exterior** que ha sido calificado en la doctrina como uno de los ***global commons***. Es un **entorno complejo** resultante de la interacción entre las personas, *software* y los servicios en Internet por medio de dispositivos tecnológicos (TIC) conectados a redes, las cuales no existen ningún tipo de forma física sino virtuales.

EL PAPEL DEL ESTADO EN LAS GUERRAS DE CUARTA GENERACIÓN BAJO LA ÓPTICA DE LA TEORÍA DE LA EFICIENCIA DINÁMICA

- Resumen: El Estado ha dejado de ser el único actor relevante en el ámbito internacional y, en ciertos lugares del mundo, su monopolio del ejercicio de la violencia se ha visto erosionado.
- Mientras que las guerras interestatales clásicas parecen haberse convertido en una posibilidad remota, las amenazas planteadas por actores armados no estatales han proliferado en las últimas décadas.
- Las respuestas implementadas por los Estados no siempre han resultado adecuadas; incluso han llegado a alimentar todavía más los conflictos.
- En nuestro análisis de tales problemas de seguridad recurriremos a la teoría de la eficiencia dinámica de Jesús Huerta de Soto, lo que nos permitirá explicar los casos de resolución exitosa de un conflicto armado a través de la iniciativa privada, así como cuestionar la legitimidad del monopolio estatal del ejercicio de la violencia; todo ello en aras de proponer una alternativa viable desde el mercado.

- Palabras clave: Estado, guerra de cuarta generación, eficiencia dinámica, terrorismo.

Ciberseguridad

- La ciberseguridad son acciones desarrolladas en organizaciones, tanto públicas como privadas, aplicadas de forma transversal por medio de procesos, controles, concientización y tecnologías con el fin de proteger sus sistemas y usuarios, a través de la reducción de riesgos de posibles ciberataques

  Las acciones que se deben generar tienen que estar acompañadas de regulaciones de gobierno sólidas.
- Identificar, Proteger, Detectar, Responder y Recuperar

  Chile puesto 56 a nivel mundial






Agenda del Seminario

- **Introducción** al tema Ciber Guerra
- **Presentación** de los expositores
- **Desarrollo** de las exposiciones
- **Foro** con los expositores
- **Cierre** del seminario

LAS GUERRAS DE CUARTA GENERACIÓN

JULIO E. SOTO SILVA
Coronel (R)
Profesor de Estrategia
ORCID ID: http://orcid.org/0000-0002-4195-4914
jesoto21@gmail.com

PROPÓSITO

Entregar un marco de referencia sobre el estado del arte de la guerra en el actual escenario internacional, para comprender la importancia del papel que juegan las Ciber amenazas, la Ciber Guerra y la Ciberseguridad en el campo de batalla actual y del futuro.

- **Antecedentes generales.**
- **Cambios en el escenario político- estratégico internacional.**
- **Las llamadas Guerras de Cuarta Generación (4GW).**
- **Reflexiones finales.**

ANTECEDENTES GENERALES

LA PAZ DE WESTFALIA

(Tratados Osnabrûk 15 de mayo y Mûnster 24 de octubre de 1648)

Término "Guerra de los 30 años" en Alemania y de la "Guerra de 80 años" entre España y Países Bajos

- **MARCA DIFERENCIA ENTRE GUERRAS ANTIGUAS Y "MODERNAS"**
- **ESTADO ESTABLECE EL MONOPOLIO SOBRE LA GUERRA.**

  (SOBERANÍA E INTEGRIDAD TERRITORIAL)
- **NATURALEZA DE LA GUERRA Y CONCEPTOS PRIMARIOS NO HAN CAMBIADO**

EDENTES GENERALES

PAZ DE WESTFALIA

rûb 15 de mayo y Münster 24 de octubre de 1648)

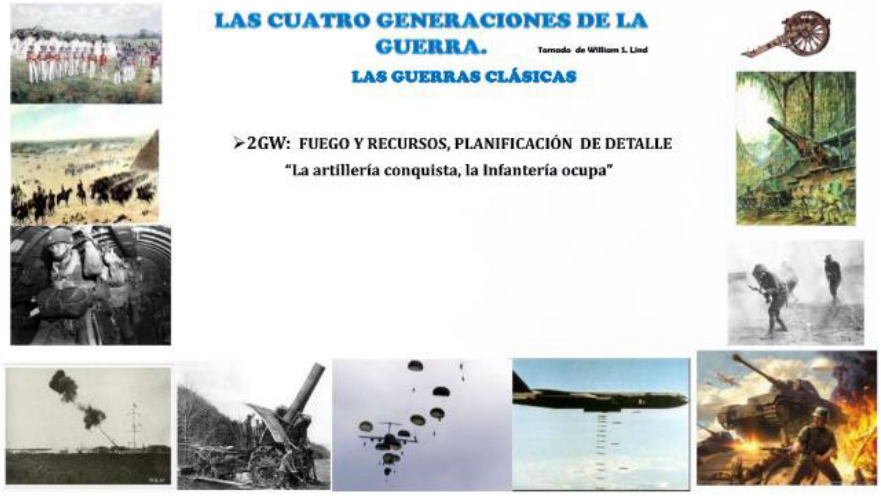
los 30 años" en Alemania y de la "Guerra de 80 años" entre España y Países Bajos

- MARCA DIFERENCIA ENTRE GUERRAS ANTIGUAS Y "MODERNAS"
- ESTADO ESTABLECE EL MONOPOLIO SOBRE LA GUERRA.

