El nuevo estrecho virtual: la ciberseguridad en las relaciones China-Taiwán

Desde el año 1949, el Estrecho de Taiwán ha sido una zona de tensión entre los dos actores que reivindican ser el legítimo gobernante de China: la República de China (ROC - en adelante, Taiwán), y la República Popular de China (RPC - en adelante, China). El conflicto ha pasado por distintas etapas de militarización, llegando incluso a la movilización de tropas. La amenaza del uso de la fuerza convencional sigue presente en el estrecho; sin embargo, las contiendas diarias ya no se dan de la misma manera que antes; el siglo XXI ha introducido un nuevo ámbito donde este conflicto se desarrolla: el informático.

La ciberseguridad refiere "al esfuerzo para proteger sistemas de información y comunicación, e información en general, del acceso no autorizado, uso, control, publicación, daño, alteración, destrucción, u otro tipo de vulneración, para asegurar la confidencialidad, integridad, y disponibilidad de la información y los sistemas"[1]. Para Taiwán, este nuevo campo de batalla es uno en el que los daños que puede recibir tienen la potencialidad de afectar no sólo a la sociedad civil sino también a la estructura gubernamental. El desarrollo tecnológico característico de la isla llevó a una creciente modernización y tecnificación del sistema burocrático del gobierno taiwanés, lo que lo hace altamente vulnerable a los ciberataques. Desde bases de datos gubernamentales, como por ejemplo del registro civil o sistemas policiales, hasta los sistemas que controlan la red eléctrica nacional, todo se maneja mediante sistemas informáticos que son potencial objetivo de hackers, tanto independientes como al servicio de un gobierno extranjero. Para dar una dimensión al riesgo en el que Taiwán se encuentra, en 2020 ha registrado cerca de 15 millones de ciber incidentes[2], y desde 2005 hasta hoy en día ha sido víctima de 28 ciber operaciones, definidas como "todas las instancias de conocimiento público de ciberactividad patrocinada por un Estado, que incluye incidentes y actores amenazantes involucrados en ataques de negación de servicio, espionaje, defacement, destrucción de datos, sabotaje, y doxing"[3]. No es sorpresivo que el actor estatal que más frecuentemente se encuentra detrás de estos ciberataques sea

[1] Cyber Security Management Act 2018, art. 3, inc. 3
[2] Kaushal Kishore Chandel, "China as a Factor in Taiwan's National Cyber Security Strategy", *Occasional Paper*, octubre 2022, 24.
[3] Council of Foreign Relations, "Cyber Operations Tracker", Council of Foreign Relations s.f., https://www.cfr.org/cyber-operations/#Glossary

China (20 de las 28 ciber operaciones antes mencionadas han sido patrocinadas por China)[4].

La ciberseguridad se ha convertido en un elemento de creciente importancia en el ejército chino. Desde 1999, con lo que los intelectuales en ciberseguridad llaman la primera guerra de hackers del mundo, donde se enfrentaron China y Taiwán, el ejército chino ha ido aumentando sus capacidades en infringir daños informáticos: de acuerdo a estimados taiwaneses, China tiene 100,000 personas trabajando en un ciber ejército nacional.[5] En respuesta a una creciente amenaza por un actor que es muy superior en recursos materiales, el gobierno de Taipéi ha desarrollado una estrategia de potenciación de sus capacidades para la ciber guerra: el Programa Nacional de Ciber Seguridad de Taiwán se materializó a través de 5 fases (2001-2005; 2005-2008; 2009-2012; 2012-2016; 2016-2020) mediante las cuales el Estado fue estableciendo definiciones, marcos legales, planes de acción y una estructura burocrática para poder desarrollar la ciberseguridad nacional.

En su más reciente fase (2020-2024), la importancia de la ciberseguridad se vio reflejada al más alto nivel gubernamental con la creación de un nuevo Ministerio de Asuntos Digitales[6] a cargo de Audrey Tang, personalidad de renombre tanto en Taiwán como en el extranjero por su apoyo a la innovación tecnológica como herramienta para potenciar las instituciones democráticas. Sabiendo la debilidad en capacidades en las que se encuentra el gobierno de Taipéi, la versión de 2021 del Reporte Nacional de Defensa establece el plan de acción a seguir: “la ROC no participará en una carrera armamentística con la PRC ante su gran amenaza militar, sino que aplicará capacidades asimétricas para lograr una ventaja relativa de nuestras fuerzas armadas y asegurará que la estrategia militar -de resoluta defensa y disuasión multidominio- sea implementada”[7]. Es decir, Taiwán plantea de aquí a futuro una estrategia de disuasión cibernética que, podemos asumir, se basará en estrategias de negación (*denial strategies*): partiendo del conocimiento base que en los ciber conflictos prima la ofensa, las estrategias de negación “implican aumentar los riesgos y reducir los beneficios de

---

[4] Council of Foreign Relations, “Cyber Operations Tracker”, Council of Foreign Relations s.f., https://www.cfr.org/cyber-operations/#Timeline

[5] Chris Zappone, “Taiwan a canary in the coalmine of cyber warfare”, *The Age*, 8 de Diciembre de 2014.

