# BIBLIOGRAPHY

A Frost & Sullivan Executive Briefing. (2017). *2017 global information security workforce study*. Retrieved from https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

AICPA. (2017). *AICPA*. Retrieved from https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/cyber-security-resource-center

Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, *100*, 212–223.

Allison, L. (2016). You can't hack this: The regulatory future of cybersecurity in automobiles. *Journal Technology Law & Policy*, *21*, 15.

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35.

Anwar, S., Mohamad Zain, J., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. *Algorithms*, *10*(2), 39.

Arafah, M., Bakry, S. H., Al-Dayel, R., & Faheem, O. (2019, March). Exploring cybersecurity metrics for strategic units: A generic framework for future work. In *Future of information* *and communication conference* (pp. 881–891). Cham: Springer.

Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: Stock market reaction. *Journal of Hospitality and Tourism Technology*, *11*(2), 277–290.

Baden-Fuller, C., & Haefliger, S. (2013). Business models and technological innovation. *Long Range Planning*, *46*(6), 419–426.

Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT Professional*, *12*(1), 24–31.

Barth, A., Jackson, C., & Mitchell, J. C. (2008). Robust defenses for cross-site request forgery. In *Proceedings of 15th ACM Conference*, CCS.

Beauchamp, C. L. (2022). *Exploring cyber ranges in cybersecurity education* (Doctoral dissertation, Virginia Tech).

Blair, J. R., Hall, A. O., & Sobiesk, E. (2019). Educating future multidisciplinary cybersecurity teams. *Computer*, *52*(3), 58–66.

Bourgeois, D. T., Smith, J. L., Wang, S., & Mortati, J. (2019). *Information systems for business and beyond.*

Boyes, H. (2015). *Security, privacy, and the built environment* (Vol. 17, No. 3, pp. 25–31). IT Professional, Institute of Electrical and Electronics Engineers (IEEE).

Brayshaw, M., Gordon, N., & Karatazgianni, A. (2020). Identifying gaps in cybersecurity teaching and learning. *INSPIRE XXV*, 165.

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Santa Barbara, CA: ABC-CLIO.

Burley, D. (2021). The future of cyber: Educating the cybersecurity workforce (podcast series).

Burley, D. L., & McDuffie, E. L. (2015). An interview with Ernest McDuffie on the future of cybersecurity education. *ACM Inroads*, *6*(2), 60–63.

Burris, J., Deneke, W., & Maulding, B. (2018, July). Activity simulation for experiential learning in cybersecurity workforce development. In *International Conference on HCI in Business, Government, and Organizations* (pp. 17–25). Springer, Cham.

Callahan, G., & Benzing, C. (2004). Assessing the role of internships in the career-oriented employment of graduating college students. *Education & Training*, *46*(2), 82–89.

CAQ. (2018). *CAQ*. Retrieved from https://www.thecaq.org/cybersecurity-risk-management-oversight-tool-board-members/

Career Opportunities in the Internet of Things (IOT). (2021). *Futureoftech.org*. Retrieved from https://www.futureoftech.org/internet-of-things/6-career-opportunities-in-iot/

Chapple, M., Stewart, J. M., & Gibson, D. (2018). *(ISC) 2 CISSP certified information systems security professional official study guide*. Hoboken, NJ: John Wiley & Sons.

Chaudhary, H., Detroja, A., Prajapati, P., & Shah, P. (2020, December). A review of various challenges in cybersecurity using artificial intelligence. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 829–836). IEEE.

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed? *Journal of Information Systems*, *33*, 163–182. doi: 10.2308/isys-52410

Chudasama, D. (2021). Why choose cyber security as a career.

Coulton, P., Gradinar, A., & Lindley, J. (2021). Anticipating the adoption of IoT in everyday life.

Crumpler, W., & Lewis, J. A. (2019). *The cybersecurity workforce gap* (p. 10). Washington, DC: Center for Strategic and International Studies (CSIS).

Cyberspace solarium commission report. (2020). Retrieved from https://www.solarium.gov/report

D'Abate, C. (2010). Developmental interactions for business students: Do they make a difference? *Journal of Leadership & Organizational Studies*, *17*(2), 143–155.

Davies, G., Qasem, M., & Elmisery, A. M. (2020, December). Cyber security education and future provision. In *International Conference on Service-Oriented Computing* (pp. 612–626). Springer, Cham.

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, *9*, 744.

