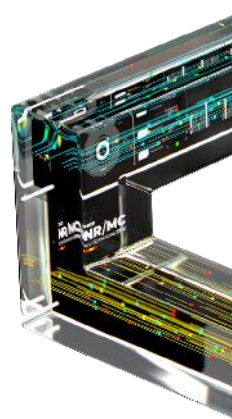




#XIVJORNADASCCNCERT

“Ciberinteligencia, pieza clave en la empresa en la era del desorden digital”



Presentación



José María Blanco



Licenciado en Empresariales y en Derecho



Manager Oficina de Inteligencia y
Prospectiva (Prosegur)



jose-maria.blanco-navarro@prosegur.com



<https://www.linkedin.com/in/jose-mar%C3%ADa-blanco-navarro-5b511137/>



Jorge Alcaín Pro



Grado en Ingeniería Informática



Business Solution Services Senior
Consultant (PwC)



jalcain@chronoseye.com



[@jorgeapro](https://twitter.com/jorgeapro)



<https://www.linkedin.com/in/jorgeapro/>

1. La era del desorden digital

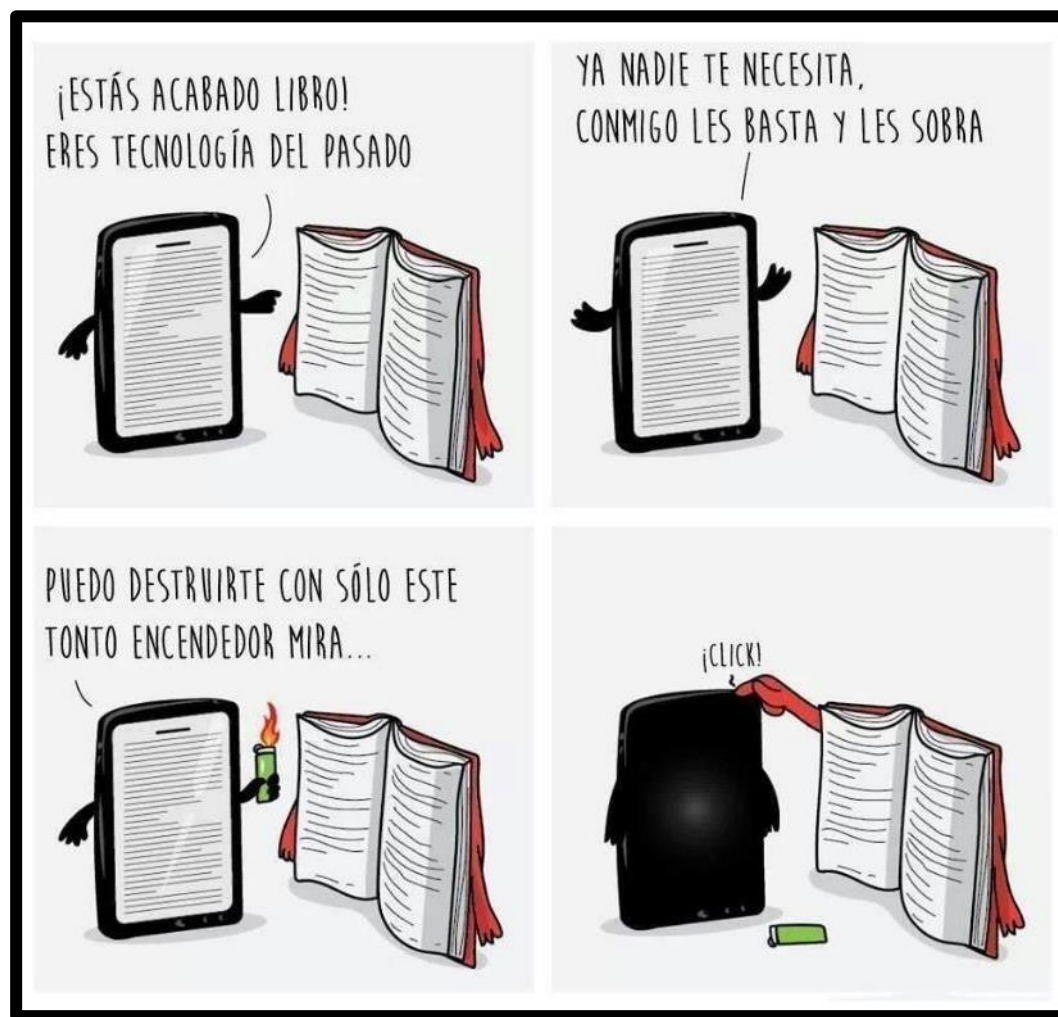
Los analfabetos del siglo XXI no serán aquellos que no sepan leer o escribir, sino aquellos que no puedan aprender, desaprender y reaprender

