

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

EL DILEMA DE INTERPRETACIÓN EN EL CIBERESPACIO



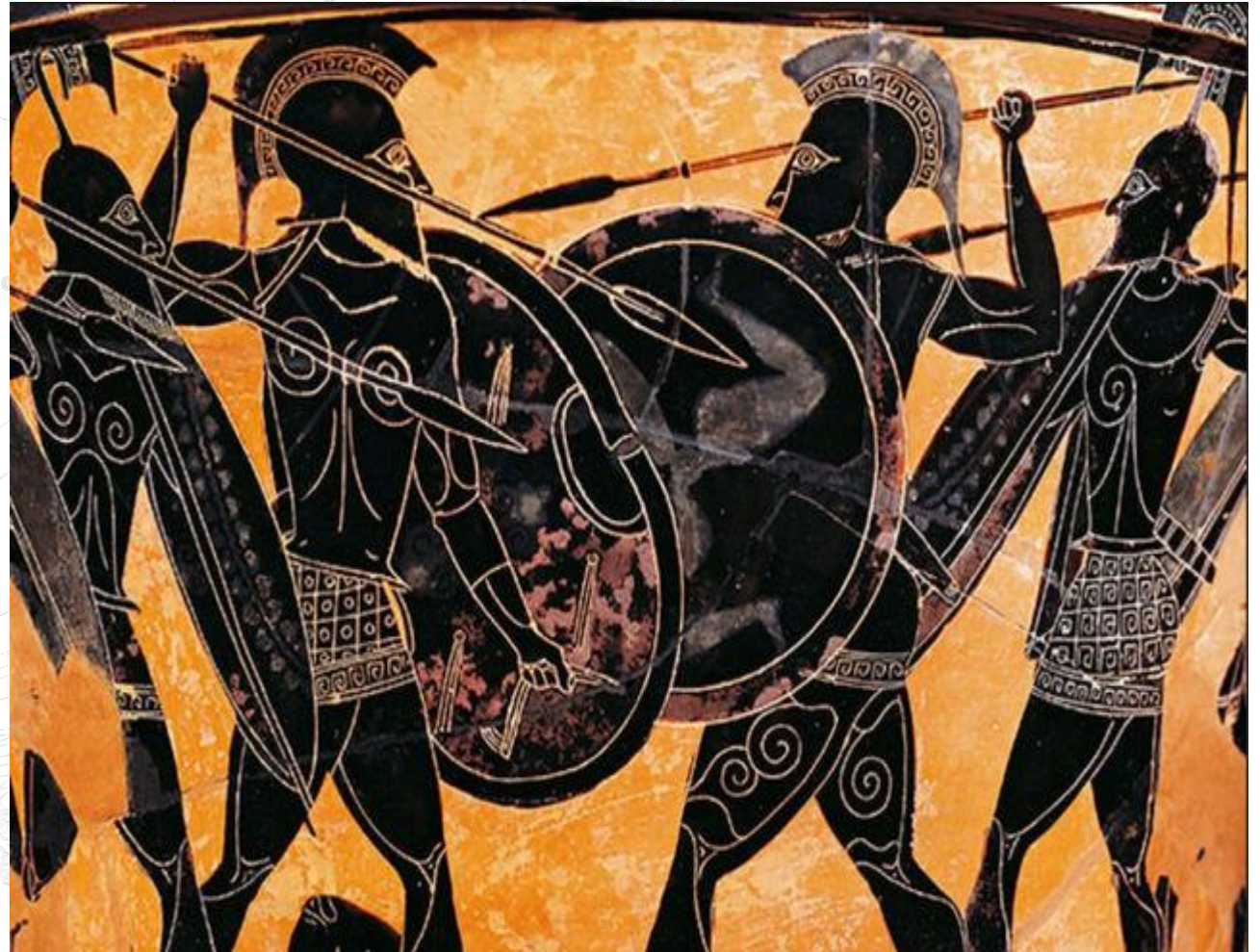
- Manuel R. Torres Soriano
- Universidad Pablo de Olavide de Sevilla
- mrtorsor@upo.es

Índice

1. El dilema de seguridad
2. Testeo a través del ciberespacio
3. Requisitos operacionales
4. Sesgos cognitivos
5. Cómo atenuar el dilema de interpretación