Deloitte. (2022). *Blockchain and quantum technologies: Driving the future of digital trust*. Retrieved from https://www2.deloitte.com/lu/en/pages/risk/articles/Blockchain-and-quantum-technologies-Driving-the-future-of-digital-trust.html

Dewar, R. S. (2014). *The "triptych of cyber security": A classification of active cyber defense*. Retrieved from https://www.academia.edu/6412868/_The_Triptych_of_Cyber_Security_A_Classification_of_Active_Cyber_Defence

Diogenes, Y., & Ozkaya, E. (2019). *Cybersecurity–Attack and defense strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals*. Birmingham: Packt Publishing Ltd.

Dorsey, D. W., Martin, J., Howard, D. J., & Coovert, M. D. (2017). Cybersecurity issues in selection. In *Handbook of employee selection* (pp. 913–930).

Enoch, S. Y., Ge, M., Hong, J. B., & Kim, D. S. (2021). Model-based cybersecurity analysis: Past work and future directions. arXiv preprint arXiv:2105.08459.

Fafinski, S., Dutton, W. H., & Margetts, H. Z. (2010). *Mapping and measuring cybercrime*.

Finch, A., Burrell, D. N., Lu, S., Dawson, M., Springs, D., Bilberry, K., . . . Modeste, R. (2020). Cybersecurity workforce development in minority, low income, and native American reservation communities. *International Journal of Smart Education and Urban Society (IJSEUS)*, *11*(4), 35–52.

Fischer, E. A. (2014). *Federal laws relating to cybersecurity: Overview of major issues, current laws, and proposed legislation*: Congressional Research Service.

Fleishman, G. (2018). *Equifax data breach, one year later: Obvious errors and no real changes, new report says*. Retrieved from https://fortune.com/2018/09/07/equifax-data-breach-one-year-anniversary/

Gault, J., Redington, J., & Schlager, T. (2000). Undergraduate business internships and career success: Are they related? *Journal of Marketing Education*, *22*(1), 45.

Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In *International conference on computer networks and communication technologies* (pp. 739–747). Singapore: Springer.

Geluvaraj, B., Satwik, P. M., & Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In *International Conference on Computer Networks and Communication Technologies* (pp. 739–747). Springer, Singapore.

Ghadiminia, N., Mayouf, M., Cox, S., & Krasniewicz, J. (2021). BIM-enabled facilities management (FM): A scrutiny of risks resulting from cyber attacks. *Journal of Facilities Management*.

Greenberg, A. (2018). *Marketing firm exactis leaked a personal info database with 340 million records*. Retrieved from https://www.wired.com/story/exactis-database-leak-340-million-records/

Greenfield, R. S. (2002). *Cyber forensics: A field manual for collecting, examining, and preserving evidence of computer crimes*. Auerbach Publications.

Haney, J. M., & Lutters, W. G. (2019, June). Motivating cybersecurity advocates: Implications for recruitment and retention. In Proceedings of the 2019 on *Computers and People Research Conference* (pp. 109–117).

Hargreaves, C., & Prince, D. (2013). Understanding cyber criminals and measuring their future activity.

Hargreaves, C., & Prince, D. D. (2013). Understanding cyber criminals and measuring their future activity developing cybercrime research. Security Lancaster. Lancaster University, Tech. Rep.

Hayes, A. (2023). *Blockchain facts: What is it, how it works, and how it can be used*. Retrieved from https://www.investopedia.com/terms/b/blockchain.asp

Hertzog, R., O'Gorman, J., & Aharoni, M. (2017). *Kali linux revealed. Mastering the penetration testing distribution*.

Hey, A. J., Tansley, S., Tolle, K. M., et al. (2009). *The fourth paradigm: Data-intensive scientific discovery* (Vol. 1). Redmond, WA: Microsoft Research.

Höhne, S., & Tiberius, V. (2020). Powered by blockchain: Forecasting blockchain use in the electricity market. *International Journal of Energy Sector Management*, *14*(6), 1221–1238.

Hott, J. A., Stailey, D., Haderlie, D. M., & Ley, R. F. (2020). The CYBER security–competency health and maturity progression (CYBER-CHAMP) model: Extending the national initiative for cybersecurity education (NICE) framework across organizational security. *Cybersecurity Skills Journal: Practice and Research*. (INL/JOU-20-59690-Rev000).

