Ciber-capacidades: Entre los usos del Estado y el Crimen Organizado

Pablo Agustín Mastragostino[2] y Milagros Agustina Sosa[3]

Ciberespacio y Ciber Capacidades

Una de las cuestiones principales sobre el ciberespacio surge desde la percepción del mismo como un escenario de doble lógica, es decir, con atributos en el dominio virtual (datos, información y redes) y físico al mismo tiempo. Además, incluye multiplicidad de actores compitiendo entre sí y construyendo formas de aprovechamiento de las debilidades e inseguridades del mismo, puesto que los datos e información que fluyen por sus medios pueden convertirse en suministros y blancos de ataque.

A medida que la inversión en el mundo digital y sus aplicaciones aumentan, también se complejizan y multiplican las formas de afectarlo; aunque en este sentido el impacto es indirecto y no "kinético". Por otra parte, las ciber-capacidades en el ámbito criminal, resultan facilitadoras en términos de tiempo, energía y riesgos: hay una percepción de reversibilidad de los efectos, el mantenimiento de la criminalidad es menos costosa ya que observan únicamente cuestiones de actualización/desarrollo de software y porque cuentan con una vida útil extensa puesto que pueden utilizarse en múltiples ocasiones (Van Puyvelde & Brantly, 2019).

Por su parte, la principal misión de una ciber-capacidad es explotar las debilidades de su objetivo por lo que, si bien las capacidades ofensivas son importantes para la efectividad de una acción, las capacidades defensivas (las que tenga un Estado o empresa) serán más importantes aún. ¿Pueden considerarse las ciber-capacidades como armas virtuales? Los puntos en común con las armas tradicionales se relacionan a su aplicación, puesto que están conectadas a las decisiones humanas, planificación estratégica y tareas de inteligencia para sus resultados, pero creemos que no corresponde utilizar dicho concepto ya que al reducirlas a esa caracterización se evade su propia naturaleza compleja, *"se pueden desarrollar, usar y descartar y dependen totalmente de la meta y los objetivos que se buscan"* (Van Puyvelde & Brantly, 2019b, p.116). Los autores proponen que el arma es meramente humana (o sea, el usuario perjudicado), mientras el medio es digital y la ciber-capacidad es una herramienta utilizada en múltiples niveles de la seguridad o inseguridad. Para demostrar la complejidad que hace a dichas herramientas y justificar el empleo del concepto de "capacidad", los autores mencionados emplean la denominación de la empresa estadounidense Lockheed Martin, que se conoce como *Cyber Killer Chain*, es decir, un modelo operacional por el cual se examina cómo los actores desarrollan y utilizan sus capacidades en el ciberespacio. Esta consta de siete pasos enumerados a continuación: 1) *Reconnaissance*, 2) *Weaponization*, 3) *Delivery,* 4) *Exploitation,* 5) *Installation*, 6) *Command and control* y 7) *Action on objectives*. A pesar que, no necesariamente todos los estados u organizaciones criminales utilizan en la misma intensidad en cada uno de los pasos de este modelo, como dijimos anteriormente, es de utilidad para demostrar la complejidad de las ciber capacidades y por qué éstas son más complejas que un arma (Van Puyvelde & Brantly, 2019).

El uso del ciberespacio por el Crimen Organizado

Así como la Criminalidad Organizada tiene una fuerte presencia a nivel "*Off-line*", es decir, las operaciones que realiza en el mundo real en término de narcotráfico, trata de personas, venta de armas, etc.; también podemos encontrar expresiones de crimen organizado en el ciberespacio (Musotto &

[2] Estudiante avanzado de la Licenciatura en Relaciones Internacionales de la Universidad Nacional de Lanús (UNLa)

[3] Estudiante avanzada de la Licenciatura en Relaciones Internacionales de la Universidad Nacional de Lanús (UNLa)

Wall, 2019). A estas manifestaciones cuyos objetivos pueden variar desde el espionaje y el sabotaje de información, hasta poder dañar sistemas enteros de computación e infraestructuras críticas, se las conoce como ciberataques.

