INTERNACIONAL

Rusia-Ucrania y la ausencia de una guerra cibernética total

Por Ernesto Ángeles · 27 de mayo de 2022 · 8 min de lectura

El conflicto Rusia-Ucrania ha dejado una serie de lecciones a nivel internacional que tienen el potencial de transformar múltiples áreas del saber humano y del orden mundial en general, una de estas áreas es el uso de la tecnología en la guerra y la importancia estratégica del ciberespacio.

Pese a que diversas figuras pensaban que el inicio de la operación especial/invasión de Rusia en Ucrania iba a desencadenar una ciberguerra a gran escala o, lo que algunos alertaron, un ciber Pearl Harbor, esto no sucedió, no ha habido un ataque digital a gran escala y mucho menos uno que tenga como objetivo a Europa o Estados Unidos, sino que han habido diversas operaciones mutuas que se ciñen a objetivos aislados y específicos, cuya peligrosidad no excede los límites aceptados de agresiones digitales.

En este punto la pregunta que salta es ¿por qué no ha sucedido un conflicto digital a gran escala? ¿por qué no escuchamos de virus y ataques como el Stuxnet? Conocido como la primer ciber arma, la cual fue dirigida contra las centrales de centrifugación nuclear de Irán y cuya complejidad evidenciaba a varios grupos de personas coordinadas y financiadas detrás de su realización, lo más probable Estados Unidos o Israel.

Es necesario señalar una serie de consideraciones que permitirán comprender la íntima relación entre las tecnologías, entornos digitales y la guerra, tal como que una conflagración digital es una condición subyacente y continua, más que un conflicto que se activa, así ha sucedido entre Rusia y Ucrania, los cuales han estado en ciberguerra desde el 2014 hasta la fecha; en este proceso la versatilidad de las tecnologías digitales es tal que bien pueden ser vistas y usadas como un escenario, una herramienta o un dominio de la guerra (así como el aire, el agua o la tierra).

Dicha versatilidad permite que la tecnología pueda ser empleada en diferentes entornos y con múltiples objetivos, tales como la mente humana y su cognición (y con ello estructuras político-sociales); estructuras físicas que dependan de sistemas digitales de control, tal como presas, estaciones eléctricas o infraestructuras de comunicación; estructuras digitales como programas, redes o plataformas, junto con los datos, información y conocimiento digitalizados del enemigo, como el caso de comunicaciones militares, posiciones de armamento o de personal; así como algunas estructuras internacionales, entre otras áreas relacionadas y dependientes del ciberespacio.

Los ataques a la cognición humana tienen el potencial de subvertir sistemas sociales a gran escala y en el cual ambos bandos (la coalición pro Ucrania y la coalición pro Rusia) han tomado acciones pertinentes, como el bloqueo de diversos canales y medios de información (tal como el caso de RT y Spunik en Occidente y NBC, CNN, Facebook, entre otros, en Rusia); así como la creación y promoción de propaganda y narrativas en torno al conflicto, lo que en última instancia genera diversas víctimas directas e indirectas, tanto del bando enemigo como del bando propio y la verdad en general. Las armas más usadas en este campo son las noticias falsas, información sin contexto, propaganda, bots, trolls, grupos de ciberactivistas (en la contienda Rusia-Ucrania resalta el rol de Anonymous y activistas pro Ucrania, los cuales no sólo han filtrado información sensible de Rusia, sino que han ayudado en la

defensa digital ucraniana), grupos cibercriminales, espionaje y filtración de información, entre otros; los escenarios predilectos son las redes sociales, los foros en línea y diferentes medios de comunicación (masiva o de persona a persona, como WhatsApp).

En el caso de un ataque a infraestructuras digitales sus objetivos pueden ser: inhabilitar o imposibilitar la integridad de la información, la integridad del servicio o recurso de red o atacar los medios de conexión de red; entre las principales armas usadas en el contexto del conflicto Rusia-Ucrania están los programas maliciosos conocidos como wipers, los cuales se enfocan en eliminar la información de los dispositivos que atacan (entre las operaciones recientes de Rusia contra Ucrania resaltan la operación Whisper Gate, Issac Wiper, Double Cero y Hermetic Wiper, y de Ucrania contra Rusia está el RURansom Wiper), en donde el medio de infección suele ser por medio de técnicas conocidas como el phishing, el cual consiste en mandar mensajes altamente personalizados a personajes con acceso clave a redes con el fin de acceder e implantar diversos tipos de software malicioso, aquí resalta la actividad contra Ucrania del grupo ruso APT28, el cual también estuvo inmiscuido en la intromisión a las elecciones presidenciales en Estados Unidos en 2016. Asimismo se han usado técnicas conocidas como "defacement", principalmente con el objetivo de vandalizar páginas web, tal como lo ha hecho Bielorrusia contra Ucrania en la operación UNC1151.