Hott, J. A., Zohner, D. D., Fetzer, K. M., & Malzahn, T. E. (2019). Creating cybersecurity professionals of the future.

How to ace cybersecurity recruitment. (2022). Cybersn.com. Retrieved from https://cybersn.com/ace-cybersecurity-recruitment/

*IBM security report*. Retrieved from https://www.ibm.com/security/data-breach

Igor, Z., Dmitry, M., Andrey, S., Dmitry, K., Anastasia, T., & Alexander, Z. (2013). Security software green head for mobile devices providing comprehensive protection from malware and illegal activities of cyber criminals. *International Journal of Computer Network and Information Security*, *5*(5), 1–8.

Ikeda, K., Marshall, A., & Zaharchuk, D. (2019). Agility, skills and cybersecurity: Critical drivers of competitiveness in times of economic uncertainty. *Strategy & Leadership*, *47*(3), 40–48.

ITU. (2008). *Committed to connecting the world*. Retrieved from https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Jahankhani, H., & Al-Nemrat, A. (2012). Examination of cyber-criminal behaviour. *International Journal of Information Science and Management (IJISM)*, 41–48.

Javed, A. R., Zikria, Y. B., Shahzad, F., & Jalil, Z. (2021). Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects. *Cities*, *129*, 103794.

Jennifer, M., & Sandy, B. (2016). Trends in community colleges: Enrollment, prices, student debt, and completion. *College Board Research Brief*, *4*, 1–23.

Jovanovic, V. M., Kuzlu, M., Popescu, O., Badawi, A. R., Marshall, D. K., Sarp, S., … Wu, H. (2020). An initial look into the computer science and cybersecurity pathways project for career and technical education curricula.

Juniper Research. (2019). Retrieved from https://www.juniperresearch.com/

Kanellos. (2021). Cybersecurity challenges with emerging technologies. *JAPCC*. Retrieved from https://www.japcc.org/articles/cybersecurity-challenges-with-emerging-technologies/

Kaspersky. (2022). *What is the deep and dark web?* Retrieved from https://www.kaspersky.com/resource-center/threats/deep-web

Kerman, A., Borchert, O., & Rose, S. (2020). *Division, E. Tan, A.: Implementing a zero trust architecture, draft.* National Cyber Security Center of Excellence, National Institute of Standards and Technology, The Mitre Corporation. Retrieved from https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf

Kim, D. J., Love, B., & Kim, S. (2019). A comparison study of cybersecurity workforce frameworks and future directions. In *National cyber summit* (pp. 85–96).

Kirvan, P., & Granneman, J. (2022). Top 10 IT security frameworks and standards explained. Techtarget.com. Retrieved from https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one

Knaves, M. (2022). Cybersecurity risk management: Frameworks, plans, & best practices.

Knouse, S. B., & Fontenot, G. (2008). Benefits of the business college internship: A research review. *Journal of Employment Counseling*, *45*(2), 61–66.

Knouse, S., Tanner, J., & Harris, E. (1999). The relation of college internships, college performance, and subsequent job opportunity. *Journal of Employment Counseling*, *36*(1), 35–43.

Koch, R. (2017). On the future of cybersecurity. In *ICMLG 2017 5th International Conference on Management Leadership and Governance* (p. 202). Academic Conferences and Publishing Limited.

Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. In *Digital policy, regulation and governance*.

Kumar, S., Velliangiri, S., Karthikeyan, P., Kumari, S., Kumar, S., & Khan, M. K. (2021). A survey on the blockchain techniques for the Internet of Vehicles security. *Transactions on Emerging Telecommunications Technologies*, e4317.

Kwan, L., Ray, P., & Stephens, G. (2008, January). Towards a methodology for profiling cyber criminals. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*. IEEE (p. 264).

Lachow, I. (2011). The Stuxnet enigma: Implications for the future of cybersecurity. *Georgetown Journal of International Affairs*, 118–126.

Landwehr, C. (2008, September/October). Cybersecurity and artificial intelligence: From fixing the plumbing to smart water. In *IEEE, Security and privacy* (p. 3).

Lapena, R. (2017). *Survey says: Soft skills highly valued by security team*. Retrieved from https://www.tripwire.com/state-of-security/featured/survey-says-soft-skills-highly-valued-security-team/

Li, Z. (2020). Seven cybersecurity considerations. In *Routledge handbook of international cybersecurity*.