  (SOBERANÍA E INTEGRIDAD TERRITORIAL)
- NATURALEZA DE LA GUERRA Y CONCEPTOS PRIMARIOS NO HAN CAMBIADO

regto.sangabriel. jesoto21@gmail.com

regto.sangabriel. jesoto21@gmail.com



regto.sangabriel. jesoto21@gmail.com

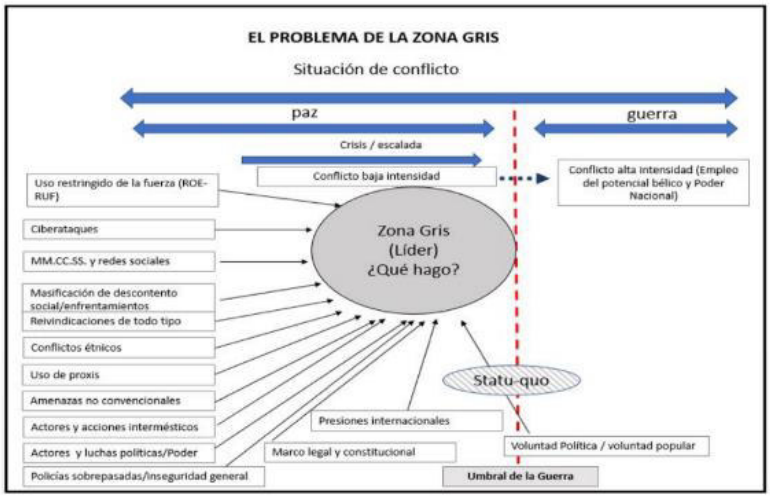
VUCA

- VOLÁTIL
- INCIERTO (UNCERTAINTY)
- COMPLEJO
- AMBIGÜO

regto.sangabriel. jesoto21@gmail.com

LA ZONA GRIS

La Zona Gris es la zona del espectro de los conflictos donde predominan las actuaciones situadas al margen del principio de buena fe (bona fides), entre los actores políticos, que pese a alterar notablemente la paz, no cruzan los umbrales que permitirían o exigirían el uso total de la fuerza para restaurar el clima de buena convivencia social y política de un país.



regto.sangabriel. jesoto21@gmail.com

LAS CUATRO GENERACIONES DE LA GUERRA.

Tomado de William S. Lind

4GW: GUERRA DE LA INFORMACIÓN.

- **Todos los días, durante las 24 horas, hay un ejército que apunta a su cabeza: no utiliza tanques, aviones ni submarinos, sino información direccionada y manipulada por medio de imágenes y titulares.**
- **Un Ejército invisible se está apoderando de su mente, de su conducta y de sus emociones.**
- **No es una guerra por conquista de territorios, sino de una guerra por conquista de cerebros**

GUERRAS DE CUARTA GENERACIÓN (4GW)

- Cambio más radical desde la Paz de Westfalia.
- El Estado pierde su monopolio de la guerra. Las FF.AA. se hallan hoy luchando en contra de oponentes no estatales tales como Al-Qaeda, Hamas, Hezbolá, DAESH, entre otros.
- Caracterizada por un retorno al mundo de culturas, y no simplemente estados en conflicto.
- En casi todos los lugares, el Estado está perdiendo por las llamadas "nuevas amenazas".

regto.sangabriel. jesoto21@gmail.com

¿CÓMO ES LA 4GW?

- La invasión mediante la inmigración masiva puede ser tan peligrosa como la invasión que emplea un ejército de Estado.
- La "guerra contraterrorista" y la "guerra psicológica" son las dos columnas estratégicas que sostienen a la 4GW, con los medios de comunicación convertidos en los nuevos ejércitos de conquista.
- El desarrollo tecnológico e informático, las TICs, la globalización del mensaje y las capacidades para influir en la opinión pública mundial convierten a la guerra psicológica mediática en el arma estratégica dominante de la 4GW .
- Ello permite superar a veces la asimetría entre actores en pugna mediante el empleo de medios y estrategias no convencionales por parte del más débil.

regto.sangabriel. jesoto21@gmail.com

LA ÉTICA Y LA MORAL

- **El poder de las redes sociales puede debilitar a una institución militar, desde dentro por la falta u omisión de atención a los valores por parte de uno de sus integrantes. (Abu Graib (2003)**

LA ÉTICA Y LA MORAL

- **O bien, un desconocido "hacker" que usando esta herramienta puede llegar a trastocar los valores y virtudes de los soldados mediante la entrega de información falsa y tendenciosa, para minar la voluntad de lucha, logrando sin disparar un tiro, quebrantar su esquema de valores y virtudes y conducirlo a la derrota. Fake News, Guerra Psicológica.**

regto.sangabriel. jesoto21@gmail.com

GUERRAS DE CUARTA GENERACIÓN (4GW)

- Las fuerzas militares, son sustituidas por grupos operativos descentralizados especialistas en insurgencia y contrainsurgencia, y por expertos en comunicación y psicología de masas.
- No se desarrolla en teatros de operaciones visibles.
- No hay frentes de batalla con elementos materiales: la guerra se desarrolla en escenarios combinados, sin orden aparente y sin líneas visibles de combate; los nuevos soldados no usan uniforme y se mimetizan con los civiles.

"GUERRA SIN FUSILES"

GUERRA IRRESTRICTA
GUERRA HÍBRIDA
GUERRA ASIMÉTRICA

GUERRAS DE CUARTA GENERACIÓN (4GW)

"LA ESTRATEGIA"

- FINES
- MEDIOS
- FORMAS

regto.sangabriel. jesoto21@gmail.com

GUERRAS DE CUARTA GENERACIÓN (4GW)

- Las tácticas y estrategias militares son sustituidas por tácticas y estrategias de control social, mediante la manipulación informativa y la acción psicológica orientada a direccionar una conducta social masiva.
- El objetivo ya no apunta a la destrucción de elementos materiales (bases militares, soldados, infraestructuras civiles, etc), sino al control del cerebro humano.
- El objetivo estratégico ya no es el apoderamiento y control de áreas físicas (poblaciones, territorios, etc.) sino el apoderamiento y control de la conducta social masiva.
- Además del uso de las "nuevas amenazas" o "híbridas" usándolas como una estrategia concertada.

