From cybercrime to cyborg crime

van der Wagen, Wytske

References

- Agee, J. (2009). Developing qualitative research questions: a reflective process. *International Journal of Qualitative Studies in Education*, *22*(4), 431-447.
- Akrich, M. (1992). The De-scription of Technological Objects. In W.E. Bijker & J. Law (Eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change* (pp. 205-224). Cambridge, MA: MIT Press.
- Akrich, M. & Latour, B. (1992). A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies. In W.E. Bijker & J. Law (Eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change* (pp. 259-264). Cambridge, MA: MIT Press.
- Balzacq, T. & Dunn Cavelty, M.D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176-198.
- Bauman, Z. (2000), *Liquid Modernity*. Cambridge: Polity.
- Baxter, P. & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The qualitative Report*, *13*(4), 544-559.
- Becker, H.S. (1963). *Outsiders. Studies in the Sociology of Deviance*. New York: The Free Press.
- Benschop, A. (2013). *Cyberoorlog. Slagveld Internet.* Utrecht: Ef & Ef Media.

- Bilge, L., Balzarotti, D. Robertson, W. K., Kirda, E. & Kruegel, C. (2012). Disclosure: detecting botnet command and control servers through large-scale netflow analysis. In *ACSAC* (pp. 129-138). ACM.
- Blankwater, E. (2011). *Hacking the field. An ethnographic and historical study of the Dutch hacker field*. Sociology Master's Thesis. University of Amsterdam.
- Blok, A. & Jensen, T.E. (2011). *Bruno Latour. Hybrid thoughts in a hybrid world.* London/New York: Routledge.
- Blumer, H. (1954). What is Wrong with Social Theory? *American Sociological Review, 19*(1), 3-10.
- Bossler, A.M. & Holt, T.J. (2009). On-Line Activities, Guardianship and Malware Infection: An examination of Routine Activity Theory. *International Journal of Cyber Criminology, 3*(1), 400-420.
- Bossler, A.M. & Holt, T.J. (2011). Malware Victimization: a Routine Activities Framework. In K. Jaishanker (Ed.), *Cybercriminology: Exploring Internet Crime and Criminal Behaviors* (pp. 317-346). CRC Press.
- Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies.* Oxford University Press.
- Bourne, M. (2012). Guns don't kill people, cyborgs do: a Latourian provocation for transformatory arms control and disarmament. *Global Change, Peace & Security*, *24*(1), 141-163.
- Brenner, S.W. (2002). Organized cybercrime. How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology, 4*(1), 1-50.

- Brenner, S. (2007). *Law in an Era of Smart Technology*. Oxford: Oxford University Press.
- Brown, S. (2006). The Criminology of Hybrids. Rethinking Crime and Law in Technosocial Networks. *Theoretical Criminology*, *1*(4), 223-244.
- Burden, K., & Palmer, C. (2003). Cyber crime - a new breed of criminal? *Computer Law and Security Report, 19*(2), 222–227.
- Cairncross, F. (2001). *The Death of Distance. How the Communications Revolution is Changing our Lives.* Boston: Harvard Business School Press.
- Callon, M. (1986). The sociology of an actor-network: The case of the electric vehicle. In M. Callon, J. Law & A. Rip (Eds.), *Mapping the dynamics of science and technology* (pp. 19-34). Basingstoke, UK: Macmillan Press.
- Callon, M. (1999). Actor-Network Theory – the market test. *The Sociological Review*, 47(1), 181-195.
- Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social and Legal Studies, 10*(2), 229-242.
- Casey, E. (2011). *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet.* San Diego/London: Elsevier Inc.
- Castells, M. (2001). *The Internet Galaxy: Reflections on the internet, business, and society*. Oxford: Oxford University Press.
- Castells, M. (2009). *Communication Power*. New York: Oxford University Press.

