El desarrollo de ciberarmas y su impacto en la seguridad nuclear internacional

Ana Albarracín Keticoglu[6]

En un escenario donde el desarrollo de ciberarmas representa la nueva ventaja tecnológica, los esfuerzos realizados para estabilizar la seguridad nuclear internacional podrían dejar de surtir efectos.

Los bombardeos realizados por Estados Unidos a las ciudades japonesas de Hiroshima y Nagasaki en 1945 convulsionaron el siglo XX por la irrupción de una nueva tecnología con capacidades letales. Luego de finalizada la segunda Guerra Mundial, la comunidad internacional concentró sus esfuerzos en prohibir la proliferación de tecnología nuclear con fines bélicos.

La primera respuesta norteamericana a esta convulsión fue la de mantener ocultos los avances científicos del desarrollo de tecnología nuclear. Posteriormente, el presidente Truman presentó en 1946, el Plan Baruch ante Naciones Unidas, mediante el cual se comprometía al traspaso de información y desarme a cambio del compromiso internacional de no desarrollar combustible nuclear. En 1953, este plan se transformaría en "Átomos para la paz", el cual focalizaba la cooperación internacional para desarrollar energía nuclear con fines pacíficos (Castro Madero: 1990). En esta misma línea se creó la Organización Internacional de Energía Atómica (OIEA) en 1957, que trajo consigo la definición de un sistema de salvaguardias con el objeto de controlar programas de desarrollo y transferencia de tecnología nuclear. El Tratado de No Proliferación Nuclear de 1968, fue considerado el acuerdo más importante en materia de desarme nuclear, mientras que el Tratado de Tlatelolco en 1967 fue el primero en establecer una zona libre de armas nucleares. La creación del Club de Londres, conocido hoy como Grupo de Suministradores Nucleares, en la década del 70, tuvo la intención de concentrar los esfuerzos de los países proveedores de tecnología nuclear para que dicha transferencia se realice únicamente con fines pacíficos.

Lo cierto es que estos esfuerzos no han surtido los efectos esperados. Por el contrario, el número de Estados poseedores de armas nucleares ha ido en aumento durante la segunda mitad del siglo XX[7].

6 Licenciada en Relaciones Internacionales

[7] Estados Unidos, Rusia, Reino Unido, Francia y China son los países habilitados por el TNP a poseer armas nucleares, mientras que India, Pakistán, Israel y Corea del Norte se han hecho con el control de estas armas dejando de lado los acuerdos internacionales.

A pesar de los intentos de controlar la proliferación de armas nucleares durante la Guerra Fría, las dos superpotencias se vieron envueltas en una carrera armamentística que surtió efectos en el sector nuclear. Así, Estados Unidos y la URSS tuvieron que comprometerse en la firma de diversos acuerdos para reducir y limitar sus arsenales nucleares. Sin embargo, Luis Alberto Moniz Bandeira (2017) nos recuerda que la responsabilidad moral de lograr un mundo libre de armas nucleares fue dejada de lado en el siglo XXI, dado que Estados Unidos expandió su producción de armas nucleares, mientras que Rusia se encargó de modernizar sus fuerzas armadas e incrementar su capacidad nuclear.

Esta renovación de la producción de armas nucleares se ha hecho en consonancia con el desarrollo de ciberarmas. Las capacidades cibernéticas en el siglo XXI constituyen la nueva ventaja tecnológica. Esto se debe a que el ciberespacio, para algunos se manifiesta como un nuevo dominio donde hacer la guerra y, para otros, como un espacio que atraviesa transversalmente a los lugares tradicionales donde se libró la guerra a lo largo de la historia. En ambos casos, permite desarrollar operaciones militares para incrementar las capacidades propias y desgastar las del oponente.

La utilización de ciberarmas proporciona ventajas relativas a quien utiliza el ciberespacio, ya que permite desarrollar tareas de inteligencia para proporcionar información errónea al oponente respecto a la situación estratégica y los recursos, pero también la capacidad de desarrollar una guerra psicológica que permita destruir la imagen del enemigo.

Un claro ejemplo de esto fue la guerra de Georgia y Osetia del Sur en 2008. En esta guerra, Rusia consiguió infiltrarse en los sistemas informáticos de Georgia, obstruir sus comunicaciones y así quebrantar su proceso de toma de decisiones. A la vez, utilizó las redes sociales para influir en la opinión pública y cooptar adeptos a su causa en territorio enemigo (Ganuza Artiles: 2010).

Torres Soriano (2018) nos recuerda que la introducción de ciberarmas en operaciones militares contribuye a aumentar la “niebla de la guerra” y, por ende, dificulta el proceso de toma de decisiones del adversario. Para él, la militarización del ciberespacio abre la posibilidad hipotética de que un Estado pierda momentáneamente su capacidad de comunicación y transmisión de órdenes sobre su arsenal nuclear o bien reciba información adulterada sobre los usos del arsenal de su oponente.

Siendo capaz de interferir en los sistemas de comunicación del enemigo, el comando y control de sus sistemas de armas y realizar tareas de inteligencia y contrainteligencia, entonces las ciberarmas podrían ocasionar la neutralización de todos los sentidos del oponente.

Estas nuevas armas permiten dejar todo al descubierto, por lo que resulta casi imposible esconder algo ante los ojos de quien las utilice. La utilización de códigos maliciosos brinda la posibilidad de rastrear al oponente, para así llegar a sus bases y conocer la cantidad y capacidad real de sus sistemas de armas.

Por esto, cabe pensar que la utilización de ciberarmas puede dejar sin efecto la capacidad disuasoria de las armas nucleares, tentando a quien controla el ciberespacio de hacerse con el control del arsenal de su oponente y utilizarlo según sus intereses.

En síntesis, en un mundo en que el compromiso de los Estados de no hacerse con el control de tecnología nuclear con fines bélicos sigue vigente, pero donde las grandes potencias refuerzan reiteradamente su dominio y control sobre estas armas, el desarrollo de capacidades cibernéticas constituye un medio capaz de equiparar e incluso superar las ventajas tecnológicas del enemigo.

Referencias bibliográficas

- Castro Madero, C. & Takacs, Esteban. (1990). *Política Nuclear Argentina ¿avance o retroceso?* Buenos Aires, Instituto de Publicaciones Navales. pp 26-87
- Ganuza Artiles, N. (2010). Situación de la ciberseguridad en el ámbito internacional y en la OTAN. En. Joyanes Aguilar, L. *Cuadernos de Estrategia N° 149. Ciberseguridad: retos y amenazas a la Seguridad Nacional en el ciberespacio*, (pp 166 - 214), España: IEEE.
- Moniz Bandeira, L. A. (2017). *El desorden mundial: Estados Unidos y su proyección de dominio total.* Lanús, Buenos Aires, Argentina: Capital intelectual.
- Torres Soriano, M. (2018). El dilema de la interpretación del ciberespacio. *IEEE, 8 de enero de 2018*