Ciberseguridad. La gran grieta en el sistema electoral estadounidense

Sofía Vicente Facio (México)*

Título original: *Kill chain: the cyber war on America's elections*.
Año: 2020.
Duración: 91 minutos.
País: Estados Unidos de América.
Dirección/producción: Simon Ardizzone, Russell Michaels y Sarah Teale.
Reparto: Michael Daniel, Alex Halderman, Sue Halpern, Harri Hursti, Amy Klobuchar, James Lankford, Jeff Moss, Ion Sancho, Carsten Schürmann, Mark Warner y Ron Wyden.
Productora: HBO.

El concepto "Cyber Kill Chain" fue acuñado por analistas de Lockheed Martin Corporation, llegando incluso a registrar el nombre. En el año 2011 publicaron un artículo donde explicaban lo que llamaban Intrusion Kill Chain, con la intención de ayudar a la toma de decisiones para detectar y responder de una forma más adecuada a los posibles ataques o intrusiones a los que se encuentra expuesto cualquier sistema. Esta cadena definida en el informe es lo que ha venido a llamarse Cyber Kill Chain dentro del mundo de la ciberseguridad. La Intrusion Kill Chain es un proceso dirigido

* Licenciada en Derecho y en Periodismo, comentarista de radio y editora en medios informativos digitales. sofya_facio@hotmail.com.

> contra un objetivo con la intención de conseguir unos efectos deseados. Se trata como una cadena, porque se compone de una serie de pasos necesarios donde una mitigación en cualquiera de ellos supone la ruptura de la cadena, reflejada en una frustración del atacante. La Intrusion Kill Chain se compone de una secuencia de siete pasos, que caracterizan las diferentes etapas de un ataque avanzado. Esta cadena facilita a la potencial víctima el proceso de identificar y aprender de cada fase del ataque, lo que le permite determinar si las medidas de protección son las adecuadas en función de la etapa del ataque (Incibe 2016).

De acuerdo con Harri Hursti, "Votar es nuestra capacidad de tener una manera pacífica de transferir el poder... si no la tenemos, las alternativas son las revoluciones" (Ardizzone, Michaels y Teale 2020, 1:12).

Como una auténtica pesadilla, Hursti, hacker finlandés experto en ciberseguridad y elecciones, muestra las deficiencias del sistema electoral de Estados Unidos de América, la fragilidad de la democracia y cómo la tecnología empleada provoca una vulnerabilidad pocas veces expuesta abiertamente al mundo, pero ya detectada no solo por el atávico enemigo de ese país, los rusos, sino también por intrusos de otras nacionalidades.

Hursti, con gran destreza, modestia y, sobre todo, preocupación, asume la voz premonitoria en una tragedia anunciada; es una especie de oráculo tecnológico que ha emprendido una cruzada contra las empresas y el gobierno, a fin de demostrar, a lo largo y ancho de esa poderosa nación ubicada en el norte del hemisferio, los agujeros que hay en su sistema electoral, en su *software* y en las máquinas de votación de una marca en particular, cuya obsolescencia evidenció Hursti hace más de 15 años en el documental *Hacking democracy* (2006), dirigido también por Simon Ardizzone, Rusell Michaels y Sarah Teale; como respuesta a las fallas expuestas, la empresa fabricante atacó al ciberexperto y a los cineastas con demandas y campañas publicitarias agresivas.

En palabras de la escritora y periodista Sue Halpern,

> Como votamos en Estados Unidos es complicado, pues no hay un sistema de elección nacional, no hay una agencia oficial [en un país donde prácticamente hay agencias gubernamentales para todo], la responsabilidad recae en los estados, los condados y los oficiales electorales; no hay una forma de decir, así vota Estados Unidos, es un sistema caótico (Ardizzone, Michaels y Teale 2020, 4:34).

Sin embargo, basar la impenetrabilidad y la solidez del aparato electoral en su propio caos es una tremenda ingenuidad, lo cual se demostró en Florida en 2016, cuando Ron DeSantis (actual gobernador de esa entidad) reconoció la intrusión de hackers rusos en los sistemas electorales de dos condados y sus bases de datos, quienes, de acuerdo con DeSantis, si bien cometieron una irrupción en la ciberseguridad, no manipularon la información ni alteraron los resultados electorales (¡qué alivio!).

Al respecto de las intrusiones, James Lankford, senador republicano del referido país, menciona: "solo supusimos que somos el perro grande [Estados Unidos de América] y nadie se meterá con el perro grande del porche, eso no aplica para los rusos" (Ardizzone, Michaels y Teale 2020, 21:22).