- Charmaz, K. (2006). *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis.* London: Sage Publications.
- Chandler, A. (1996). The Changing Definition and image of hackers in popular discourse. *International Journal of the Sociology of Law, 24*(2), 229-251.
- Choo, K-K.R. (2008). Organized crime groups in cyberspace: a typology. *Trends in Organized Crime*, *11*, 270-295.
- Churchill, D. (2016). Security and Visions of the Criminal: Technology, Professional Criminality and Social Change in Victorian and Edwardian Britain. *British Journal of Criminology, 56*(5), 857-876.
- Clarke, R.V. & Cornish, D.B. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Springer-Verlag.
- Clynes, M.E., & Kline N.S. (1960). Cyborgs and Space. *Astronautics, 5*(9), 26-27.
- Cohen, L.E. & Felson, M. (1979). Social Change and Crime Rates Trends: A Routine Activity Approach, *American Sociological Review*, *44*(4), 588-608.
- Cole, A., Mellor, M. & Noyes, D. (2007). Botnets: The rise of the machines. In Proceedings on the 6th Annual Security Conference (pp. 1-14).
- Consoli, L. & Hoekstra, R. (2008). Inleiding. In I.L. Consolie & R. Hoekstra (Eds.), *Annalen van het Thijmgenootschap* (pp. 7-13). Nijmegen: Valkhof Pers.
- Cross, C. (2013). "Nobody's holding a gun to your head." Examining current discourses surrounding victims of online

fraud. In K. Richards & J. Tauri (Eds.), *Crime, Justice and Social Democracry: Proceedings of the 2nd International Conference* (pp. 25-32). Brisbane: Queensland University of Technology.

- Dant, T. (2004). The Driver-car. *Theory, Culture & Society*, *21*(4/5), 61-79.
- Deibert, R. & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *Papers from the British Criminology Conference*, *8*, 3-17.
- De Graaf, D., Shosha, A.F. & Gladyshev, P. (2013). Bredolab: shopping in the cybercrime underworld.' In M. Rogers & K.C. Seigfried-Spellar (Eds.), *Digital Forensics and Cybercrime* (pp. 302-313). 4th International Conference, ICDF2C 2012. Springer, available online at http://ulir.ul.ie/handle/10344/2896.
- Demant, J. & Dilkes Frayne, E. (2015). Situational Crime Prevention in Nightlife Spaces. In D. Robert & M. Dufresne (Eds.), *Actor-Network Theory and Crime studies. Explorations in Science and Technology* (pp. 5-19). London/New York: Ashgate.
- De Mul, J. (2002). *Cyberspace Odysee*. Kampen: Klement.
- De Laet, M. & Mol, A. (2000). The Zimbabwe Bush Pump: Mechanics of a Fluid Technology, *Social Studies of Science, 30*(2), 225–263.
- Deleuze, G. & Guatarri, F. (1987). *A Thousand Plateaus: Capitalism and schizophrenia*. Minneapolis: University of Minnesota Press.
- Deseriis, M. (2017). Hacktivism: On the Use of Botnets in Cyberattacks. *Theory, Culture & Society*, *34*(4), 131-152.

- Dolwick, J.S. (2009). 'The Social' and Beyond: Introducing Actor-Network Theory. *J Mart Arch*, 4, 21-49.
- Douillet, A-C & Dumouline, L. (2015). Actor Network Theory and CCTV Development. In D. Robert & M. Dufresne (Eds.), *Actor-Network Theory and Crime studies. Explorations in Science and Technology* (pp. 21-35). London/New York: Ashgate.
- Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime Law & Social Change, 67*, 97-116.
- Feenan, D. (2002), Legal Issues in Acquiring Information about Illegal Behaviour Through Criminological Research. *British Journal of Criminology*, *42*(4), 762–81.
- Ferrell, J. (1996). *Crimes of Style: Urban Graffiti and the Politics of Criminality*. Boston: North-eastern University Press.
- Ferrell, J. (1997). Criminological Verstehen: Inside the immediacy of crime. *Justice Quarterly, 14*(1), 3-23.
- Finch, E. (2001), Issues of Confidentiality in Research into Criminal Activity: the Legal and Ethical Dilemma. *Mountbatten Journal of Legal Studies*, *1*(2), 34–50.
- Flyvbjerg, B. (2013). Case Study. In N.K. Denzin & Y.S. Lincoln (Eds.), *Strategies of Qualitative Inquiry* (pp. 169-203). Thousand Oaks: Sage.
- Forlano, L. & Jungnickel, K. (2015). Hacking Binaries/Hacking Hybrids: Understanding the Black/White Binary as a Socio-technical Practice. *Ada: A Journal of Gender, New Media and*

Technology, 6, available online at http://adanewmedia.org/2015/01/issue6-forlano-jungnickel/.