Liu, F., & Tu, M. (2020). An analysis framework of portable and measurable higher education for future cybersecurity workforce development. *Journal of Education and Learning (EduLearn)*, *14*(3), 322–330.

Martellini, M., Abaimov, S., Gaycken, S., & Wilson, C. (2017). Future attack patterns. In *Information security of highly critical wireless networks* (pp. 59–62). Cham: Springer.

Mathew, A. (2021). Artificial intelligence for offence and defense-the future of cybersecurity. *Educational Research*, *3*(3), 159–163.

Maughan, D., Balenson, D., Lindqvist, U., & Tudor, Z. (2015). Government-funded R&D to drive cybersecurity technologies. *IT Professional*, *17*(4), 62–65.

McBride, S., Schou, C., & Slay, J. An initial industrial cybersecurity workforce development framework.

McDonough, B. R. (2018). *Cyber smart: Five habits to protect your family, money, and identity from cyber criminals*. Hoboken, NJ: John Wiley & Sons.

McDuffie, E. L., & Piotrowski, V. P. (2014). The future of cybersecurity education. *IEEE Annals of the History of Computing*, *47*(08), 67–69.

McQuaid, P. A., & Cervantes, S. (2019). How to achieve a seasoned cybersecurity workforce. *Software Quality Professional*, *21*(4).

Milošević, Đ. M. (2022). Frequent occurring forms of internet frauds. *Baština*, (56), 209–227.

Miranda-Calle, J. D., Reddy, V., Dhawan, P., & Churi, P. (2021). Exploratory data analysis for cybersecurity. *World Journal of Engineering*, *18*(5), 734–749.

Molloy, I., Rao, J. R., & Stoecklin, M. P. (2021, April). AI vs. AI: Exploring the intersections of AI and cybersecurity. In *Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics* (p. 1).

Momani, A. M., & Jamous, M. (2017). The evolution of technology acceptance theories. *International Journal of Contemporary Computer Research (IJCCR)*, *1*(1), 51–58.

Morel, B. (2011, October). Artificial intelligence and the future of cybersecurity. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence* (pp. 93–98).

Morgan, S. (2015). *Cybersecurity market reaches $75 billion in 2015; Expected to reach $170 billion by 2020*. Retrieved from https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/?sh=16f0a0ba30d6

Mpuru, L., & Kgoale, C. (2019). Cybercrime-biggest cyberthreats in future? *Servamus Community-based Safety and Security Magazine*, *112*(10), 22–23.

Murray, G., Johnstone, M. N., & Valli, C. (2017). *The convergence of IT and OT in critical infrastructure*.

Nakamoto, S. (2008). *Bitcoin whitepaper*. Retrieved from https://bitcoin.org/bitcoin.pdf. Accessed on July 17, 2019.

Nelson, R. R. (1994). The co-evolution of technology, industrial structure, and supporting institutions. *Industrial and Corporate Change*, *3*(1), 47–63.

Newhouse, W., et al. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST Special Publication 800.2017 (2017), 181.

Newhouse, B., Keith, S., Scribner, B., & Witte, G. (2016). Nice cybersecurity workforce framework (ncwf). Draft NIST Special Publication 800, 181, 800-181.

Nye, J. (2018). *How will new cybersecurity norms develop?*, Project Syndicate.

Oxford Analytica. Connected cars have a large cybersecurity risk surface. Emerald Expert Briefings (oxan-db).

Oxford Analytica. Prospects for cybersecurity to end-2020. Emerald Expert Briefings (oxan-db).

Oxford Analytica. (2016). Cybercrime is set for global growth. Emerald Expert Briefings (oxan-db).

Peng, Y., Lu, T., Liu, J., Gao, Y., Guo, X., & Xie, F. (2013). Cyber-physical system risk assessment. In *Proceedings - 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IIH-MSP 2013. doi:10.1109/IIH-MSP.2013.116

Perry, A. M. (2019). *Black workers are being left behind by full employment*. Retrieved from https://www.brookings.edu/blog/the-avenue/2019/06/26/black-workers-are-being-left-behind-by-full-employment/

Ponemon. (2019). *Cost of a data breach report*. Retrieved from https://www.ibm.com/downloads/cas/RDEQK07R

Quade, P. (2019). *The digital big bang: The hard stuff, the soft stuff, and the future of cybersecurity*.

Rai, M., & Mandoria, H. (2019). A study on cyber crimes cyber criminals and major security breaches. *International Research Journal of Engineering Technology*, 6(7), 1–8.