GUERRAS DE CUARTA GENERACIÓN (4GW)

Amenazas Híbridas:
Combinación de fuerzas regulares, irregulares, terroristas o criminales de actores estatales o no estatales, con acceso a armas sofisticadas y que no se adhieren necesariamente al Derecho Internacional Humanitario.

DESAFÍOS QUE NOS DEJA LA 4GW

- Lecciones que las FF.AA. puedan aprender de las policiales ¿cambio de roles?

POLIVALENCIA? MULTIFUNCIONALIDAD?
NO SER EFICIENTES EN LO EQUIVOCADO

DESAFÍOS QUE NOS DEJA LA 4GW

- Lecciones que las FF.AA. puedan aprender de las policiales ¿cambio de roles?
- Habilidades en el combate urbano y entre la población civil.
- No humillar a las fuerzas adversarias derrotadas.

DESAFÍOS QUE NOS DEJA LA 4GW

- Lecciones que las FF.AA. puedan aprender de las policiales ¿cambio de roles?
- Habilidades en el combate urbano y entre la población civil.

- No humillar a las fuerzas adversarias derrotadas.
- Valor y ejemplo de los Comandantes.... "estar más cerca de su gente"
- Usar los medios de acuerdo a sus fortalezas.
- Desarrollar capacidades para fortalecer la "Inteligencia cultural".

- Adecuarse al concepto de "Tiempo Real" y rapidez del ciclo de toma de decisiones.

LA "TRINIDAD" Y LA 4GW

El primer acto de discernimiento, el mayor y más decisivo que ejecutan el estadista y el jefe militar es establecer correctamente la clase de guerra que van a enfrentar.

Esta trinidad, la constituyen el odio la enemistad y la violencia primitiva,(ciego impulso natural) pertenece al pueblo, el azar y las probabilidades al general y el carácter subordinado de instrumento político, problema del estadista. El problema es mantener a la teoría en el equilibrio estas tres tendencias como tres polos de atracción.

La 4GW altera en forma dramática la segunda componente, lo que para el **E-N percibe como ruido aleatorio, es un alto flujo de informaciones** que circula por las redes

¡ RUIDOS Y SEÑALES!

A MODO DE CONCLUSIONES

- No habrá marco regulatorio (Ginebra).
- Lo que funciona a nivel táctico y físico no funcionará a nivel operativo, estratégico, mental y moral, donde se decide la 4GW.
- Las FF.AA. Son el "partido más débil", a pesar de la RAM y la tecnología asociada.
- "Perder para ganar," para no destruir el Estado.
- No es algo novedoso, sino retorno a las guerras antes del Estado.

A MODO DE CONCLUSIONES

- "Perder para ganar," para no destruir el Estado.

regto.sangabriel. jesoto21@gmail.com

A MODO DE CONCLUSIONES

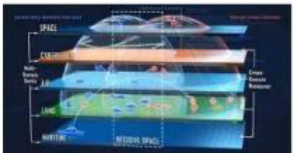
- ❖ No habrá marco regulatorio (Ginebra).
- ❖ Lo que funciona a nivel táctico y físico no funcionará a nivel operativo, estratégico, mental y moral, donde se decide la 4GW.
- ❖ Las FF.AA. Son el "partido más débil", a pesar de la RAM y la tecnología asociada.
- ❖ "Perder para ganar," para no destruir el Estado.
- ❖ No es algo novedoso, sino retorno a las guerras antes del Estado.

- ❖ Muchos actores diferentes librarán guerras por otras razones, no solo por "la extensión de la política por otros medios"
- ❖ Tácticas no son nuevas, muchas son de la guerrilla.
- ❖ Mayor acceso a TICs y otras tecnologías que le dan capacidad asimétrica; los estados moralmente restringidos.

- ❖ Muchos actores diferentes librarán guerras por otras razones, no solo por "la extensión de la política por otros medios"
- ❖ Tácticas no son nuevas, muchas son de la guerrilla.
- ❖ Mayor acceso a TICs y otras tecnologías que le dan capacidad asimétrica; los estados moralmente restringidos.
- ❖ No hay nada nuevo: Sólo es novedoso para las FF.AA. de un Estado diseñadas para luchar en contra de las FF.AA. de otro Estado.
- ❖ Necesidad de inteligencia robusta que pueda distinguir "Ruidos de Señales"

- ❖ **VOLUNTAD DEL ESTADO PARA ENFRENTARLA aspectos legales, estrategias, trabajo interagencial. etc.**
- ❖ **ADECUACIÓN DE LAS FF.AA. : Nuevas capacidades, Uso de FF. EE., Operaciones Multidominio ¿?.**

- Muchos actores diferentes librarán guerras por otras razones, no solo por "la extensión de la política por otros medios"
- Tácticas no son nuevas, muchas son de la guerrilla.
- Mayor acceso a TICs y otras tecnologías que le dan capacidad asimétrica; los estados moralmente restringidos.
- No hay nada nuevo: Sólo es novedoso para las FF.AA. de un Estado diseñadas para luchar en contra de las FF.AA. de otro Estado.
- Necesidad de inteligencia robusta que pueda distinguir "Ruidos de Señales"



Las operaciones multidominio consideran en su accionar las diferentes dimensiones del campo de batalla moderno. Por ello, su ámbito de influencia se da en lo terrestre, marítimo, aéreo, ciberespacial, aeroespacial, como también en el espectro electromagnético .

