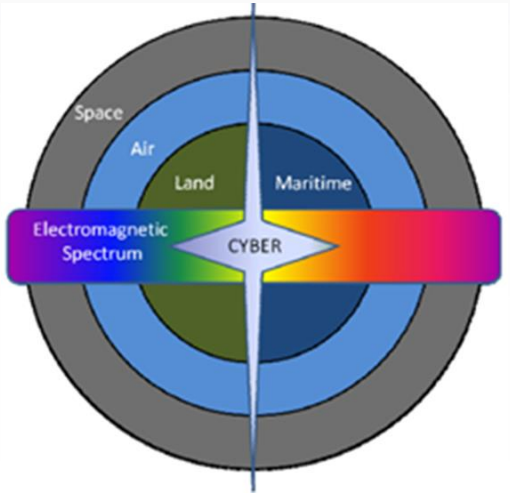
Ciberdefensa

¿Cómo enfrentar este nuevo domínio militar?
Nivel operacional e gerencial – Visión Militar

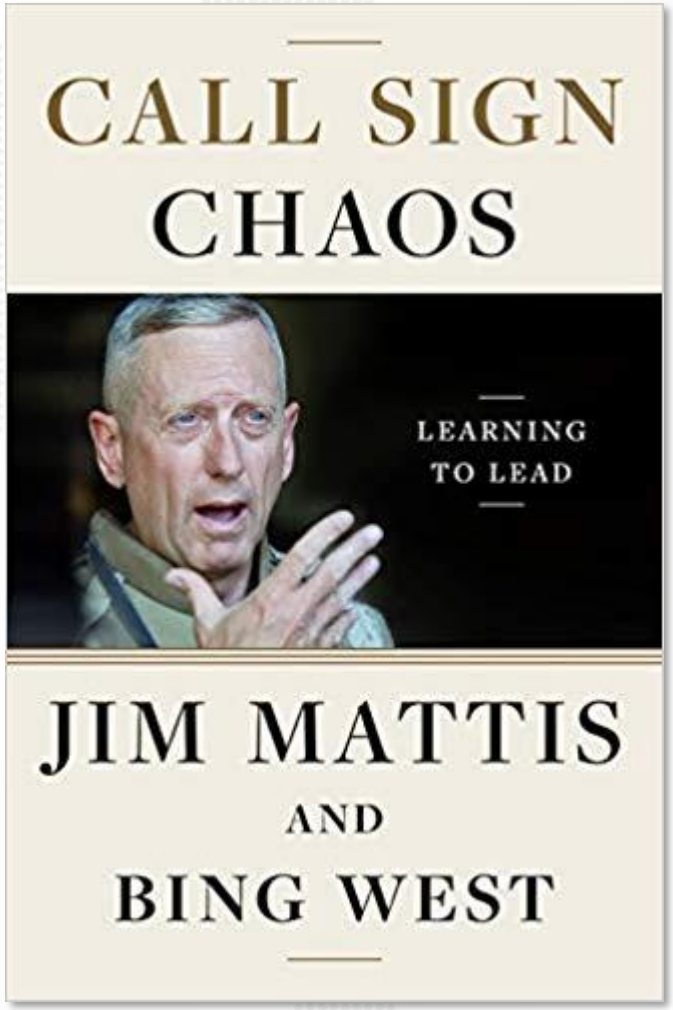
Col João M E Carneiro (Ph.D.) – Ejército Brasileño
joao.carneiro@iadc.edu / carneiro.joao@eb.mil.br
Octobre 10, 2019



¡Todo lo dicho aquí refleja solo las opiniones personales del orador!

¿Cuáles son los valores que busca su institución?