- Franko Aas, K. (2006). 'The body does not lie': Identity, risk and trust in technoculture. *Crime Media Culture*, *2*(2), 143-158.
- Franko Aas, K. (2007). Beyond 'The Desert of The Real': Crime Control in a Virtual(ised) Reality. In Y. Jewkes (Ed.), *Crime Online* (pp. 160-178). Collumpton: Willan Publishing.
- Franko Aas, K. (2010). Beyond 'The desert of the Real': Crime Control in a Virtual(sed) reality. In C. Greer (Ed.), *Crime and Media. A reader* (pp. 551-564). London/New York: Routledge.
- Franko Aas, K. (2015). Preface. In D. Robert & M. Dufresne (Eds.), *Actor-Network Theory and Crime studies. Explorations in Science and Technology* (pp. 9-13). London/New York: Ashgate.
- Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. London: Addison-Wesley.
- Gad, C. & Jensen, C.B. (2010). On the Consequences of Post-ANT. *Science, Technology & Human Values*, *35*(1), 55-80.
- Gaggi, S (2003). The Cyborg and the Net: Figures of the Technological Subject. *Bucknell Review: A Scholarly Journal of Letters, Arts and Sciences*, *46*(2), 125-139.
- Garfinkel, H. (1967). *Studies in Ethnomethodology*. Englewood Cliffs, NJ: Prentice-Hall Inc.
- Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal in Computer Virology*, *6*(1), 77-90.
- Geertsema, H.G. (2006). Cyborg: Myth or Reality? *Zygon, 41*(2), 289-327.

- George, A.L, & Bennett, A. (2005). *Case studies and theory development in the social sciences*. Cambridge, MA: MIT Press.
- Gerring, J. (2004). What is a case study and what is it good for? *The American Political Science Review*, *98*(2), 341-354.
- Giese, L. (2008). How material are cyberbodies? Broadband Internet and embodied subjectivity. *Crime Media Culture*, *4*(3), 311-330.
- Glaser, B.G. & Strauss, A.L. (1967). *The discovery of Grounded Theory: strategies for qualitative research*. Chicago: Aldine Publishing Co.
- Goffman, E. (1959). *The presentation of self in everyday life.* London: Penguin Books.
- Goffman, E. (1963). *Stigma. Notes on the Management of Spoiled Identity.* Englewood Cliffs: Prentice-Hall.
- Goldschmidt, A. & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112-130.
- Goodman, M. (2010). *Future Crime. Inside the digital underground and the battle for our connected world*. London: Transworld Publishers.
- Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.
- Gottfredson, M. & Hirschi, T. (1990). *A general theory of crime*. Stanford CA: Stanford University Press.
- Gough, N. (2004). RhizomANTically Becoming-Cyborg. Performing posthuman pedagogies. *Educational Philosophy and Theory, 36*(3), 253-265.

- Graboski, P. (2001). Virtual criminality: old wine in new bottles? *Social & Legal Studies, 10*(2), 243-249.
- Guga, J. (2015). Cyborg Tales: The Reinvention of the Human in the Information Age. In J. Romportl, E. Zackova & J. Kelemen (Eds.), *Beyond Artificial Intelligence. Topics in Intelligent Engineering and Informatics* (pp. 45-62). Springer, Cham.
- Guinchard, A. (2010). Crime in virtual worlds: The limits of criminal law. *International Review of Law, Computers & Technology*, *24*(2), 175-182.
- Gunkel, D. (2001). *Hacking Cyberspace.* Boulder, CO: Westview Press.
- Halbert, D. (1997). Discourses of Danger and the computer hacker. *The Information Society, 13*(4), 361-374.
- Hall, M. (2011). Environmental Victims. Challenges for Criminology in the 21st Century. *Journal of Criminal Justice and Security*, 13(4), 345-371.
- Halsey, M. & White, R. (1998). Crime, Ecophilosophy and Environmental Harm. *Theoretical Criminology*, *2*(3), 371-391.
- Haggerty, K.D. & Ericson, R.V. (2000). The surveillant assemblage. *British Journal of Sociology*, 51(4), 605-622.
- Haraway, D.J. (1987). A Manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, *2*(4), 1-42.
- Haraway, D.J. (1991). *Simians, Cyborgs and Women: The reinvention of nature*. New York: Routlegde.