GUERRAS DE CUARTA GENERACIÓN (4GW)

MOSSAD?

CIA ?

MI6?

PENTÁGONO ?

¿ES ALGO NUEVO?

……Existen cinco clases de agentes secretos que pueden utilizar: los agentes indígenas, los interiores, los dobles, los liquidables y los agentes flotantes. Cuando estos cinco tipos de agentes están actuando simultáneamente sin que nadie conozca sus procedimientos se les llama "La Divina Red" y constituyen el tesoro más preciado de un soberano…."

GUERRAS DE CUARTA GENERACIÓN (4GW)

¿ES ALGO NUEVO?

……Existen cinco clases de agentes secretos que pueden utilizar: los agentes indígenas, los interiores, los dobles, los liquidables y los agentes flotantes. Cuando estos cinco tipos de agentes están actuando simultáneamente sin que nadie conozca sus procedimientos se les llama "La Divina Red" y constituyen el tesoro más preciado de un soberano…."

GUERRAS DE CUARTA GENERACIÓN (4GW)

"…..De esta forma, los que son expertos en el arte de la guerra, someten al ejército enemigo sin combate. Toman las ciudades sin efectuar el asalto, y derrocan un estado sin operaciones prolongadas.
……..
Sun Tzu….. "El Arte de la Guerra". SigloV AC.

¿ES ALGO NUEVO?

LAS GUERRAS DE CUARTA GENERACIÓN

MUCHAS GRACIAS

JULIO E. SOTO SILVA
Coronel (R)
Profesor de Estrategia
ORCID ID: http://orcid.org/0000-0002-4195-4914
jesoto21@gmail.com

1

Las Ciber Amenazas y la Ciberguerra.

RENÉ LEIVA V

2

Las Ciber Amenazas y la Ciberguerra

RENÉ LEIVA V
Rene.Leiva@acague.cl
leivarene@yahoo.com
+569 53341167

3

Temario

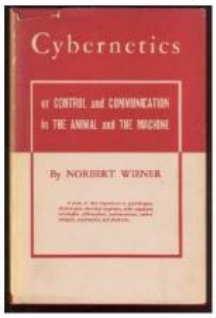
- ✓ Hacia la Ciberguerra
- ✓ Infoops
- ✓ Combate por el Mando y Control
- ✓ Objetivos rentables para la ciberguerra en el campo de batalla futuro.
- ✓ La Ciberguerra en el Conflicto Híbrido

4

CONCEPTUALIZANDO

El matemático Norbert Wiener, en la década de los 40´, implantó el término inglés "Cybernetics", orientado a la toma de decisiones, generación de órdenes o simples comandos de acción .

Aparición de un espacio virtual o "ciberespacio", como medio de transmisión de datos. Ya no bastaba contar con un computador aislado, sino que su integración a la transferencia de información vino a catalizar notoriamente su importancia como medio informático.



1951	1969-Octubre	1972	1975	1977/1981	1983	1995	1997	2005	2008	2010	2013
Computadoras comerciales Mainframes	ARPANET	Primer virus informático	Primera microcomputadora	Microcomputadores	Internet	El libera internet	Propiedades de seguridad de la información	ISO 27000	IEU	ISO 27K002	ISO 27001
1950-53, Alemania 1951-MAPA I, Inglaterra 1951-UNIVAC I, EU.	Red que comienza como un proyecto científico, académico y militar que conecta UCLA, Standford y Utah.	Se da en mainframe DEC-PDP-10.	Altair 8800 con procesador Intel 8080, programable en ensamblador.	Apple II 6502/Tarh 6502) y la IBM PC (Intel 8088) programable con sistema operativo y en lenguaje de alto nivel.	ARPANET evoluciona en INTERNET y otras redes. MILNET, la red militar se separa de ARPANET y esto desaparece en 1990.		Confidencialidad, integridad y disponibilidad.	Sistema de gestión de la seguridad de la información.	Definición formal de seguridad cibernética y espacio cibernético.	Seguridad cibernética.	Nueva versión.

Figura 1. Hitos de la seguridad de la información, de la seguridad informática a la seguridad cibernética

5

Hacia la Ciberguerra
Infoops
Combate por el Mando y Control
Objetivos rentables para la ciberguerra en el campo de batalla futuro.
La Ciberguerra en el Conflicto Híbrido

CONCEPTUALIZANDO

Ciberespacio

Red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores.

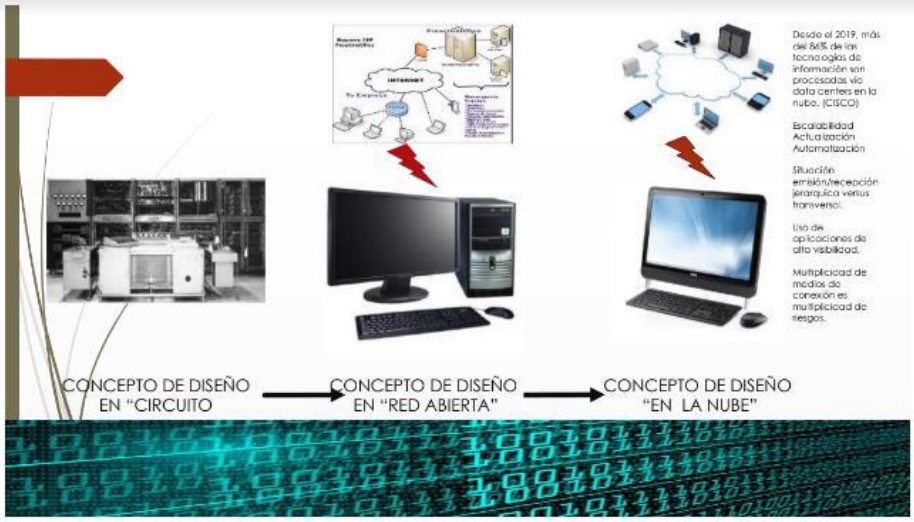
Se puede complementar esta definición con lo que conceptualiza la Comisión Europea como "***el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo***" y por último la UIT (Unión Internacional de las Telecomunicaciones) como el "***lugar creado a través de la interconexión de sistemas de ordenador mediante Internet***".