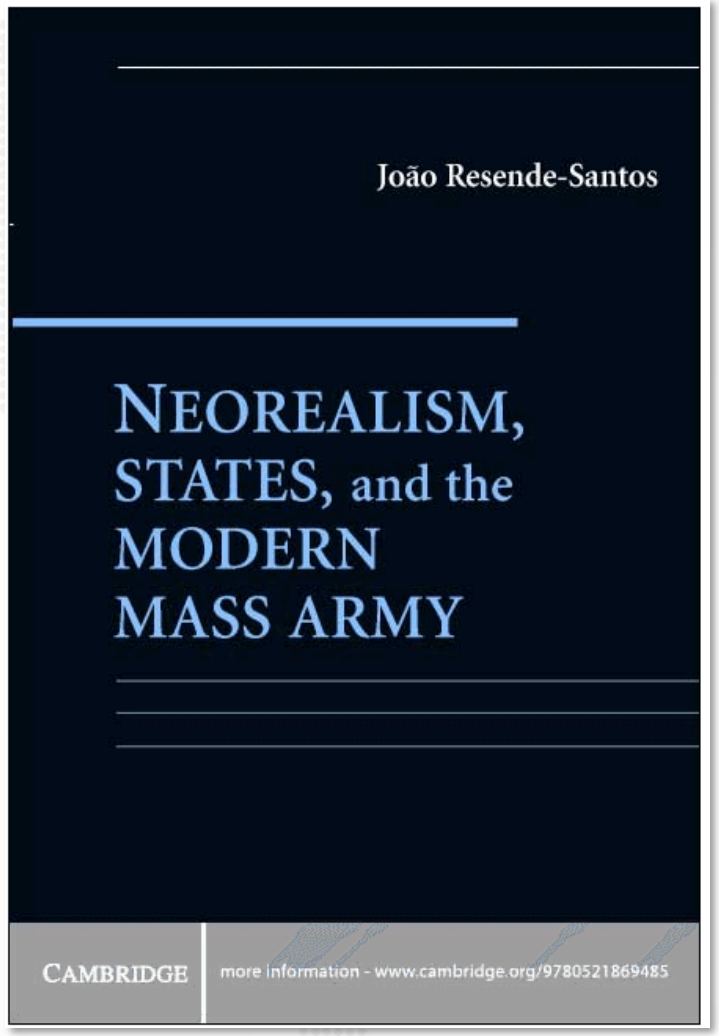
En cualquier organización, se trata de seleccionar el equipo adecuado. Las dos cualidades que me enseñaron a valorar más en la selección de otros para ascensos o roles críticos fueron la iniciativa y la agresividad. Busqué esos sellos distintivos en los que serví al lado. Las instituciones obtienen los comportamientos que recompensan.



Fuente: https://www.amazon.com/Call-Sign-Chaos-Learning-Lead/dp/0812996836

Teoría de la emulación militar

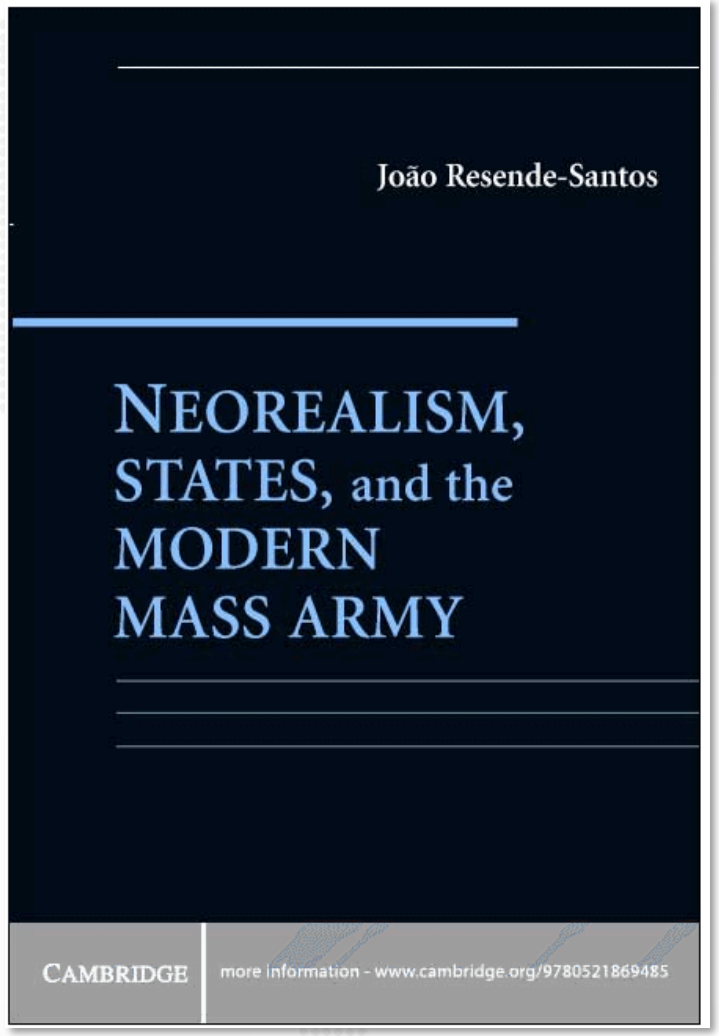
Desde los tiempos en que los humanos comenzaron a organizarse en colectivos políticos, los estados han imitado las mejores prácticas entre sí: lo último en armamento militar, procesos industriales, política reguladora e incluso órganos completos del estado, como los bancos centrales.