Alvin Toffler

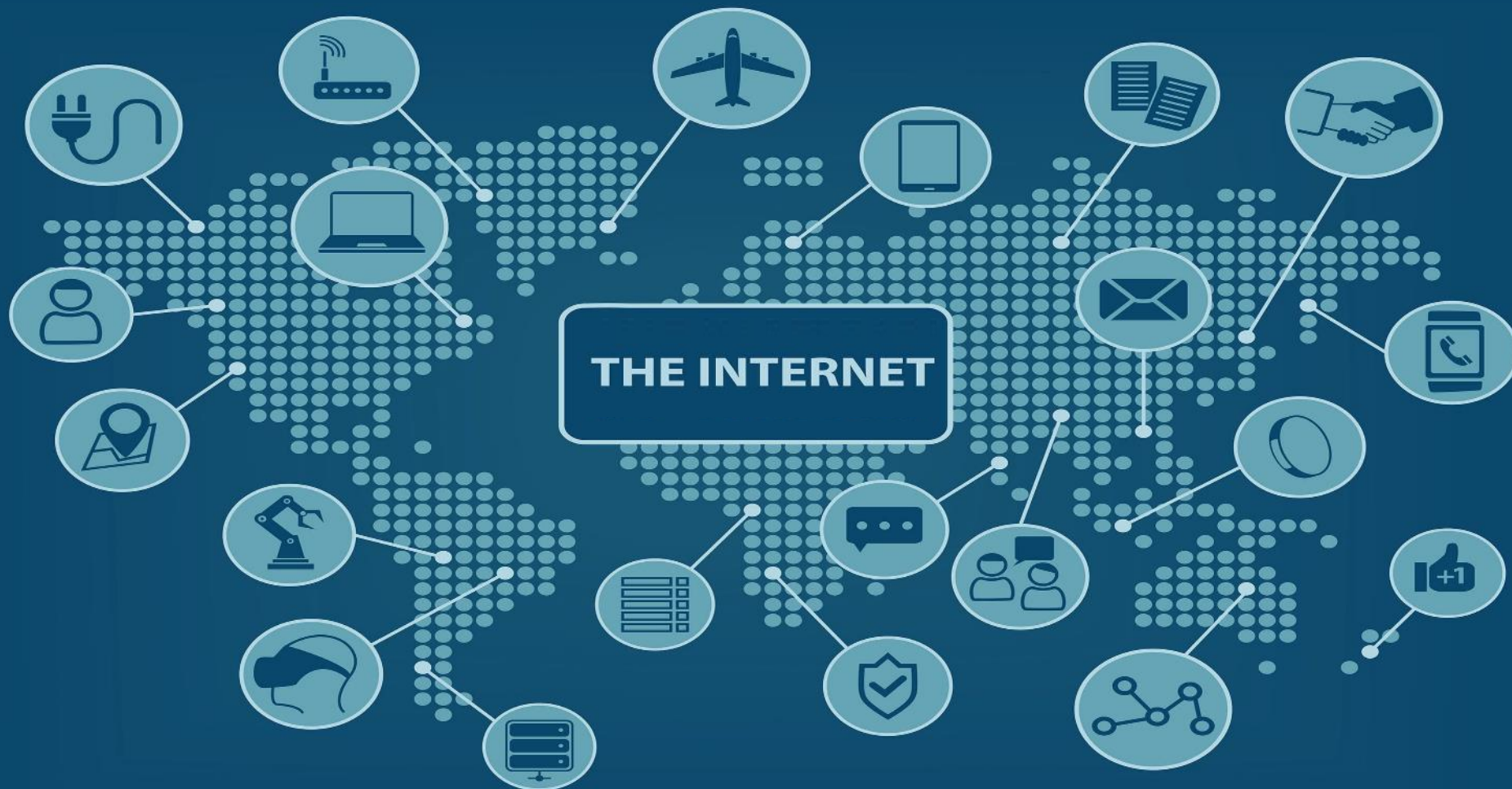


La era del desorden digital

Primer paso: Transformación del dato

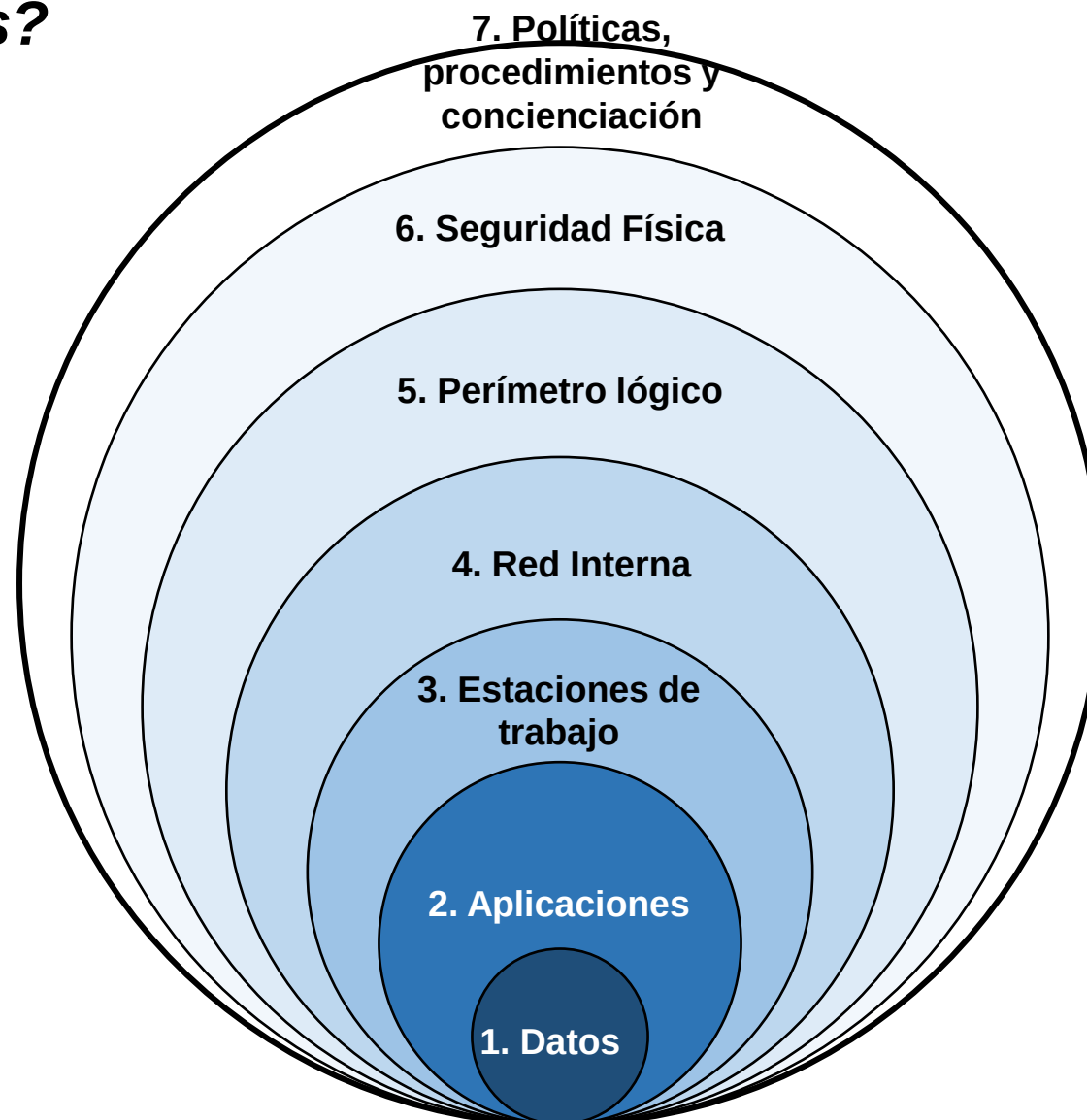


Segundo paso: **INTERNET**



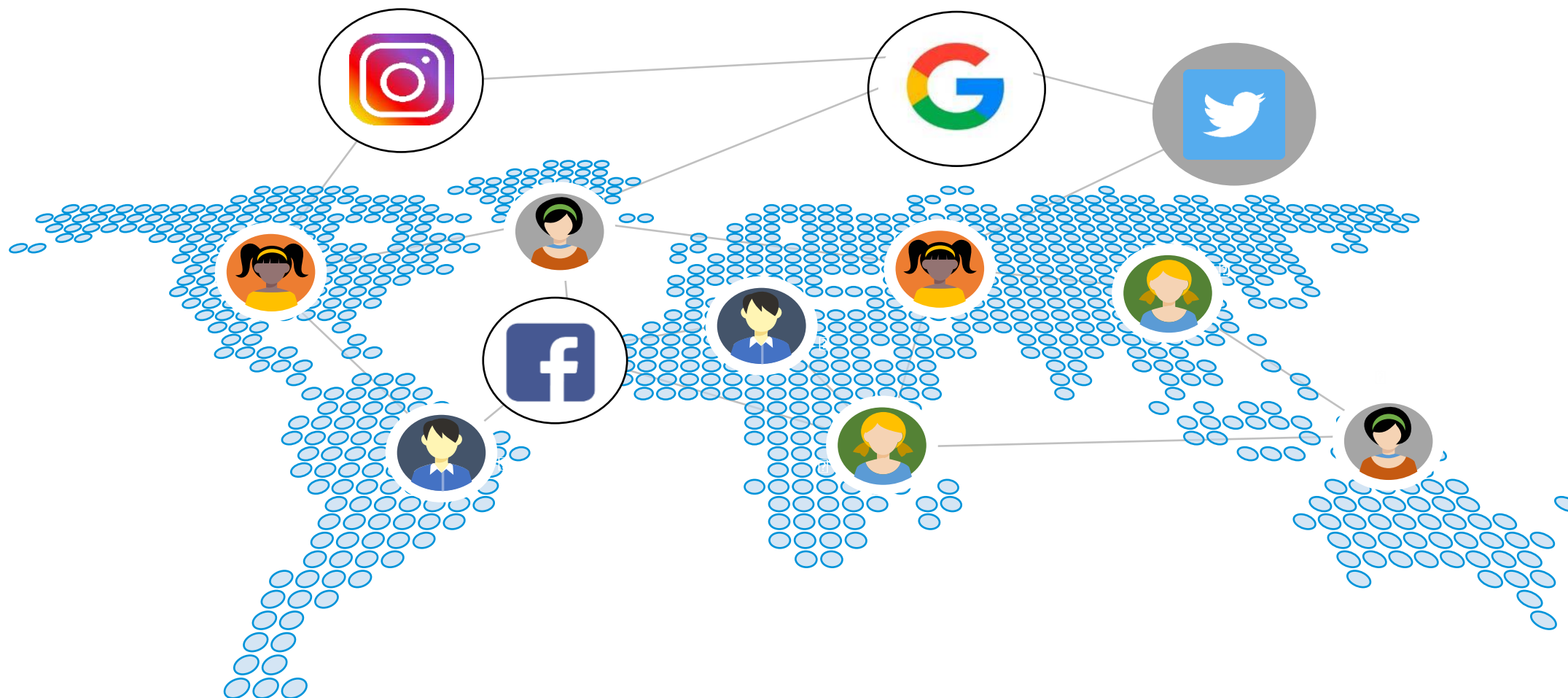
La era del **desorden digital**

¿Qué protegemos?



