Instituto de Relaciones Internacionales

Departamento de Seguridad Internacional y Defensa

seguridadydefensa@iri.edu.ar

Estudios

Ciber amenazas: ¿espionaje económico o nuevos actos de agresión?

Sebastián Do Rosario 1

En 2009 una planta iraní de enriquecimiento de uranio fue atacada por un virus informático denominado Stuxnet, provocando que las centrífugas de la planta de Natanz comenzaran a girar erráticamente. Según se conoció por un artículo del periódico norteamericano New York Times2, el virus habría sido desarrollado conjuntamente entre Israel y Estados Unidos como un arma de ciberguerra diseñada específicamente para el ataque de determinadas instalaciones nucleares iraníes.

A fines de 2011 se conoció que las fuerzas armadas iraníes pudieron violar el sistema de seguridad informático de un avión no tripulado3 (dron) norteamericano que sobrevolaba el espacio aéreo iraní, que supuestamente estaba en una misión de patrullaje de espacio aéreo afgano. Pese a las presiones de la diplomacia de Estados Unidos para que Irán regrese el artefacto, varios portavoces reconocieron que el gobierno no lo devolvería y que incluso comenzaría a extraer toda la información contenida en él y procedería a analizarlo para copiar su tecnología.

Los casos mencionados son sólo unos pocos entre millones que se suceden en el mundo. Algunos otros de los casos más relevantes hasta el momento van desde el robo masivo de información de tarjetas de crédito hasta ataques informáticos perpetrados por virus que pueden afectar sistemas de gasoductos, redes eléctricas o sistemas de control de armamento nuclear. De hecho, hace unos pocos meses atrás se conoció que la Comisión de Regulación Nuclear4 de Estados Unidos ha sido víctima de ataques informáticos que lograron infiltrar sus computadoras y acceder a correos electrónicos de dicha comisión. Este tipo de ataques tienen como objetivo no sólo infiltrar y afectar infraestructuras críticas, sino que también son herramientas de espionaje industrial y económico a nivel internacional.

---

[1] Maestrando en Relaciones Internacionales (IRI – UNLP).

[2] *New York Times*, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", 15 de Enero de 2011.

[3] *The Telegraph*, "Iran refuses to hand back US drone", 11 de Diciembre de 2011.

[4] *Reuters*, "U.S. government's nuclear watchdog victim of cyber attacks: report", 19 de Agosto de 2014.

Recientemente se han hecho públicas las acusaciones[5] de Estados Unidos a miembros del Ejército de la República Popular de China de espionaje económico y robo de información secreta a varias industrias de ese país. El robo de información sensible a agencias estatales e industrias representa una doble amenaza no sólo por los perjuicios económicos que acarrea, sino también por el impacto que puede tener en la carrera de desarrollo tecnológico –tanto civil o militar- para los países que logren apropiarse ilícitamente con estos conocimientos.

Si bien el carácter de novedoso de este tipo de amenazas es discutible, en lo concreto éstas se dan en un contexto de vacío normativo a nivel internacional, ya que hasta el momento no hay acuerdo entre los Estados sobre cómo tipificar adecuadamente estas amenazas; además de que la línea divisoria entre espionaje económico y un acto de agresión que pueda deliberadamente coaccionar a un Estado todavía es muy difusa. Por lo pronto sólo ha habido respuestas a nivel doméstico, como el documento conjunto sobre Estrategias de Ciber-Seguridad de la Unión Europea, el cual refleja la visión común de los Estados miembros sobre la materia. En él se destaca que esta nueva categoría de amenazas pueden tener diferentes orígenes y motivaciones diversas (políticas, criminales o terroristas) pudiendo afectar no sólo a los Estados sino también a grandes empresas.

Lo disperso y variado de los objetivos de estas amenazas podría indicar que no habría aún fines claros y concretos de parte de quienes cometen estos actos. Lo cierto es que la multiplicidad de potenciales orígenes y objetivos de los mismos le plantea un desafío a los Estados en cuanto a la estrategia a adoptar para combatirlos; la cual deberá estar fundada en el concepto de vigilia estratégica[6]. Dicho concepto -desarrollado a partir del concepto de vigilia de Clausewitz- plantea que, en un contexto de incertidumbre como el actual, en el cual las amenazas se han desterritorializado y han adquirido un carácter omnidireccional, la vigilia debe ser la postura estratégica que debe primar para poder hacer frente a enemigos no designados.

Junto con la discusión sobre el rol de la cooperación entre Estados y el sector privado interesado respecto de las estrategias de prevención que deberán adoptar para hacer frente a esta problemática, el principal debate deberá darse en los organismos internacionales para establecer un marco normativo internacional que cubra el vacío legal existente. Estas amenazas podrán parecer intangibles pero las consecuencias pueden materializarse en catástrofes que afecten a ciudades enteras, incluso en aquellos casos en los que las motivaciones no hayan sido cometer un acto terrorista.

[5] *CNN Money*, "China's long history of spying on business", 20 de Mayo de 2014.

[6] Tello, Ángel (2002). "Nueva visión estratégica". Ponencia presentada por el autor en el Primer Congreso en Relaciones Internacionales del Instituto de Relaciones Internacionales de la Universidad Nacional de La Plata.