La Guerra Fría de Las Nuevas Tecnologías

Es sorprendente pensar que la Generación Z no entiende lo que fue la Guerra Fría: todas esas décadas vividas bajo la amenaza de la aniquilación nuclear.

la increíble tensión del Fiasco de Bahía de Cochinos bajo la administración Kennedy, la constante paranoia generada por la idea de que nuestras instituciones habían sido penetradas o comprometidas por agentes extranjeros de la Unión Soviética, y si naciste en la Generación X, como yo, luego, la Guerra Fría fue parte de tu vida hasta los veintitantos años.

La Guerra Fría fue un conflicto ideológico entre Occidente y la Unión Soviética, y el término Guerra Fría se refiere al hecho de que no hubo intercambio directo de balas o bombas entre los dos partidos principales de la Guerra Fría. La Guerra Fría se libró enteramente mediante poderes, propaganda y una carrera armamentista interminable. Finalmente terminó cuando el presidente Ronald Reagan inició la carrera espacial. El entonces líder de la Unión Soviética, Mikhail Gorbachev, cruzó la mano en la mesa de póquer de esta Guerra Fría y no dijo nada más. Poco a poco comenzó a desmantelar la Unión Soviética mediante dos programas conocidos como Perestroika y Glasnost.

Aunque la Generación Z no experimentó la Guerra Fría, las guerras frías se han vuelto endémicas en la experiencia humana. Ya no libramos estas guerras frías entre Estados-nación, pero todavía las libramos. Las características de una guerra fría son una constante escalada de armamentos para mantenerse al día con el enemigo, entonces el mundo de la tecnología está en un constante estado de guerra fría, y al igual que la guerra que acuñó la frase, en estas guerras frías modernas no hay balas. Se disparan y no se lanzan misiles, pero existe un estado constante de conflicto por poder, donde uno de los principales agentes proxy es el mundo del robot en constante avance. Puede que Rusia y Estados Unidos hayan definido el concepto de guerra conceptual como si no fuera una agresión de combate, pero siempre existió y su expresión actual es la tecnología.

Una Nueva Guerra Fría

De hecho, ahora estamos en una guerra fría sin Estados-nación en el mundo intangible, amorfo y misterioso de las redes y la tecnología. Muchos de los elementos de la Guerra Fría siguen vigentes. La Guerra Fría fue perpetuada por complejos militares-industriales tanto en el mundo occidental como en la Unión Soviética. Cada uno tuvo que intensificar su juego para alcanzar la capacidad del otro. Esto podría definirse como la firma de una guerra fría, gasto mutuo y evolución mutua en la tecnología utilizada en la guerra. Esto es precisamente lo que está sucediendo ahora en el sector tecnológico. Los parámetros de participación en esta guerra fría son la privacidad, la seguridad, la continuidad del comercio digital, los mercados digitales, la banca digital y la prevención del fraude y el robo de acuerdo con un espacio de mercado digital seguro.

Esta guerra fría está teniendo lugar entre una parte que quiere maximizar el uso de computadoras y redes para el comercio y las transacciones y otra parte que quiere hacerlo lo más difícil posible por diversas razones. Algunas de estas razones son ideológicas (como la Guerra Fría original); en esta nueva guerra fría la ideología podría ser sentimientos de anticapitalismo, anarquismo y antimonopolio. Algunas razones son el robo y las ganancias ilícitas, y esto también fue una característica de la Guerra Fría original, que fue muy rentable para las empresas seleccionadas para luchar en la guerra mediante el diseño y la fabricación de armas. Y algunas razones carecen totalmente de razón. A estas podríamos llamarlas, en el lenguaje coloquial, razones para aplastar y acaparar, no diferentes del saqueo durante los disturbios cívicos.