La era del desorden digital

Interconexión



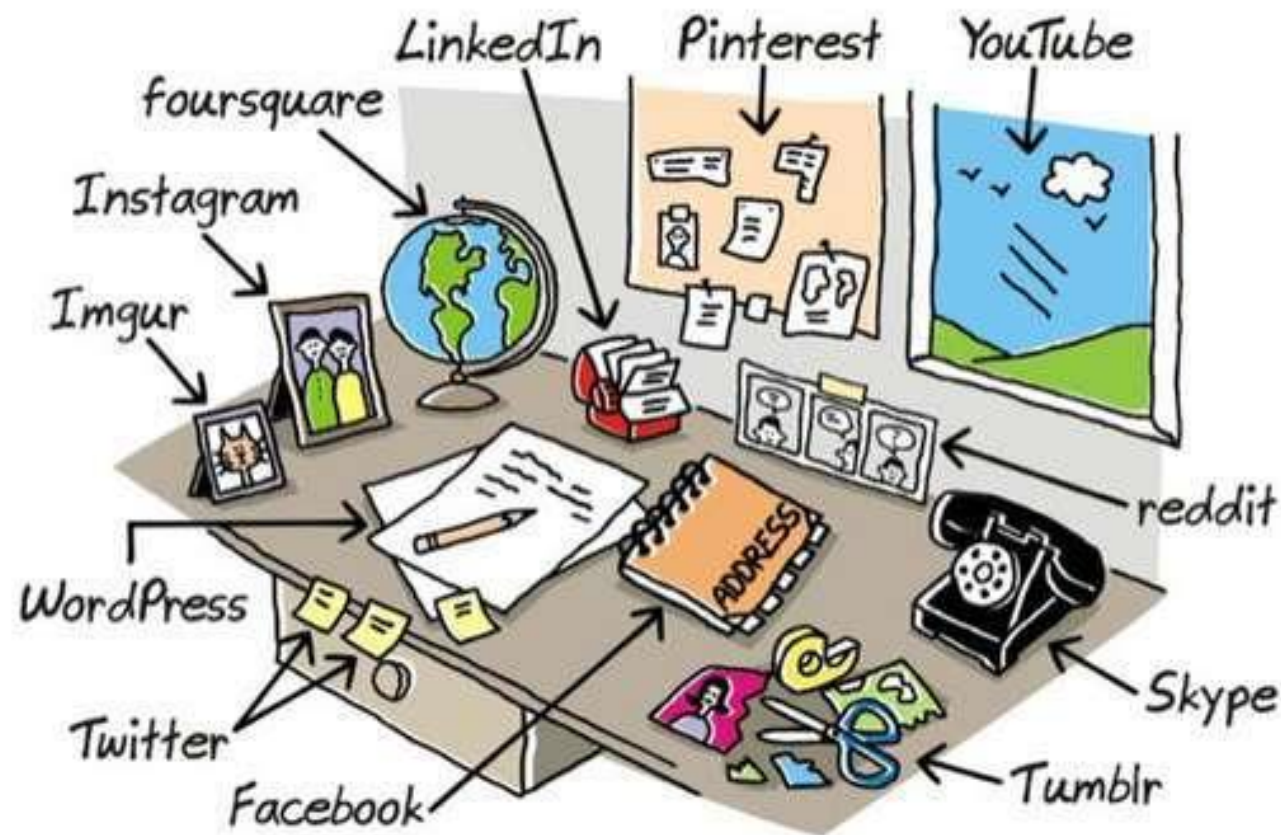
La era del **desorden digital**

Comunicación Inmediata



La era del desorden digital

¿En qué nos hemos **TRANSFORMADO**?



La era del desorden digital

¿Y cómo nos **PROTEGEMOS AHORA?**



La era del **desorden digital**

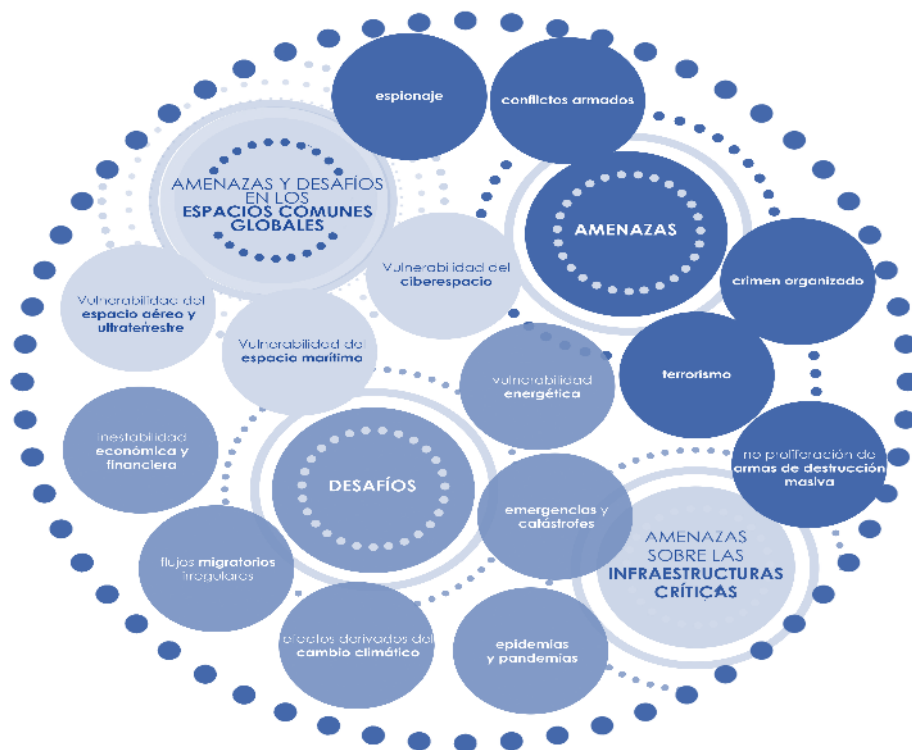
¿Y el **FUTURO**?



La era del **desorden digital**

Convergencia o hibridación mundo físico y lógico

AMENAZAS Y DESAFÍOS PARA LA SEGURIDAD NACIONAL



LEYENDA

- AMENAZAS
- AMENAZAS Y DESAFÍOS EN LOS ESPACIOS COMUNES GLOBALES
- AMENAZAS SOBRE LAS INFRAESTRUCTURAS CRÍTICAS
- DESAFÍOS



DSN



- Diferentes sistemas de seguridad física -

La era del desorden digital

¿Cómo impacta COVID-19?

