[1] M. Golling and B. Stelte, “Requirements for a future ews-cyber defence in the internet of the future,” in Cyber conﬂict (ICCC), 2011 3rd international conference on. IEEE, 2011, pp. 1–16.

[2] BSIMM, “Attack models with bsimm frameworks,” Online, vol. https://www.bsimm.com/framework/intelligence/attack-models/, 2016.

[3] B. of England, “Cbest intelligence-led testing- an introduction to cyber threat modelling,” ank of England Publication, vol. http://www.bankofengland.co.uk/anintroductiontocbest.pdf, 2016.

[4] X. Lin, P. Zavarsky, R. Ruhl, and D. Lindskog, “Threat modeling for csrf attacks,” 2013 IEEE 16th International Conference on Computational Science and Engineering, vol. 3, pp. 486–491, 2009.

[5] C. Phillips and L. P. Swiler, “A graph-based system for network-vulnerability analysis,” in Proceedings of the 1998 Workshop on New Security Paradigms, ser. NSPW ’98. New York, NY, USA: ACM, 1998, pp. 71–79. [Online]. Available: http://doi.acm.org/10.1145/310889.310919

[6] B. Schneier, “Attack trees,” Dr. Dobbs journal, vol. 24, no. 12, pp. 21– 29, 1999.

[7] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, and E. R. Weippl, “Dark clouds on the horizon: Using cloud storage as attack vector and online slack space.” in USENIX Security Symposium. San Francisco, CA, USA, 2011, pp. 65–76.

[8] P. K. Manadhata and J. M. Wing, “An attack surface metric,” Software Engineering, IEEE Transactions on, vol. 37, no. 3, pp. 371–386, 2011.

[9] S. Caltagirone, A. Pendergast, and C. Betz, “The diamond model of intrusion analysis,” DTIC Document, Tech. Rep., 2013.

[10] U. S. J. C. of Staff, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace. Joint Chiefs of Staff, 2000.

[11] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,” Leading Issues in Information Warfare & Security Research, vol. 1, p. 80, 2011.

[12] W. L. Sharp, “Joint publication 3-60: Joint targeting,” Washington DC: Joint Chiefs of Staff, 2007.

[13] T. Sakuraba, S. Domyo, B.-H. Chou, and K. Saku, “Exploring security countermeasures along the attack sequence,” in Information Security and Assurance, 2008. ISA 2008. International Conference on. IEEE, 2008, pp. 427–432.

[14] N. Ghosh and S. K. Ghosh, “A planner-based approach to generate and analyze minimal attack graph,” Applied Intelligence, vol. 36, no. 2, pp. 369–390, 2012.

[15] V. Shandilya, C. B. Simmons, and S. Shiva, “Use of attack graphs in security systems,” Journal of Computer Networks and Communications, vol. 2014, 2014