Ciberterrorismo, un reto para los próximos años

Daniel Acuña Calviño

Director de Defensa y Seguridad

ISDEFE

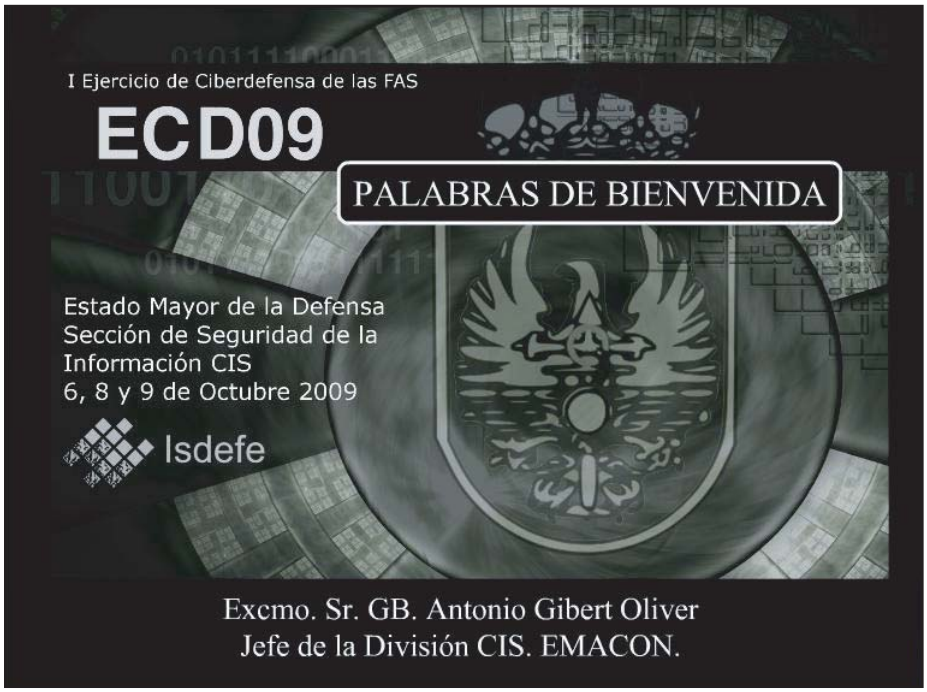
Durante los últimos años, hemos sido testigos de excepción de una gran revolución tecnológica, que ha permitido integrar los sistemas de información en el día a día de cada uno de nosotros y, en especial, en los propios sistemas de producción de las sociedades modernas. Esto ha traído consigo ventajas por todos conocidas, pero también ha motivado la aparición de nuevos problemas, originados por delincuentes de todo tipo que han sabido aprovechar las enormes ventajas que la aparición y el asentamiento del ciberespacio han permitido.

Las características que hacen diferente estos nuevos problemas frente a los ya tradicionales son las propias del ciberespacio: eliminación de fronteras, anonimato, dificultad en la trazabilidad, falta de regulación internacional, etc. Debido a estas carencias, existe una percepción generalizada de que las nuevas amenazas van siempre ligeramente por delante de las medidas defensivas que se intentan poner en marcha.

El ciberterrorismo es un caso concreto de delincuencia que ha encontrado en el ciberespacio un medio idóneo para desarrollar sus actividades. Supone la convergencia del terrorismo tradicional y el ciberespacio. Se puede definir como el uso de medios de tecnologías de la información, comunicación, informática, o similar, con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno. Sus fines suelen ser económicos, políticos o religiosos.

Los ciberterroristas hacen uso de las TIC:

- **Como instrumento:** Al igual que el resto de la sociedad, aprovechan las posibilidades que ofrecen las TIC en su propio beneficio, mediante el uso del correo electrónico, chats, cifrado de comunicaciones, ...
- **Como medio:** El empleo de las TIC favorece objetivos de guerra psicológica, desinformación, difu-



sión de amenazas, reclutamiento, canales de financiación, ...

- **Como objetivo:** Internet como objetivo es la razón última del ciberterrorismo. Los objetivos propios del terrorismo a través de Internet son los mismos que ya lo son en la actualidad, telecomunicaciones, infraestructuras críticas, economía, empresas, servicios públicos, ...

Ante la nueva amenaza, la reacción tanto nacional como internacional no se ha hecho esperar. Cabe destacar la proliferación, a nivel nacional, de equipos de respuesta rápida, CERTs, CSIRTs, etc. A nivel internacional, impulsados por OTAN o UE entre otros, son varios los organismos, centros, agencias y foros que están empezando a tratar el tema en profundidad.

Desde Isdefe estamos comprometidos con este problema y son varios los proyectos directamente relacionados con la ciberdefensa y el ciberterrorismo en los que estamos trabajando. Veamos algunos de ellos:

- **Informe de Seguridad Nacional y Ciberdefensa:** Se ha realizado un informe, que pretendemos esté actualizado de forma continua, para reflejar la situación actual de la Seguridad Nacional desde la vertiente TIC como medio de protección y ataque. Se recogen en él, el marco regulador, las responsabilidades, los planes, las estrategias de financiación, etc.; para una serie de países y asociaciones.

El Informe también recoge información pública relevante sobre determinados países que han puesto en marcha iniciativas para crear ciberunidades militares, o una colección de noticias en relación con la ciberseguridad y las infraestructuras críticas.

- **NATO Cooperative Cyber Defense Centre of Excellence (CCD CoE):** La OTAN cuenta con 12 centros de investigación acreditados como Centros de Excelencia, cuyo objetivo es aportar conocimiento en materias muy específicas. La misión del CCD CoE es la de mejorar la capacidad de ciberdefensa de la OTAN y sus naciones. Actualmente son siete las naciones que han firmado el acuerdo para participar oficialmente en el Centro (aunque existen representantes de algunas más, como p. e. EEUU, cooperando en el mismo), teniendo España una participación relevante, tanto en el plano militar (con un Teniente Coronel del Estado Mayor de la Defensa, que dirige la rama de formación y doctrina), como en el civil (con un ingeniero de Isdefe, que trabaja como experto-científico en proyectos de I+D).

- **Primer Ejercicio de Ciberdefensa de las Fuerzas Armadas:** Organizado por el Estado Mayor de la Defensa y patrocinado por Isdefe. En él participaron de forma remota veinte equipos, representando prácticamente a todas las unidades con un peso significativo dentro del ámbito CIS de las FFAA. Dados los resultados de este primer ejercicio, se espera que se repita de forma anual.

Si bien es cierto que son muy numerosas las medidas que se han tomado hasta ahora para combatir el ciberterrorismo, no debemos olvidar que dadas las características del escenario en cuestión, una defensa eficaz no puede limitarse a acciones individuales. La estrategia a seguir deberá ser coordinada a nivel internacional, teniendo como objetivo asegurar la concienciación, mejorar el nivel de seguridad de los sistemas y abarcar aspectos tanto técnicos como legislativos.

El reto, por tanto, consistirá en establecer una mejor cooperación en materia de seguridad, que permita un óptimo manejo de situaciones de crisis, así como el desarrollo de tecnologías avanzadas que mejoren la lucha contra el terrorismo.