Crisis sanitaria y económica
Elevada incertidumbre



Crisis de poder
Era del desorden



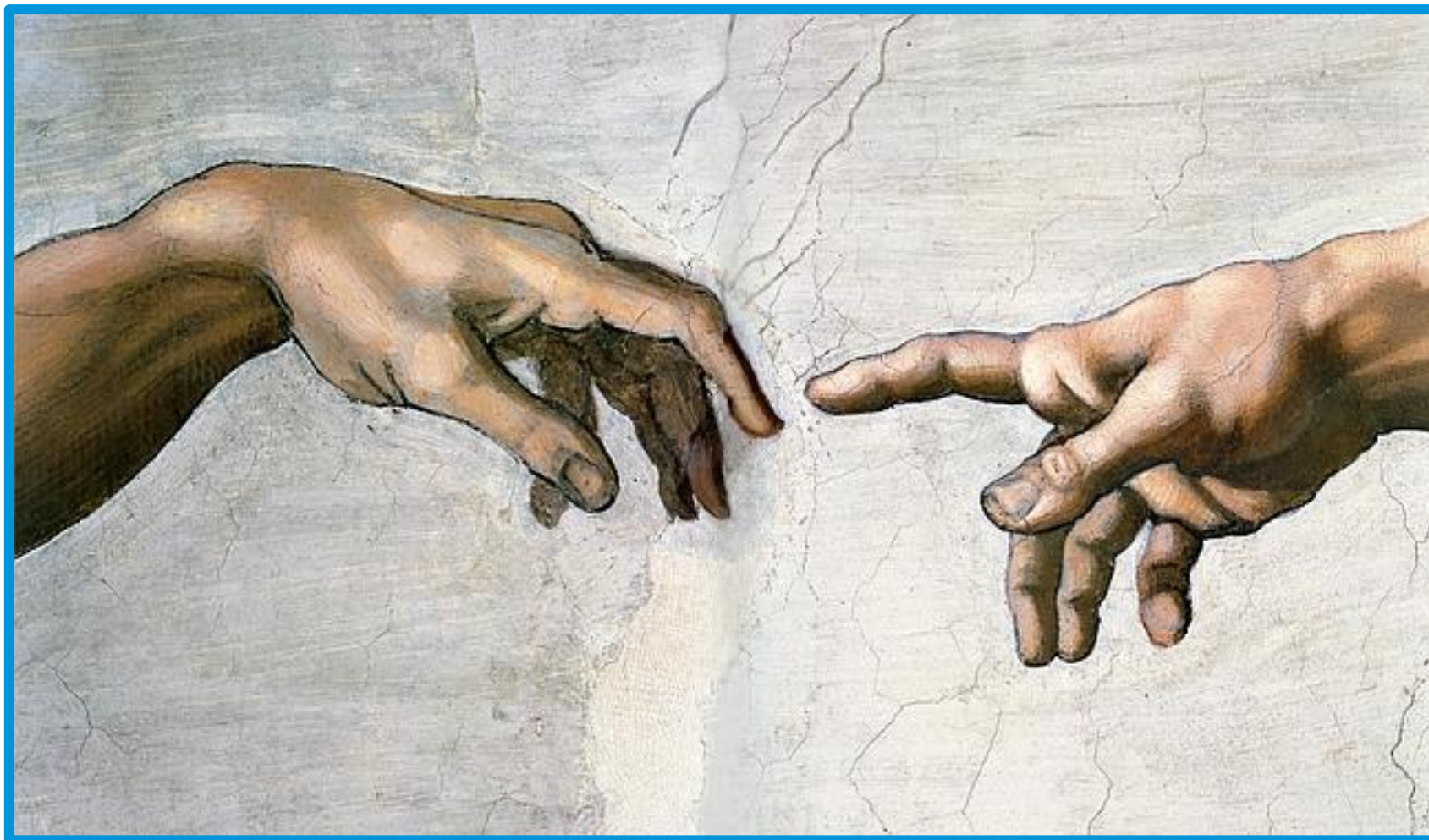
Globalización digital
Poder en red



Cambio de hábitos y valores
Trabajo, ocio, consumo

La era del **desorden digital**

Convergencia o hibridación **mundo físico y lógico**



2. Ciberinteligencia en tiempos de desorden

El conocimiento si no se sabe
aplicar es peor que la ignorancia

Charles Bukowski



Ciberinteligencia en tiempos de desorden

Diversidad de **CONCEPTOS**

“El **conocimiento sobre los ciber-adversarios y sus métodos**, además del conocimiento sobre la posición de seguridad de una organización sobre sus adversarios en el ciberespacio y sus métodos” (RSA, 2012)

“Los **productos y los procesos del ciclo de inteligencia** para analizar las capacidades, intenciones y actividades – no sólo técnicas- de los potenciales adversarios y competidores en el ciberespacio” (INSA, 2015)

“La **adquisición y análisis de información** para identificar, seguir y predecir ciber-capacidades, intenciones y actividades que ofrezcan líneas de acción para apoyar la toma de decisiones” (Carnegie Mellon Software Engineering, 2013)



Ciberinteligencia en tiempos de desorden

*¿Posibilidad de un **CONCEPTO** consensuado?*

Proceso y producto de la **obtención y análisis** de datos e información **en/sobre el ciberespacio**, realizado por **especialistas**, y orientado a la **toma de decisiones** en forma, tiempo y lugar

Adaptación basada en definiciones de Javier Candau (CCN-CERT) y Manuel Torres Soriano (GESI)

Ciberinteligencia en tiempos de desorden

Tipos de Ciberinteligencia

ESTRATÉGICA

- Amplia en la obtención.
- Más allá del sector.
- Mira a medio y largo plazo.
- Amplia en identificar adversarios
- Analiza el entorno
- Menos técnica
- Vinculada a análisis de riesgos

TÁCTICA

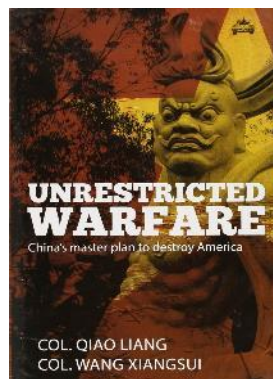
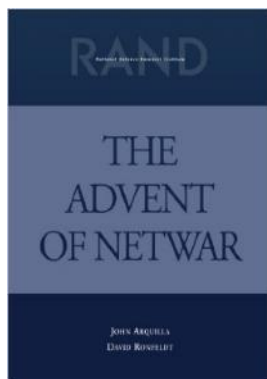
- Donde las batallas se planifican y ejecutan
- Equipos de respuesta a incidentes
- Resiliencia y análisis forense
- Análisis del atacante: modus operandi, motivaciones, capacidades, etc.
- Carácter técnico

OPERACIONAL

- Orientada a los managers de IT, CIO, CISO.
- Apoyo a decisiones
- Foco en procesos y operaciones: negocio, clientes, proveedores...
- Análisis adversario técnico
- Combina tareas técnicas y no técnicas (vectores de mayor riesgo)

Ciberinteligencia en tiempos de desorden

Aportación de la *Inteligencia* a la Ciberinteligencia



La violencia (y el delito) ha dejado de ejercerse, parcialmente, a través del uso de armas de fuego. Ha derivado hacia la desinformación y el control de áreas sensibles de países y sociedades, como la economía, la energía y los recursos, siendo la tecnología parte de ese engranaje.

1

Intereses a proteger

2

Fundamentos y doctrina

3

Ciclo o proceso de Inteligencia

4

Trabajo con fuentes diversas

5

Técnicas estructuradas de análisis

6

Conocimiento sobre desinformación

7

Prospectiva

Ciberinteligencia en tiempos de desorden

Aportación de la Ciberinteligencia a la Inteligencia

Ser capaz de superar la seguridad no te convierte en un hacker, de la misma forma que hacer un puente a un coche no te convierte en ingeniero mecánico

Eric S. Raymond



Ciberinteligencia en tiempos de desorden

Herramienta de *VISIÓN EN EL MUNDO DIGITAL*



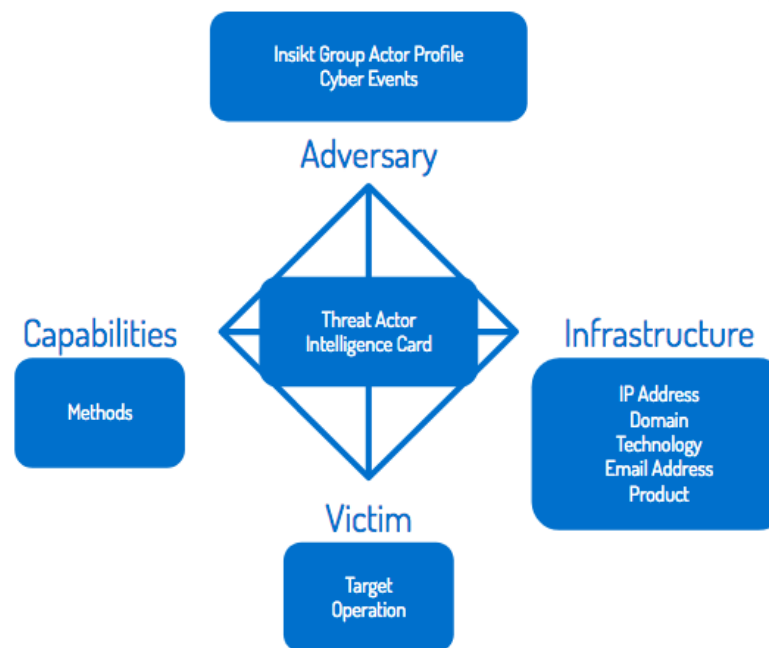
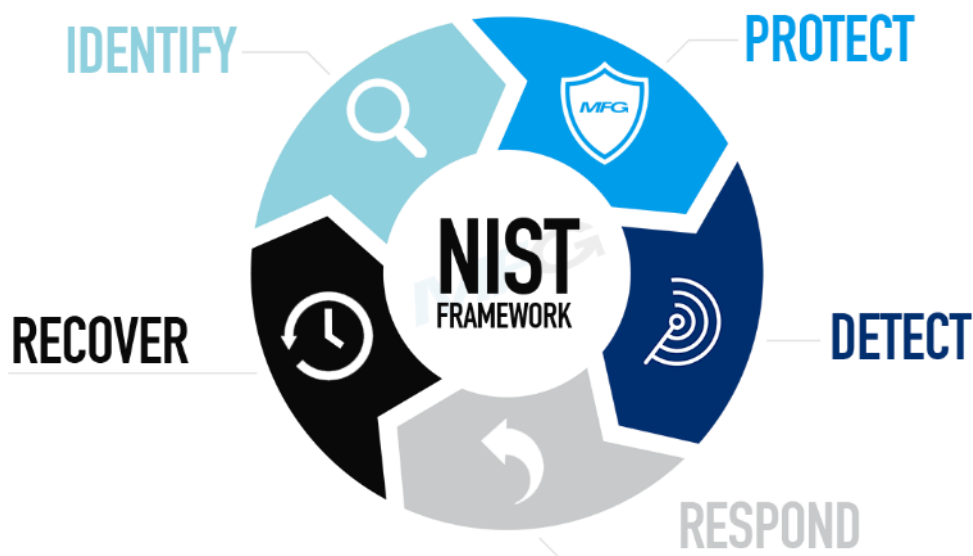
OPSEC