Raj, R. K., Ekstrom, J. J., Impagliazzo, J., Lingafelt, S., Parrish, A., Reif, H., & Sobiesk, E. (2017, October). Perspectives on the future of cybersecurity education. In *2017 IEEE Frontiers in Education Conference (FIE)* (pp. 1–2). IEEE.

Ray, L. (2017). Survey says: Soft skills highly valued by security team. Retrieved from https://www.tripwire.com/state-of-security/featured/survey-says-soft-skills-highly-valued-security-team/

Richet, J. L. (2013). From young hackers to crackers. *International Journal of Technology and Human Interaction (IJTHI)*, *9*(3), 53–62.

Richet, J. L. (2015). How to become a cybercriminal?: An explanation of cybercrime diffusion. In *Human behavior, psychology, and social interaction in the digital era* (pp. 229–240).

Rogers, K. (2019, November 1). Jobs: Companies struggle to find skilled cybersecurity workers as attacks intensify. Retrieved from https://www.cnbc.com/2019/11/01/jobs-companies-need-cybersecurity-workers-asattacks-intensify.html

Roohani, S. J., & Zheng, X. (2019). Using ten teaching modules and recently publicized data-breach cases to integrate cybersecurity into upper-level accounting courses. In *Advances in accounting education: Teaching and curriculum innovations*. Bingley: Emerald Publishing Limited.

Rose, L. A. (2021). Bridging the realms between cyber and physical: Approaching cyberspace with an interdisciplinary lens.

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016, June). Cybercriminals, cyberattacks and cybercrime. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1–9). IEEE.

Saleem, J., Islam, R., & Kabir, M. A. (2022). The anonymity of the dark web: A survey. *IEEE Access*, *10*, 33628–33660.

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *7*(1), 1–29.

Savino, J. O., & Turvey, B. E. (Eds.). (2011). *Rape investigation handbook*. Academic Press.

Schehl, M. (2019). NPS intern prepares to take on next-gen cybercriminals.

Schiks, J. A., van de Weijer, S. G., & Leukfeldt, E. R. (2022). High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals. *Computers in Human Behavior*, *126*, 106985.

Seals, B. (2019). PELP fall speaker series addresses the future of cybersecurity.

Segal, A., Akimenko, V., Giles, K., Pinkston, D. A., Lewis, J. A., Bartlett, B., . . . Noor, E. (2020). The future of cybersecurity across the Asia-Pacific. *Asia Policy*, *15*(2), 57–59.

Sharma, A. C., Gandhi, R. A., Mahoney, W., Sousan, W., & Zhu, Q. (2010, August). Building a social dimensional threat model from current and historic events of cyber attacks. In *2010 IEEE Second International Conference on Social Computing* (pp. 981-986). IEEE.

Sharma, R., & Mishra, R. (2014). A review of evolution of theories and models of technology adoption. *Indore Management Journal*, *6*(2), 17–29.

Sharp Sr, W. G. (2010). The past, present, and future of cybersecurity. *Journal of National Security Law & Policy*, *4*, 13.

Silverstein, J. (2019). *Hundreds of millions of Facebook user records were exposed on Amazon cloud server*. Retrieved from https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/

Singapore's Cybersecurity Strategy. (2016). CSA Singapore, 10 October. Retrieved from www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

Skertic, J. (2021). Cybersecurity legislation and ransomware attacks in the United States, 2015–2019.

Smith, Z. M., Lostri, E., & Lewis, J. A. (2020). The hidden costs of Cybercrime. McAfee. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-ofcybercrime.pdf

Sobel, A., Parrish, A., & Raj, R. K. (2019). Curricular foundations for cybersecurity. *Computer*, *52*(3), 14–17.

Sommer, P., & Brown, I. (2011, January 14). *Reducing systemic cybersecurity risk*. Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS(2011)3. Available at SSRN; Retrieved from https://ssrn.com/abstract=1743384

Souppaya, M., Scarfone, K., & Dodson, D. (2021). Secure software development framework (SSDF) Version 1.1: Recommendations for mitigating the risk of software vulnerabilities (No. NIST Special Publication (SP) 800-218 (Draft)). National Institute of Standards and Technology.

Stempfley, B. (2019). *The future of cybersecurity*. Pittsburgh PA: Carnegie Mellon University.

