lacnic23
18/22 mayo - lima, perú

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

# Desarrollo de estrategias de ciberseguridad nacional y protección de infraestructuras críticas

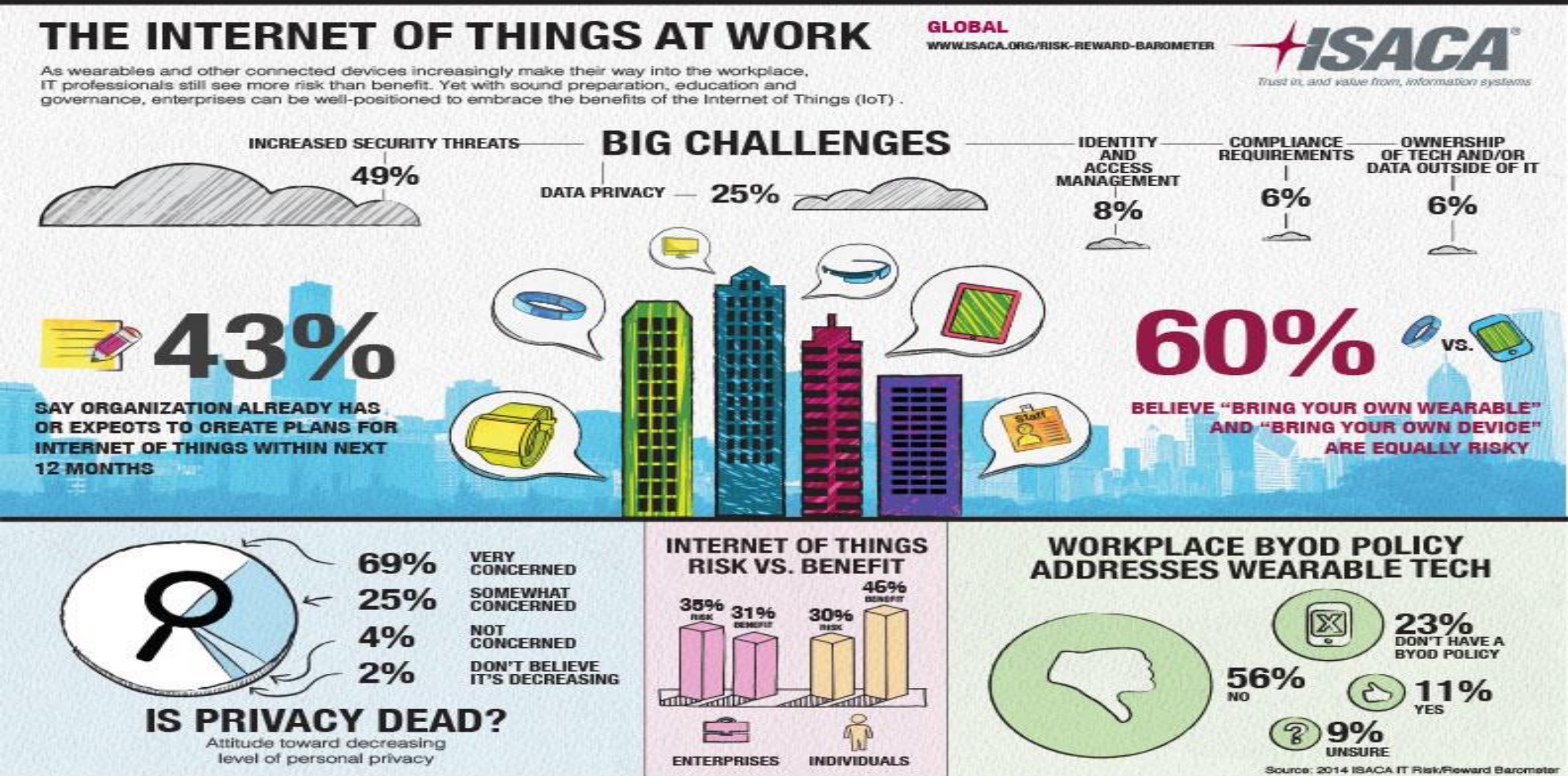
**Juan Dávila, MBA, CRISC, CISM, CISA, ISO 27001 LA, ISO 22301 LA, Cobit 5F Acc Trainer**