El dilema de seguridad

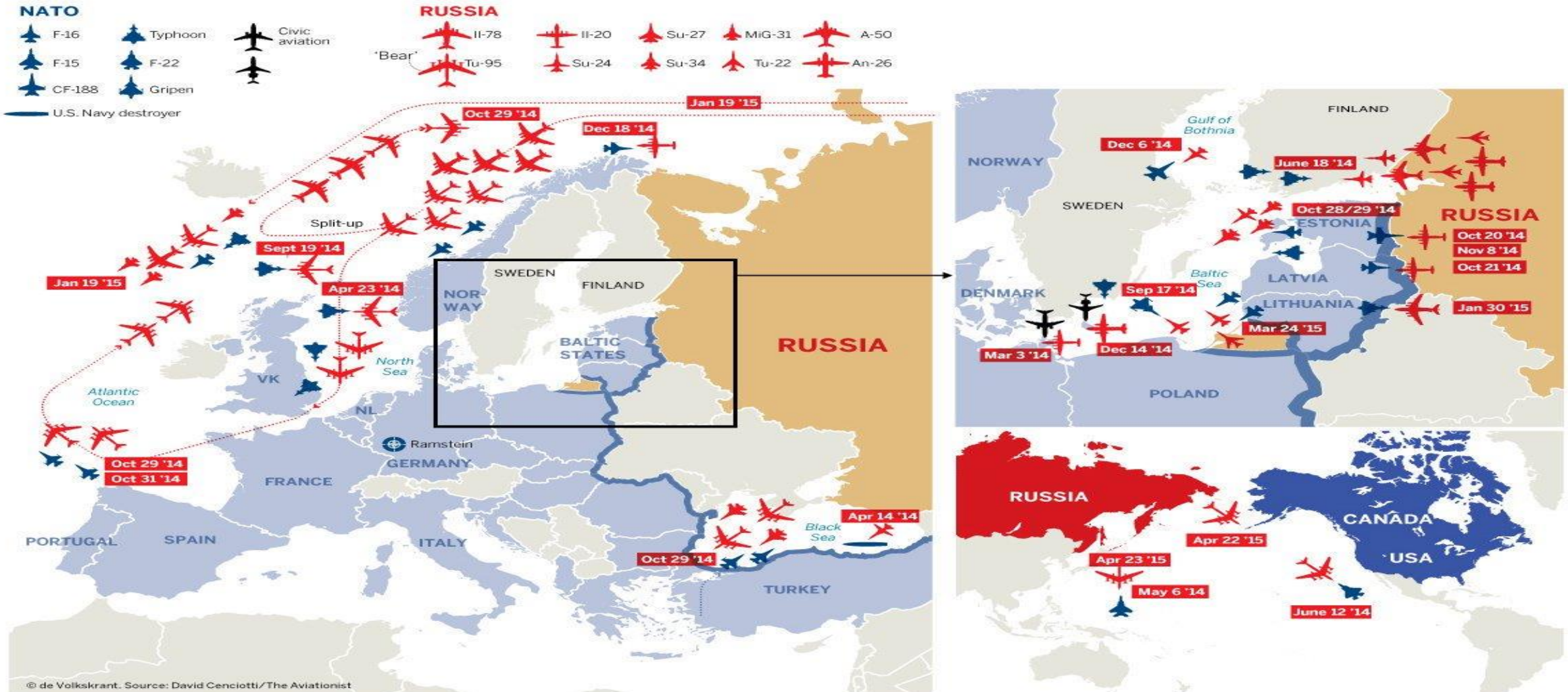
- “La causa principal y más verdadera, fue el temor que los lacedemonios tuvieron de los atenienses, viéndoles tan poderosos y tan pujantes en tan breve tiempo”
- TUCIDIDES , *La guerra del Peloponeso*, (431–404 a. C.)



“La trampa de Tucídides”

	Period		Ruling Power	Rising Power		Result
1	First half of 16th century		France	Hapsburgs		War
2	16th–17th centuries		Hapsburgs	Ottoman Empire		War
3	17th century		Hapsburgs	Sweden		War
4	17th century		Dutch Republic	England		War
5	Late 17th–early 18th centuries		France	Great Britain		War
6	Late 18th–early 19th centuries		United Kingdom	France		War
7	Mid-19th century		United Kingdom, France	Russia		War
8	19th century		France	Germany		War
9	Late 19th–early 20th centuries		Russia, China	Japan		War
10	Early 20th century		United Kingdom	United States		No war
11	Early 20th century		Russia, U.K., France	Germany		War
12	Mid-20th century		Soviet Union, U.K., France	Germany		War
13	Mid-20th century		United States	Japan		War
14	1970s–1980s		Soviet Union	Japan		No war
15	1940s–1980s		United States	Soviet Union		No war
16	1990s–present		United Kingdom, France	Germany		No war