Otro de los ataques más usados contra las infraestructuras digitales, sus servicios y contenido son los Ataques de Denegación de Servicio (DDoS, por sus siglas en inglés), estos ataques se caracterizan por manipular una gran red de dispositivos para que envíen solicitudes de acceso a recursos digitales (como una página web) con el fin de saturarlos; en este escenario Rusia ha mantenido una campaña de DDoS contra Ucrania desde febrero, con objetivos como bancos, el servicio postal de ucrania, páginas web gubernamentales y empresas de noticias.

En las infraestructuras físicas la ofensiva es más complicada, ya que no sólo se requiere saber los distintos vectores de ataque, sino que se necesita tener el medio de ataque, el arma y un mecanismo de entrega; su papel en un conflicto armado es tangible y puede afectar múltiples instancias y países, ya sean combatientes o no, tal imprevisibilidad es uno de los factores más importantes por los cuales difícilmente se usa una ciberarma, ya que el potencial que se desencadene una escalada en el conflicto es algo bastante viable; además, al tratarse de una arma compuesta por líneas de código, ésta sólo puede ser usada una vez.

Usualmente los ataques a las infraestructuras físicas están dirigidas hacia Sistemas de Supervisión, Control y Adquisición de Datos (SCADA, por sus siglas en inglés), los cuales, como su nombre lo dice, permiten controlar y supervisar procesos industriales, tal como la provisión de energía, agua o el control de instalaciones químicas y, aunque Rusia los ha ocupado otras veces contra centrales eléctricas, bancos y empresas de telecomunicación en Ucrania, el uso de tales ataques ha sido bastante limitado desde que empezó la conflagración armada. Rusia ha lanzado ataques contra la infraestructura eléctrica de Ucrania (Industroyer 2), mientras que fuerzas pro Ucrania (Belarusian Cyber Partisans) atacaron diversos recursos en el sistema de trenes de Bielorrusia; sin embargo, estos ataques han sido bastante limitados.

Históricamente Rusia ha lanzado diversos ciberataques con múltiples objetivos a nivel internacional; sin embargo, se esperaba que con el inicio de las sanciones internacionales y el apoyo dado a Ucrania Rusia lanzaría ataques más sofisticados y destructivos, entre las razones por las cuales no ha sucedido se pueden pensar: 1) porque EUA ya amenazó de una respuesta ante un ciberataque; 2) porque el nivel de inteconectividad e interdependencia de los sistemas y estructuras internacionales afectaría a Rusia, sus aliados e intereses; 3) porque no es necesario. Esta última posibilidad se refuerza con el uso limitado de armamentos y estrategias tecnológicamente sofisticadas, tal como las armas hipersónicas, las cuales sólo se han usado en momentos clave de la conflagración como una muestra de fuerza de parte de Rusia, lo cual exhibe un cálculo estratégico en la escalada del conflicto más que una señal de debilidad del arsenal ruso, tal como algunos analistas apuntan de manera sobradamente errónea.

Lo que hemos visto hasta el día de hoy es una conflagración en donde el uso de armamento tradicional ha opacado a las promesas tecnológicas y futuristas que en una conflagración entre Estados en pleno siglo XXI podría esperarse; sin embargo, no es que no existan una serie de tecnologías armamentísticas físicas y digitales asociadas al ciberespacio, sino que no han querido usarse plenamente por el contexto, sus riesgos, su naturaleza y lo estratégicas que son, ya que muchas de estas están diseñadas específicamente para un modo de lucha asimétrico contra un poder armamentístico mayor como el de Estados Unidos, por lo que la sorpresa es un factor estratégico en su funcionamiento.

En conclusión: no es que las ciberarmas no sean funcionales o estratégicamente importantes, sino que el escenario de guerra es bastante inestable y requiere ser analizado sectorialmente y por medio de gradaciones de poder; así como también se requiere estar al tanto de la dependencia tecnológica y la capacidad de autosufiencia o abastecimiento alterno a la tecnología occidental, ya que conforme la dependencia e interoperatividad tecnológica hacia Occidente disminuya, países como Rusia o China tendrán más incentivos para usar estos vectores de ataque.

Publicado en Punto de Referencia. Dirección original: https://puntodereferencia.mx/internacional/rusia-ucrania-y-la-ausencia-de-una-guerra-cibernetica-total
Descargado el 21 de noviembre de 2026.