**LACSEC 2015**

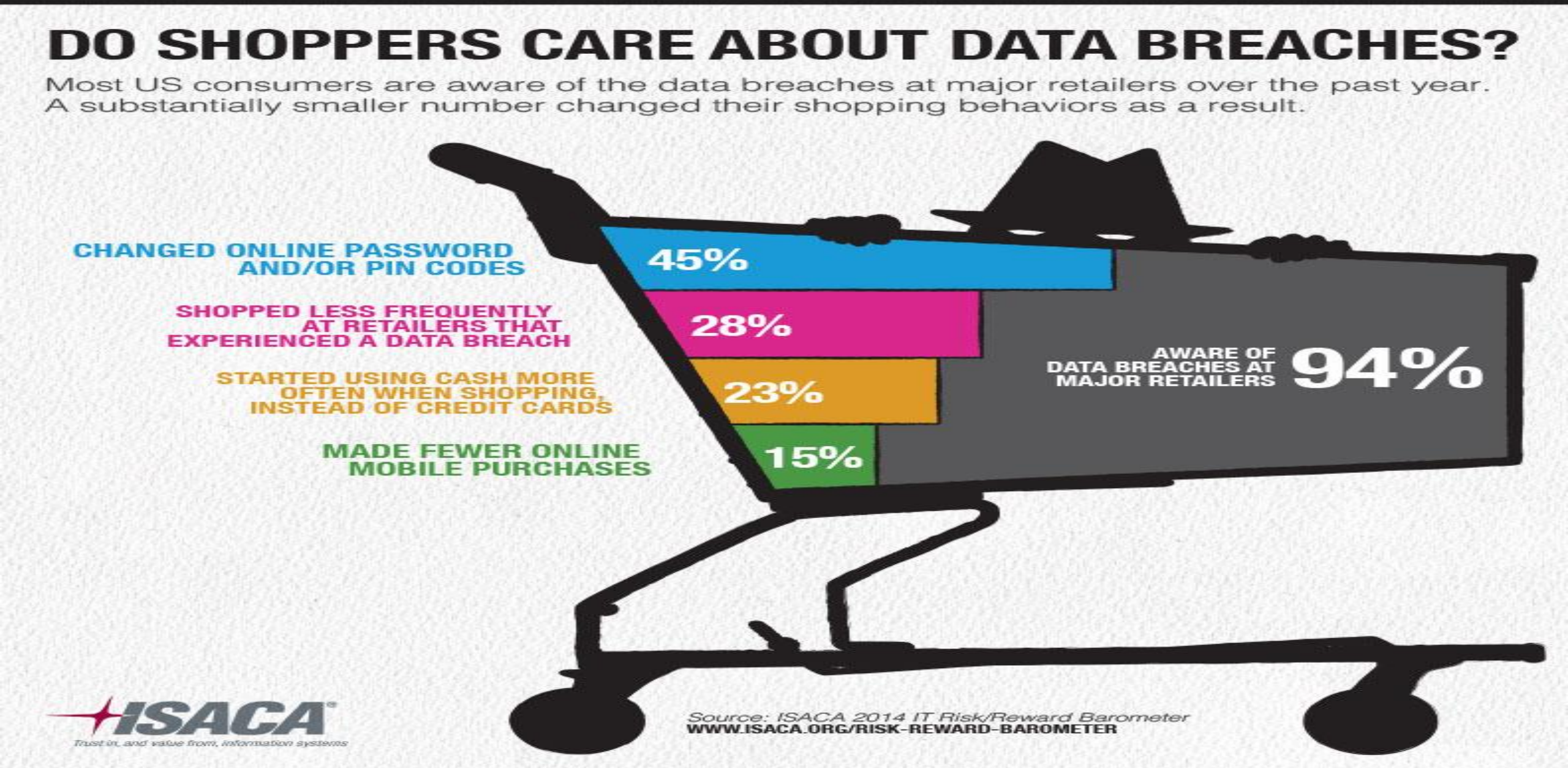

2005


2013
NBC NEWS

# Riesgos y comportamientos



# Riesgos y comportamientos



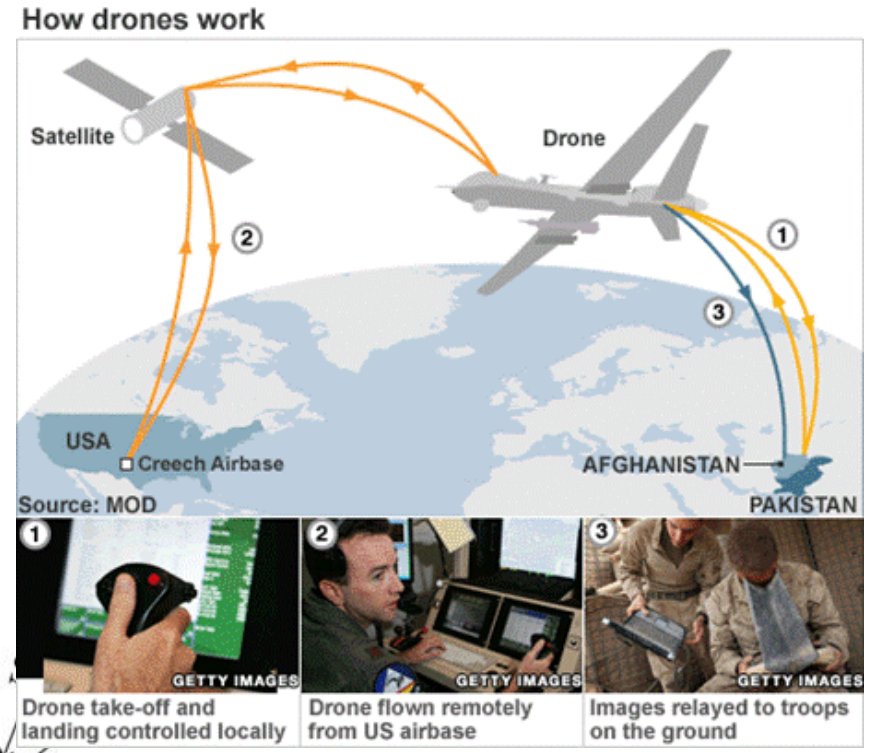
# Ciber … qué?

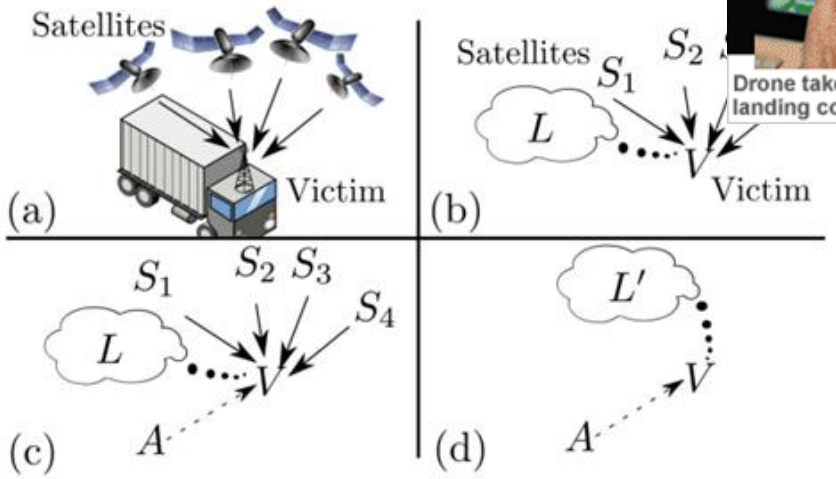

LACSEC 2015

# Facts !!!

- “Anyone can simply gather information related to the hacking of drones online with the use of Google” (Esti Peshin, Israel Aerospace Industries Cyber-programs Director).
- El mayor problema con los drones está relacionado con la tecnología obsoleta utilizada en su funcionamiento.
- Todd Humphrey (University of Texas), demostró, con aprox. US$ 1,000 en equipos y pocos colaboradores, la capacidad de enviar señales al GPS de un drone militar, secuestrarlo en el aire y controlar su ruta.

