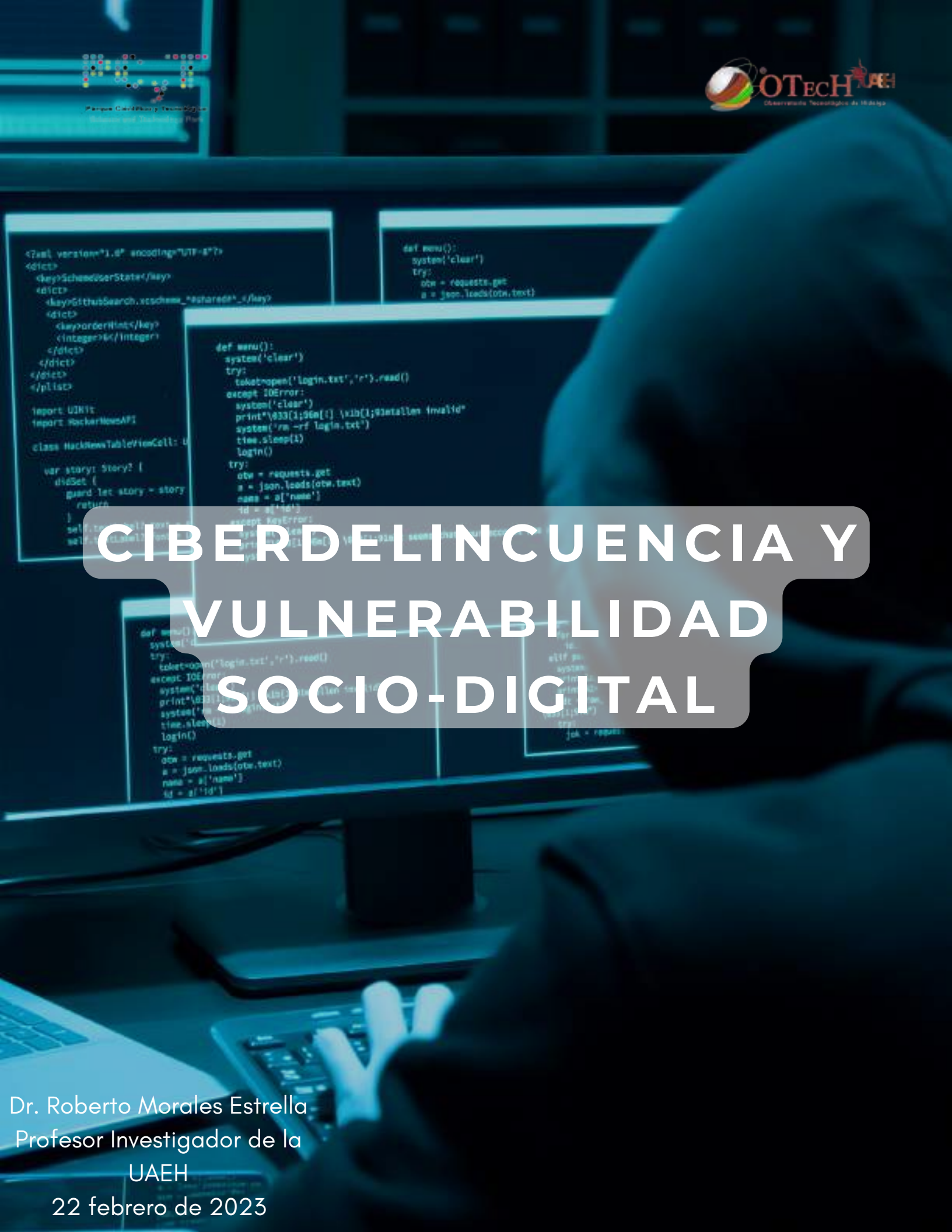

CIBERDELINCUENCIA Y VULNERABILIDAD SOCIO-DIGITAL

Dr. Roberto Morales Estrella
Profesor Investigador de la UAEH

22 febrero de 2023

De todos es sabido que vivimos una sociedad en acelerada mutación, los procesos históricos anteriores, se registraban con mayor lentitud, pero hoy con los escalamientos a mayor velocidad en los desarrollos científicos-tecnológicos, los comportamientos de la sociedad en general han pasado de ser procesos evolutivos a mutaciones aceleradas.