OPERATIONS SECURITY



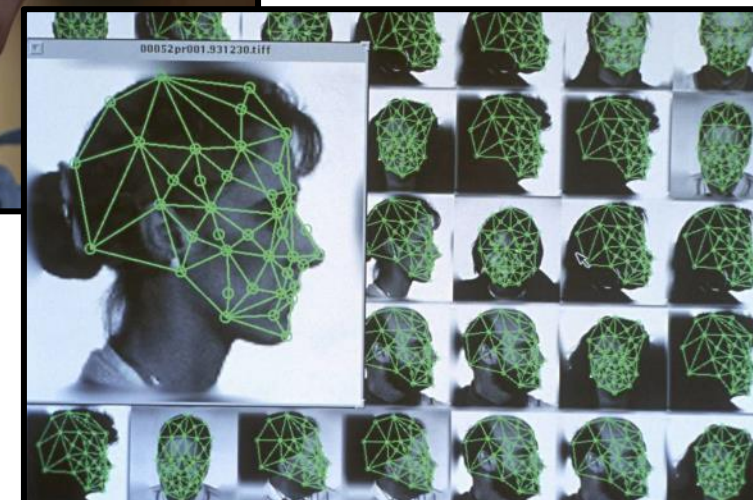
Ciberinteligencia en tiempos de desorden

Metodologías



Ciberinteligencia en tiempos de desorden

PRESENTE Y FUTURO de la Ciberinteligencia



3. Ciberinteligencia en la empresa

3

El futuro ya no es lo que era
Paul Valery



Ciberinteligencia en la empresa

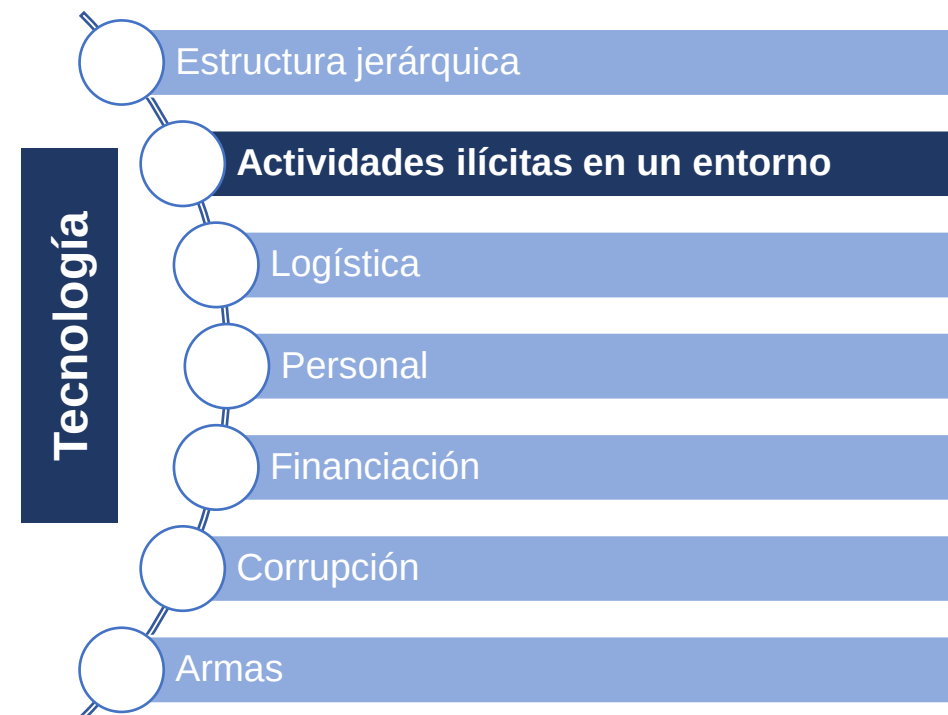
Enfoque de Riesgos

Riesgos para las empresas



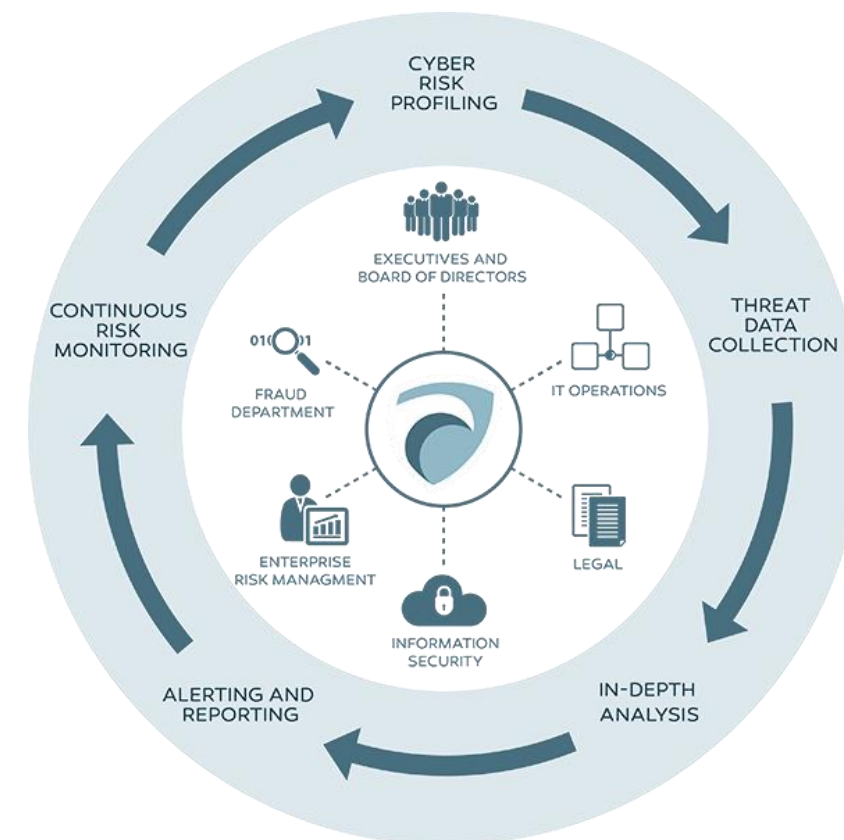
Situational Awareness

Ciber crimen organizado



Ciberinteligencia en la empresa

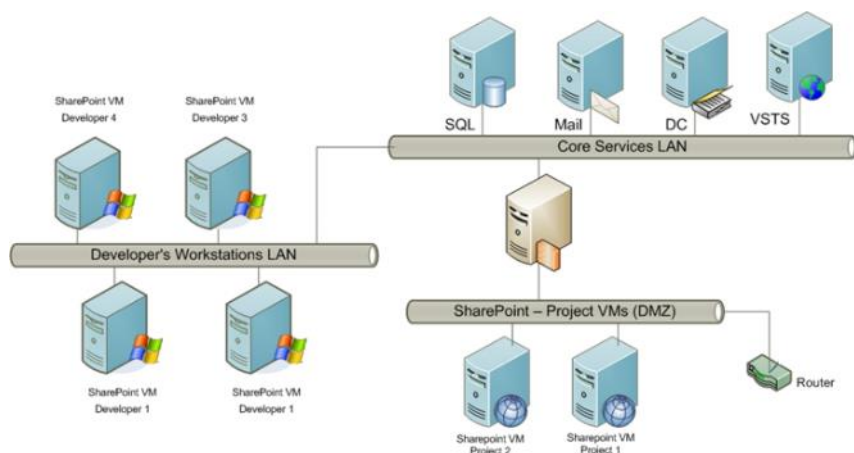
La Ciberseguridad en la Seguridad de la Empresa



