La confrontación cibernética entre Estados Unidos y Rusia está recurriendo cada vez más a la infraestructura civil crítica, particularmente con las redes eléctricas, según los informes de prensa recientes.

El conflicto típicamente furtivo se hizo público el mes pasado, cuando The New York Times informó sobre el cambio en el comando cibernético de Estados Unidos hacia un enfoque más ofensivo y agresivo para atacar la red eléctrica de Rusia.

El informe generó escepticismo de algunos expertos y una negativa del gobierno, pero la revelación llevó a Moscú a advertir que esta actividad presentaba un *«desafío directo»* que exigía una respuesta. Ese mismo día, WIRED publicó un artículo que detalla el creciente reconocimiento cibernético de las redes de Estados Unidos mediante un sofisticado malware que emana de una institución de investigación rusa, mismo malware que detuvo de forma abrupta las operaciones en una refinería de petróleo de Arabia Saudita en 2017 durante *«uno de los ataques cibernéticos más imprudentes de la historia».*

Aunque ambas partes han estado enfocándose en la infraestructura de la otra desde al menos el año 2012, según el artículo del Times, la agresión y el alcance de estas operaciones ya no tiene precedentes.

Washington y Moscú comparten varias similitudes relacionadas con la ciber-disuasión. Ambos ven al otro como un adversario altamente capaz. Los funcionarios estadounidenses se preocupan por la capacidad de Moscú de ejercer su poder autoritario para acorralar a la academia rusa, el sector privado y las redes criminales para aumentar su capacidad cibernética al tiempo que aíslan a los piratas informáticos respaldados por el estado de la atribución directa.

Moscú ve una inquebrantable omnipresencia cibernética en Estados Unidos, capaz de desarrollar malware excepcionalmente sofisticado, como el virus Stuxnet, todo esto mientras utiliza operaciones digitales para orquestar la agitación regional, como la Primavera Árabe en 2011.

Independientemente de sus similitudes en la orientación cibernética, Moscú y Washington enfrentaron distintos caminos en el desarrollo de capacidades y políticas para la guerra cibernética, debido en gran parte a las interpretaciones muy diferentes de los eventos globales de los dos lados y la cantidad de recursos a su disposición.

Un abismo tanto en la voluntad de utilizar las operaciones cibernéticas como en la capacidad para lanzarlas las separó por casi 20 años.

No obstante, los acontecimientos desde 2016 reflejan una convergencia de los dos factores. Si bien Estados Unidos mostró una creciente disposición para lanzar operaciones contra Rusia, Moscú reforzó su capacidad cibernética militar al expandir las iniciativas de reclutamiento y el desarrollo de malware.

Sin embargo, el peligro en la disuasión cibernética de ambos lados no radica tanto en su voluntad y capacidad convergentes, sino en su origen en un malentendido mutuo. Las autoridades cibernéticas del Kremlin, por ejemplo, tienen una opinión casi inmutable de que los Estados Unidos buscan socavar la posición global de Rusia en todo momento a lo largo del frente digital, apuntando a las operaciones cibernéticas de Estados Unidos detrás de incidentes globales que son desfavorables para los objetivos de la política exterior de Moscú.

Una expansión declarada para atacar las redes eléctricas rusas podría asegurar que las futuras interrupciones, que pueden ocurrir de forma espontánea, sean vistas por Moscú como un acto inequívoco de la ciberagresión de Estados Unidos.

Al parecer, en Washington se dedica muy poco esfuerzo a comprender la complejidad de la visión de Rusia sobre la guerra cibernética y la disuasión. La idea de que el esfuerzo de Rusia en 2016 para afectar las elecciones presidenciales de Estados Unidos fue un acto «cibernético» de Pearl Harbor, es una comparación apropiada solo en el sentido de que los funcionarios de Estados Unidos cuentan con operaciones técnicas que difieren de la mayoría de los conceptos occidentales.

Los operadores militares rusos llevaron a cabo lo que debería considerarse una ciber

campaña más agresiva un año antes de su intromisión presidencial, cuando se hicieron pasar por CyberCaliphate, una rama en línea de ISIS, y atacaron a los medios de comunicación estadounidenses y amenazaron la seguridad de los militares estadounidenses.

Por su parte, los rusos hicieron una comparación histórica diferente a su actividad de 2016. Andrey Krutskikh, el hombre más elocuente del Kremlin en temas de ciberemigracia, comparó el desarrollo de las capacidades cibernéticas de Rusia ese año con la primera prueba exitosa de la bomba atómica de la Unión Soviética en 1949.

Los analistas occidentales, obsesionados con desenredar el concepto ya desaparecido de la *«Doctrina Gerasimov»*, dedicaron mucha menos atención a los ciber expertos del ejército ruso, que a partir de 2008 escribieron una serie de artículos sobre las consecuencias de la militarización de Washington en el espacio cibernético, incluyendo un final a mediados de 2016 que discutió la necesidad de Rusia de buscar la paz cibernética con Estados Unidos demostrando un *«potencial de información»* igualitario.

A pesar de las nuevas autoridades del Comando Cibernético, los hackers de Moscú están comparativamente sin límites legales o normativos y tienen una gran lista de medios y métodos para competir contra Estados Unidos. Los piratas informáticos militares rusos, por ejemplo, han atacado todo, desde la iglesia ortodoxa hasta los think tanks de Estados Unidos, y lanzaron lo que la administración de Trump llamó, el ciberataque más costoso de la historia.

Las operaciones cibernéticas rusas se benefician del mandato extralegal altamente permisivo otorgado por un estado autoritario, uno que Washington probablemente detestaría replicar por frustración.

De ninguna forma la actividad del Kremlin debe quedar sin respuesta. Sin embargo, un salto de la inhabilitación del acceso a Internet para la *«Granja de Trolls»* de Rusia a la amenaza de apagar las franjas rusas podría poner en peligro las normas frágiles existentes en esta competencia cibernética bilateral, lo que quizás conduzca a un aumento de los ataques a las instalaciones nucleares.

Estados Unidos está tardando en responder a un enfrentamiento que muchos funcionarios de los círculos de defensa rusos vieron venir hace mucho tiempo, cuando los responsables de la formulación de políticas de Estados Unidos estaban comprensiblemente preocupados por las exigencias del contraterrorismo y la contrainsurgencia.

Washington podría seguir el liderazgo de Moscú al darse cuenta de que esta es una lucha a largo plazo que requiere soluciones innovadoras y bien pensadas en lugar de reflexivas.

El aumento de los costos diplomáticos de la ciberagresión rusa, el apuntalamiento de las defensas cibernéticas o incluso el fomento de canales diplomáticos de nivel militar a nivel de trabajo para discutir líneas cibernéticas, aunque sea discreta y extraoficialmente, podría presentar mejores opciones para apostar por la seguridad de los civiles, que las fuerzas de ambos lados han jurado proteger.