

# Marco conceptual para el análisis político estratégico del ambiente de Ciberseguridad

**Dr. Boris Saavedra**

***Profesor Asociado de Asuntos de Seguridad Nacional***

**Centro William J. Perry de Estudios Hemisféricos de Defensa  
Universidad Nacional de Defensa**

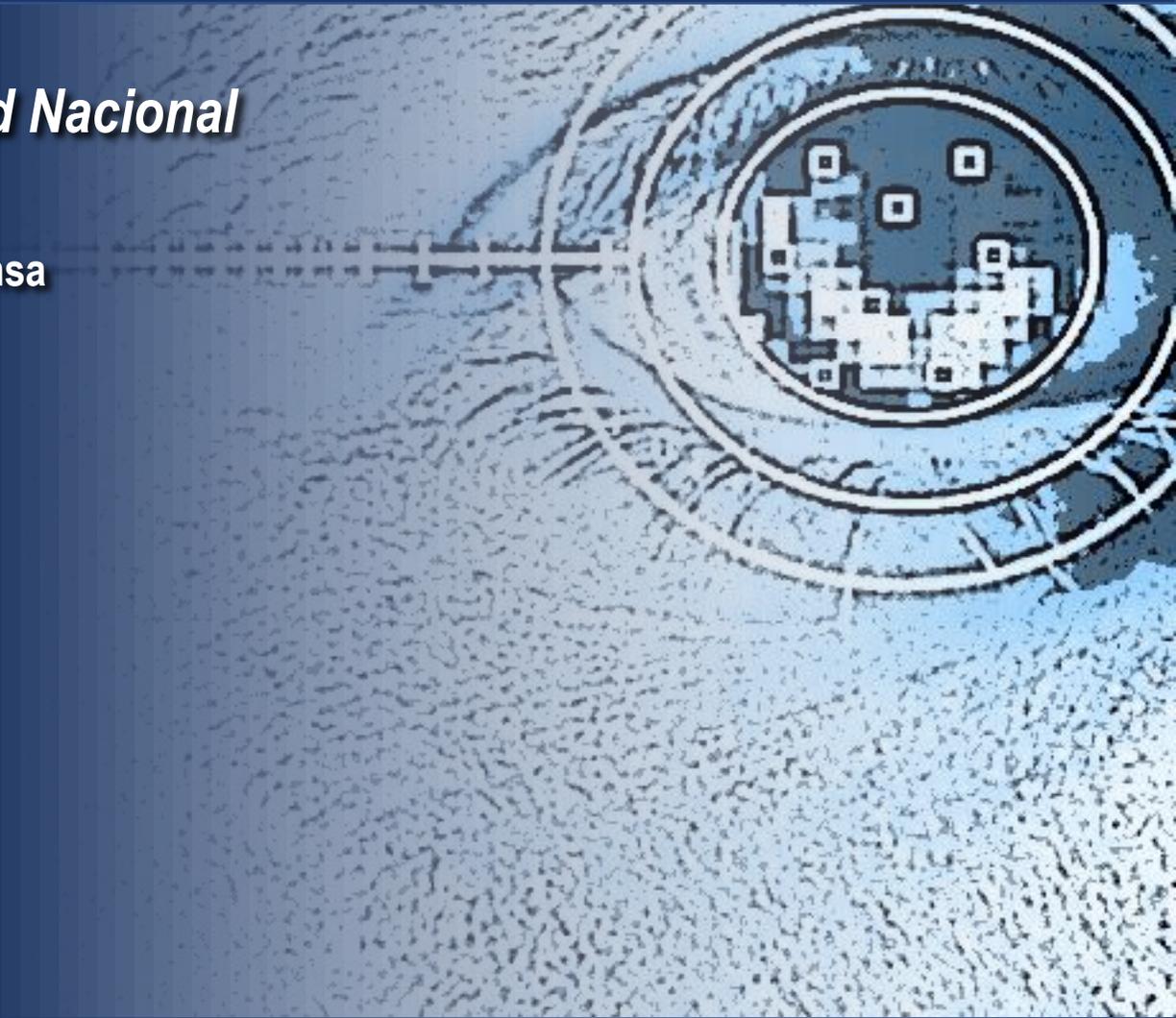
**Washington, DC 20593-0001**

**saavedrab@ndu.edu**

**202-685-2213/FAX 202-685-4675**

**Boris Saavedra**

**2-685-2213/FAX 202-685-4675**



# Principio de libertad de catedra



Las ideas contenidas en esta presentacion son de responsabilidad de su autor, sin que reflejen, necesariamente, el pensamiento del WJPC, NDU, DoD o el gobierno de EE.UU.

