revista pensamiento penal

Falsa bandera digital

Por Gustavo Sain

@grsain

En 1983 se estrenó en los cines de los Estados Unidos la película “Wargames” -Juegos de guerra- del director John Bardham. El argumento se basa en la historia de un adolescente que logra penetrar la red informática de defensa nuclear del Departamento de Defensa de ese país en plena Guerra Fría, donde los altos mandos militares deciden atacar militarmente a la Unión Soviética. El desenlace sucede cuando el mismo hacker, con sus habilidades técnicas, se encarga de subsanar su error y salva al mundo de una inminente Tercera Guerra Mundial. Lejos de Hollywood, a fines de noviembre de 2014, un ataque de un grupo hacker dañó y dejó inactivo el sistema informático de la multinacional japonesa Sony en los Estados Unidos. Los 6.000 empleados de la filial de cine y televisión de ese país se encontraron una mañana en forma repentina imposibilitados de acceder a su correo electrónico, líneas telefónicas y a los archivos informáticos de la red de oficina. Una calavera roja con la leyenda GOP -Guardians of Peace, Guardianes de la Paz- se atribuía el atentado desde las pantallas de sus computadoras.

La empresa informó que el ciberataque extrajo información personal de los 47.000 empleados de la filial, -números de seguro social, tarjetas de crédito y direcciones personales- además de mails privados de los ejecutivos de la firma y material audiovisual de la firma sin estrenar, como películas y series. Entre las producciones fílmicas sustraídas se encontraba la película “The Interview” -La entrevista- cuyo argumento versa de una operación de dos agentes encubiertos de la CIA que viajan a Corea del Norte como periodistas para asesinar a su presidente, Kim Jong Un. Pese a

que Pyongyang calificó el film como una clara provocación y “un acto de guerra” un tiempo antes del ciberataque, el FBI señaló al país asiático como responsable del atentado, atribuyéndole un matiz de tipo “terrorista”. Días después, el presidente Barack Obama firmó una orden ejecutiva aplicando sanciones económicas contra la República Popular de Corea, entre las que figuran el bloqueo de bienes e intereses de propiedad de funcionarios u organismos controlados por el gobierno de Corea. Bajo promesa de una respuesta de “iguales proporciones” al ataque, el 20 de diciembre pasado los proveedores de acceso a Internet de todo el país comunista dejaron de funcionar durante 9 horas.

Este nuevo tipo de conflictividad bélica se denomina “ciberguerra” o guerra cibernética, un área surgida justamente en Estados Unidos a principios de la década de 1990 tras la finalización de la Guerra Fría. Ésta utiliza herramientas informáticas como armas, no sólo para el espionaje de redes enemigas sino también para afectar o dañar sus redes y sistemas mediante ataques de hacking, programas espías y fallos de seguridad intencionales en aplicaciones, entre otras técnicas. Se caracteriza por el más alto secretismo y el manejo de altos fondos presupuestarios para la protección de “infraestructuras críticas de información” de un país. A diferencia de la guerra convencional, el agresor de un ciberataque intenta ocultad su identidad, favorecido por las posibilidades de anonimato que ofrece Internet y la perpetración de ataques en lugares públicos como, cibers, cafés, universidades y bibliotecas, entre otros. La identificación real de un Estado agresor en la virtualidad conlleva a la posibilidad de respuesta errónea de un Estado agredido si la responsabilidad es atribuida en forma equívoca, en tanto que puede derivar en una ofensiva militar por medio de métodos convencionales de guerra.

En la actualidad, cualquier país puede forzar un conflicto bélico con otra nación plantando pruebas falsas de un supuesto ataque informático y así justificar una invasión armada territorial en nombre de la seguridad nacional. Esto es lo que habitualmente se conoce en el mundo de las agencias de seguridad como "operaciones de falsa bandera". Con la apertura pública de Internet por parte de la Administración norteamericana a mediados de la década de 1990 y su expansión global, la red ofrece sumadas posibilidades para este tipo de procedimientos. Un agresor puede ocultar fácilmente la dirección de la computadora de origen de un ataque mediante el uso de determinadas aplicaciones, tanto así como falsearla y hacer creer al destinatario del mismo una falsa procedencia del mismo. Asimismo, las pruebas presentadas sobre un ataque pueden ser tan endebles como la misma acusación de que un Estado se encuentra detrás de cualquier ofensiva digital. ¿Qué es lo que afirma que detrás de cualquier ataque hacker mediante software malicioso existe una acción deliberada e intencional de parte de un Estado para afectar infraestructuras de seguridad de otra nación?

Tras las reiteradas negativas del gobierno coreano sobre la responsabilidad del ciberataque, algunos expertos cuestionaron el informe del FBI sobre la supuesta implicación del país asiático en el atentado. La empresa estadounidense de seguridad informática Norse Corp publicó un informe que afirma que el ataque a Sony Pictures fue perpetrado por un ex empleado de la firma con ayuda de hackers. John McAfee, dueño de una prestigiosa empresa seguridad informática declaró que tuvo contacto con el grupo que atacó la intranet de la empresa y que tuvo un fin "libertario", acorde al espíritu de algunos hackers activistas que se manifiestan en contra de las corporaciones discográficas y cinematográficas. Por último, el diario "New York Times" publicó una entrevista a varios expertos en seguridad que evidenciaron que los ataques provinieron de computadoras de Polonia, Bolivia, Italia, Tailandia,

Singapur Chipre, y el propio Estados Unidos, eximiendo a Corea del Norte de cualquier responsabilidad.