Siendo los grandes flujos de información, que en su planteamiento de la era de la información, Manuel Castells (2000, citado en su prólogo) los identifica como "nuestras sociedades se estructuran cada vez más en torno a una oposición bipolar entre la red y el Yo…de la revolución informacional y la consolidación, de los hoyos negros de la miseria humana, en la economía global"

Los ataques cibernéticos constituyen un flagelo en constante crecimiento a la par del desarrollo tecnológico y el crecimiento de los grandes flujos de información, tanto las organizaciones empresariales como las instituciones públicas y la sociedad en general, estamos todos en constante riesgo de ver nuestra privacidad violada, por delincuentes que irrumpieron en nuestros dispositivos conectados a internet, secuestrando bases de datos, contraseñas, para hacer mal uso de las mismas o extorsionarnos financieramente.

¿De qué tamaño es la vulnerabilidad? Bueno, la empresa especializada en ciberseguridad denominada F5 reveló que durante el primer semestre del 2022 se registraron en México, más de 85 mil millones de intentos de ataques, ocupamos el lugar 84 de 160 países, en materia de seguridad según el Índice de Ciberseguridad Nacional (CBIN).

La empresa CloudFlare informó que en 2023 los ataques cibernéticos como el phishing, el ransomware y los llamados ataques de denegación de servicios distribuido (DdoS) (abrumar un servidor con una avalancha de tráfico para interrumpir una red o una página web), han aumentado todos ellos en un 79%, los ataques cibernéticos, los cuales son cada vez más sofisticados, en la medida que más actividades, tanto productivas, de gobierno y sociales, se inserten en internet, incrementando con ello el riesgo; los ciberataques son ya una amenaza global, expresó en la última reunión del Foro Económico Mundial de DAVOS, Jürgen Stock, Secretario General de Interpol.

Si bien es cierto que todo tipo de organización pública y/o privada, como a nivel individual, que navegue en internet es vulnerable; también es cierto que los conflictos geopolíticos ya entraron en el terreno geotecnológico, de tal forma que una nación puede realizar ataques cibernéticos, hacia otro u otros países; por ejemplo la empresa Pegasus, una Ciber Trasnacional de Israel, que hizo uso de la ciberarma conocida como Candiru, para realizar espionaje y ciber-desinformación en 33 países, incluyendo a México; cabe citar a Tal Hanan, fundador de la empresa Demoman International, que es el experto de seguridad de Israel, quien dirige a un grupo de hackers, para manipular la política global, por sus servicios de espionaje cobra entre 6 y 16 mdd (Jalife 2023).

Ante este contexto es imperativo cerrar la brecha cibernética, lo que implica crear una resiliencia cibernética también conocida como resistencia cibernética que consiste en desarrollar la capacidad de evitar, resistir y recuperar un sistema o plataforma tecnológica, frente a errores relacionados con la ciberseguridad (Keep Coding 2023). Para Yair Lelis de CISCO la ciber-resiliencia es la capacidad de confrontar la hiper-conectividad, para emerger con mayor conocimiento que nos haga más fuertes, después de un ciberataque, o sea defender el uso de tu ciber espacio, de los ciber delincuentes.

Ya ha surgido el concepto de “soluciones de detección y respuesta gestionada” (MDR) siendo la empresa Deepwatch que proporciona este tipo de servicios mediante una plataforma de seguridad en la nube, a través de la cual, realiza la detección y respuestas automatizadas, incluyendo el soporte a pedido de expertos en seguridad, que pueden ayudar a resolver incidentes de seguridad (T. Keary 2023, Venture Beat).

Sin embargo, uno de los grande problemas que se enfrenta en materia de ciberseguridad, es la falta de personal de alto desempeño, con capacidades y competencias suficientes para realizar actividades como auditorías y codificación en ciberseguridad, desarrollo e integración de sistemas basados en Inteligencia Artificial, gestión de políticas públicas y de una normatividad, sin faltar las capacidades y competencias, para construir redes sinérgicas con múltiples partes interesadas, sobre todo liderar en situaciones de crisis. ¿Y nuestras universidades que están haciendo al respecto?