Fuente: https://www.amazon.com/Neorealism-States-Modern-Mass-Army-ebook-dp-B0012K1OFC/dp/B0012K1OFC

Teoría de la emulación militar

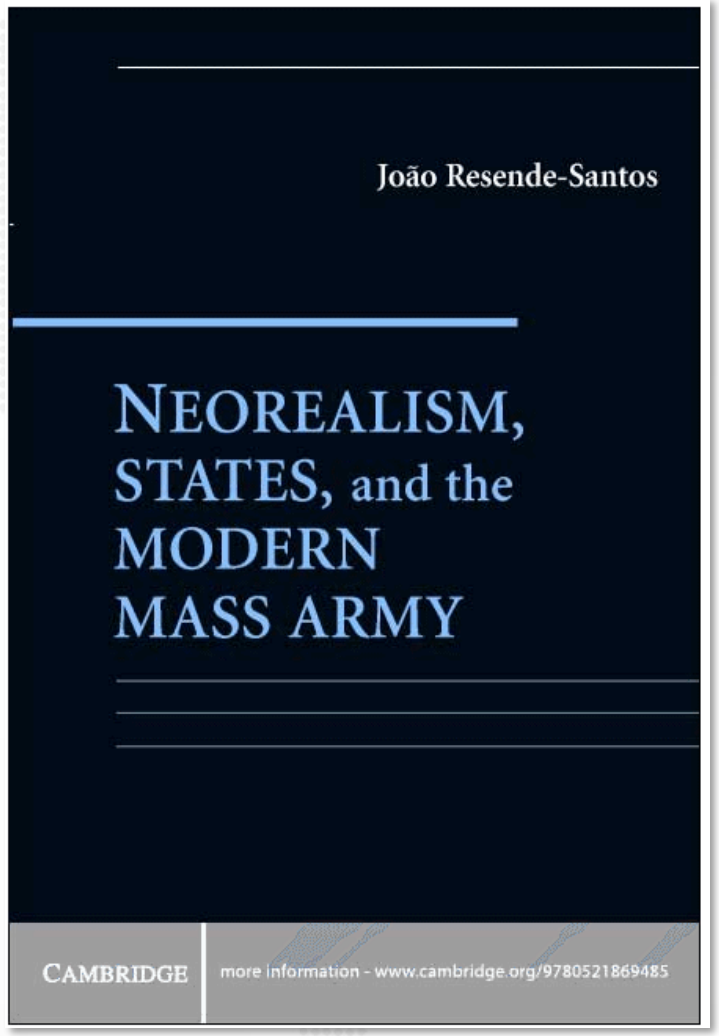
La emulación se puede definir como una imitación voluntaria, sistemática y deliberada, por un Estado o cualquier entidad, que puede actualizarse o modernizarse, en una amplia variedad de áreas, técnicas y prácticas de otro, normalmente motivado / impulsado por presiones competitivas. Esto también puede ocurrir en el marco de prácticas económicas, administrativas, regulatorias e incluso constitucionales.