<https://www.surfwatchlabs.com/threat-categories>

Ciberinteligencia en la empresa

La Ciberinteligencia en la Ciberseguridad



Hacking

DF

Integración

Ciber Inteligencia

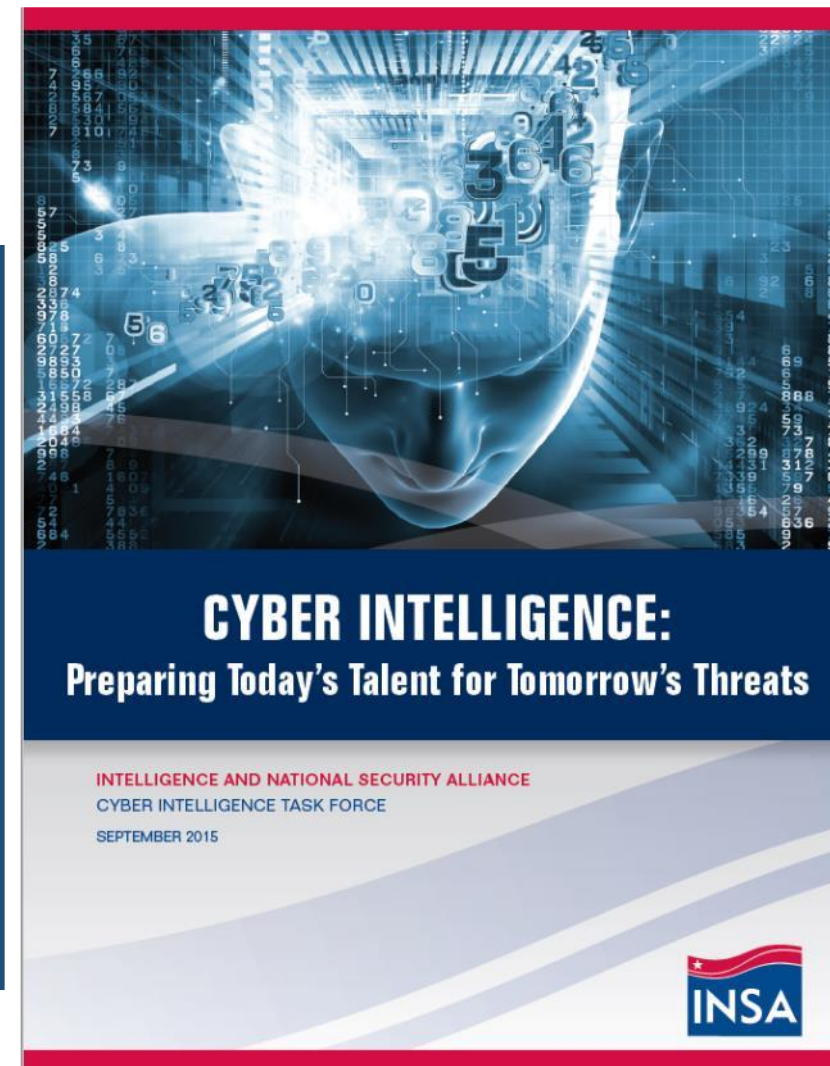
MSS

3. El analista de ciberinteligencia

4

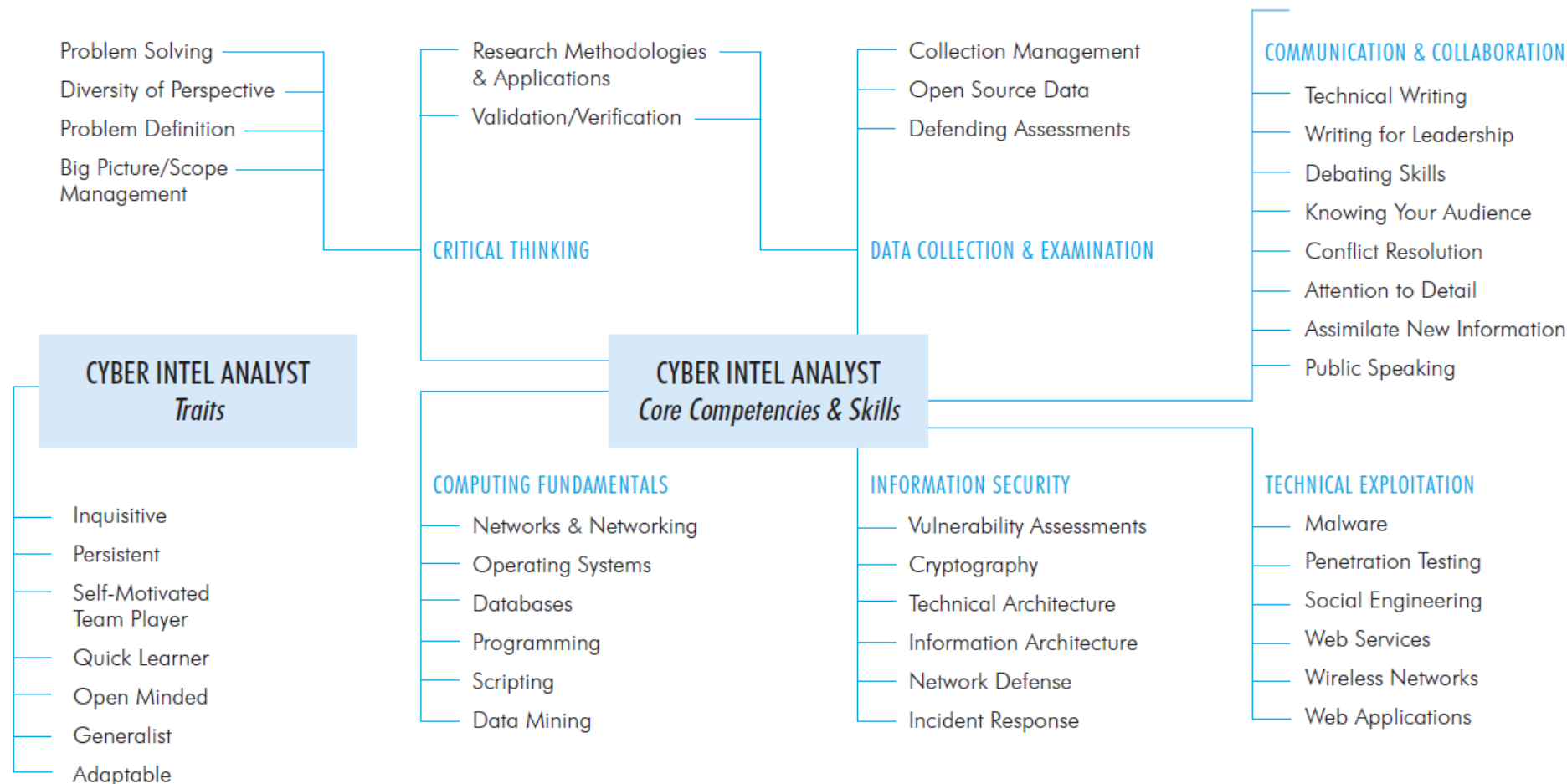
“Conocimiento de la superficie de ataque, sus objetos de mayor valor y objetivos, y cómo sus vulnerabilidades pueden ser explotadas; mantener un situational awareness sobre actores maliciosos; desarrollar técnicas y aplicaciones para contrarrestar, identificar y vigilar; en su versión más avanzada entender las motivaciones de los atacantes, su lenguaje, organización, comportamiento individual y grupal, con objeto de perfilar grupos, actores y campañas”

