REDES Revista Hispana para el Análisis de Redes Sociales

Vol.30#1, (2019), 119-121

http://revistes.uab.es/redes https://doi.org/10.5565/rev/redes.833

Teoría y práctica de las redes ilegales encubiertas

Deniza Alieva[1]

Management Development Institute of Singapore in Tashkent

RESEÑA

Cunningham, D., Everton, S., & Murphy, P. (2016). *Understanding dark networks: A strategic framework for the use of social network analysis*. Rowman & Littlefield, 388 pp.

Contacto con la autora: Deniza Alieva (deniza.alieva@gmail.com)

****

El análisis de relaciones entre diferentes grupos sociales y de su interacción apareció como una parte integral de la sociología hace tiempo. Una de las dificultades con las que se enfrentaron los investigadores era y sigue siendo la falta de información sobre las actividades de algunos grupos. Sin embargo, la situación cambió con la aparición de Internet y el desarrollo de sitios de networking online que permiten recoger un volumen grande de información para analizar después los patrones de conducta e interacción de los usuarios, lo cual permite la determinación de sus grupos de contactos y su clasificación según distintas características.

El desarrollo de la tecnología y la amenaza constante de diferentes grupos criminales y terroristas centraron los intereses de los investigadores en la posibilidad de aplicar los métodos de análisis de la información obtenida del ciberespacio para el estudio e, incluso, la predicción de la actividad criminal. Poco a poco la teoría y el análisis de redes sociales se convirtieron en un instrumento poderoso de estudio de "redes oscuras" (*dark networks*), que se forman entre las organizaciones ilegales. La interacción entre los participantes adquiere gran importancia, ya que los terroristas o criminales tienden trabajar en grupos o colaborar con otros en sus actividades (Zhang et al, 2009).

Generalmente, los investigadores se centran en los problemas de reclutamiento de nuevos miembros (Scanlon & Gerber, 2014; Bright, 2015), y la dinámica de los grupos criminales (Bright, Hughes & Chalmers, 2012), así como en la resistencia y la resilencia de las propias redes (Roberts & Everton, 2016). Otra parte de los estudios la forman los trabajos de investigadores que analizan la interacción dentro y entre los grupos extremistas, terroristas o criminales (L'Huillier, Alvarez, Ríos & Aguilera, 2011), el contenido potencialmente criminal y peligroso de la información que circula en la red (Zulkarnine, Frank, Monk, Mitchell & Davies, 2016), y el intercambio de creencias y valores entre los miembros de una red (Karimov & Matthews, 2017).

El libro de Cunningham, Everton y Murphy ocupa un lugar importante en la literatura dedicada a la aplicación del análisis de redes sociales en el estudio de las "redes oscuras". Por un lado, es un buen manual que puede ser de interés tanto para un principiante, como para un investigador avanzado en el análisis de redes sociales. Por otro lado, los ejemplos propuestos por los autores analizan datos de gran interés, siendo buenos ejemplos prácticos de la aplicación de la teoría aprendida.

La primera parte del libro está constituida por tres capítulos que introducen el análisis de redes sociales. Se presentan los orígenes de la teoría de redes, la aplicación de este método de análisis a la práctica, en particular su uso en el estudio de las "redes oscuras". Además, se destacan los puntos fuertes y débiles del análisis de redes sociales desde el punto de vista metodológico. Se hace la comparación de este método de análisis con otros. También se explica la diferencia con las "redes sociales" como Facebook o Twitter y su relación con ellas.

En el primer capítulo se introduce una amplia gama de nociones básicas del análisis de redes sociales, que serán necesarios en los siguientes capítulos. Además aquí el lector obtiene información sobre los casos que se

presentarán como ejemplos prácticos a lo largo del libro.

El segundo capítulo se centra más en diferentes métodos de análisis de "redes oscuras", y habla de los problemas con los que puede enfrentarse el investigador a la hora de recoger la información.

El siguiente capítulo está vinculado al proceso de recogida de datos. Aquí se presentan diferentes pistas útiles para recoger, codificar y manipular los datos de redes sociales, que después podrán ser aplicados en el análisis de "redes oscuras".

La segunda parte del libro presenta distintas métricas de las redes sociales que son necesarias para la realización de los análisis. Además, aquí se comparan los lazos fuertes y débiles, se analiza la influencia de la posición de un nodo en su posibilidad de atraer más miembros a una "red oscura". Se asume que la topografía y la estructura de las redes afectan el comportamiento de sus miembros y están relacionados con su resilencia y la eficiencia de su funcionamiento. Se dan los términos básicos de las redes (nodos, lazos, matrices, etc.) en el cuarto capítulo, mientras que el siguiente estudia los métodos más comunes de detección de grupos y subgrupos dentro de una red. Se determinan los componentes, cliques, *k-cores*, facciones y se presentan los algoritmos necesarios para detectar una comunidad de actores en la red. El libro hace hincapié en diferentes métodos de detección de subgrupos y presenta las limitaciones de varios algoritmos usados con este fin.