- Harman, G. (2009). *Prince of Networks: Bruno Latour and Metaphysics*. Melbourne: Re-pres & Graham Harman.
- Harvey, D. (1989). *The condition of postmodernity.* Oxford: Blackwell.
- Hayward, K. (2002). The vilification and pleisures of youthful transgression. In J. Muncie, G. Hughes & E. McLaughlin (Eds.), *Youth Justice: Critical Readings* (pp. 80-93). London: Sage.
- Hayward, K. (2012). Five Spaces of Criminology. *British Journal of Criminology*, *52*(3), 441-462.
- Hennink, M., Hutter, I. & Bailey, A. (2011). *Qualitative Research Methods*. London: Sage.
- Himanen, P. (2001). *The Hacker Ethic and the Spirits of the Information Age*. New York: Random House.
- Hindelang, M.J., Gottfredson, M.R. & Garofalo, J. (1978). *Victims of personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Cambridge, MA: Ballinger Publishing Co.
- Hinduja, S. (2012). The Heterogeneous Engineering of Music Piracy: Applying Actor-Network Theory to Internet-Based wrongdoing. *Policy and Internet, 4*(3-4), 229-248.
- Holt, T.J. (2010). Examining the role of Technology in the Formation of Deviant Subcultures. *Social Science Computer review*, *28*(4), 466-481.
- Holt, T.J. & Bossler, A.M. (2014). An Assessment of the current state of cybercrime scholarship. *Deviant behavior*, *35*(1), 20-40.
- Holt, T.J., Bossler A.M. & Seigfried-Spellar, K.C. (2015). *Cybercrime and digital forensics. An Introduction*. New york: Routledge.

- Holt, T.J. & Kilger, M. (2008). Techcrafters and Makecrafters: a comparions of two populations of hackers. WOMBAT *Workshop On Information Security Threats Data Collection and Sharing,* 67-78.
- Hutchings, A. & Hayes, H. (2009). Routine activity theory and phishing victimization: Who gets caught in the 'net'? *Current Issues in Criminal Justice 20*(3), 432-451.
- Hutchings, A. & Holt, T.J. (2016). The online stolen data market: disruption and intervention approach. *Global Crime*, *18*(1), 11-30.
- Ienca, M. (2015). Neuroprivacy, Neurosecurity and Brain-hacking: Emerging issues in Neural Engineering. *Bioethica Forum, 8*(2), 51-53.
- Ihde, D. (1990). *Technology and the Lifeworld*. Bloomington/Minneapolis: Indiana University Press.
- Iliopoulos, D., Szor, C. & Adami, P. (2011). *Darwin Inside the Machines. Malware Evolution and the Consequences for Computer Security*, available online at: arXiv:1111.2503v1
- Israel, M. (2004). Strictly Confidential? Integrity and Disclosure of Criminological and Socio-Legal Research. *British Journal of Criminology*, *5*(1), 715-740.
- Jaishankar, K. (Ed.). (2011). *Cyber criminology: Exploring Internet crimes and criminal behavior*. Boca Raton, FL: CRC Press.
- Jansen, J. & Leukfeldt, R. (2016). Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology*, *10*(1), 79-91.

- Jennings W.G., Piquero, A.R. & Reingle, J.M. (2012). On the overlap between victimization and offending: A review of the literature. *Aggression and Violent Behavior*, *17*(1), 16-26.
- Jewkes, Y. & Yar, M. (Eds.) (2010). *The Handbook of Internet Crime*. Routledge.
- Jordan, T. & Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review*, *46*(4), 757-780.
- Katz, J. (1988). *The Seductions of Crime: Moral and Sensual Attraction in Doing Evil*. New York: Basic Books.
- Kearon, T. & Leach, R. (2000). Invasion of the 'Body Snatchers': Burglary Reconsidered. *Theoretical Criminology*, *4*(4), 451-472.
- Kerstens, J. & Veenstra, S. (2015). Cyber Bullying in the Netherlands: A Criminological Perspective. *International Journal of Cybercriminology*, *9*(2), 144-161.
- Kilger, M. (2010). Social Dynamics and the Future of Technology-Driven Crime. In T.J. Holt & B. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 2015). Hershey, PA: IGI-Global.
- Kipnis, A.B. (2015). Agency between humanism and posthumanism. *Hau: Journal of Ethnographic Theory*, *5*(2), 43-58.
- Kitchin, R. & Dodge, M. (2011). *Code/Space: Software and Everyday Life*. Cambridge. MA: MIT Press.
- Kleemans, E., Weerman, F. & Enhus, E. (2007). Theoretische vernieuwing in de criminologie. *Tijdschrift voor Criminologie*, *49*(3), 239- 251.

