High level Conference on the

EU Cybersecurity Strategy

Brussels, 28th February 2014

ENHANCING NETWORK AND INFORMATION SECURITY IN EUROPE: AN URGENT NEED FOR NOVEL APPROACHES TO SHARING INFORMATION

Dr. Jorge López Hernández-Ardieta
HEAD OF CYBERSECURITY RESEARCH GROUP

indra

SOME FACTS

Interdependence of networks and systems.

Increasing complexity of technology.

Knowledge dispersed amongst different and heterogeneous entities.

The authority to decide and act is split across different domains.

Evolution of threat landscape (distributed attacks, targeted complex cyber weapons, nation-sponsored actors).

No single entity can protect itself effectively without leveraging various collaboration instruments with different partner and allies.

This is especially relevant in national security and the fight against cyber crime and cyber terrorism, where multi-national/multi-organisational approaches are mandatory.

Information sharing becomes a fundamental aspect to meet an adequate level of NIS

THE TIME DIMENSION

OK, WE SHARE, BUT…

Cyber attacks spread and may cause cascade effects in a "computer-time" fashion

We shall not react to cyber threats in "human-time"

We have to face the threats considering the time dimension, especially for tactical/operational aspects (strategic level and legal enforcement shall be treated differently)

THE TRUST DIMENSION

BINARY TRUST BOUNDARIES are no longer acceptable.

We cannot foresee who will possess the **VALUABLE** information for which incident.

We cannot guarantee the **TRUSTWORTHINESS** of the information at operational level.

We have to accept **UNCERTAINTY** and **NON-ABSOLUTE TRUST** as inherent factors of information sharing.

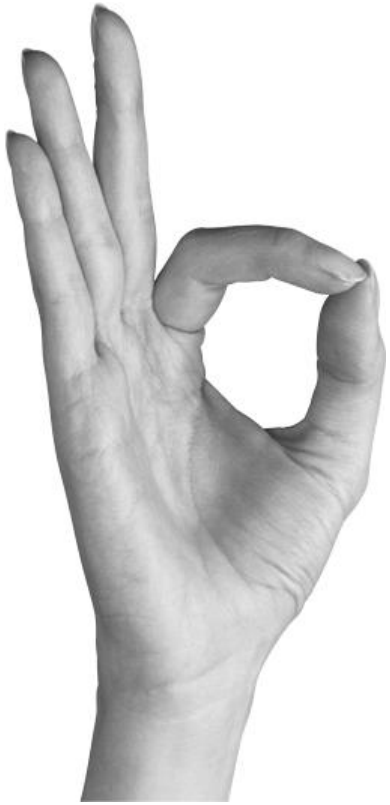
TOWARDS AUTOMATED REAL-TIME INFORMATION SHARING

We need to move from human-driven to automated real time actionable cyber security information sharing

Standards that focus on automating the 'how' exist, but we need advances towards the 'what', 'with whom', and the 'repercussions of' sharing

Balance Need-to-Share vs. Risk-of-Sharing

PRIVATELY HELD CYBERSECURITY OPERATIONS CENTRES AND THEIR ROLE IN INFORMATION SHARING



Privately held CSOCs (PH-CSOC) protect a significant portion of the European productive fabric.

PH-CSOCs, as a strategic asset for Europe, shall be given explicit relevance by the European Commission.

Cooperation mechanisms amongst PH-CSOCs, ENISA, CERTs, NIS Authorities, LEAs, CERTs, and others shall be encouraged by the European Commission and National Bodies.

OTHER IDEAS TO DISCUSS...

Voluntary vs. Mandated sharing

Economic exploitation of information and the repercussions on sharing behaviours

Data protection and privacy

Dr. Jorge Lopez Hernandez-Ardieta

HEAD OF CYBERSECURITY RESEARCH GROUP

jlhardieta@indra.es

Avda. de Bruselas 35
28108 Alcobendas,
Madrid Spain
T +34 91 480 60 00
F +34 91 480 60 31
www.indracompany.com