Russian airforce tests NATO reaction time



Testeo a través del ciberespacio



Elimina el
factor
distancia

Multiplicación
de objetivos

Reducido
coste político

The 'Wannacry' ransomware attack

The attack has hit more than 200,000 victims in at least 150 countries, says Europol



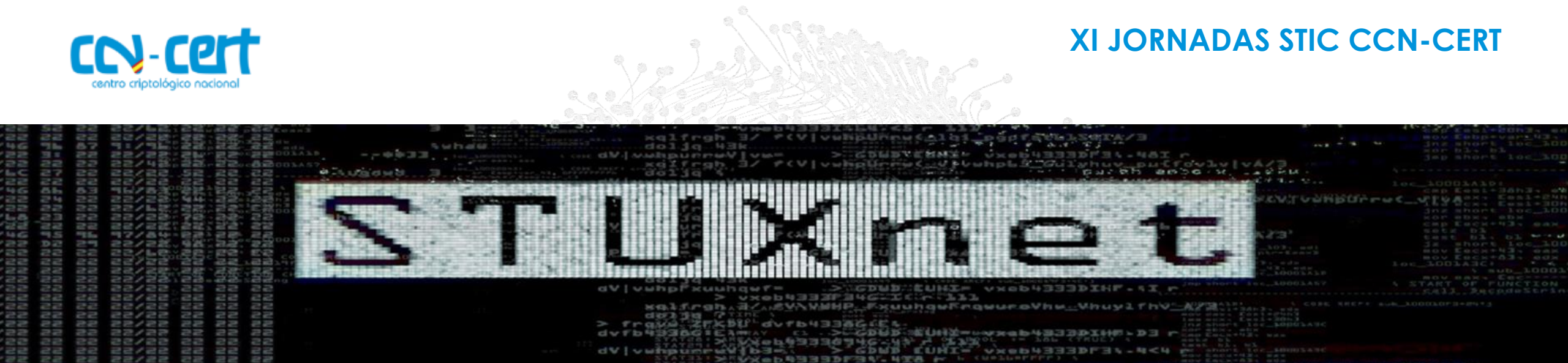
The 'Wannacry' ransomware attack

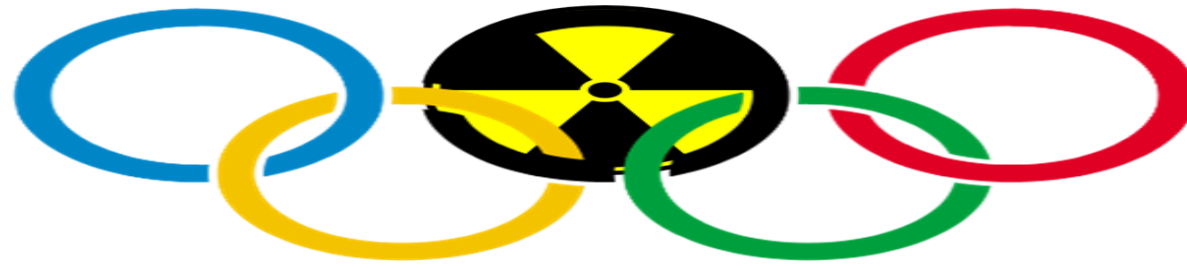
The attack has hit more than 200,000 victims in at least 150 countries, says Europol



Requisitos operacionales

- Acción prolongada y persistente
- Enfoque indiscriminado
- Necesidad de recurrir a herramientas automatizadas