Department of Homeland Security, 2012



El analista de ciberinteligencia

Competencias y habilidades



El analista de ciberinteligencia

Formación base

1

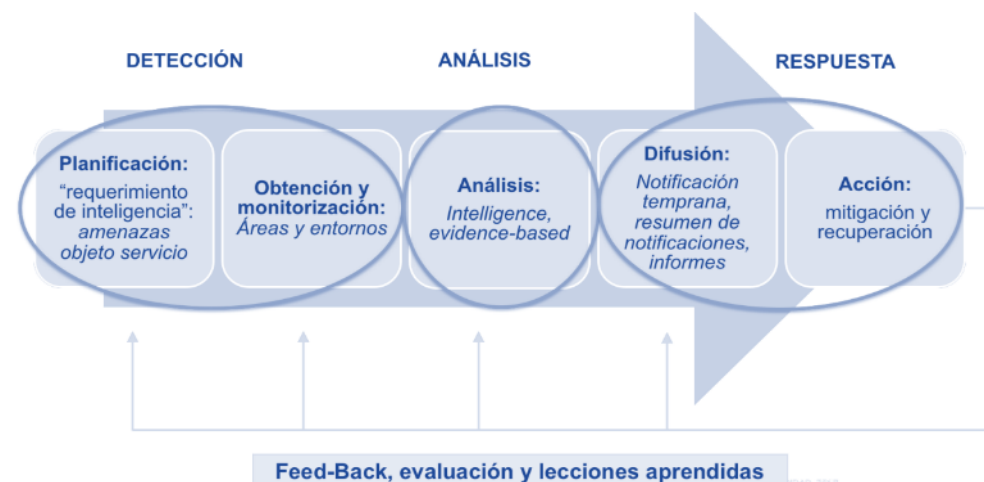
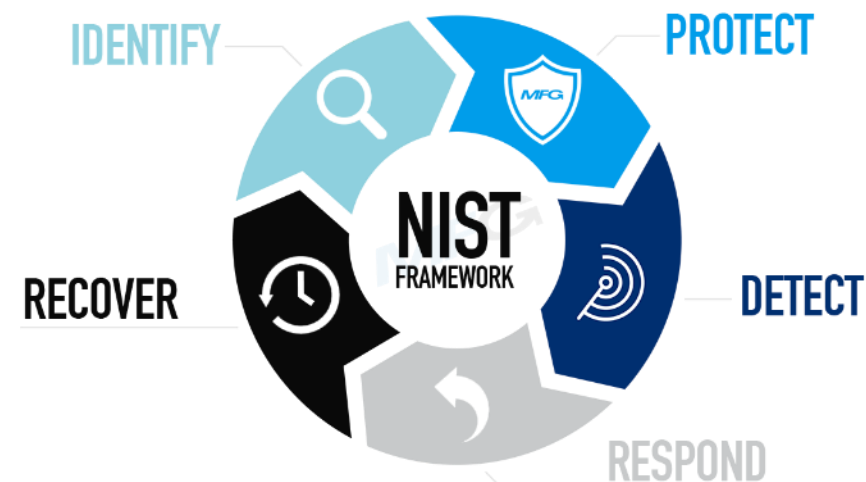
Competencias técnicas

2

Competencias analíticas

3

Conocimiento del dominio



El analista de ciberinteligencia

Formación continua

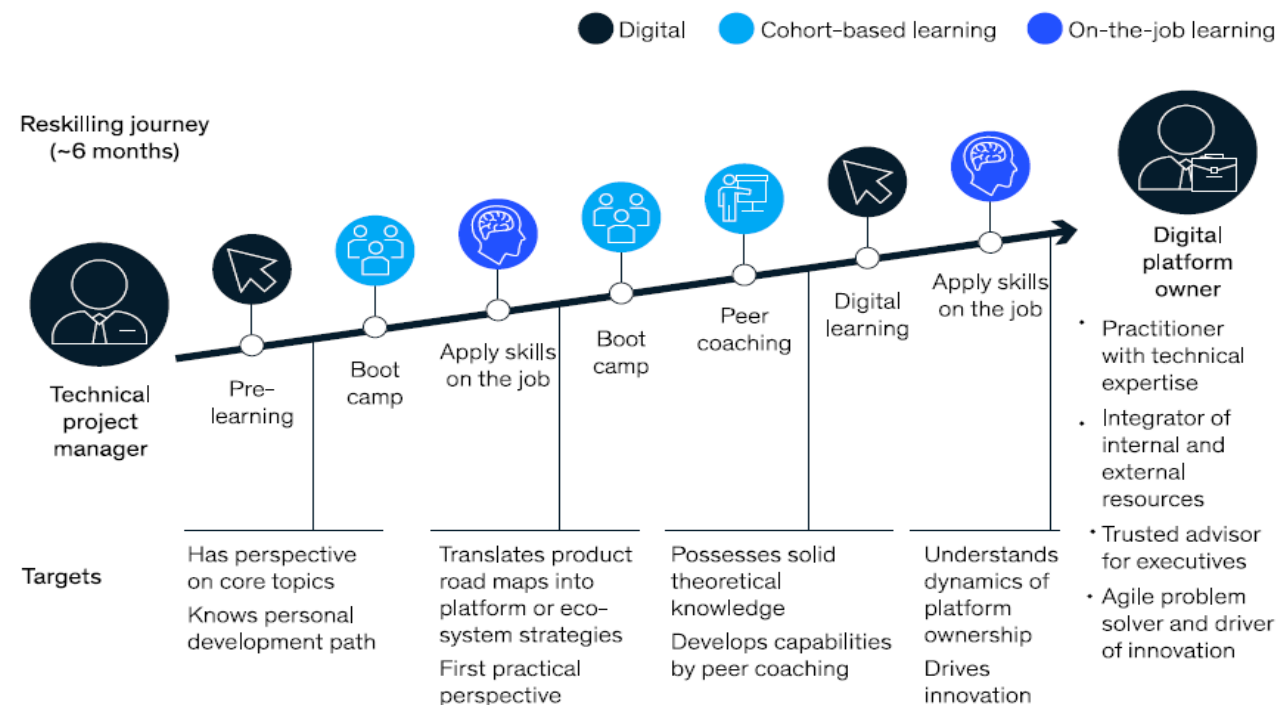


El analista de ciberinteligencia

Reclutamiento

Individual learning journeys are tailored to specific skills needs over a range of formats.