Siguiendo la definición del DD-10001 Ejército (edición 2017), "***el ciberespacio es entendido como el ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se***

6

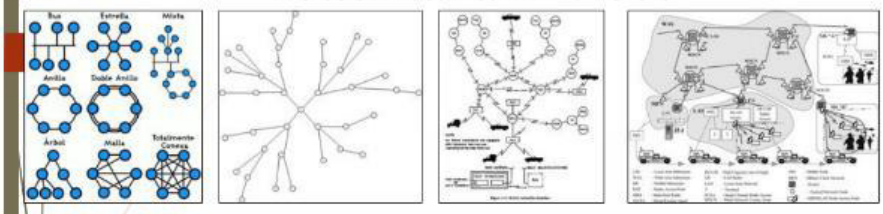
Dominios físicos	Dominio abstracto	Ambientes abstractos/cognitivos
Tierra Mar Aire Espacio	Ciberespacio	Espectro electromagnético Información Cognitivo

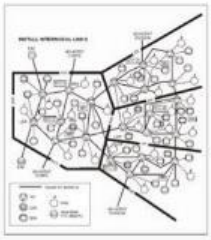
regto.sangabriel. jesoto21@gmail.com

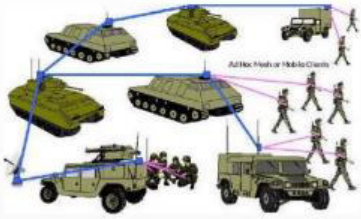


regto.sangabriel. jesoto21@gmail.com

EVOLUCIÓN DE LOS TIPOS DE REDES TÁCTICAS







OPERACIONES DE INFORMACIÓN Infoops

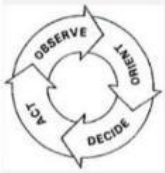
10

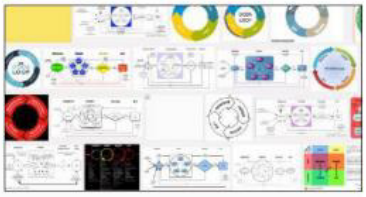
- Hacia la Ciberguerra Infoops
- Combate por el Mando y Control
- Objetivos rentables para la ciberguerra en el campo de batalla futuro.
- La Ciberguerra en el Conflicto Híbrido

Visión de la Guerra desde un punto de vista de la gestión de la información.
Boid vio que la victoria constantemente recaía en el lado que podía pensar con más creatividad (orientarse a sí mismo) y luego actuar rápidamente sobre tal entendimiento.
Levanta teoría del OODA Loop. Establecer que cualquier crisis debería considerar una estrategia dirigida a afectar el pensamiento del liderazgo enemigo.

Infoguerra o guerra de la información se ha convertido en una herramienta cada vez más relevante

Guerra de la Información como "Cualquier acción para denegar, explotar, corromper o destruir la información del enemigo y sus funciones, protegiendo la nuestra contra sus acciones, y explotando nuestras propias operaciones de información".



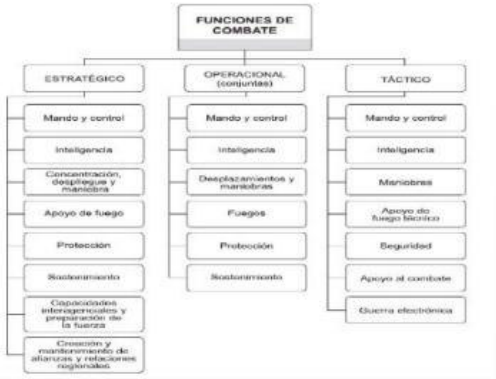


Fuente : John Boid, The School of Advanced Airpower Studies (1997

regto.sangabriel. jesoto21@gmail.com

Hacia la Ciberguerra
Infoops
Combate por el Mando y Control
Objetivos rentables para la ciberguerra en el campo de batalla futuro.
La Ciberguerra en el Conflicto Híbrido

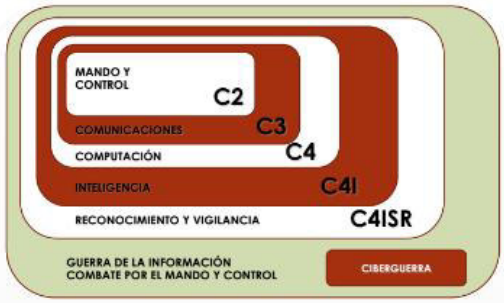
Funciones Primarias del Mando (D-10001. 2017: p.95)



Funciones de Combate (D-10001. 2017: p.94)

Funciones de Combate equivalen a las actividades o capacidades que debe poseer un sistema operativo y que le permitan concretar operaciones militares.

regto.sangabriel. jesoto21@gmail.com



C7I3STAR

Command
Control
Cognition
Consultation
Coordination
Communications
Computer
Information
Intelligence
Integration,
Surveillance &
Reconnaisance
Targeting
Adquisition

Fuente: CC E. Cubeiro C., LOS SISTEMAS DE MANDO Y CONTROL ampliado

Fuente: Elaboración Propia basado en Joint Pub 3-13.1

Operaciones sobre Redes de Ordenadores (**CNO**, Computer Network Operations)

– ***Capacidad de Defensa*** (**CND**, Computer Network Defence), que es la protección frente a enemigos de la explotación o ataque a nuestras redes de ordenadores, CNE y CNA.