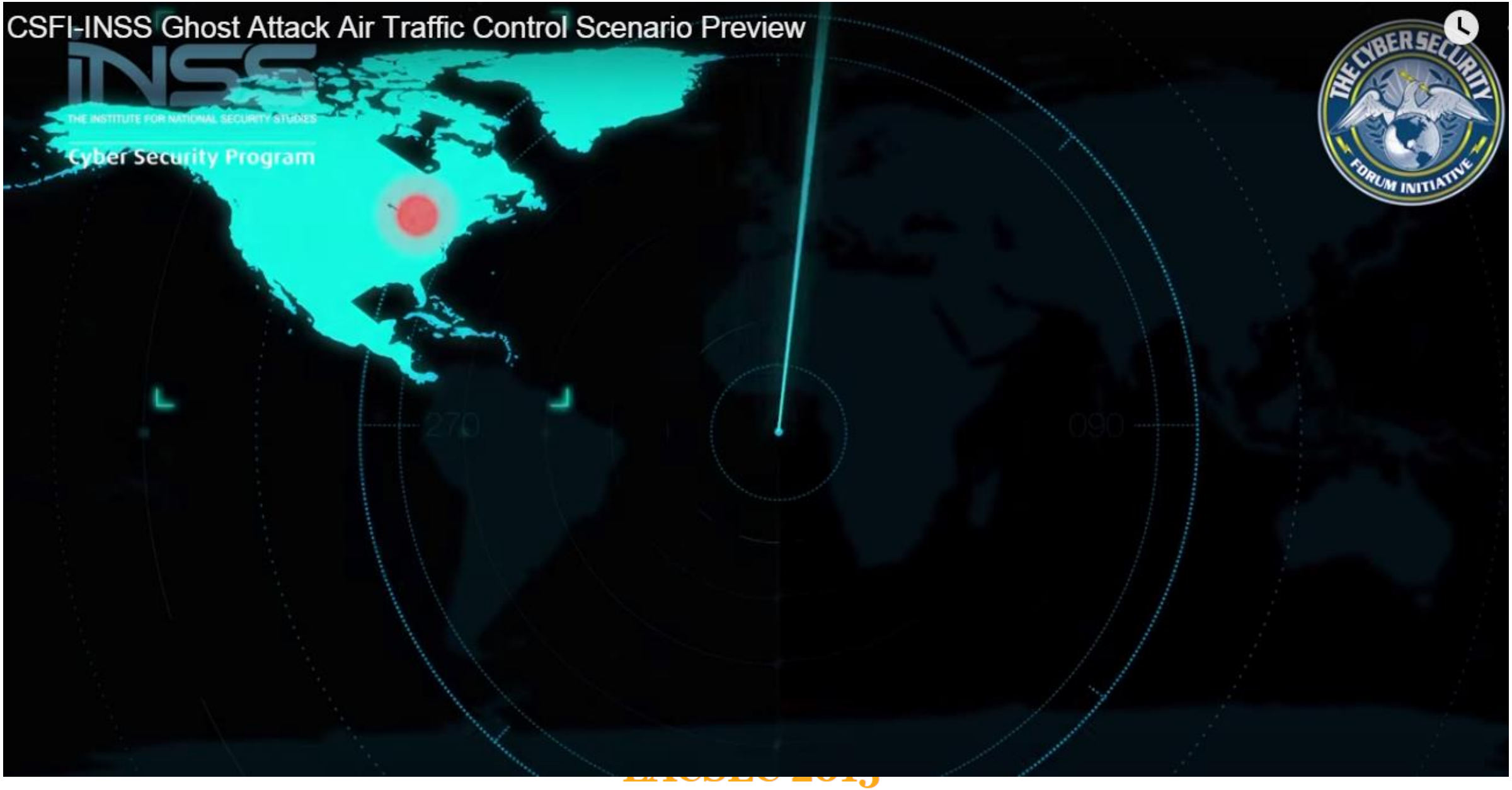
# Ciber … qué?