Tech company example



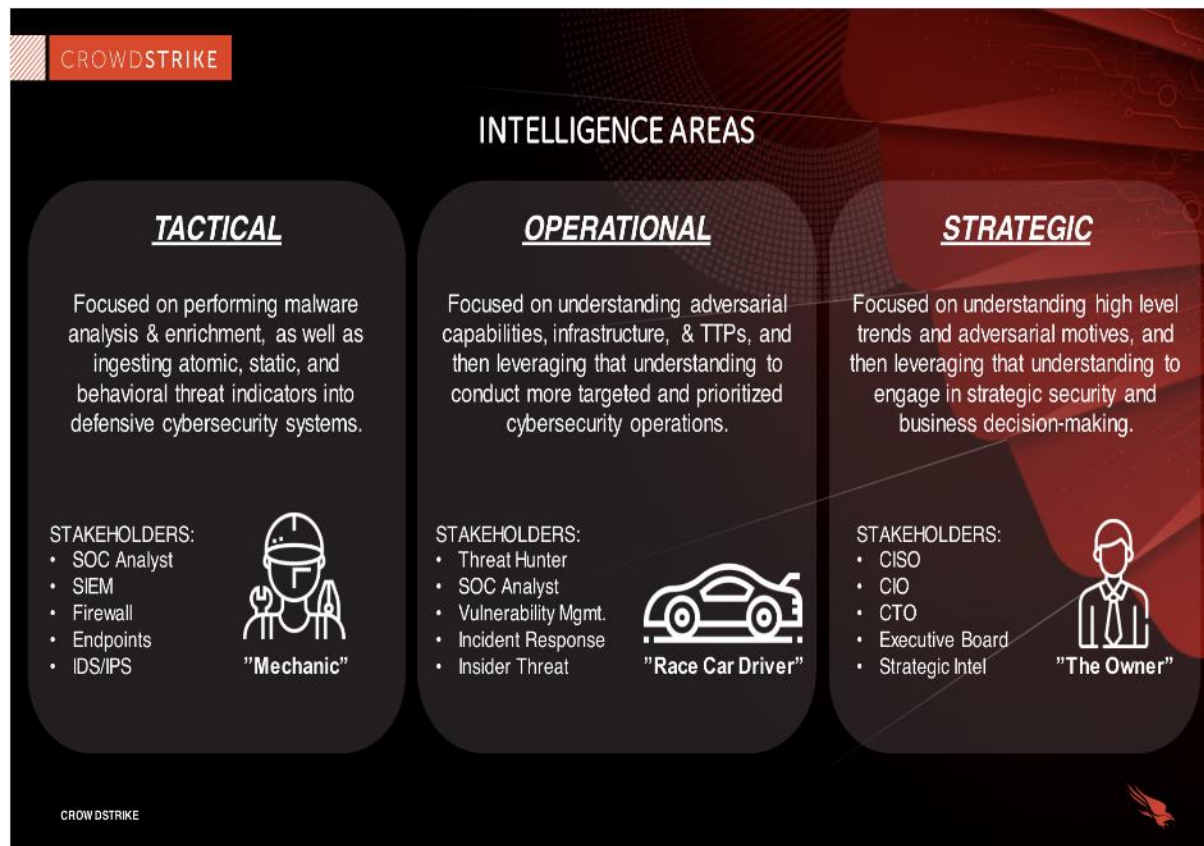
McKinsey & Company

#XIVJORNADASCCNCERT



El analista de ciberinteligencia

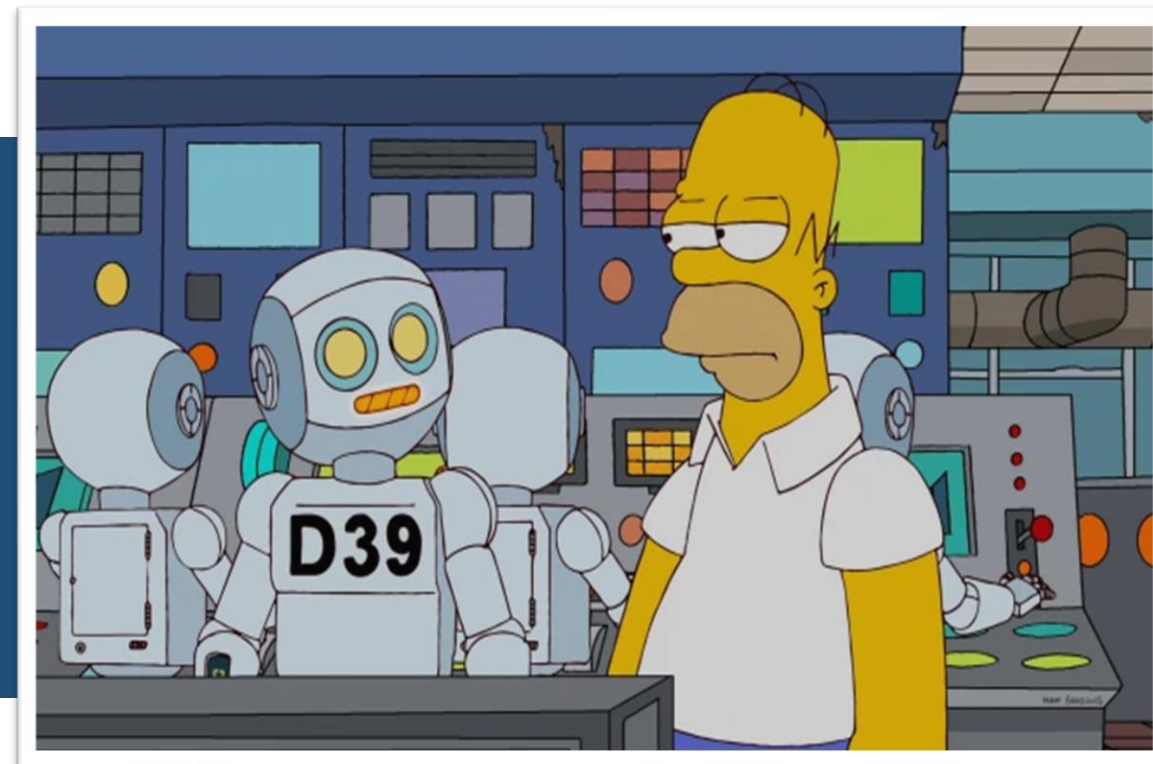
Promoción y carrera profesional



4. Hacia un futuro (ciber)inteligente

5

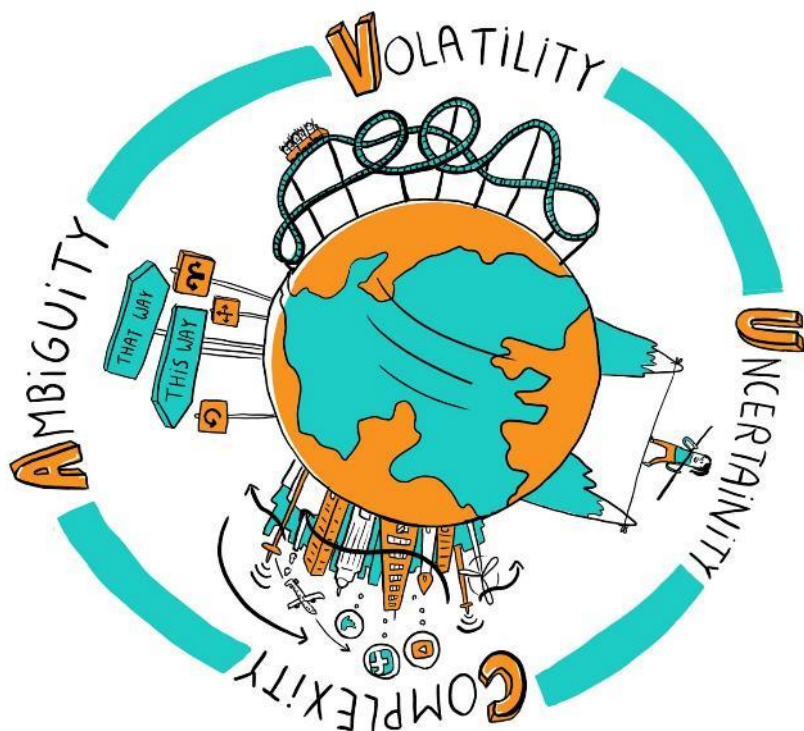
En tiempos de cambio, quienes estén abiertos al aprendizaje se adueñarán del futuro, mientras que aquellos que creen saberlo todo estarán bien equipados para un mundo que ya no existe
Eric Hoffer



Hacia un futuro (ciber)inteligente

VUCA: aceleración exponencial, interdependencia, discontinuidad

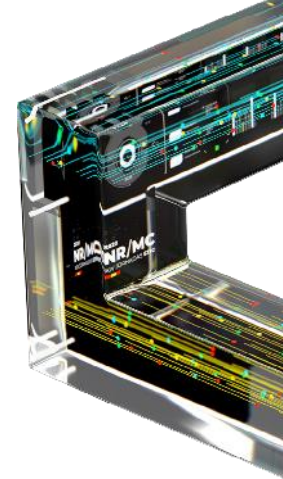
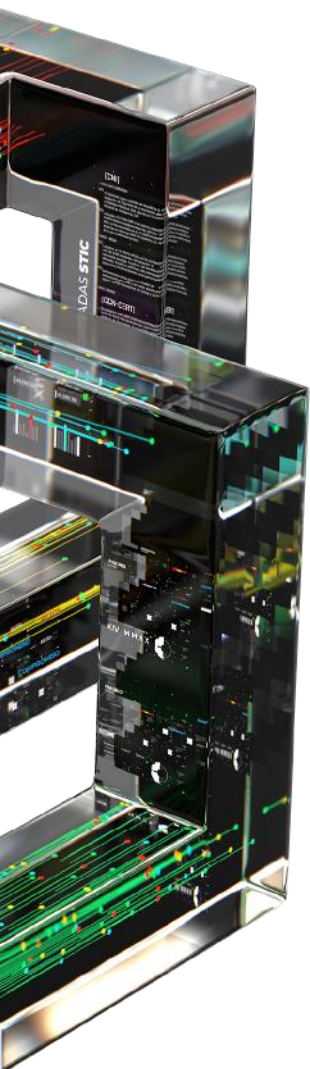
we live in a **VUCA** World



Hacia un futuro (ciber)inteligente

10 puntos para el FUTURO

1. **Extrema convergencia entre el mundo físico y lógico. Los riesgos para estados, organizaciones, empresas e individuos pueden tener aspectos tanto físicos como lógicos.**
2. **Desde ambas inteligencias se trata de proteger los mismos intereses: personas, infraestructuras, imagen y marca, datos e información, patrimonio y continuidad de negocio.**
3. **(CYBER)INTEL no es una ciencia. Debe ser desarrollada en muchos ámbitos**
4. **La INTEL precisa pragmatismo, uso de cualquier fuente o metodología que sea ÚTIL para apoyar toma de decisiones. NO DEBEMOS SER DOGMÁTICOS**
5. **La (CYBER)INTEL recoge marcos y metodologías de muchas disciplinas ajenas, de las ciencias sociales**
6. **Las 2 INTEL precisan de aproximaciones cuantitativas y cualitativas, para abordar la complejidad de los riesgos de nuestro mundo. IA, ML, data science, risk intelligence como aproximaciones muy relacionadas**
7. **La (CYBER)INTEL debe ser HOLÍSTICA. Para conocer el ciberespacio es preciso conocer el mundo físico y viceversa. Geopolítica, estrategia, conocimiento de las organizaciones, etc.**
8. **Prospectiva. Ir más allá del cortoplacismo, de lo inmediato. ANTICIPAR**
9. **MUNDO COMPLEJO. TENDREMOS CISNES NEGROS. Anticipar (ciberinteligencia) + Resiliencia (FDIR). No compartimentar la Inteligencia**
10. **Se precisa desarrollar el "oficio" de analista de (ciber)inteligencia, en base a las premisas previas**



MUCHAS GRACIAS

#XIVJORNADASCCNCERT