Fuente: https://www.amazon.com/Neorealism-States-Modern-Mass-Army-ebook-dp-B0012K1OFC/dp/B0012K1OFC

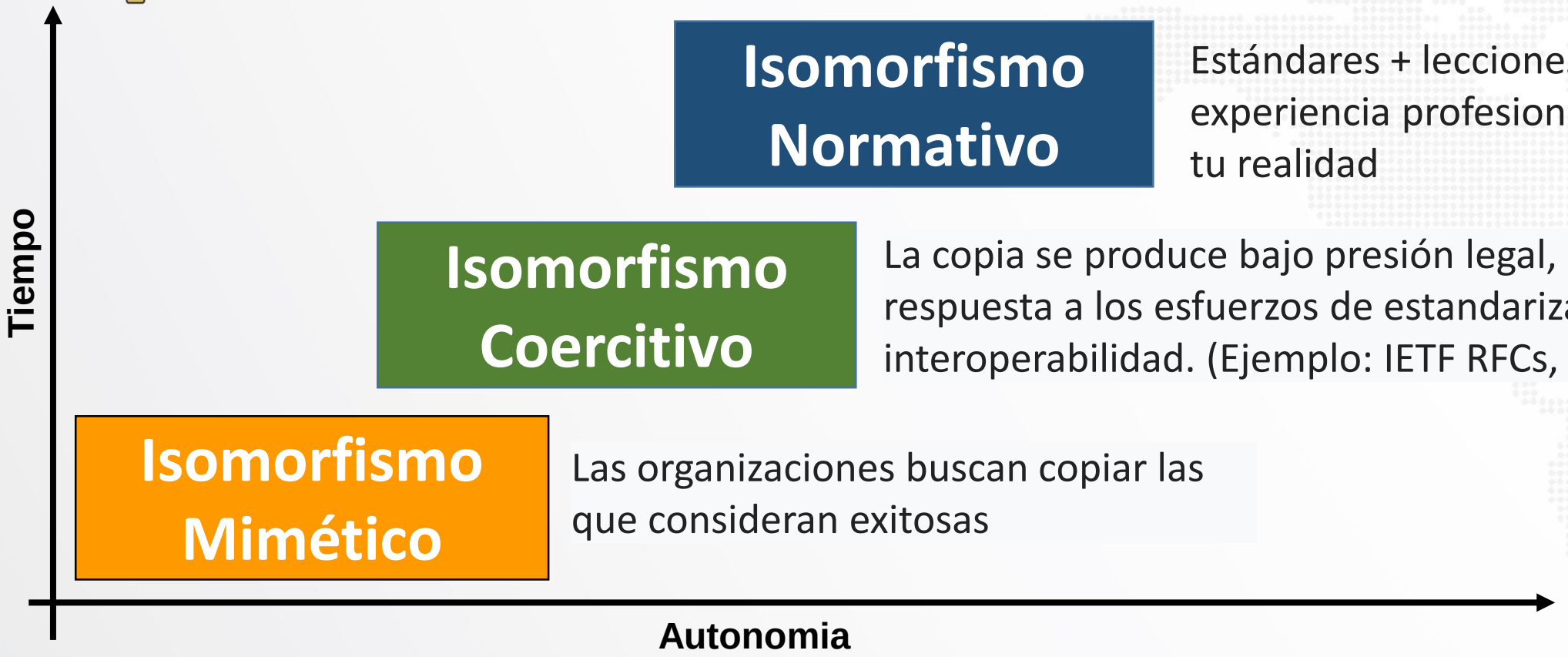
Teoría de la emulación militar

Resende-Santos afirma que innovar es costoso y arriesgado, consume mucho tiempo y tiene resultados inciertos. A medida que crece la competitividad, los Estados, en cuidadosa consideración de los riesgos y beneficios potenciales, se vuelven más reacios al riesgo, optando por la certeza y el retorno inmediato de la emulación, de lo cual se conocen los resultados.