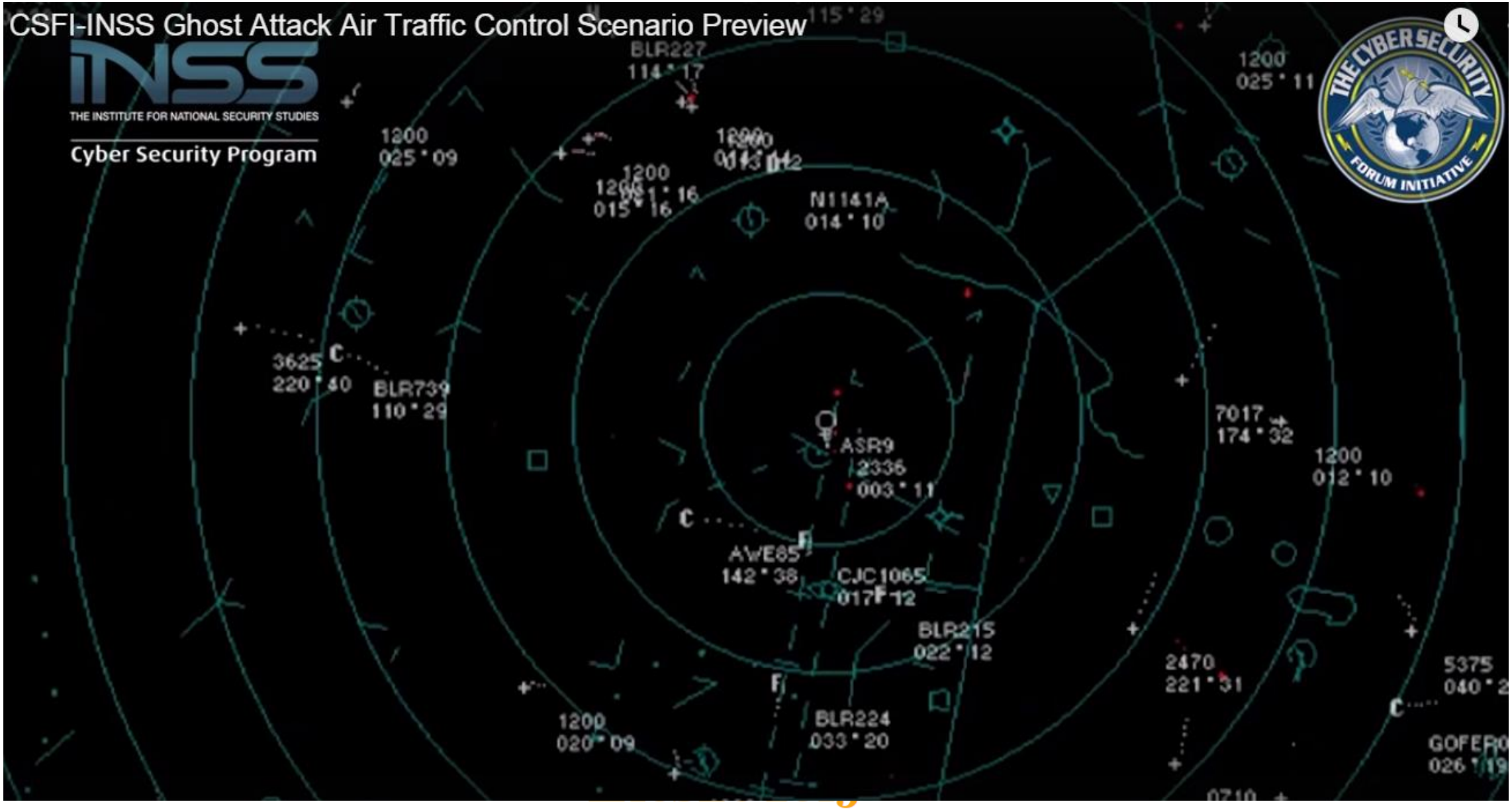




LACSEC 2015

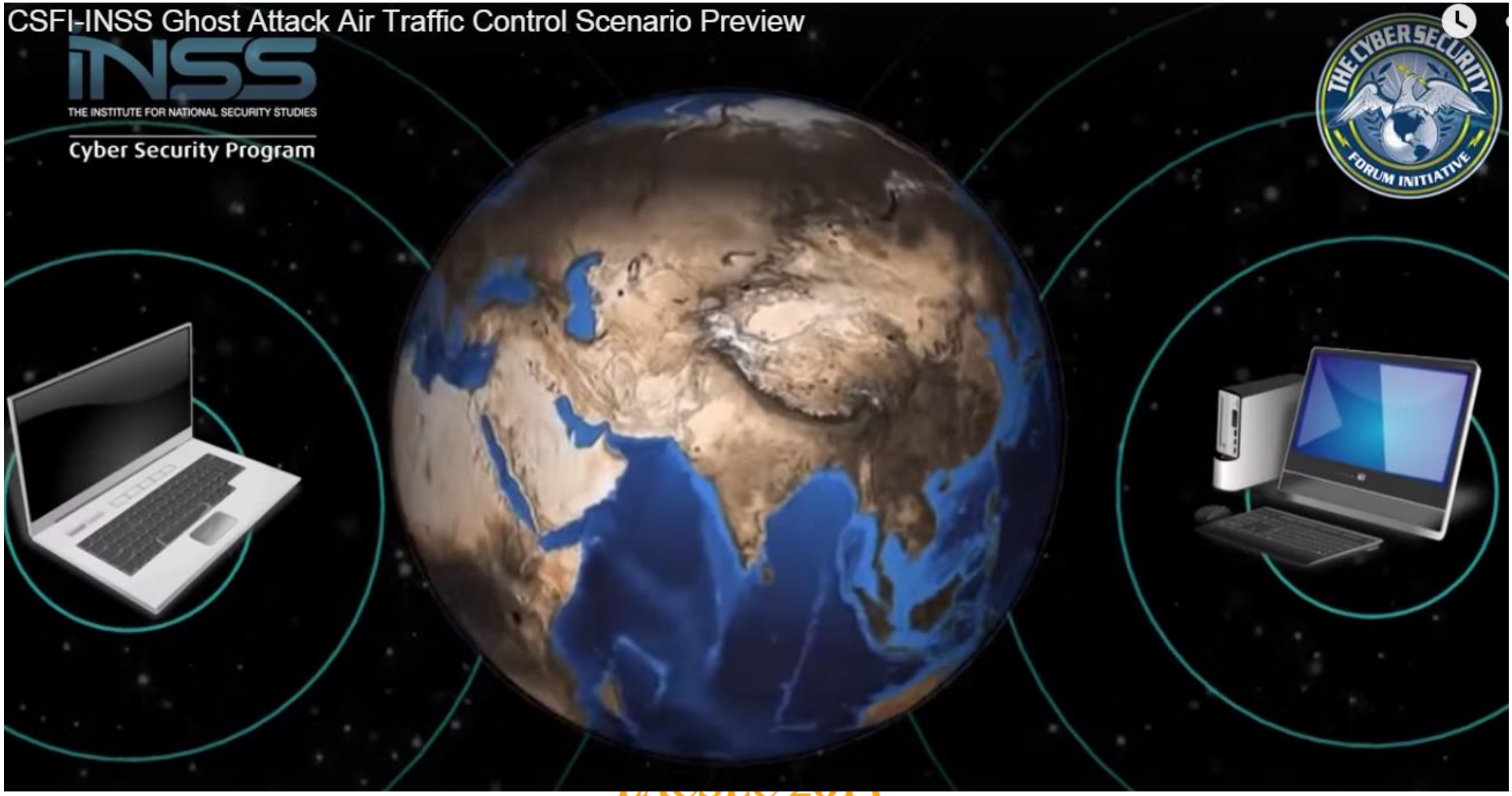
# Ataques y …. más ataques



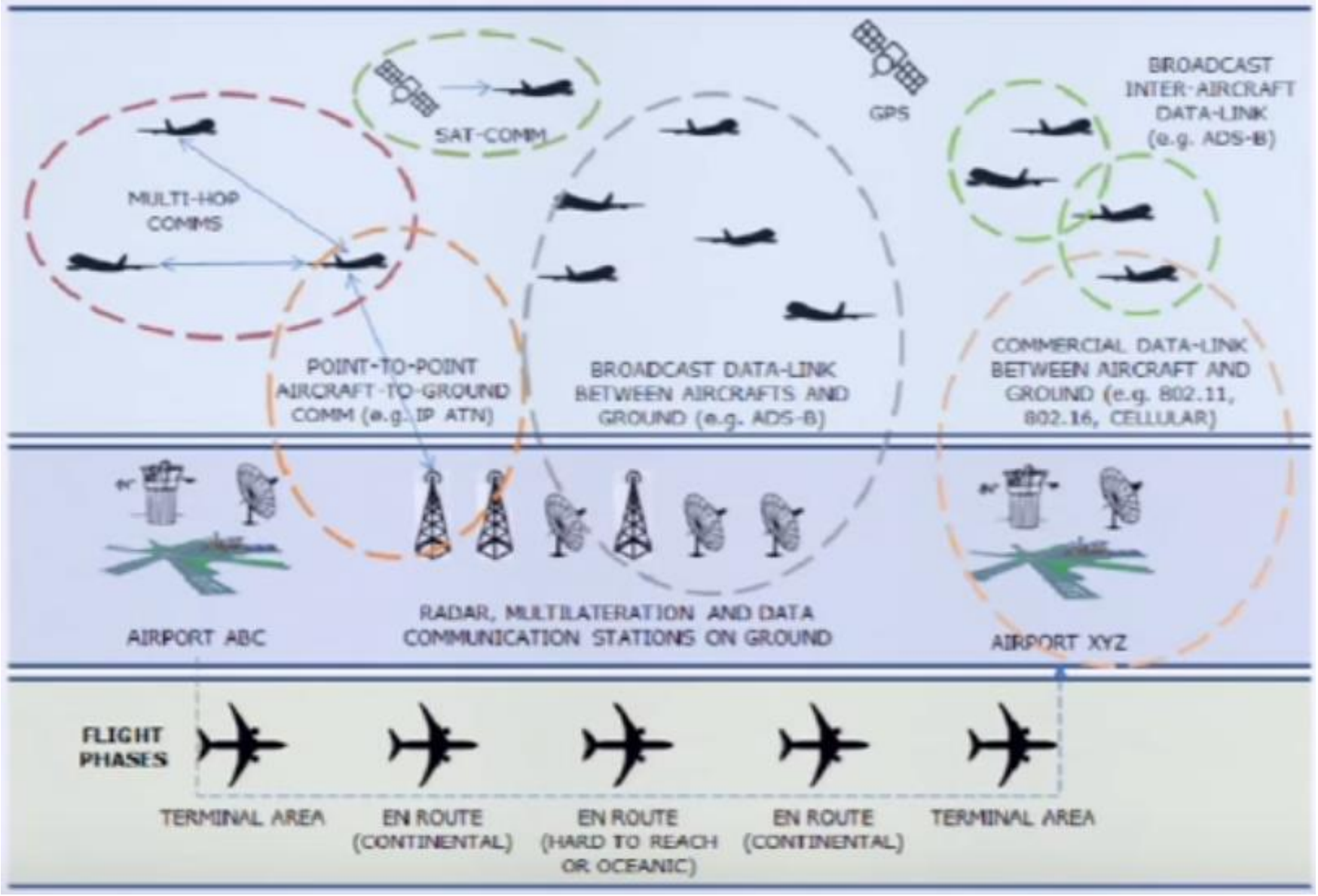
# Ataques y …. más ataques



# Ataques y …. más ataques



# Ataques y …. más ataques

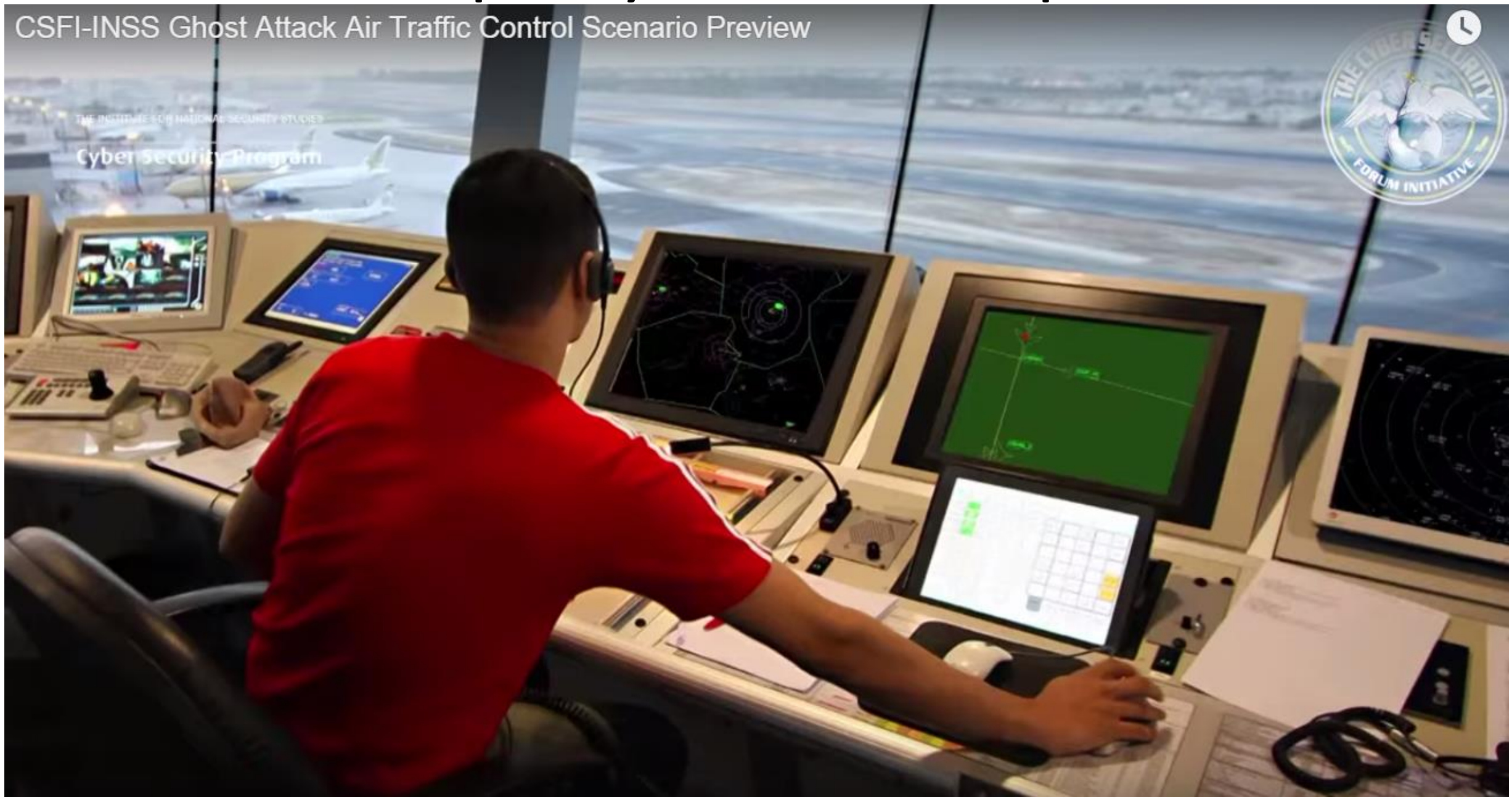



LACSEC 2015

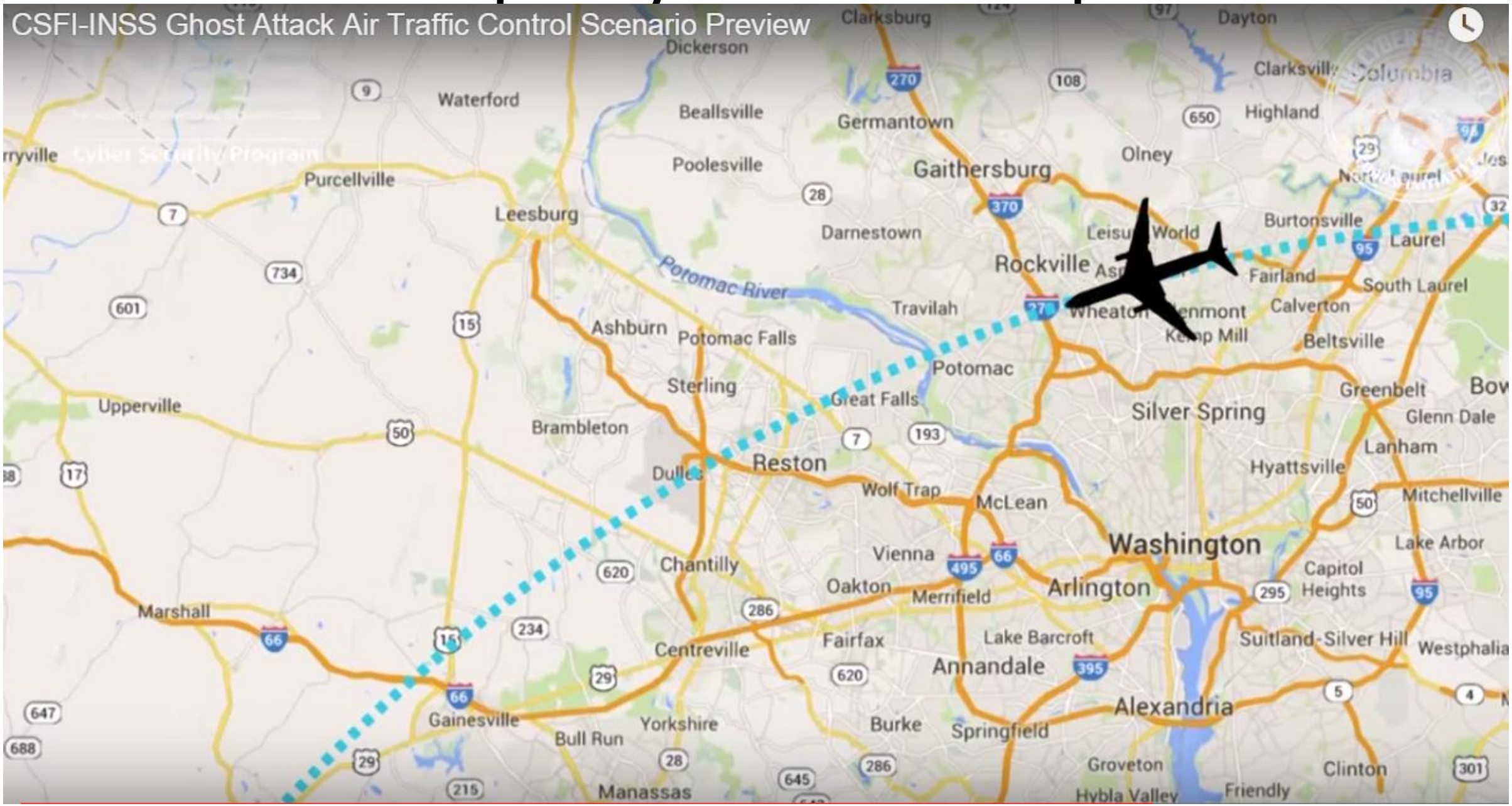
# Ataques y …. más ataques

# Ataques y …. más ataques

# Ataques y …. más ataques



# Ataques y …. más ataques



# Ataques y …. más ataques

# Más hechos !!!


NORSE
ATTACK ORIGINS
# Country
907 United States
574 China
77 Netherlands
70 Russia
67 Austria
51 Hong Kong
48 Thailand
47 Taiwan
44 France
38 Mil/Gov
ATTACK TARGETS
# Country
1871 United States
73 Hong Kong
55 Thailand
39 Netherlands
34 Portugal
32 Turkey
31 Canada
30 Liechtenstein
23 Austria
23 Norway
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
ATTACK TYPES
# Service Port
524 vnc 5900
241 unknown 33435
180 http 80
143 http-alt 8080
126 ssh 22
94 microsoft-ds 445
67 sip 5060
64 telnet 23
© Norse