[6] Sam Robbins y Chia-Shuo Tang, “Hopes and Concerns for Taiwan’s New Ministry of Digital Affairs”, *The Diplomat*, 22 de Agosto de 2022, sección Política, Asia del Este.

[7] Republic of China, Ministry of National Defense. 2021. National Defense Report 2021.

los ciberataques"[8]. Es decir, no esperan poder castigar a quienes realizan, o patrocinan, ciberataques, sino que buscan minimizar los posibles beneficios que sus perpetuadores puedan obtener.

La amenaza de ciberseguridad le ofrece a Taiwán una oportunidad de colaboración internacional de amplia gama. Por un lado, es una ventana para ampliar la relación de cooperación con los Estados Unidos. Uno de los avances más recientes en la relación bilateral con respecto a este tema ha sido el foro estratégico sobre cooperación en ciberseguridad llevado a cabo en Taipéi en 2021[9]. Por otro lado, que el gobierno de Taiwán no sea reconocido como legítimo por la comunidad internacional no merma las posibilidades de cooperación con países que buscan potenciar su propias capacidades para la ciber guerra. A través del Global Cooperation & Training Framework, fundado en 2015 junto con EE. UU., Taiwán busca utilizar sus fortalezas y expertise para lidiar con asuntos globales, dentro de los que se encuentra la ciberseguridad. A este foro se han sumado países como Suecia, Canadá, el Reino Unido, Israel, y la Unión Europea, y son miembros plenos junto con Taiwán y EE.UU., Australia y Japón.[10]

El gobierno de Taipéi siempre se ha percibido bajo amenaza de las fuerzas del Ejército de Liberación del Pueblo, en el pasado corriendo el riesgo de sufrir acciones militares convencionales, en el presente por las vulneraciones de sus sistemas informáticos, tanto civiles como militares. Y esta amenaza es cada día más dañina. Por motivo de la visita de la Vocera de la Cámara de Representantes de EE. UU., Nancy Pelosi, hackers han interrumpido la actividad del sitio web oficial de la presidencia de Taiwán, entre otros sitios oficiales, y el gobierno chino amenazado con actuar en represalia a dicha visita.[11] Además, el ciberataque se cobró víctimas dentro de la sociedad civil: en distintos minimercados y estaciones de tren se transmitieron mensajes de los hackers chinos incitando al pánico social, así como se accedieron a cientos de miles de dispositivos IoT (Internet of Things), por los cuales se podría perpetuar el robo de información personal.[12]

---

[8] John B. Sheldon, "The Rise of Cyberpower", en *Strategy in the Contemporary World* (Oxford), cap. 16, pág. 313-314.

[9] "Cybersecurity cooperation strategy forum held by Taiwan, US in Taipei", *Taiwan Today*, 10 de Noviembre de 2021.

[10] Global Cooperation & Training Framework, "Participating Countries", (consultado el 07 de Octubre de 2022).

[11] Maggie Miller, "Taiwan presidential office website hit by cyberattack ahead of Pelosi visit", *Politico*, 02 de Octubre de 2022.

[12] Jonathan Greig, "Cyberattacks on Taiwan started several days before Pelosi arrival: report", *the Record*, 30 de Septiembre de 2022.

La capacidad taiwanesa para lidiar con estas ciber amenazas ha ido en crecimiento gracias a un plan liderado por el Estado y en conjunción con la sociedad civil y el apoyo proveniente de fuera de sus fronteras. Que esta capacidad surta efecto en defender al gobierno de Taipéi y a sus ciudadanos de los ataques chinos es algo que será puesto a prueba periódicamente.

Bibliografía

Chandel, Kaushal Kishore. "China as a Factor in Taiwan's National Cyber Security Strategy." *Occasional Paper* (Institute of Chinese Studies), no. 94 (Agosto 2022).

Council of Foreign Relations. *Cyber Operations Tracker.* n.d. https://www.cfr.org/cyber-operations (accessed Agosto 07, 2022).

Cyber Security Management Act. 2018.

Global Cooperation & Training Framework. *Global Cooperation & Training Framework.* n.d. https://www.gctf.tw/en/ (accessed Octubre 07, 2022).

Greig, Jonathan. "Cyberattacks on Taiwan started several days before Pelosi arrival: report." *The Record*, Septiembre 30, 2022.

Miller, Maggie. "Taiwan presidential office website hit by cyberattack ahead of Pelosi visit." *Politico*, Octubre 02, 2022.

República de China, Ministerio de Defensa Nacional. "National Defense Report." 2021.

Robbins, Sam, and Chia-Shuo Tang. "Hopes and Concerns for Taiwan's New Ministry of Digital Affairs." *The Diplomat*, Agosto 22, 2022.

Shelby, John B. "The Rise of Cyberpower." In *Strategy in the Contemporary World*, by John Baylis, James Wirtz and Colin Gray. Oxford, n.d.

Taiwan Today. "Cybersecurity cooperation strategy forum held by Taiwan, US in Taipei." *Taiwan Today*, Noviembre 10, 2021.

Zappone, Chris. "Taiwan a canary in the coalmine of cyber warfare." *The Age*, Diciembre 08, 2014.