Fuente: https://www.amazon.com/Neorealism-States-Modern-Mass-Army-ebook-dp-B0012K1OFC/dp/B0012K1OFC

Tipos de isomorfismo



Isomorfismo Normativo

Estándares + lecciones aprendidas + experiencia profesional = adaptación de tu realidad

Isomorfismo Coercitivo

La copia se produce bajo presión legal, a menudo en respuesta a los esfuerzos de estandarización e interoperabilidad. (Ejemplo: IETF RFCs, OTAN)

Isomorfismo Mimético

Las organizaciones buscan copiar las que consideran exitosas

Fuente: http://bibliotecadigital.fgv.br/ojs/index.php/rae/article/viewFile/37123/35894

Modelo CSIAC

El cuadro de políticas de ciberseguridad del DoD

ORGANIZAR

LIDERAR Y GOBERNAR

ORGANIZAR	HABILITAR	PREVER	PREPARAR	
Diseño para la lucha	Protege los datos en tránsito	Comprender el espacio de batalla	Desarrollar y mantener la confianza	Autoridades
Desarrollar la fuerza laboral	Administrar acceso	Prevenir y retrasar a los atacantes y evitar que los atacantes se queden	Fortalecer la preparación cibernética	Nacional / Federal
Alianza para el fortalecimiento	Asegurar el intercambio de información		Mantener misiones	Operacional
				Políticas subordinadas

Fuente: Cyber Security & Information Systems – Information Analysis Center - https://www.csiac.org/resources/the-dod-cybersecurity-policy-chart/

https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework#

NICCS™
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Training | Formal Education | Workforce Development | About NICCS

Home › Workforce Development › NICE Cybersecurity Workforce Framework

NICE Cybersecurity Workforce Framework

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), published by the National Institute of Standards and Technology (NIST) in NIST Special Publication 800-181, is a nationally focused resource that establishes a taxonomy and common lexicon to describe cybersecurity work, and workers, regardless of where, or for whom, the work is performed.

Click the blue headers below to search within the NICE Framework components or by keyword. Learn more about how to use the NICE Framework here.

Categories/Specialty Areas | Work Roles | Tasks | Skills | Knowledge | Abilities | Keyword Search

Analyze
Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Specialty Areas

Collect and Operate
Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

Specialty Areas

Investigate
Investigates cybersecurity events or crimes related to information technology (IT) systems,

Specialty Areas

https://www.nist.gov/cyberframework

NIST

Search NIST | NIST MENU

CYBERSECURITY FRAMEWORK

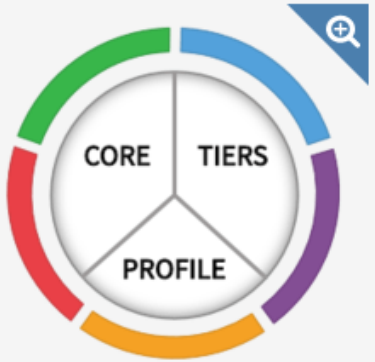
Helping organizations to better understand and improve their management of cybersecurity risk

- Framework +
- New to Framework +
- Perspectives +
- Success Stories +
- Online Learning +
- Evolution +
- Frequently Asked Questions +
- Events and Presentations +
- Related Efforts (Roadmap)
- Informative References +
- Resources +

Framework Version 1.1

The Cybersecurity Framework is ready to download.

Learn More



New to Framework

This voluntary Framework consists of standards, guidelines and best practices to manage cybersecurity risk.