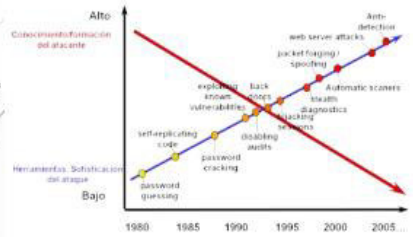
– ***Capacidad de Explotación*** (**CNE**, Computer Network Exploitation), que es la habilidad para acceder a la información guardada en un sistema de información, y la capacidad de hacer uso del propio sistema.

– ***Capacidad de Respuesta*** (**CNA**, Computer Network Attacks), que es el uso de técnicas novedosas para entrar en las redes de ordenadores y atacar los datos, los procesos o el hardware.

regto.sangabriel. jesoto21@gmail.com

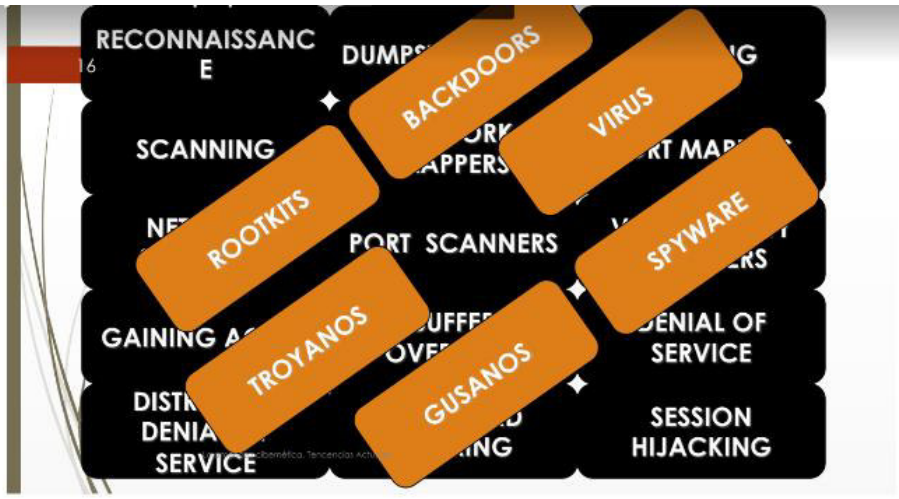
Nuevo contexto y las ciberamenzas

Hacia la Ciberguerra
Infoops
Combate por el Mando y Control
Objetivos rentables para la ciberguerra en el campo de batalla futuro.
La Ciberguerra en el Conflicto Híbrido



- Guerra asimétrica
- Irrupción de ciberactivistas y ciberterroristas.
- Nuevos tipos de amenazas:
  - Amenazas Persistentes Avanzadas (APT, APA).
  - Subversive Multi-Vector Threats (SMT).
  - Advanced Evasion Techniques (AETs).

FUENTE: JUAN CARLOS BATANERO. CIBERDEFENSA



regto.sangabriel. jesoto21@gmail.com

"El próximo Pearl Harbor podría llegar vía Internet"

Leon Panetta,
Ex Secretario de Defensa de Estados Unidos

18

Hacia la Ciberguerra
Infoops
Combate por el Mando y Control
Objetivos rentables para la ciberguerra en el campo de batalla futuro.
La Ciberguerra en el Conflicto Híbrido

Cibercrimen

Piratería de software, juegos, música o películas; estafas, transacciones fraudulentas, acoso y explotación sexual, pornografía infantil, fraudes de telecomunicaciones, amenazas, injurias, calumnias, etc. Busca conseguir un beneficio económico, pero también incluye el dominio de internet con fines inmorales.

Ciberterrorismo

No persigue principalmente un fin económico sino que se centra más en intimidar, coaccionar y causar daños con fines fundamentalmente políticos-religiosos.

Ciberguerra

Ciberespacio como un nuevo campo de batalla, donde se lleve a cabo la ciberguerra. Esta nueva forma de hacer la guerra no se limita solo a efectos sobre los equipos informáticos sino que sus consecuencias pueden trasladarse al mundo físico.

Jesús Reguera S. refiriendo Manual de Tallin

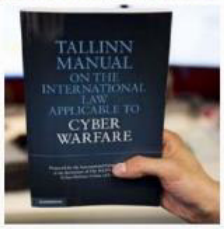
Se ha modificado o alterado el **Tempus**, **Locos** y **Pugnator.**

20

Hacia la Ciberguerra
Infoops
Combate por el Mando y Control
Objetivos rentables para la ciberguerra en el campo de batalla futuro.
La Ciberguerra en el Conflicto Híbrido

Conflicto de la Estonia y Rusia el 2007, debido al ataque masivo denominado ataque distribuido de denegación de servicio (distributed denial-of-service (DDoS) en contra Estonia.

Estos ciberataques marcaron un antes y un después en lo relativo a la ciberguerra.
La consecuencia más inmediata fue que la OTAN decidió establecer en su capital, Tallín, el Centro de Excelencia para la Ciberdefensa Cooperativa de OTAN (CCD COE).



21

- Hacia la Ciberguerra Infoops
- Combate por el Mando y Control
- Objetivos rentables para la ciberguerra en el campo de batalla futuro.
- La Ciberguerra en el Conflicto Híbrido

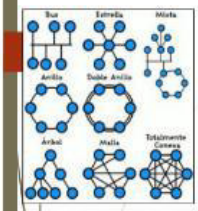
Objetivos con Características Comunes
Asociados al combate por el C2, para así magnificar y asegurar el resultado.

