Globalización
Centro de Investigación
Sobre Globalización

Fraudes electorales 2.0

Por: Jorge Majfud
Globalizacion, 11 de octubre 2023
Rebelión

Región: América Latina, Caribe
Tema: Democracia, Política

En el Sur Global las democracias independientes se corregían con un golpe de Estado. Aun así, los medios jugaban un rol fundamental, al extremo de que la CIA o sus sucursales criollas solían "preparar el terreno" con editoriales plantados, advirtiendo de un peligro inminente, como el secuestro de niños o algún plan para asesinar a los padres cuyos nombres comenzaran con la letra H o B.

Las dictaduras solían legitimarse con elecciones fraguadas. Las democracias también. Es decir, hasta no hace muchos años, era necesario manipular los sistemas electorales. Luego se procedió con una innovación: *en lugar de hackear los sistema electorales, era mucho más efectivo (y hasta legal) hackear a los electores*.

No es necesario dinero para producir bots, pero sí es necesario, y mucho, para implementar una logística que logre manipular la opinión pública a través de la desinformación y la exacerbación de los miedos más ancestrales.

Como todos saben, el programa más poderoso de hackeo de teléfonos privados es Pegasus. Sus clientes suelen ser gobiernos o grandes compañías, ya que el club es selecto y, como en cualquier club exclusivo (como alguno con piscinas donde mean solo los ricos) la matrícula es costosa, para que no se acerque la chusma. Pegasus cobra 650.000 dólares, más una tarifa de instalación de 500.000. En otros casos, como los *back doors*, ya vienen incluidos con las computadoras, son instaladas en secreto en las aduanas o se las instalan gratis apenas el usuario conecta su nueva herramienta de trabajo a Internet.

Es gratis porque el usuario no es el cliente; es el producto, y el electrónico que compra es cada vez menos su propiedad. Sus fabricantes han encontrado la forma legal para establecer el milagro postcapitalista de que cuando compramos un objeto, el objeto no es nuestro; sólo el derecho a usarlo. Pronto esto se extenderá a los automóviles y otros productos. Sistemas gratis, como Linux, son más seguros porque son abiertos, algo así como Wikipedia, pero aun así las agencias secretas han logrado infiltrarlo, como suelen infiltrar Wikipedia.

Los bots son más económicos y efectivos que la inteligencia artificial y ya han demostrado su efectividad en el pasado. Por otro lado, con un poco de conocimiento, un poco de tiempo y voluntad, tampoco es difícil identificarlos. Uno de los rasgos más notables, aparte de la monotemática que señalábamos en un artículo anterior, es su capacidad de producción que sobrepasa la de cualquier ser humano, como lo es escribir miles de tweets o participar en miles de diálogos en pocas horas.

Cuando Elon Musk tomó el gobierno de la red social más política de todas comprando la mayoría de las acciones, lo hizo prometiendo solucionar el problema de los bots. Como todo buen político y gran hombre de negocios, fue pura demagogia. La cantidad de bots, un tercio antes del golpe de Musk, aumentó.

¿Por qué Twitter no incluye una marca que indica la probabilidad de que una cuenta sea un bot? Existen IA e, incluso, otros bots que pueden hacerlo. Existen sitios que identifican el porcentaje de seguidores falsos… No, por el contrario, Twitter ha eliminado el conteo de la cantidad de tweets de un usuario, lo cual es el principal indicio para detectar bots. En 2016, el más famoso de los bots, Tay, escribió cien mil tweets en 16 horas. Lo sabemos porque Twitter solía mostrarlo en cada cuenta. Ahora, ese indicador no es público.

Ese mismo año, la campaña de Donald Trump denunció fraude en las elecciones. Los demócratas derrotados hicieron lo mismo, pero acusaron a Rusia de haber interferido en las elecciones con campañas de desinformación. Los expertos consideran este año como un punto de inflexión, pero el hackeo de la opinión pública por medios electrónicos es mucho más antiguo.

En 2012 se criticó al presidente Hugo Chávez de haber ganado unas elecciones opacas. Hoy sabemos que Team Jorge participó en el hackeo de la opinión pública venezolana y mundial para perjudicar a Chávez. Más recientemente, en 2022, Jorge llevó a cabo una campaña de desinformación afirmando que el Frente Polisario tenía vínculos con Hezbollah e Irán.

Jorge es el nombre dado a un equipo de contratistas con base en Tel Aviv, especializados en el uso de actividades cibernéticas que incluyen piratería informática, sabotaje y campañas de desinformación en redes sociales dirigidas por bots para manipular los resultados de múltiples elecciones. Una de sus principales herramientas es un paquete de software llamado Advanced Impact Media Solutions (AIMS). Su fundador, el ex agente de las fuerzas especiales israelíes Tal Hanan, se ha dedicado a este negocio desde principios de siglo. Según el mismo Hanan e emails filtrados, su cybermafia manipuló 33 elecciones en 30 países, de las cuales ganaron 27, cuyos beneficios iban de 200.000 dólares mensuales hasta más de diez millones.

“¿De dónde sacas esos datos personales?”, le preguntó un cliente.

“No puedo decirte; si lo hago, luego tendría que matarte”, bromeó (¿?) Hanan.

Otro grupo similar y más conocido es el británico Cambridge Analytica, el cual prestó servicios para el referéndum del Brexit y para las elecciones estadounidenses.

Según Samuel Woolley, diez años atrás Ucrania era el epicentro de nuevas formas de manipular la opinión pública usando información de muy baja calidad. “Más tarde nos dimos cuenta de que Ucrania era la avanzada de la propaganda computacional en el mundo. Ahora [2020] cuando queremos tener una idea de hacia dónde va el futuro de las *fake news* y de los bots políticos, simplemente miramos hacia Ucrania. Es un caso de estudio”.

En 1997, la OTAN fundó en Ucrania agencias (como el “Centro de Información y Documentación, NIDC) dedicadas al arte de la guerra moderna, es decir, de la propaganda computacional. El objetivo era “crear conciencia y comprensión sobre los objetivos de la OTAN en Ucrania”, formando por décadas a “periodistas independientes”. Entre 2014 y 2016, el Consejo Nacional de Radiodifusión y Televisión de Ucrania le retiró los derechos de

emisión a decenas de canales rusos. En 2017, la prohibición se extendió a los canales independientes.

El 16 de marzo de 2022, Sean McFate, integrante del Atlantic Council, fue directo: “Rusia puede estar ganando la guerra en el campo de batalla, pero Ucrania está ganando la guerra de la información. Esa es la clave para obtener el apoyo y la simpatía de los aliados”. Un oficial del Departamento de Estado señaló que “los ucranianos han dado una clase magistral en guerra de información”.

¿Estos grupos descubiertos, como Team Jorge, continúan activos? Negarlo sería tan ingenuo como afirmar que la CIA dejó de conspirar cuando en 1975 el senado de Estados Unidos descubrió Operación Mockingbird. Basta con echar una mirada a las elecciones de Argentina para observar la proliferación de bots rales o de carne y hueso. Naturalmente, tomando partido. Aunque grupos como Team Jorge son mercenarios (como lo era el padre de la manipulación de la opinión pública Edward Bernays), en todos los casos beneficiaron a candidatos y a opciones electorales de derecha, a miembros o a mayordomos del Club Exclusivo.

Por pura casualidad.

Jorge Majfud

Comentario sobre artículos de Globalización en nuestra página de Facebook
Conviértase en miembro de Globalización

Artículos de: **Jorge Majfud**