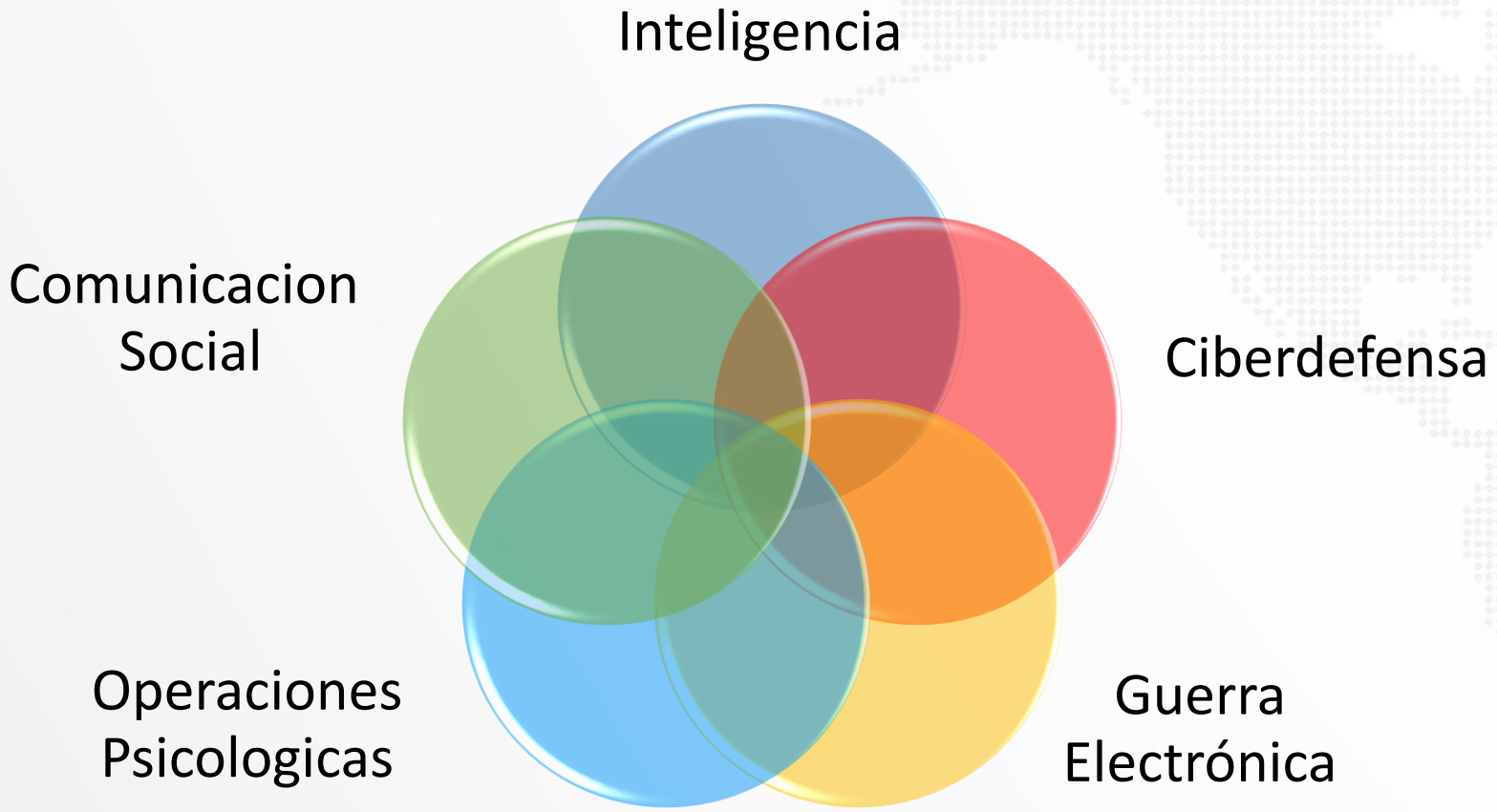
Learn More

Online Learning

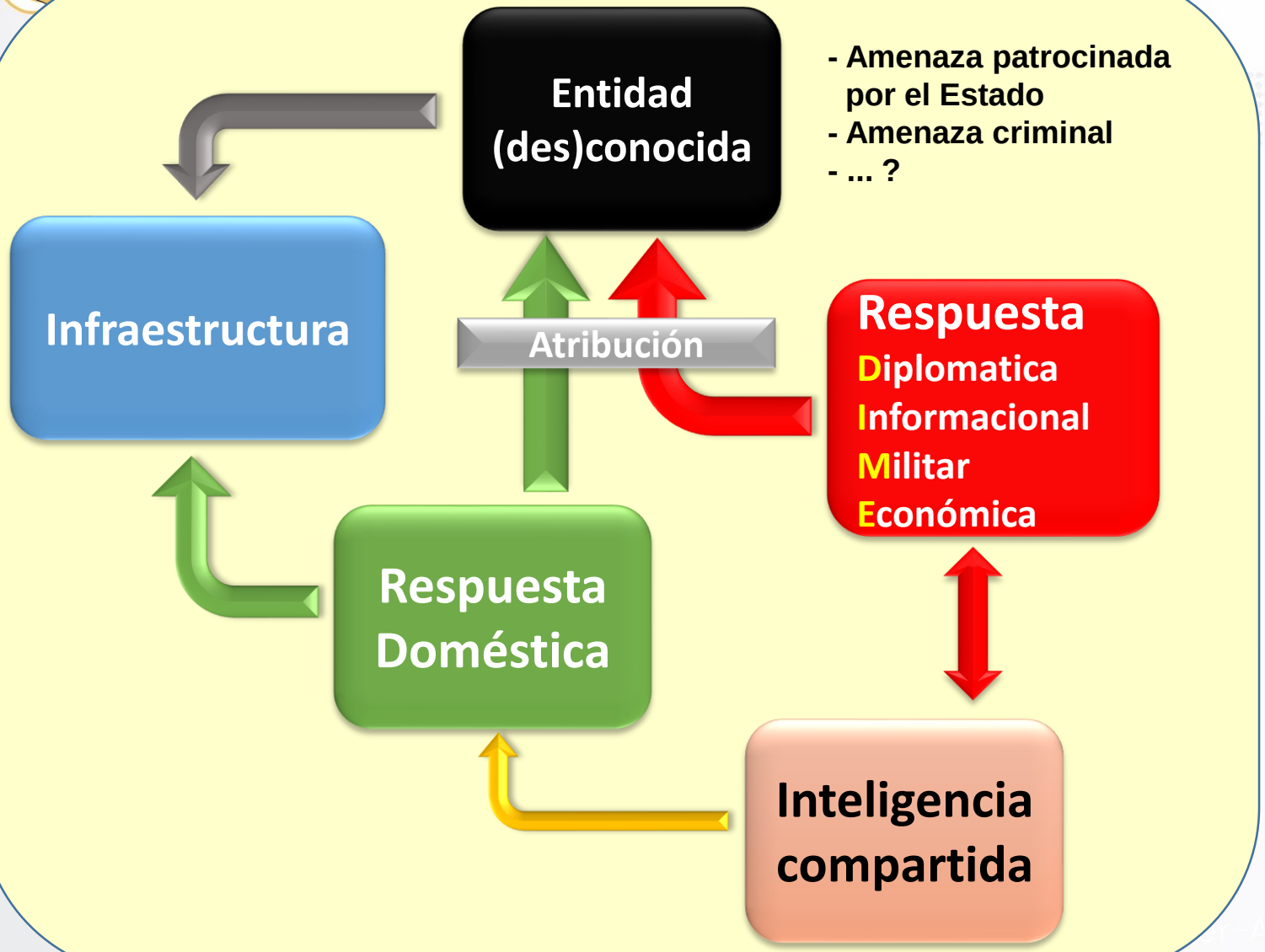
Intro material for new Framework users to implementation guidance for more advanced Framework users.

Learn More

Operaciones de Información



Entorno complejo con respuesta compleja



Diferentes Autoridades:

- DIME (exterior)
- Imposición de la ley (doméstica)
- Guardia Nacional (doméstica)

Debemos

- Trabajar juntos
- Emplear todas las autoridades
- Coordinación e Integración de esfuerzos

Coordinación e integración de esfuerzos

- **Coordinación**: armonizar los esfuerzos, apuntando al objetivo, optimizando los resultados y aumentando la eficacia de las acciones conjuntas entre todas las entidades involucradas.

- **Integración**: Contribuir a los procesos de Ciberseguridad y Ciberdefensa mediante acciones de coordinación en relación con los socios; manejo de incidentes; auto protección cibernética; y la inteligencia cibernética con el fin de identificar el intento de actos contra la seguridad.

