Internet

Eduardo Fainé Celis*

¿Qué hacer después de Wikileaks?

El escándalo diplomático y comunicacional de Wikileaks tiene para rato y la novela de intrigas que ha tejido alrededor del mundo ya salpicó a Chile y sus vecinos. Con su fundador, Julian Assange, detenido en el Reino Unido y su sitio acosado por los gobiernos, especialmente los Estados Unidos, los trapos sucios continúan saliendo a la luz y su actividad no tiene visos de parar.

Por de pronto, un sitio rival se prepara para hacer más de lo mismo y con una promesa de "más transparencia": Openleaks – un sitio fundado por el ex número dos de Wikileaks y actual rival de Assange – debiera salir a la publicidad a corto plazo.

Pero, más allá de lo interesante que pueda ser la lectura de los documentos revelados por estos sitios, ha quedado demostrado que no existe nadie a salvo de la inteligencia mal intencionada y bien ejecutada. Si Estados Unidos y sus enormes recursos en seguridad han quedado sorprendidos por la capacidad de Wikileaks para obtener información clasificada en volúmenes impresionantes, qué duda cabe que en estados menos equipados y sin las mismas capacidades tecnológicas el riesgo de las filtraciones es mayor. Fenómenos similares serán con seguridad una cuestión de tiempo, así como también es probable que esas fugas de información ya estén ocurriendo entre nosotros.

Hoy en día es difícil imaginar el mundo sin la tecnología computacional, en la que hemos puesto toda nuestra confianza, convencidos de su capacidad de simplificar nuestras vidas. Pero esa misma confianza es nuestro talón de Aquiles, puesto que las medidas de seguridad que implementamos para evitar las penetraciones por parte de agentes externos, son creadas por seres tan humanos como los hackers que se proponen violarlas. En este juego de medidas y contramedidas, hay un enorme riesgo de ser vulnerados y expuestos a la luz pública y, aunque no haya nada turbio que ocultar en la Armada, la reserva de la información es vital para la defensa de nuestra nación.

Ahora bien, Wikileaks no se alimenta del robo directo de documentos y Assange no busca la información navegando a través de Internet, sino que la obtiene de "colaboradores" que pueden hackear determinados servidores de datos o también mediante personas que trabajan al interior de las organizaciones atacadas y que, ya sea por motivos económicos, ideológicos o simple venganza personal, deciden traicionar la confianza que se les ha otorgado, facilitando copias del material a su alcance.

Es en este último caso donde radica el peligro, ya que hoy en día es cada vez más fácil copiar información digital en pendrives y teléfonos celulares, así como captar las emisiones de redes inalámbricas o incluso de bluetooth. Por lo tanto, toda medida que tienda a minimizar esos riesgos, por incómoda que sea para los usuarios, debe ser puesta en práctica. Hoy en día es preferible ser tildado de paranoico que estar arriesgando la seguridad de la vital información que manejamos al ser descuidados en su empleo.

* * *

* Capitán de Navío. Oficial de Estado Mayor. AV. Máster en Diseño y Comunicación Multimedia. Preclaro Colaborador de Revista de Marina, desde 2007.