Son varios ataques...

bueno, más que varios

# Ciberseguridad – Objetivo

- Utilización segura y efectiva de la infraestructura crítica, a través de capacidades nacionales de prevención, identificación, defensa, respuesta y recuperación ante ciberataques.

# Protección de infraestructuras críticas

# Ciberseguridad

- Desafíos y soluciones para gestionar el ambiente multi-amenazas: Cibertaques, desastres naturales, escenarios de guerra, cambio climático, …
- Sector público y privado: centrales hidroeléctricas, Camisea, puertos, bancos, etc.) ¿Cuál es el impacto de esto?
- Probabilidades, amenazas, seguridad, medio ambiente, servicios públicos, etc.
- ¿Cómo es la ciberseguridad ahora?
- Personas – Procesos – Tecnología:
  - Seguridad en 8 capas.
  - ¿Es suficiente?

# Cibercrimen

- Se cometen fácilmente.
- Cualquiera es capaz de hacerlo bajo la percepción de anonimato  e impunidad.
- Posibilidad de obtención de rápidos beneficios/daños.
- Relación costo/beneficio altamente conveniente
- La ubicuidad genera desafíos jurisdiccionales y legales.
- Costo de un ciberataque: € 435.000 (M.O., Hw, Sw, indemnizaciones. No incluye lucro cesante). Fuente: Symantec – *Costo del Cibercrimen*.

# Protección de infraestructuras críticas

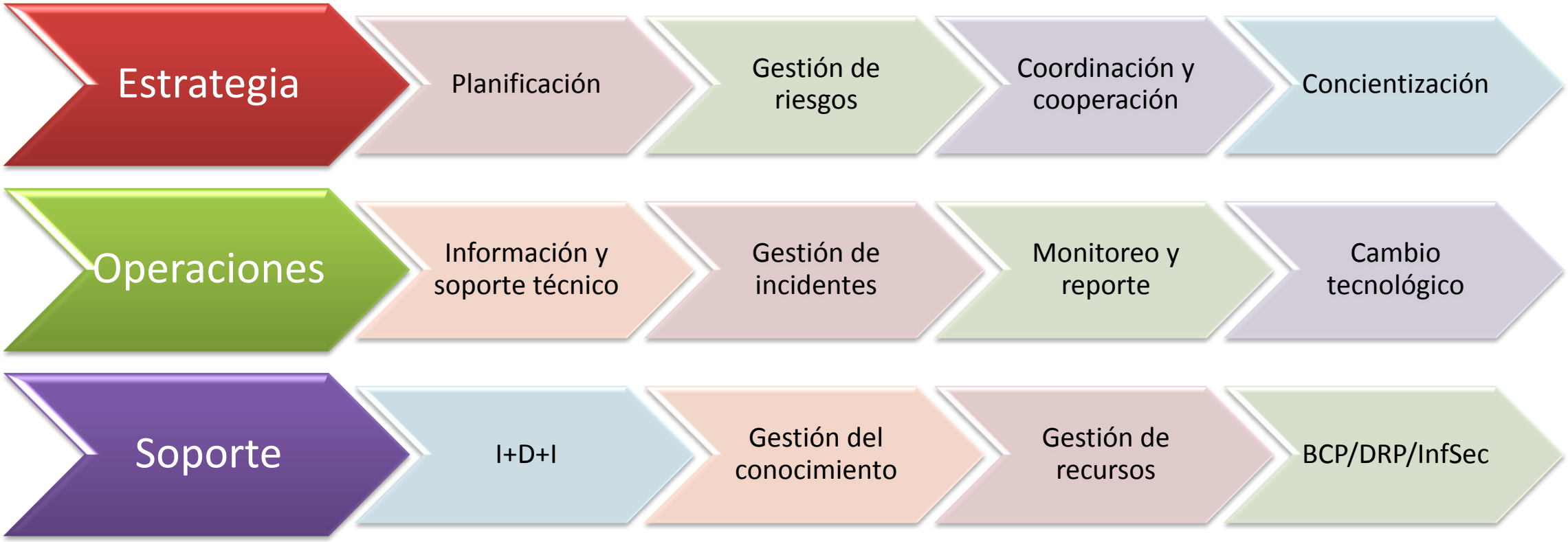
- Las ciberamenazas son una realidad  latente. En cualquier momento, y sin que lo sepamos, podemos ser objetivos de algún tipo de ciberataque capaz de paralizar las operaciones de las IC.
- Los desafíos, más que técnicos, son estratégicos, políticos, sociales y culturales.
- Resiliencia ante ciberataques a la IC.

# Construir ciber-resiliencia

- Respuesta técnica: Backup, redundancia, alta disponibilidad, etc.
- Respuesta estratégica: Política integral de PIC:
  - Aspectos políticos, sociales, económicos, oragnizacionales, respaldados por una autoridad nacional efectiva.
  - Esquemas mixtos y masivos de colaboración, local, nacional, regional y global.
- Complejo????
- Si consideramos el contexto actual de los servicios públicos , el desafío es …..
- Algunos países ni siquiera pueden defender su orden interno,…
- Se requiere dedicar recursos para proteger el ciberespacio y las IC.