Coordinación y Integración

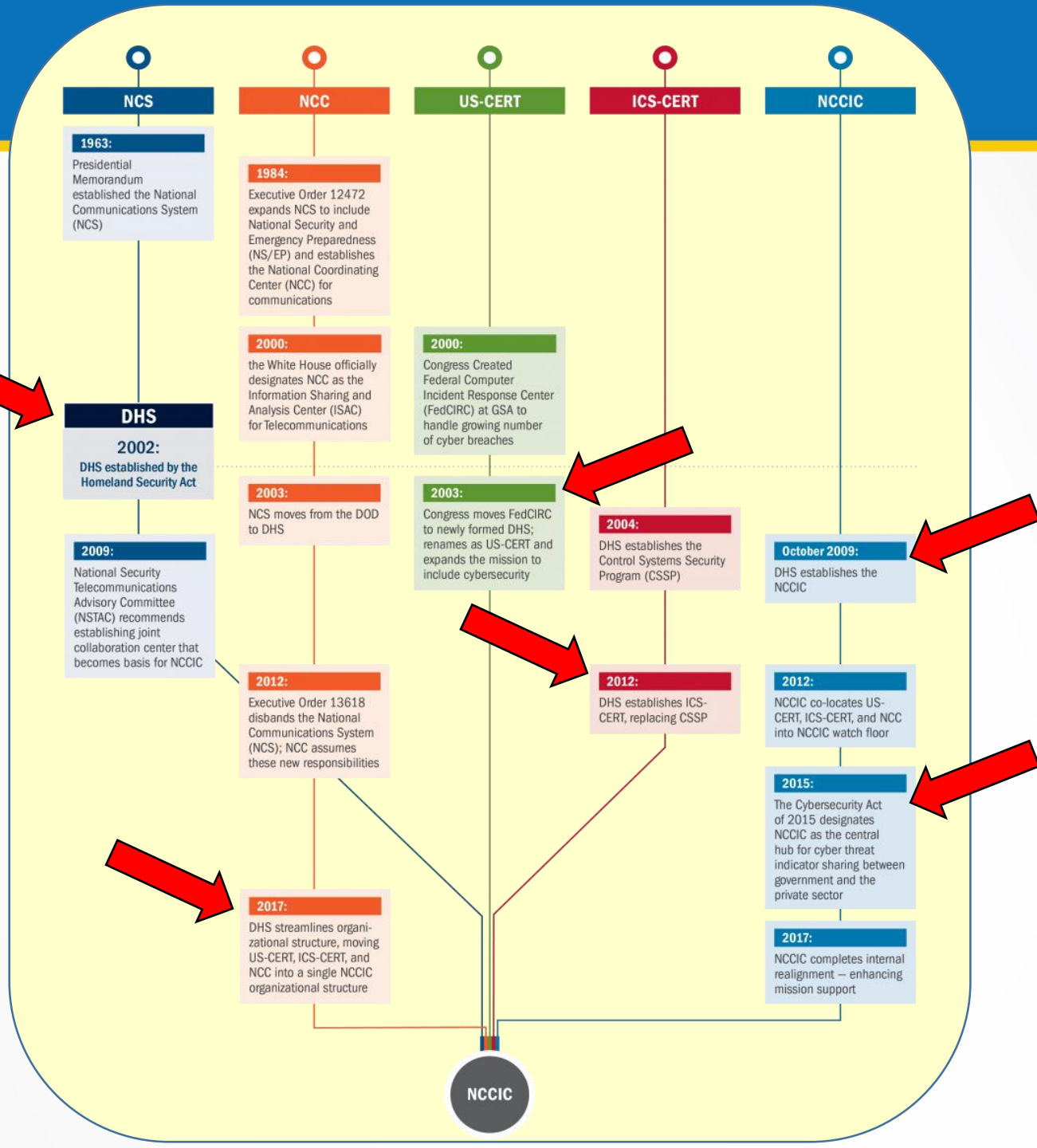
NCS – National Communications System

NCC – National Coordination Center (for comms)

US-CERT – US Computer Emergency Readiness Team

ICS-CERT – Industrial Control Systems Cyber Emergency Response Team

NCCIC – National Cybersecurity and Communications Integration Center



Fuente: https://www.us-cert.gov/about-us


Gracias
Thank You
Dank Je
Obrigado
Danke
Grazie
Arigato
Spasibo
Juspaxar
Chokrane
Multumesc
Kiitos
Dankon
Matondo
Mochchakkeram
Vinaka
Welalin
Kia Ora
Merci
Mamana
Terima Kasih
Obrigado
Grazie

Ciberdefensa

¿Cómo enfrentar este nuevo domínio militar?
Nivel operacional e gerencial – Visión Militar

Col João M E Carneiro (Ph.D.) – Ejército Brasileño
joao.carneiro@iadc.edu / carneiro.joao@eb.mil.br
Octobre 10, 2019