Por qué Irán apagó la red para detener la violencia

Por: Claudio Fabián Guevara. Alainet. 05/12/2019

Irán sufrió una oleada de violencia que destruyó 730 bancos, 70 estaciones de servicio, 140 inmuebles gubernamentales, y más 50 bases de fuerzas de seguridad. El ataque se paralizó cuando el gobierno apagó Internet y las redes inalámbricas. Claves para entender por qué funcionó una estrategia ampliamente criticada entre sus enemigos.

"La tecnología pondrá a disposición de los líderes de las principales naciones una amplia gama de técnicas para llevar a cabo guerras secretas, para las cuales se necesitará de apenas un mínimo de fuerzas de seguridad en el campo". Zbigniew Brzezinski, "Entre dos edades: el rol de los Estados Unidos en la era tecnotrónica". 1970

La República Islámica de Irán, otro escenario de la guerra híbrida, sufrió una devastadora ola de violencia a partir del anuncio de un aumento del 50% en los precios del combustible. Miles de manifestantes enardecidos se volcaron a las calles durante días y atacaron en enjambre gasolineras, bancos y edificios de gobierno.

Súbitamente, el ataque se detuvo cuando el gobierno desactivó Internet y las redes inalámbricas. El apagón informático duró 6 días. Restablecida la calma, el gobierno iraní culpó a una conspiración extranjera por la ola de incidentes, y detuvo en las últimas horas a 8 personas acusadas de tener vínculos con la CIA.

El "apagón de Internet" fue ampliamente criticado por los enemigos de Irán, que le adjudicaron una sola intención: desconectar al país del resto del mundo para ocultar la "represión". Sin embargo, hay indicios de que la desconexión de las redes inalámbricas responde a una estrategia militar defensiva que dio en el corazón de un ataque organizado a alta escala.

La táctica del enjambre

El balance de la erupción de violencia en Irán no parece el resultado simplemente de una "ola de protestas ciudadanas". A lo largo de varios días, 730 bancos, 70 estaciones de servicio y 140 inmuebles gubernamentales fueron incendiados. Más de 50 bases de las fuerzas de seguridad fueron atacadas, e incontables comercios

privados destruidos. El balance de los muertos no conoce cifras oficiales aún, pero Amnistía Internacional lo ubica en 143, entre manifestantes y policías.

¿Pueden los ciudadanos de un país realizar tal nivel de destrucción espontáneamente? ¿Cómo se explica el nivel de coordinación colectiva necesario para derribar todas las salvaguardas de seguridad de cada objetivo atacado?

La investigadora Soraya Sepahpour-Ulrich, presente en estos días en Teherán, describe que se utilizó la "táctica del enjambre": grupos de personas que se comunican con otras mediante mensajes de textos para reunir una muchedumbre en los puntos de ataque. Este concepto es manejado por teóricos de la guerrilla urbana moderna. La consultora RAND, en "Swarming and the Future of Conflict" lo describe así:

"El enjambre ya está surgiendo como una doctrina apropiada para las fuerzas en red para librar el conflicto de la era de la información. Esta naciente doctrina deriva del hecho de que la conectividad robusta permite la creación de una multitud de pequeñas unidades de maniobra, conectadas en red de tal manera que, aunque podrían estar ampliamente distribuidas, aún pueden unirse, a voluntad y repetidamente, para dar golpes rotundos a sus adversarios".

El enjambre está constituido por unidades pequeñas, dispersas y conectadas a Internet. La táctica depende de un flujo de información robusto, condición necesaria para un enjambre exitoso. Al controlar la comunicación y enviar mensajes de texto a los "manifestantes", grupos aleatorios se movilizan juntos a uno o varios lugares. El uso de tecnologías de información modernas, desde Internet hasta teléfonos celulares, ha facilitado los planes y las operaciones de pandillas delictivas y grupos paramilitares en escenarios diversos.

Esa es la explicación de cómo la ola de violencia de Irán, que se extendió por muchas ciudades, fue rápidamente paralizada cuando se desactivó Internet y las redes inalámbricas. Este fue un duro golpe, inesperado por los organizadores de la sedición.