Sukhai, N. B. (2004, October). Hacking and cybercrime. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 128–132).

Sulek, D., Moran, N., & Principal, B. A. H. (2009). What analogies can tell us about the future of cybersecurity. In *The virtual battlefield: Perspectives on cyber warfare* (Vol. 3, pp. 118–131).

Summit, H. B. C. U., Platform, N. L., Polls, N. Q., Briefs, N. A. C. E., & Market, J. (2017). The positive implications of internships on early career outcomes. *NACE Journal.*

Szyliowicz, J. S., & Zamparini, L. (2014). *Maritime security: Issues and challenges. Maritime transport security*, 13–23.

Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. *EAI Endorsed Transactions on Creative Technologies*, *8*(28), e3–e3.

Terry, I. (2017). The future of cybersecurity regulations: 2017 New York DFS changes.

10 Skills and attributes of a successful cybersecurity pro. (2021). Terranovasecuirty.com. Retrieved from https://terranovasecurity.com/10-attributes-of-a-natural-born-cyber-security-professional/

Top 11 Most Powerful CyberSecurity Software Tools In 2022. (2022, July). Softwaretestinghelp.com. Retrieved from https://www.softwaretestinghelp.com/cybersecurity-software-tools/

Vaishy, S., & Gupta, H. (2021, September). Cybercriminals' motivations for targeting government organizations. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (pp. 1–6). IEEE.

Van Hardeveld, G. J., Webber, C., & O'Hara, K. (2017). Deviating from the cybercriminal script: Exploring tools of anonymity (mis) used by carders on cryptomarkets. *American Behavioral Scientist*, *61*(11), 1244–1266.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. doi:10.1016/j.cose.2013.04.004

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, *35*(1), 155–186.

Wang, P., & Sbeit, R. (2020). A comprehensive mentoring model for cybersecurity education. In *17th International Conference on Information Technology–New Generations (ITNG 2020)* (pp. 17–23). Springer, Cham.

Waters, J. (2020). 5G 101 guide: What it is and what it's not (and why). *Future Tech 360*. Retrieved from https://futuretech360.com/articles/2020/04/14/5g-101-guide.aspx

Watters, P. A., McCombie, S., Layton, R., & Pieprzyk, J. (2012). Characterising and predicting cyber attacks using the cyber attacker model profile (CAMP). *Journal of Money Laundering Control*, *15*(4), 430–441.

What is quantum computing? (2021). IBM.com. Retrieved from https://www.ibm.com/topics/quantum-computing

What is the deep and dark web? (2022). *Kasperky.com*. Retrieved from https://www.kaspersky.com/resource-center/threats/deep-web

What is Hardware and Software Security? (2022, June). *Wheelhouse.com*. Retrieved from https://www.wheelhouse.com/resources/what-is-hardware-and-software-security-a11018#gref

What is the Internet of Vehicles (IoV). (2022). *EasternPeak.com*. Retrieved from https://easternpeak.com/definition/internet-of-vehicles-iov/

What is IOT. (2022). *Oracle.com*. Retrieved from https://www.oracle.com/internet-of-things/what-is-iot/

What's the role of HR in cybersecurity and why is it important. (2021). *You.com*. Retrieved from https://www.yoh.com/blog/whats-the-role-of-hr-in-cybersecurity-and-why-is-it-important

What is a Zero Trust Architecture. (2021). *PaloAltoNetworks.com*. Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and organization*, *16*(4), 304–324.

Wood, B. J. (2000). *An insider threat model for adversary simulation*. Albuquerque: SRI International, Cyber Defense Research Center. System Design Laboratory.

Yadav, K., Sethi, A., Kaur, M., & Perakovic, D. (2022). Machine learning for malware analysis: Methods, challenges, and future directions. In *Advances in malware and data-driven network security* (pp. 1–18). Hershey, PA: IGI Global.

Yampolskiy, R. V. (2019). Predicting future AI failures from historic examples. *Foresight*.

Yar, M. (2005). The novelty of 'Cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427.

Yusuf Enoch, S., Ge, M., Hong, J. B., & Kim, D. S. (2021). Model-based cybersecurity analysis: Past work and future directions. arXiv e-prints arXiv-2105.

Yu, S., Zhou, W., Dou, W., & Makki, S. K. (2012, June). Why it is hard to fight against cyber criminals? In *2012 32nd International Conference on Distributed Computing Systems Workshops* (pp. 537–541). IEEE.