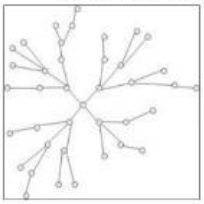
Características de objetivos para manipular al enemigo
Centradas en la diversión o engaño y en la guerra electrónica (decepción), donde deberán servir a una historia de diversión.

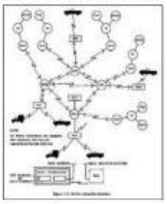
Para degradar la capacidad del enemigo de tomar decisiones
Su empleo puede considerar la saturación, obstaculización, deterioro, daño temporal o permanente de parte de sus sistemas informáticos de apoyo a la toma de decisiones o gestación de la resolución.

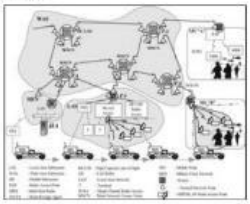
Para la obtención de inteligencia
Aquellos subsistemas o componentes con baja capacidad de respuesta, detección o alarma a las intrusiones, representarán objetivos de alto valor. La importancia del objetivo será directamente proporcional al acceso que permita a archivos de data de gran valor de uso y calidad. A su vez, la calidad de esa información se relacionará a la oportunidad y pertinencia para su empleo.

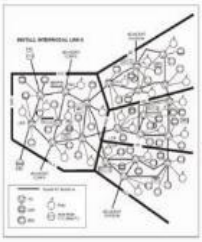
EVOLUCIÓN DE LOS TIPOS DE REDES TÁCTICAS

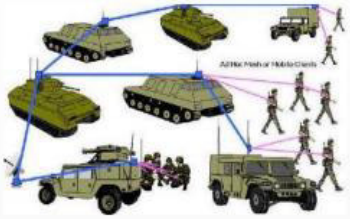












Hacia la Ciberguerra
Infoops
Combate por el Mando y Control
Objetivos rentables para la ciberguerra en el campo de batalla futuro.
La Ciberguerra en el Conflicto Híbrido

- EJEMPLOS EN LO TÁCTICO

- Geolocalización de las fuerzas propias y adversarias sobre cartografía digital.
- Ingreso automático de la posición (coordenadas y distancia al blanco) mediante telémetros lasércicos inalámbricos de Observadores Adelantados(OA).
- Transmisión de data a la Central de Tiro, mediante equipos de comunicaciones integrados al SCF.
- Clasificación de blancos asociados a toma de decisiones del Comandante de la Base de Fuegos.
- Ralentizar cálculo automático de datos iniciales para cada arma.

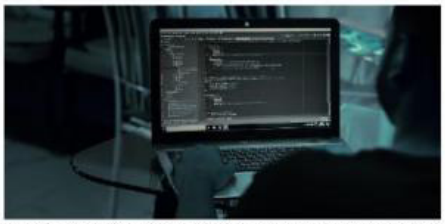
Hacia la Ciberguerra
Infoops
Combate por el Mando y Control
Objetivos rentables para la ciberguerra en el campo de batalla futuro.
La Ciberguerra en el Conflicto Híbrido

25

- Hacia la Ciberguerra
- Infoops
- Combate por el Mando y Control
- Objetivos rentables para la ciberguerra en el campo de batalla futuro.
- La Ciberguerra en el Conflicto Híbrido

Conflicto en Oriente Próximo

La guerra entre Israel y Hamás dispara una ola de ciberataques en la región



Fuente: https://www.elperiodico.com/es/internacional/20231011/ciberataques-israel-hamas-gaza-palestina-guerra-netanyahu-ciberguerra-ciberdefensa-hacker-93184521

26

Dominios físicos	Dominio abstracto	Ambientes abstractos/cognitivos
Tierra Mar Aire Espacio	Ciberespacio	Espectro electromagnético Información Cognitivo

Actualidad

Ucrania anuncia que ha herido al jefe del Estado Mayor ruso, Valery Gerasimov, durante un ataque

Milicias ucranianas asegura que en su ataque en Izum dio con un "gran número" de altos oficiales muertos mientras que hirió al general

Fuente de la imagen : DIARIO ELECTRÓNICO MARKA, ESPAÑA

27

Amenaza Híbrida

- Hacia la Ciberguerra
- Infoops
- Combate por el Mando y Control
- Objetivos rentables para la ciberguerra en el campo de batalla futuro.
- La Ciberguerra en el Conflicto Híbrido

28

Amenaza Híbrida

- Amenazas y Riesgos, sus diferencias para el entendimiento del Conflicto.
- Ciberseguridad y Ciberdefensa, sus diferencias y cercanías.
- El Conflicto Híbrido

- La "amenaza híbrida" incorpora **un amplio espectro de métodos y uso de la fuerza**, que combina el empleo del instrumento militar convencional
- Puede usar tácticas y actos de terrorismo y pueden incluir la coerción y la violencia indiscriminada (Hoffman, 2007).

- **Guerra multimodal y multidimensional** Dimensión física como en la psicológica del conflicto.

- **Su concepción ha sido creada en lo político, teniendo a la vista lo estratégico**.

Dominios físicos	Dominio abstracto	Ambientes abstractos/cognitivos
Tierra Mar Aire Espacio	Ciberespacio	Espectro electromagnético Información Cognitivo

29

Reflexiones Finales

Principal característica de las **guerras venideras será la asimetría de sus actores.**

Presencia de un amplio espectro de métodos y uso de la fuerza. La ciberguerra entre ellos.

Se mantendrán rivalidades interestatales y entre los Estados con actores no estatales. Incluso podrán n**o tener necesariamente vínculos estatales. Aparece el Ciberguerrero.**

Las fases, propias del conflicto clásico, se alteran, son más difusas.