Soraya Sepahpour-Ulrich narra que cuando comenzaron los incidentes violentos, los mensajes de texto vía celular aumentaron rápidamente en número, junto con el vandalismo y el comportamiento destructivo: “Esta no era la primera vez que esta táctica se había utilizado en Irán. Pero fue la primera vez que **los adversarios de Irán se sorprendieron, incluso conmocionados, al ver que Irán era capaz de cerrar Internet tan rápido para detener la propagación de la violencia y restaurar la calma”.**

Sinergia de elementos como indicios de guerra híbrida

No siempre el accionar de grupos violentos, ni las protestas populares, están respaldados en planes de mayor envergadura, ni en estrategias militares profesionales. Sin embargo, en este caso, una sinergia de elementos permite inferir que esta ola de violencia en Irán fue impulsada desde el exterior:

- Medios internacionales y referentes políticos se movieron en forma convergente para legitimar y “blanquear” la violencia, ya que los mismos hechos, de ocurrir en cualquier país del mundo occidental, serían presentados de una manera completamente opuesta: en lugar de “protestas ciudadanas” se hablaría de “ataques terroristas”.

- Reza Pahlavi, el depuesto Shah de Irán, apareció en Irán International alentando a la gente a protestar en las calles. El secretario Mike Pompeo tuiteó un mensaje de aliento “al pueblo iraní”. Otros referentes del hostigamiento internacional contra Irán amplificaron las “protestas” en el mismo sentido.

- BBC Persian, VOA, Radio Farda e Irán International entre otros medios alentaron a las personas a salir a las calles y protestar. Aunque Irán estaba cubierto por una capa de nieve, la BBC Persa mostró imágenes de “manifestantes” en camisetas. Cuando Internet fue desconectado, los medios extranjeros presentaron “informes espontáneos” desde dentro de Irán, que informaban de los eventos como “testigos presenciales”.

- Los destrozos estuvieron circunscriptos a zonas geográficas precisas: “Ninguno de los bancos y estaciones de servicio incendiados, los edificios quemados ylas empresas arruinadas no estaban ubicados en las partes pro-occidentales de Teherán”, informa Soraya Sepahpour-Ulrich. “Su vida continuó sin problemas: hogares seguros, negocios seguros”.

El potencial militar de Internet y las redes inalámbricas

El potencial militar de Internet y sus tecnologías asociadas maximiza las capacidades operativas de escuadrones irregulares dispersos entre la población. Pequeños grupos entrenados, con datos de inteligencia y logística mínima, pueden sembrar el terror en territorios desguarnecidos, y arrastrar a contingentes de jóvenes a una lucha fratricida. También permite sembrar la desinformación y la confusión a través las redes sociales, y/o crear falsas realidades virtuales que se viralizan en las mentes de millones de ciudadanos (y se convierten en involuntarios soldados de una causa ajena a sus intereses).

Otro aspecto sistemáticamente ocultado, además, es el potencial militar de la red de emisiones inalámbricas de la industria civil. No se puede descartar que, a la par del despliegue de grupos armados irregulares y estrategias de reclutamiento de disidentes en los territorios enemigos, la guerra híbrida utilice emisiones de energía electromagnética para inducir cambios en las emociones, en el funcionamiento del cerebro y la salud de las poblaciones.

Las ondas son direccionables a distancia, invisibles e indetectables, lo cual las convierten en la materia prima ideal de la nueva guerra fría. Hace muchas décadas que las potencias desarrollan programas orientadas a desarrollar este tipo de armamento. Han sido referentes públicos de este tipo de programas Elizabeth Rauscher, física nuclear del Laboratorio de Investigación Tecnológica de San Leandro (EE.UU); el neurocientífico Michael Persinger; David Krech de la Universidad de Berkeley; José Manuel Rodríguez Delgado, de la Universidad de Yale, o Richard Cesaro, director del Proyecto Pandora. El canadiense John McMurtry recopila cerca de 200 referencias técnicas y bibliográficas sobre el tema, incluyendo patentes y precisas descripciones sobre las bases de funcionamiento de distintas tecnologías.

Un rápido sumario de las armas encubiertas que pueden ser utilizadas en estos conflictos incluye no solo tecnologías de alcance global, sino también múltiples

dispositivos locales de alcance corto y mediano, fácilmente ocultables en edificios, así como la propia red de telecomunicaciones de cada país.

Es inquietante calcular que, por ejemplo, las emisiones inalámbricas podrían incrementarse a niveles insoportables para la población, impidiendo el descanso y la concentración, y provocando otros múltiples trastornos sin que nadie pudiera advertir el sabotaje invisible.

Así lo sugiere Barrie Trower, ex agente de inteligencia inglés en el área de *microwave warfare*. La red mundial de antenas, desarrollada y montada en casi todo Occidente por las mismas corporaciones, se puede convertir en un caballo de Troya insospechado en escenarios bélicos: *"El sistema está instalado y funcionando. En cualquier momento, alguien lo puede usar para otros fines".*

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ.

Fotografía: Twitter

Fecha de creación
2019/12/04