DEPARTAMENTO DE COMUNICACIONES

RESUMEN DE TESIS DOCTORAL – JAVIER HINGANT GÓMEZ
Doctorado en Telecomunicación

ARQUITECTURA DE CYBER SITUATIONAL AWARENESS PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

La seguridad en el ciberespacio supone hoy en día un reto fundamental para cualquier organización ante el incesante aumento de ciberataques en todo el mundo. En una realidad tecnológica como la actual, en la que los dominios físico y lógico son cada vez más interdependientes, esta tarea es todavía más imprescindible pues las acciones en cualquiera de estos ámbitos pueden acarrear consecuencias devastadoras en ambos. Esto es si cabe más importante en el caso de infraestructuras críticas (IC), pues de su correcto funcionamiento depende el bienestar de toda una nación y sus ciudadanos.

Se hacen por tanto necesarias nuevas soluciones que permitan afrontar de manera eficiente la defensa de toda clase de IC en este escenario híbrido, en el que las herramientas tradicionales de seguridad (*firewall*, IDS/IPS e incluso sistemas SIEM) resultan por sí solas insuficientes ante ataques a gran escala y donde alternativas más completas como los sistemas SCADA más recientes siguen orientadas a sectores muy específicos.

La presente tesis doctoral plantea un enfoque innovador de *Situational Awareness* (SA) para la adecuada protección de IC en el contexto ciber-físico. En concreto, se propone una arquitectura genérica de SA híbrida que proporcione, mediante técnicas avanzadas de representación, la *Common Operational Picture* conjunta de las dimensiones física y ciber en un espacio único de visualización con el fin de facilitar la toma de decisiones al operador correspondiente.

La arquitectura definida ha sido aplicada en dos soluciones distintas de *Cyber Command & Control* para la protección de IC: el sistema GESTPIC para la visualización avanzada de la SA ciber-física, y HYBINT como novedosa herramienta para la integración y el análisis de información de inteligencia.

El modelo presentado en esta investigación ha sido validado en entornos de uso tanto simulados como reales, suscitando el interés de potenciales usuarios finales y confirmándose como propuesta pionera en su campo en los foros especializados en los que ha participado.