Necesidad de una **estrategia nacional** de ciberseguridad

EN el ciberespacio, donde no hay barreras de distancia y tiempo y las fronteras nacionales están diluidas, los riesgos y amenazas se acrecientan día a día. La rentabilidad económica, política o de otro tipo que se obtiene; la facilidad y el bajo coste en el empleo de las herramientas utilizadas, así como el bajo riesgo para el atacante que lo puede hacer de forma anónima y desde cualquier lugar de mundo, han posibilitado esta situación. Incluso se observa que los posibles atacantes (estados, grupos extremistas ideológicos o políticos, crimen organizado...) utilizan cada vez más técnicas depuradas y que existe una mayor interrelación entre los ciberdelincuentes de distintos países, algunos de los cuales suelen contratar capacidades técnicas de ataque disponibles en el mercado negro ofertado por hackers y organizaciones criminales si no disponen de la capacidad necesaria.

Sus motivaciones pueden ser diferentes (robo de información, robo de identidades, fraude telemático, espionaje industrial, hacking político, terrorismo...), pero todas ellas, aunque en distinto grado, constituyen una amenaza para la seguridad nacional y exigen de una repuesta coordinada, con unas líneas de acción definidas y unas estructuras de decisión claras a las que se dote del presupuesto económico necesario.

CCN-CERT
Javier Candau Romero
Jefe de Política y Servicios
Centro Criptologico Nacional (CNN)

> **"Las motivaciones de los atacantes pueden ser diferentes pero todas constituyen una amenaza para la seguridad nacional"**

Así lo han entendido muchos países que han desarrollado o están desarrollando estrategias nacionales de ciberdefensa con las que persiguen conseguir un ciberespacio más seguro mediante el intercambio de información de alertas, vulnerabilidades y amenazas; la mejora de las capacidades de contrainteligencia, la seguridad de sus productos y tecnologías, y la concienciación y formación de sus ciudadanos y servidores públicos en seguridad de sistemas TIC.

Estados Unidos, Gran Bretaña, Francia, Canadá son algunas de las naciones que han llevado a cabo este tipo de iniciativas y cuyos gobiernos han realizado un incremento en sus dotaciones presupuestarias como reflejo de la importancia concedida a estas amenazas.

En términos generales, estos países han apostado por una aproximación global al problema tratando de forma conjunta todos los niveles sobre los que se debe actuar en ciberdefensa: gobiernos centrales, regionales y locales; infraestructuras críticas, Fuerzas y Cuerpos de Seguridad del Estado y ciudadanos.

De igual modo, se decantan por la centralización de las responsabilidades y uno o dos organismos que coordinan las acciones, potenciando las capacidades de monitorización y aler-