Como forma de criminalidad "*on-line*", los ciberataques se destacan por su efectividad metodológica dentro de las medidas coercitivas de acción o amenaza —a comparación del uso directo de la violencia—, ya que resulta un recurso económico desde tres aspectos sustanciales: (a) no es evidente en primera instancia, (b) evita la mediatización casi instantánea del ataque, y (c) provee un mejor margen de acción para ejecutar ataques de tipo coercitivo a impulsado por las ganancias (Musotto & Wall, 2019b). También, su utilización se relaciona a la posibilidad de proteger a los miembros de las organizaciones criminales su información y recursos; un factor llamativo que provoca la incorporación de las redes de alianzas criminales en actividades completamente lícitas. Otro tipo de uso del espacio cibernético, es la manipulación de información, no sólo por "chantaje", sino también para la inyección de ideas particulares en sectores específicos de la población, dedicadas a cambiar las estructuras de pensamiento.

Tres aspectos son centrales a la hora de referirnos a cómo el crimen organizado se manifiesta en el ciberespacio. El primero refiere a las capacidades disponibles que pueden ser utilizadas por las organizaciones criminales, en términos ofensivos, como los Malwares (Puyvelde & Brantly. 2019d). Debido a los múltiples usos disponibles, objetivos y grados de complejidad que se les puede asignar, hace de la tipología una muy densa y diversa lista. No será lo mismo una capacidad cibernética situada en unos pocos códigos de programación a una con miles de líneas de códigos. La más común o, la que ha tenido mayor repercusión desde el punto de vista de la efectividad y de los costos de adquisición son las *Distributed Denial of Service* (DDoS). A éstas se las define como aquellas herramientas que saturan los servidores debido a la gran cantidad de información que se transfiere o mobiliza (*Weaponized Data*) en un mismo momento a ese servidor (Musotto & Wall, 2019c). Esto hace que se debiliten y sean susceptibles a otros tipos de ciberataques ya sea, para robar información o para secuestrar información a cambio de un pago (lo que se conoce habitualmente como *ransomware*). Estos ataques, pueden provocar graves daños a su destinatario, pero grandes beneficios económicos para quien los utiliza.

En segundo lugar, se encuentra la posibilidad de existencia de un nexo entre el Crimen Organizado y el Terrorismo, ésto sucede cuando "[…] *algunas características de las organizaciones terroristas* [son] *adaptadas por el crimen organizado para su uso propio, o para organizaciones terroristas que despliegan actividades típicas de organización crimen*" (Mussoto & Wall, 2020c, p. 43). Sin embargo, tales autores lo caracterizan como un fenómeno efímero, unido por redes de interconexión que les permiten accionar en conjunto cuando comparten un fin común para actuar "*on-line*". En relación a esto, el híbrido entre ambas organizaciones no es considerado como una entidad entre los distintos grupos que se identifican dentro del Crimen Organizado o Terrorismo —separándolos correctamente por sus metodologías o modelos organizacionales—, sino que se limita su interpretación al nexo entre ellos y los incidentes "aislados" que causan esos "grupos criminales". Por nuestra parte nos permitiremos comentar la necesidad de abordar el análisis desde significados concretos que permitan establecer un marco sólido para examinar el objeto de estudio. Entendemos, entonces, como híbrido a una amenaza que combina, en cierto grado, características diversas entre unos y otros fenómenos, independientemente del protagonista circunstancial (Bartolomé, 2019).

Por último, se encuentra la atribución del cibercrimen a un particular o grupo definido, sin embargo, la multiplicidad de efectos y actores involucrados en los ataques en red, resultan en una profundización de las dificultades para identificarlos. Esto hace que el análisis de los conflictos en el plano cibernético dependa sustancialmente del tipo de información comprometida y los resultados finales del incidente causado. A raíz de esto nos resulta importante aportar al trabajo la pertinencia de establecer herramientas de observación del escenario, a partir del cual se puedan definir las motivaciones que

dirigirán el accionar del "contrincante"; parafraseando a Ángel Tello, se trata de deducir las intenciones y estimar los propósitos guarecidos en las amenazas (Tello, 2001), para luego comprarlo con los resultados reales que arrojan las medidas de seguridad.

Respuestas del Estado: Capacidades defensivas y estrategias de ciberseguridad nacional

Existe una clara diferenciación entre las ciber-capacidades que puede tener un Estado Nacional y las que puede ostentar una Organización de Crimen Organizado. Hablamos siempre en término de potencialidad, entendiendo que no todos los estados poseen los mismos recursos, así como también sucede con las organizaciones criminales, haciendo que la capacidad de daño dependa de las aptitudes ofensivas del atacante y las defensivas de su objetivo. Allí, en esa relación, es donde se encuentra la diferencia. Las herramientas más complejas suelen estar más ligadas al desarrollo por el propio Estado, mientras las más simples son de mayor acceso para hackers individuales como para organizaciones criminales. Esto, sin embargo, no quita que una organización que tenga los recursos o cuente con el patrocinio de un Estado, no pueda adquirir capacidades más complejas.