El sexto capítulo está dedicado a la identificación de los actores centrales de una red. Los lectores obtienen información de diferentes medidas de centralidad y de dirección de los lazos. El séptimo capítulo explora dos términos importantes en cuanto a análisis de "redes oscuras": *bridges* y *brokers*. Se presentan las diferencias en los algoritmos utilizados calcularlos, con ejemplos prácticos.

El octavo capítulo se centra en el análisis del posicionamiento de los nodos en la red. Los autores estudian la posibilidad de que los actores que comparten la posición actúen de manera similar aunque no tengan relaciones entre ellos.

La tercera parte del libro se enfoca en diferentes técnicas que se usan para analizar específicamente las "redes oscuras". El noveno capítulo presenta dos técnicas de prueba de hipótesis: *QAP* y *CUG analysis*. Además, se hace una comparación de estas técnicas con modelos estadísticos estándares, enumerando tres diferencias principales entre ellos.

Los *ERGM* (modelos exponenciales para grafos aleatorios) se presentan en el décimo capítulo. Dichos modelos ofrecen la posibilidad de estudiar los procesos sociales internos y externos de la red, lo que ayuda a detectar los patrones de comportamiento de los miembros de la misma.

Se entiende que las redes no son estáticas, sino dinámicas, que sufren cambios con el tiempo. El estudio de desarrollo longitudinal de las "redes oscuras" permite entender los procesos que tienen lugar dentro de la red y predicir posibles actos de violencia o delincuencia que pueden ser cometidos por los miembros de la misma. Este tipo de análisis se presenta en el undécimo capítulo, que propone varios ejemplos de estudios longitudinales de "redes oscuras" y las técnicas aplicadas en cada caso.

El último capítulo del libro presenta un resumen completo de la información relevante de cada parte.

CONCLUSIÓN

Podemos concluir que el trabajo de Cunningham, Everton y Murphy proporciona la información relevante y necesaria tratando los temas actuales en el ámbito. La presentación de la información teórica y práctica permite abarcar temas complejos y los hace comprensibles incluso para los principiantes en la materia del análisis de redes sociales. Además, los capítulos proponen una lista de preguntas de autoevaluación y una lista de artículos y libros de interés que ayudan a los lectores a profundizar su conocimiento en el tema.

Todas estas características nos permiten constatar que "*Understanding dark networks*" puede servir de gran ayuda para los académicos y profesionales en el ámbito, siendo un buen ejemplo de trabajo teórico-práctico.

REFERENCIAS

Bright, D. A. (2015). Disrupting and dismantling dark networks: Lessons from social network analysis and law enforcement simulations. *Illuminating dark networks: The study of clandestine groups and organizations, 39*, 39-51. https://doi.org/10.1017/cbo9781316212639.004

Bright, D. A., Hughes, C. E., & Chalmers, J. (2012). Illuminating dark networks: A

social network analysis of an Australian drug trafficking syndicate. *Crime, law and social change, 57*(2), 151-176. https://doi.org/10.1007/s10611-011-9336-z

Karimov, R., & Matthews, L. J. (2017). A simulation assessment of methods to infer cultural transmission on dark networks. *The Journal of Defense Modeling and Simulation, 14*(1), 7-16. https://doi.org/10.1177/1548512916679900

L'Huillier, G., Alvarez, H., Ríos, S. A., & Aguilera, F. (2011). Topic-based social network analysis for virtual communities of interests in the dark web. *ACM SIGKDD Explorations Newsletter, 12*(2), 66-73. https://doi.org/10.1145/1964897.1964917

Roberts, N., & Everton, S. F. (2011). *Strategies for combating dark networks.*

Roberts, N., & Everton, S. (2016). Monitoring and disrupting dark networks: A bias toward the center and what it costs us. In *Eradicating Terrorism from the Middle Eas*t (pp. 29-42). Springer, Cham. https://doi.org/10.1007/978-3-319-31018-3_2

Scanlon, J. R., & Gerber, M. S. (2014). Automatic detection of cyber-recruitment by violent extremists. *Security Informatics, 3*(1), 5. https://doi.org/10.1186/s13388-014-0005-5

Zhang, Y., Zeng, S., Fan, L., Dang, Y., Larson, C. A., & Chen, H. (2009, June). Dark web forums portal: searching and analyzing jihadist forums. In *2009 IEEE International Conference on Intelligence and Security Informatics* (pp. 71-76). IEEE. https://doi.org/10.1109/isi.2009.5137274

Zulkarnine, A. T., Frank, R., Monk, B., Mitchell, J., & Davies, G. (2016, September). Surfacing collaborated networks in dark web to find illicit and criminal content. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 109-114). IEEE. https://doi.org/10.1109/isi.2016.7745452

Enviado: 21-06-2019

Aceptado: 21-06-2019