# Era de Aceleración del Cambio

- Tres grandes Fuerzas en el mundo: Tecnología digital, globalización y cambio climático
- El factor definidor es la aceleración de los cambio y el aumento de la régimen de cambio.



Thomas L. Friedman  
Thanks You For Being Late  
an optimist's guide to thriving  
in the age of acceleration 2016

# Objetivo

Conocer y entender el empleo de los elementos fundamentales del análisis político estratégico para el desarrollo de la estrategia de seguridad y defensa del ciberespacio.



# Entendimientos preliminares para el ciberespacio

## Definición

*El ciberespacio es un dominio operativo enmarcado en el uso de electrones y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de un sistema de información interconectado a Internet y sus infraestructuras asociadas.*

*Daniel T. Kuehl*

*Profesor de estrategia militar y política de seguridad nacional en el Colegio de Gestión de los Recursos Informáticos de la Universidad Nacional de Defensa*

1997 - 2017



Years Empowering Defense and Security Professionals in the Americas.

# El ciberespacio como dominio implicancias

- ¿Que implica el concepto dominio?

- Superioridad
- Control
- Influencia
- Competencia

Fanfarronear

- ¿Es poder militar y el ciberespacio o poder militar cibernético?

- Implica cambios en: cantidad, velocidad, e interactividad de la información

1997 - 2017



Years Empowering Defense and Security Professionals in the Americas.

**Internet de  
las Cosas**

**Infraestructura  
Critica**

**Ciberseguridad**

**Big Data**

1997 - 2017



*Years Empowering Defense and Security Professionals in the Americas.*

# El ciberespacio: Estrategia en un contexto dinámico

- Es una creación humana sujeta al perfeccionamiento
- Rápido crecimiento con cambios súbitos tecnológicos, organizacionales y otros
- Facilidad de acceso por la globalización del conocimiento
- Excelente entendimiento de la amplitud y complejidad para tomar los pasos acertados que afecten los hechos



# Marco político estratégico

## Elementos estructurales

- Mayor seguridad
- Desarrollo de la investigación y capital humano
- Mejora de la gobernanza
- Organización efectiva

## Elementos geopolíticos

- Desarrollo sofisticado de operaciones centradas en la red
- Planificación integrada de las capacidades de ataque y defensa de la red informática
- Establecimiento de una doctrina de disuasión que incorpore a ciber
- Expansión de capacidades efectivas de ciber influencia
- El establecimiento de una doctrina cibernética por parte de los elementos no militares para ser utilizada eficazmente en un contexto conjunto y multinacional
- Generación de esfuerzos a nivel internacional en ciber por ser intrínsecamente internacional y no puede lograrse más eficazmente sin socios internacionales

1997 - 2017



Years Empowering Defense and Security Professionals in the Americas.

# Temas estructurales

- **Seguridad**
  - Que nivel de protección es apropiado y como podría ser alcanzado
  - Cual es el balance entre los aspectos positivos y el costo de los riesgos
- **Capital humano, investigación y desarrollo**
  - Que clase de sistema educativo para satisfacer la demanda
  - Cual debe ser la relación publico-privada para preparar el capital humano
- **Gobernanza y gobernabilidad a nivel internacional**
  - Que papel jugaran el sector publico y privado para ejercer el control
- **Organización de un consejo de política cibernética**
  - La necesidad de un consejo al mas alto nivel de gobierno que pueda integrar las diferentes perspectivas del sector publico y privado en el campo cibernético

# Algoritmo/Inteligencia Artificial/Inteligencia aumentada

- ¿Que es un algoritmo?
- ¿ Que hace?
- ¿ Como lo hace?
- ¿ Que es Inteligencia Artificial e Inteligencia Aumentada?
- ¿ Cual es su importancia para el análisis de la información en la base de datos?

# Temas geopolíticos

- Analizar el ciberespacio como dominio en comparación con los otros cuatro dominios
- El ciberespacio como dominio y sus consecuencias
- La combinación de complejidad y el bajo costo tiene consecuencias importante de tiempo y espacio
- La superioridad del dominio y su relación con la acción de los hackers

1997 - 2017



Years Empowering Defense and Security Professionals in the Americas.

# ¿Qué es ciberespacio en el contexto militar?

**REDES DE TRANSFERENCIA DE INFORMACIÓN INTERACTIVAS DE DOS VÍAS SIENDO LAS REDES EL ELEMENTO ESENCIAL POR DOS RAZONES: PRIMERO, CIBER REQUIERE CONTROL QUE ES RETROALIMENTACIÓN, Y SEGUNDO, LA PRESENCIA DE MOVIMIENTOS OMNIDIRECCIONALES**

1997 - 2017



Years Empowering Defense and Security Professionals in the Americas.