Los Piratas informáticos son los nuevos espías

Al igual que el espía de la Guerra Fría original (pensemos en John le Carré, Tom Clancy e Ian Fleming), ha surgido una especie de romance en torno al hacker. En algunos casos, el hacker es un héroe. Si un hacker puede destruir la infraestructura enemiga, entonces es un héroe para el lado que lo emplea. Si el lado en el que estamos es violado por un hack, entonces ese hacker en particular es un villano. No se puede vivir con hackers y no se puede vivir sin ellos. Los necesitamos para salvarnos de los otros hackers, al igual que los espías de la Guerra Fría original.

Al igual que el Estado-nación en la Guerra Fría, es imposible gestionar una red o negocio a gran escala sin un equipo de seguridad, al igual que se necesitaban la CIA, el MI6 y la KGB, así como también lo son una miríada de expertos, consultores y tecnología. Estos equipos necesitan recursos y personal. Los recursos toman la forma de software y tecnología y el personal que asesora en la compra de estos productos y los instala, configura y mantiene. Y, como todas las guerras, es la gente común la que paga por ella. En la Guerra Fría original, los contribuyentes occidentales pagaban la factura. En esta nueva guerra fría, otra persona paga la factura. De una forma u otra, el costo de esta guerra fría entre las personas que quieren piratear transacciones en Internet, defraudar a la gente en sus identidades y su poder adquisitivo, y las fuerzas que quieren protegerlo, lo paga la persona común que llamamos el consumidor. La guerra fría tecnológica la paga el consumidor porque el costo de proteger las redes es un costo de valor agregado para los productos que se venden en línea.

Herramienta del Oficio

En la profesión del artista del fraude digital y del ladrón digital, la herramienta a la que recurrir es el bot. La palabra bot es solo una abreviatura pegadiza de robot. Al mundo de la informática le gusta producir su propio lenguaje, que es muy coloquial, casi una especie de lenguaje tecnológico hip-hop. En el caso de la seguridad de la red, un bot es una aplicación que puede realizar cualquier cantidad de tareas. En sus inicios, los bots eran bastante unidimensionales. Si recuerdas la Guerra Fría, recuerda el comienzo de los videojuegos. ¿Recuerdas a Pong? Dos paletas que podrían moverse verticalmente en una pantalla de televisión para hacer rebotar un punto blanco. Básicamente era ping pong en tu televisor. Eche un vistazo a los juegos de hoy. Está fusionado con la realidad virtual. Hay torneos en los que los mejores jugadores son millonarios y celebridades, como deportistas profesionales por derecho propio y en su propio espacio, aunque sea digital. Puede tomar casi el mismo tiempo dominar ciertos videojuegos dignos de competencia que perfeccionar algo como el patinaje artístico u otro deporte profesional. Todo empezó con Pong.

Lo mismo ocurre con los robots. La primera versión de los bots era como un perro que podía coger un palo y devolvértelo, pero al igual que los videojuegos, los bots han avanzado enormemente. La razón principal de esto es la inteligencia artificial (IA). Junto a esto está el aprendizaje automático (ML). También ha habido avances significativos en las tecnologías de automatización. Aquí hay un breve resumen de lo que los bots pueden hacer ahora en comparación con los bots originales que solo buscaban un palo. Los robots ahora pueden interpretar el lenguaje. Esto es gracias al procesamiento del lenguaje natural (PNL). Los algoritmos asociados al procesamiento del lenguaje natural han avanzado hasta tal punto que los ordenadores ya pueden hablar. Esto ha producido bots que pueden comunicarse con nosotros. La mayoría de nosotros los hemos encontrado como asistentes virtuales o en algún tipo de servicio al cliente.

El próximo gran avance de los bots es su capacidad de aprender. Clasificamos esto bajo el paraguas de aprendizaje automático (ML). Pero se trata simplemente de aprender de la misma manera que aprende un ser humano. Los niños aprenden sus habilidades sociales interactuando con sus hermanos y hermanas, sus madres y padres, y los demás niños en la guardería y la escuela y luego en la universidad y el mundo laboral. Ahora no es diferente para los bots. Cuando un bot se implementa en determinadas circunstancias, puede crecer y madurar a través de las interacciones que tiene con usuarios humanos y, una vez más, esto se debe en gran medida al avance de los algoritmos.