A lo largo de la cinta se puede observar reiteradamente la vulnerabilidad y la débil tecnología que sostienen la democracia del otrora "país más poderoso del mundo", situación que ya se había mostrado en el documental *Hacking democracy*, el cual se puede considerar la precuela de *Kill chain*.

Las fallas develadas en el filme son evidentes; en él se exhibe cómo los hackers pueden manipular fácilmente el resultado de la votación en una elección, o bien bloquear las máquinas de votos. Según Halpern, "Si su meta es dañar la democracia, realmente no tienen que cambiar votos para hackear una elección, cuando evitas que las personas llenen una boleta, hackeaste una elección" (Ardizzone, Michaels y Teale 2020, 16:06).

La cinta también da cuenta de la insistente negación de los asesores en ciberseguridad del gobierno acerca de la fragilidad de su sistema elec-

toral, el cual está basado en máquinas electrónicas de votación de mala calidad (como repetidamente afirma el protagonista) que pueden ser encontradas a la venta en internet: Hursti responde a un anuncio de un vendedor en un mercado electrónico local y acude al lugar indicado para que le muestren las máquinas de votación; los aparatos están al alcance de todo el público por decenas de dólares, cuando se supone que deberían estar resguardados en instalaciones de seguridad.

Diversos críticos y especialistas en la materia han considerado a *Kill chain* como un audiovisual escalofriante y espeluznante, así como una amenaza a la democracia (Filmaffinity España 2020; Rotten Tomatoes 2020) y, en cierto grado, a las elecciones de noviembre de 2020, en las que al menos una veintena de entidades de Estados Unidos de América usó las máquinas multihackeadas y cuestionadas por el finlandés. Sin embargo, en un movimiento previsorio, el Departamento de Seguridad Nacional y expertos en ciberseguridad del United States Cyber Command, también conocido como USCC, monitorearon las potenciales amenazas, tratando de tranquilizar la situación. No obstante esas previsiones, la sombra de un fraude electoral se mantuvo por algunas semanas después de celebradas las elecciones, como acusó sin éxito el entonces presidente Donald Trump.

El filme está lleno de momentos y diálogos espontáneos, pero que cimbran al más estoico, lo cual demuestra que la realidad siempre supera a la ficción; por ejemplo, las escenas en las que la joven Reality Winner, por dar a conocer información catalogada como clasificada acerca de las intrusiones extranjeras en la ciberseguridad electoral, fue considerada como una delincuente federal y se hizo acreedora a una pena corporal de cinco años en prisión.

Sin duda, lo que sucede en *Kill chain* es un panorama de lo que podría pasar en México si en algún momento se llega a proponer la modernización electoral y se implementa el voto electrónico; sin embargo, dicho mecanismo de votación se observa aún lejano, ya que ni siquiera el vecino país del norte ha sido capaz de regularlo.

Como corolario y moraleja del filme, cabe decir que no parece quedar más remedio que volver a las "anticuadas" boletas de papel, las cuales pueden ser recontadas fácilmente cuando un resultado dudoso es cuestionado, pues el voto electrónico "seguro" aún es una utopía para Estados Unidos de América y para el mundo entero.

Fuentes consultadas

Ardizzone, Simon, Rusell Michaels y Sarah Teale, Dirs. 2020. *Kill chain: the cyber war on America's elections* [Documental]. HBO.

Filmaffinity España. 2020. Crítica sobre el documental *Kill chain: the cyber war on America's elections*. Disponible en https://www.filmaffinity.com/es/film669494.html (consultada el 5 de agosto de 2020).

Incibe. 2016. *Cyber kill chain en sistemas de control industrial*. Disponible en https://www.incibe-cert.es/blog/cyber-kill-chain-sistemas-control-industrial (consultada el 3 de agosto de 2020).

Rotten Tomatoes. 2020. Critic reviews for *Kill chain: the cyber war on America's elections*. Disponible en https://www.rottentomatoes.com/m/kill_chain_the_cyber_war_on_americas_elections (consultada el 5 de agosto de 2020).

Sanger, D. y N. Perlroth. 2020. "Estados Unidos toma previsiones ante las potenciales amenazas contra las elecciones". *The New York Times*, 30 de octubre, sección Español. [Disponible en https://www.nytimes.com/es/2020/10/30/espanol/fraude-electoral.html (consultada el 28 de abril de 2021)].

Satter, Raphael (diciembre 15 de 2020. Copyright 2020-www.reuters.com). *Smartmatic: las conspiraciones de Trump suponen una amenaza "existencial" a industria de voto electrónico*. Raphael Satter, disponible en https://www.reuters.com/article/eeuu-elecciones-votacion-electronicaidESKBN28P0JS (consultada el 28 de abril de 2021).