Natanz 2010



Sesgos cognitivos: inclinación por los peores escenarios



Sesgos cognitivos: La niebla de la guerra

Sesgos cognitivos: atribuir una unicidad inexistente



< Cozy Bear >



< Fancy Bear >



Roles of Russia's intelligence community

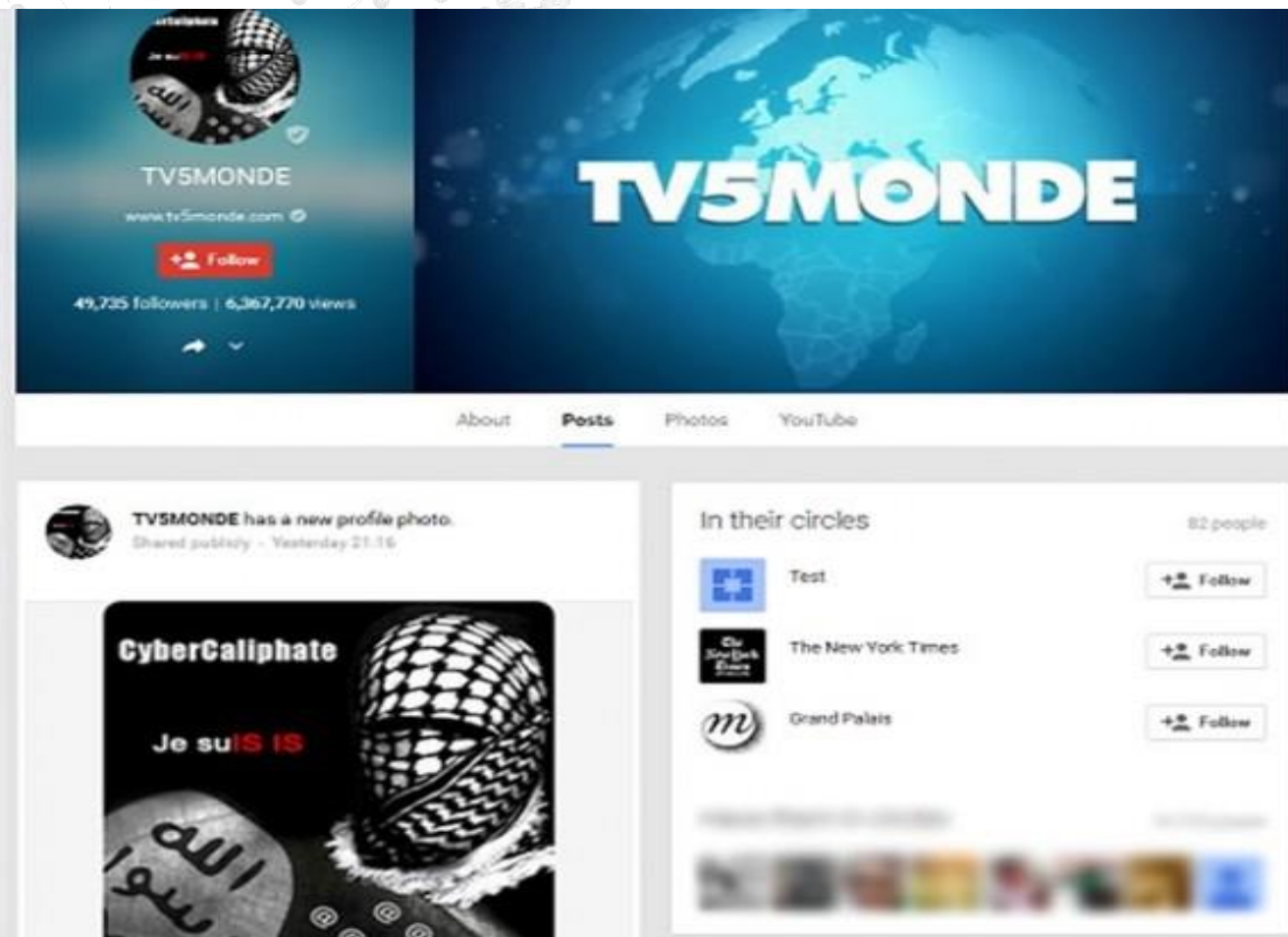
	Political intelligence	Economic intelligence	Military intelligence	Active measures	Counter-intelligence	Political security	Law enforcement
Federal Security Service (FSB)	●			●	●	●	●
Foreign Intelligence Service (SVR)	●	●	●	●	●	●	
Main Intelligence Directorate (GRU)	●	●		●	●		
Federal Protection Service (FSO)					●	●	●
Interior Ministry (MVD)					●	●	●
Prosecutor General's Office (GP)						●	●
Investigatory Committee (SK)						●	●
The Federal Anti-Drug Service (FSKN)		●					●
National Anti-Terrorism Committee (NAK)					●	●	●
Soviet KGB	●	●	●	●	●	●	●

- Main role
- Subsidiary role

Sesgos cognitivos: los límites de la medición



Cómo atenuar el dilema de interpretación: ciber-inteligencia



Cómo atenuar el dilema de interpretación: ciber-inteligencia



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