Los bots ahora también pueden realizar tareas secuenciales y muy complicadas. Usando la analogía del perro que busca un palo y lo trae de vuelta, los robots ahora pueden ir a buscar el palo y hacer un círculo, una voltereta hacia atrás, correr alrededor de un árbol, poner el palo en sus pies y luego ir a buscar una bebida del refrigerador. Es bastante alarmante el avance en la realización de tareas complejas que han logrado los bots en los últimos años.

Uno de los avances más perniciosos de los bots en el lado de la seguridad de esta guerra fría tecnológica es la capacidad de los bots para imitar el comportamiento humano. Esto significa que ciertas cosas que sólo los seres humanos podían hacer ahora pueden ser realizadas por robots. El problema con esto es que muchas de las medidas de seguridad para verificar que estás tratando con un ser humano en una transacción en línea ahora pueden ser imitadas por bots. Por ejemplo, antes sólo un ser humano podía resolver un captcha. Este ya no es el caso. Los bots ahora pueden resolver la mayoría de los captchas. Este es uno de los principales frentes de la guerra fría tecnológica. La capacidad de los proveedores para operar en línea y sentirse seguros de que están tratando con seres humanos y, por parte del consumidor, la confianza de que cualquier transacción que realicen tenga suficientes medidas de seguridad para evitar que un robot la realice, se ha visto seriamente comprometida.

Es en el espacio captcha donde la amenaza a la seguridad que representa el avance de los bots es mayor. Captcha significa (Prueba de gira pública completamente automatizada para diferenciar las computadoras de los humanos). Los conoce como esos pequeños cuestionarios, a veces molestos, que aparecen antes de pasar a la siguiente fase de acceder a un sitio web o completar una transacción, como elegir todos los autobuses de las imágenes de arriba. Han sido bastante resilientes durante la última década, pero la guerra fría sigue aumentando. Esto es lo que más distingue este estancamiento tecnológico como una guerra fría. Al igual que los soviéticos adquirieron armas nucleares poco después que Occidente, cada vez que hay un avance en la seguridad informática, los piratas informáticos toman el mismo material utilizado para obtener ventaja, como el aprendizaje automático y la inteligencia artificial, y lo emplean en sus robots.

Esta es solo una breve lista de las cosas que los robots han podido lograr en unos pocos años. Reconocimiento óptico de caracteres (OCR) mediante robots automatizados que ahora pueden emplear tecnología OCR para interpretar los caracteres en una imagen captcha. Este es un punto de inflexión. Una de las pocas formas seguras de distinguir entre un robot y un ser humano en la última década ha sido la selección de imágenes, que, hasta hace poco, ha sido competencia exclusiva de los seres humanos que miran la pantalla de una computadora. No más. Ahora los bots pueden hacerlo. Si el OCR no fuera suficiente, ahora ML cuenta con algoritmos que pueden reconocer las características de una imagen y seleccionar correctamente la imagen buscada. Finalmente, ahora existen ataques de preprocesamiento por parte de bots en los que los bots pueden intentar manipular las imágenes en la matriz captcha antes de procesarlas, lo que les permite reconocer las imágenes y resolver el enigma de la captura.

El comercio online no va a desaparecer. Los piratas informáticos y los estafadores digitales no van a desaparecer. Si es un proveedor en línea, tendrá que elegir un equipo de inteligencia que lo ayude con su seguridad en línea. No puedes hacerlo solo. Durante la actual Guerra Fría, la inteligencia era compartida por todos los países de la OTAN. En el mundo de la seguridad online y la guerra fría en curso en este panorama tecnológico, sólo un puñado de equipos de seguridad destacan. Google causó sensación cuando actualizó captcha a reCAPTCHA©, pero incluso esto quedó en el camino. Lo único que se mantiene al día con lo que sucede en el lado de los hackers es hCaptcha™ de Intuition Machines, respaldado por un equipo de ingenieros de software líderes en inteligencia artificial y aprendizaje automático, produciendo un producto en constante evolución que satisface las necesidades de esta guerra fría tecnológica.