Recordemos que, la principal misión de una ciber-capacidad es explotar las debilidades de su objetivo por lo que, si bien las capacidades ofensivas son importantes para la efectividad de una acción, las capacidades defensivas serán más importantes aún. En pocas palabras, un ciberataque a base de malwares de poca complejidad puede causar mucho daño si las capacidades defensivas presentan muchas vulnerabilidades o si no se cuentan con ellas.

La competencia por el desarrollo y vanguardia proyectada hacia el ciberespacio, resalta aún más los aspectos tecnológicos y económicos como elementos para pensar y actuar sobre la geopolítica, y por lo tanto se plantea como un espacio de rivalidad. Las Estrategias de Ciberseguridad Nacional aparecen en tanto necesidad de los Estados de garantizar el mayor nivel de seguridad posible (Puyvelde & Brantly. 2019). Esto es así debido a la gran cantidad de dispositivos conectados al ciberespacio, dando cuenta de que los múltiples ámbitos de la vida humana a nivel social, cultural, económico y militar tienen un correlato en el ciberespacio e indefectiblemente se relaciona a nivel de la seguridad nacional. En este aspecto, a medida que se desarrolla aún más el ciberespacio y por tanto las ciber-amenazas (sean de origen estatal o no estatal), más y más Estados desarrollan estrategias de ciberseguridad nacional.

Conclusión

El espacio cibernético, sus redes de conexión y la producción de equipamiento que lo componen, es comprendido como otra dimensión de construcción y ejercicio del poder, ya que, además, es utilizado como insumo y soporte de todo tipo de estrategias relacionadas a la seguridad nacional de los Estados modernos. Entonces, permite construir y desplegar poder a través del espacio cibernético, abre un nuevo flanco para la formulación de estrategias en pos de delinear objetivos, cursos de acción y asignar los recursos para éstos. Las entidades estatales realmente toman el papel de garantes de la seguridad e integridad de sus ciudadanos e instituciones, puesto que el avance tecnológico es acompañado por actores que buscan explotar sus debilidades para ganar beneficios.

Por otro lado, las organizaciones criminales hacen gala de lo inefable que resulta este espacio y del sencillo acceso a herramientas o ciber-capacidades de distinto tipo de complejidad para así poder llevar adelante sus objetivos. Escenario que plantea serios desafíos al estado para poder mejorar sus capacidades defensivas en pos de evitar grandes pérdidas monetarias y de información.

Por último, esto plantea un debate sobre seguridad en el espacio cibernético y cómo abordarla desde los distintos andamiajes teóricos. Pueden identificarse dos perspectivas de aproximación, éstas son desde el realismo clásico y el liberalismo, ubicándolo en una especie de espectro que recorre las concepciones estado-céntricas relacionadas al control del orden doméstico, así como en simultánea competencia internacional, y por otra parte los atisbos de cooperación entre las entidades estatales por la necesidad de una regulación en niveles multilaterales. Sin embargo, así como las relaciones y el balance de poder dentro del carácter anárquico del sistema se determinan por los propios actores —en palabras de Wendt—, podemos considerar que el ciberespacio es lo que sus actores hacen de él. Pero sólo algunos tienen la autoridad y recursos suficientes para coordinar respuestas efectivas.

Bibliografía

Bartolomé, M. C. (2019). Ameaças e conflitos híbridos: características distintivas, evoluçãoao longo do tempo e manifestações predominantes. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (25), 8-23.

Musotto, R., & Wall, D. S. (2019). The online crime-terror nexus: Using booter services (stressers) to weaponize data? 1. In *Organized Crime and Terrorist Networks* (pp. 42-59). Routledge.

Ruggiero, V. (Ed.). (2019). *Organized crime and terrorist networks*. Routledge.

Tello, A. (1998). La incertidumbre estratégica. *Archivos del presente: Revista latinoamericana de temas internacionales*, *4*(14), 147-155.

Van Puyvelde, D., & Brantly, A. F. (2019). *Cybersecurity: politics, governance and conflict in cyberspace*. John Wiley & Sons.