American
Megatrends
Keyboard not found
Press F1 to Resume

# Ciberseguridad– Estructuras organizativas



# Ciberseguridad – Hacia la sociedad segura !!

- ¿Cómo estiman que será la actitud ciudadana al respecto? ¿En 5 años?
- ¿Hacemos una apuesta?
- Sociedad cibersegura:
  - Cibercrimen, Ciberterrorismo, Privacidad, Confianza.
- Sociedad resiliente.

# Ciberseguridad - Awareness

# Ciberseguridad – ¿Qué se requiere?

- Definir un marco normativo.
- Definir una estructura organizativa.
- Definir planes estratégicos y operativos.
- Asignar recursos.
- Concientizar !!!
- Medir y mejora continua.

# Estrategias …

- Comando centralizado: Autoridad, coordinación, recursos, …
  - Equipos multidisciplinarios de apoyo.
  - CERTs.
- Inventario de IC (público y privado).
- Estrategias sectoriales.
- Evaluación de riesgos.
- Planes de acción articulados (público, privado y ciudadanía). Son responsabilidades compartidas.
- Monitoreo y reporte: Verificaciones de efectividad: Testing, auditorías, certificaciones, …

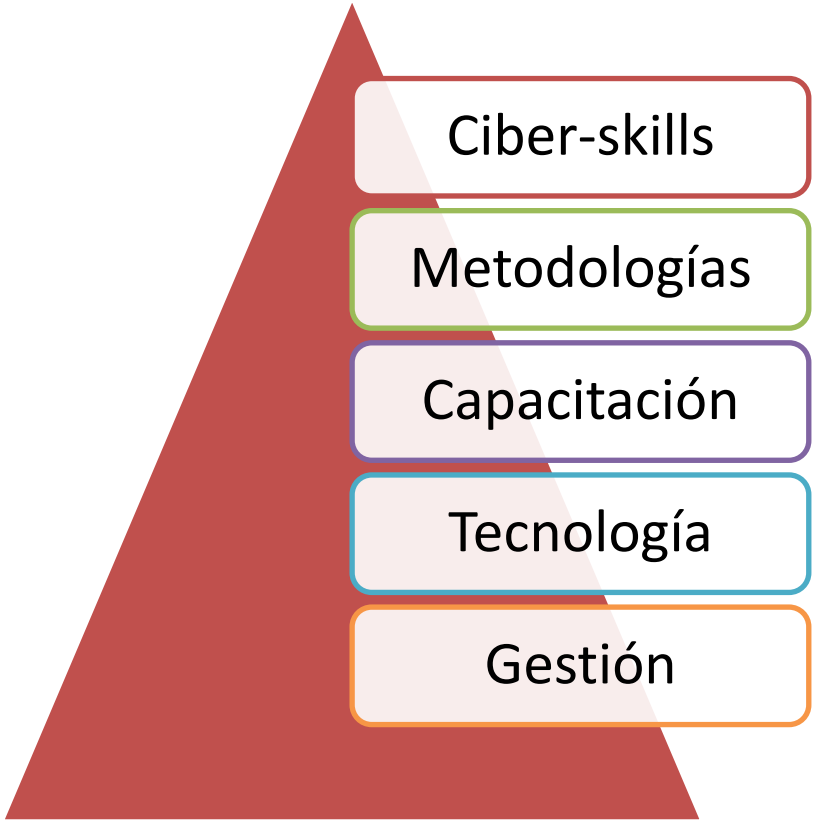

Visto en Doggue.com

# Estrategias de ciberseguridad – Drivers

- Jurisdicción.
- Colaboración.
- Coordinación.
- Autonomía
- Efecto inmediato.
- Marco jurídico.


PEPSI

# Ciberseguridad – Competencias



GO

# Ciberseguridad – Necesidades

- Pocos expertos
- Amenazas multidireccionales.
- Riesgos cambiantes.
- Privacidad.

# Ciberseguridad – Nivel Personal

# Ciberseguridad – Nivel organizacional

# Ciberseguridad – Nivel global

- Ciber-terrorismo.
- Cooperación internacional.

# Ciberseguridad – Nivel cultural

- Es un estilo de vida.
- Todos debemos evangelizar en forma multidireccional.

# Aprendamos !!

- La tecnología nos desborda, a nivel personal y a nivel organizacional.
- Al parecer nuestra actitud al respecto es ...
- Realmente pensamos que es un problema de alguien más, y que ese alguien hará algo, y no sabemos qué !!!
- ¿Entonces, el tema es cultural?
- ¿A qué nivel: personal, organizacional, nacional, regional, global?
- Cultivar la conciencia alrededor del riesgo en general, y a los riesgos tecnológicos en forma específica, es ….
- Y bueno. ¿Qué estamos haciendo al respecto?

# Aprendamos a aprender !!

- Reconozcamos el impacto del cibercrimen, en cualquiera de sus formas.
- Las organizaciones cibercriminales son organizadas, especializadas y hasta sofisticadas, por tanto, hay que analizarlas y enfrentarlas como tales (organizaciones con objetivos estratégicos, rentables, con disponibilidad de recursos, etc.)
- En este momento no hay buenas noticias, porque, hagamos lo que hagamos en PIC, …

# Aprendamos a aprender!!

- El cibercrimen opera en nuestras comunidades, por tanto, están más integrados con nosotros de lo que creemos. La información está disponible para cualquiera…
- Reconozcamos que con nuestro actual enfoque cultural somos cómplices de su acción y crecimiento, y garantizamos su impunidad.
- Se aprovechan de nuestro desconocimiento !!!
- Más aún, saben que no nos involucraremos !!!

# ¿Entendemos de qué se trata todo esto?

- ¿Estamos seguros de haber entendido el significado de la ciberseguridad y sus desafíos?
- ¿Estamos conscientes del nivel de compromiso que requiere de todos nosotros?
- ¿De qué niveles estamos hablando: Individual, organizacional, institucional, nacional, global?

# Desarrollo de estrategias de ciberseguridad y protección de infraestructuras críticas

Ing. Juan Dávila, MBA, CRISC, CISM, CISA, ISO 27001 LA, ISO 22301 LA, Cobit 5F Trainer
jdavilara@gmail.com

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

LACSEC 2015