Agenda

1. Importancia de la ciberseguridad
2. Tendencias de ataques
3. Riesgos que enfrentamos las personas
4. ¿Cómo sobrevivimos?
5. ¿Que se viene a futuro?

La importancia de la ciberseguridad

- La ciberseguridad es transversal en el funcionamiento de la sociedad
- Las empresas y el Estado deben proteger la información que entregan las personas
- Cuando las organizaciones no actúan en materia de ciberseguridad, las personas son las afectadas
- La tecnología es un medio para poner en riesgo la información que las personas u otras instituciones entregan/comparten a otras en función de la confianza.

regto.sangabriel. jesoto21@gmail.com

Importancia de la ciberseguridad

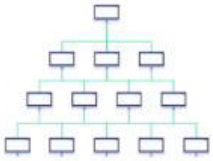
Con una gran conectividad, viene una **gran responsabilidad**

Hiperconectividad

- Toda nuestra información online forma parte de una gran red y coexiste con la de otras personas, instituciones y entidades.

Ciberseguridad

Ciberataque



- Un sólo equipo vulnerado es capaz de infectar toda la red.

La importancia de la ciberseguridad

- Considerando los ataques desde el 2020 a la fecha, el promedio anual es de 7 organizaciones relevantes víctimas y sólo durante estos primeros tres meses del año, Chile ya registra 6, por lo que se proyecta que este trimestre superará los ataques realizados durante todo el 2022.

regto.sangabriel. jesoto21@gmail.com

Tendencias de ataque

Phishing

Líder en tendencia, ya que continúa siendo altamente efectivo para propagación de virus, estafas y suplantación de identidad

Ransomware

Se ha monetizado convirtiéndolo en un servicio permitiendo la proliferación de grupo ,criminales sin conocimiento técnico puedan operar.

Ataques a infraestructura crítica

El ciberataque ya no solo afecta a los computadores, ahora tiene consecuencias físicas reales

Data leak/ data breach

Puerta de entrada para lograr accesos iniciales, se debe monitorear constantemente

regto.sangabriel. jesoto21@gmail.com

Riesgos a los cuales nos enfrentamos

técnicas más habituales que provocan **riesgos de ciberseguridad**

Phishing

Estafa que se realiza a través de un correo electrónico que genera urgencia al destinatario para que realice una acción.

Vishing

Consiste en el uso de una llamada de voz para generar confianza con el destinatario para obtener información sensible del afectado.

Smishing

Se utilizan los mensajes SMS para recrear comunicaciones de entidades de prestigio con el usuario para captar su información personal.

Baiting

Se utilizan USBs infectados abandonados en lugares públicos con la esperanza de que algún usuario los conecte en sus dispositivos.

regto.sangabriel. jesoto21@gmail.com

¿Cómo sobrevivimos?

Prácticas que ayudan a reducir los **riesgos de ciberseguridad en las empresas**

#01 Estrategia de ciberseguridad

#02 Gobernanza definida

#03 Procesos + Personas. No solo es tecnología.

#04 Entender y mapear los riesgos

#05 Alinearse con el negocio

#06 Medir! Lo que no se mide no se ve

regto.sangabriel. jesoto21@gmail.com

¿Cómo sobrevivimos?

Hábitos que nos ayudan a reducir los **riesgos de ciberseguridad**

#01 Protege tu información y equipo

#02 Sé discreto online y en público

#03 Piensa antes de hacer click o responder

#04 Mantén tus contraseñas seguras

#05 Y recuerda: si sospechas, repórtalo

Ciberseguridad es un juego en equipo

Las personas son la **primera línea de defensa**

En el fútbol, como en ciberseguridad, **defender es más difícil que atacar**, por eso, es fundamental contar con ***la tecnología adecuada y las personas*** para que seamos capaces de ***diseñar las estrategias correctas frente al adversario***"

regto.sangabriel. jesoto21@gmail.com

Lo que se viene a futuro

En resumen para los próximos años y de acuerdo con la publicación de Gartner "Top Cybersecurity Predictions 2023-2027"

Privacidad	Talento	Riesgo	Confianza cero
10%	25%	50%	10%
o menos lograrán aprovechar la privacidad como una ventaja competitiva.	de los líderes en ciberseguridad renunciarán debido al estrés.	utilizará sin éxito la cuantificación de riesgos para la toma de decisiones empresariales	tendrá un programa maduro.
2024	2025	2025	2026

Detección de amenazas	Directorio	Terceros	Factor humano
60%	70%	75%	50%
aprovechará los datos de gestión de exposición para la detección de amenazas.	de las juntas incluirán un miembro con experiencia en ciberseguridad.	adquirirá, modificará o creará tecnología fuera del ámbito de TI.	Adoptará prácticas de diseño centradas en el ser humano en el diseño de control y procesos.
2026	2026	2027	2027

regto.sangabriel. jesoto21@gmail.com

Reflexiones finales

La Guerra 4GW se caracteriza por ser asimétrica, hibrida, no tiene fronteras su campo de batalla es el ciber espacio el que no tiene limites
Principal característica de las **guerras venideras será la asimetría de sus actores**.

Presencia de un amplio espectro de métodos y uso de la fuerza. La ciberguerra entre ellos.

Se mantendrán rivalidades interestatales y entre los Estados con actores no estatales. Incluso podrán **no tener necesariamente vínculos estatales. Aparece el Ciberguerrero.**

Las fases, propias del conflicto clásico, se alteran, son más difusas.

La Ciberseguridad nos afecta a todos y es responsabilidad de todas las personas interconectadas de minimizar los riesgos de un ciberataque.