# Operaciones centradas en la red

- El enfoque en este tipo de operaciones crea muchas vulnerabilidades que podrían ser explotadas por los adversarios potenciales. Recomendaciones:
  - Identificar las vulnerabilidades de la red
  - Determinar las necesidades de investigación y desarrollo para superar las vulnerabilidades identificadas
  - Asignar los recursos necesarios y suficientes a través del proceso de adquisiciones
  - Las implicaciones de riesgo de las potenciales vulnerabilidades de la red deben evaluarse sistemáticamente

# Ataque de red informática

- El enfoque de este ataque es el uso de el ciberespacio para atacar al personal, facilidades y/o equipos con la intención de degradarlos, neutralizados o destruir las capacidades de combate del enemigo mientras protegemos los nuestros.
- Para hacer la red mas controlables se debe reducir los niveles de clasificación para ampliar la integración de los sistemas.
- Las capacidades que pueden ser discutidas conceptual y técnicamente abiertamente pueden ser utilizadas por los adversarios contra nosotros a través de Internet diariamente.

# Disuasión en Ciberseguridad

- La disuasión en el ciberespacio incluye retaliación y defensa basado en los elemento del poder nacional y se dificulta por el problema de atribución
- Disuadir mediante La retaliación es una respuesta que va mas allá del ciberespacio
- La disuasión contra actores estatales es mas factible que contra actores no estado y debe integrar al sector privado
- La disuasión en el ciberespacio tiene un componente internacional basado en la cooperación con los aliados

1997 - 2017



Years Empowering Defense and Security Professionals in the Americas.

# Influencia del ciberespacio

- La influencia no es proporcional a la capacidad en el ciberespacio sino a su variedad y complejidad
- Requiere mensajes multifacéticos basados en la naturaleza de audiencia
- Se requieren expertos en geografía, cultura y lingüística para crear el mensaje ajustado a estos elementos
- Las instituciones que conducen las relaciones internacionales deben expandir sus transmisiones como parte de la gran estrategia comunicacional del gobierno
- La estrategia comunicacional requiere de alianzas para expandir las capacidades e incrementar la efectividad



# Operaciones de estabilidad

- La información y tecnología de la información son elementos clave a ser utilizados en forma sistemática para lograr el éxito
- Permite el conocimiento para asegurar el éxito con escasos recursos
- Facilita la integración de la información mediante la identificación de los requerimientos para el uso de los escasos recursos
- Facilita la coordinación de todos los recursos públicos y privados y el proceso de toma de decisiones



# Doctrina, organización, entrenamiento, logística, recursos humano y financiero

- La doctrina es parte importante para el empleo del ciberespacio en seguridad y defensa
- La ciberseguridad necesita ser integrada a todos los procesos
- Se requiere un departamento para el análisis de ciberseguridad dentro de la institución militar en general y en lo particular a cada servicio
- La integración de las comunicaciones y la información es el paso inicial para la instituciones de seguridad y defensa

1997 - 2017



Years Empowering Defense and Security Professionals in the Americas.

# La acción internacional en el ciberespacio

- El ciberespacio en mucha de sus manifestaciones es una criatura de la globalización como la carencia de fronteras
- La naturaleza del ciberespacio demanda tener la habilidad de actuar en conjunto
- La necesidad de la influencia internacional a través de la diplomacia pública requiere su reforzamiento
- La estructura de gobernanza internacional del ciberespacio requiere su fortalecimiento para la cooperación



HACKING DETECTED

RISK ALERT

1997 - 2017



Years Empowering Defense and Security Professionals in the Americas.

# Conclusiones

- La naturaleza del ambiente del ciberespacio es dinámico, complejo y de cambios acelerados
- El análisis del ambiente de ciberseguridad tiene dos elementos los temas estructurales (capacidades) y los temas geopolíticos (el entorno)
- La infraestructura critica protegidas por estándares tecnológicos tradicionales son muy vulnerables
- Aunque no se puede lograr la seguridad al cien porciento es posible, practico y mas barato el desarrollo adecuado de la estrategia de ciberseguridad que dificulte a los potenciales adversarios ataques exitosos



# Bibliografía recomendada

- **Cybersecuty and Cyberwar What everyone needs to know.** Author P.W. Singer and Allan Friedman. 2014 ISBN: 978-0-19-9918-9
- **Thank you for Being Late** An optimist's guide to Thriving in the Age of Accelerations. Author Thomas L. Friedman 2016 ISBN: 978-0-374-27353-8
- **Future Crimes everything is connected and what we can do about it.** Author Marc Goodman 2015 ISBN: 978-0-385900
- **Cyberpower and National Security.** Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz
- **SCADA Security:** what's broken and how to fix it. Author Andrew Ginter Abterra Technology Inc. 2016 ISBN: 978-0-9952984-0-8