- Knappett, C. & Malafouris, L. (2008). *Material Agency. Towards a Non-Anthropocentric Approach*. New York: Springer.
- Kollanyi, B., Howard, P.N. & Woolley, S.C. (2016). Bots and automation over Twitter during the U.S. Election. *Comprop Data memo. Available at: http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2016/11/Data-Memo-US-Election.pdf*
- Koops, B.J. (2010). The Internet and its opportunities for cybercrime. In M. Herzog-Evans (Ed.) *Transnational Criminology Manual*. Nijmegen: WLP, 735–754.
- Krarup, T.M. & Blok, A. (2011). Unfolding the social: quasi-actants, virtual theory, and the new empiricism of Bruno Latour. *The Sociological Review*, *59*(1), 42-63.
- Kwakman, N. (2007). De causaliteit in het strafrecht. Het vereiste van condition sine qua non als enige bruikbare criterium. *Nederlands Juristenblad* 827, *16*, 992-999.
- Latour, B. (1992). Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts. In W.E. Bijker & J. Law (Eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change* (pp. 225-258). Cambridge, MA: MIT Press.
- Latour, B, (1986). The powers of association. In J. Law (Ed.), *Power, Action and Belief. A New Sociology of Knowledge?* (pp. 264-280). London: Routledge and Kegan Paul.
- Latour, B. (1987). *Science in Action. How to follow scientists and engineers through society*. Cambridge: Harvard University Press.
- Latour, B. (1993). *We Have Never Been Modern.* Harvester Wheatsheaf.

- Latour, B. (1994). On technical mediation – Philosophy, Sociology, Genealogy. *Common Knowledge*, *3*(2), 29-64.
- Latour, B. (1996). On Actor Network Theory. A few clarifications. *Sociale Welt-Zeitschrift fur Sozialwissenschaftliche forschung und praxis*, *47*(4), 369-381.
- Latour, B. (1999). On recalling ANT. In J. Law and J. Hassard (Eds.), *Actor Network Theory and After* (pp. 15-25). Oxford: Blackwell.
- Latour, B. (2000). When things strike back: a possible contribution of 'science studies' to the social sciences. *British Journal of Sociology*, *51*(1), 107-123.
- Latour, B. (2004). On using ANT for studying information systems: a (somewhat) Socratic dialogue. In C. Avgerou, C. Ciborra & F. Land (Eds.), *The Social Study of Information and Communication Technology. Innovation, Actors and Contexts* (pp. 62-76). Oxford University Press.
- Latour, B. (2005). *Reassembling the Social. An introduction to Actor-Network-Theory*. New York: Oxford University Press.
- Latour, B. (2013). An Inquiry into Modes of Existence. An Anthropology of the Moderns. Harvard University Press.
- Latour, B. & Venn, C. (2002). Morality and Technology: The End of the Means. *Theory Culture Society*, *19*(5/6), 247-260.
- Latour, B. & Woolgar, S. (1986). *Laboratory Life. The Construction of Scientific Facts.* New Jersey: Princeton University Press.
- Law, J. (1992). Notes on the Theory of the Actor-Network: Ordering, Strategy and Heterogeneity. *Systems Practice, 5*(4): 379-393.

- Law, J. (1999). After Ant: Topology, naming and complexity. In J. Law & J. Hassard (Eds.), *Actor Network Theory and After* (pp. 1-14). Blackwell.
- Law, J. (2000). *Networks, Relations, Cyborgs: On the Social Study Of Technology. Centre for Science Studies and the Department of Sociology*, Lancaster University, available online at http://www.comp.lancaster.ac.uk/sociology/soc042jl.html.
- Law, J. (2004). *After method: Mess in Social Science Research*. Routledge.
- Law, J. & Hassard, J. (1999). (Eds.), *Actor Network Theory and After*. Blackwell.
- Lemert, E. (1967). *Human Deviance, Social Problems and Social Control.* Englewood Cliffs: Prentice_Hall.
- Lehman, J. *et al* (2018). *The Surprising Creativity of Digital Evolution: A Collective of Anecdotes from the Evolutionary Computation and Artificial Life Research Communities*, available online at: arXiv:1803.03453
- Leukfeldt, E.R. (2015). Comparing victims of phishing and malware attacks. Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering*, *4*(4), 26-32.
- Leukfeldt, E.R., Domenie, M.M.L & Stol, W.Ph. (2011). Cybercrime is van het volk. Onderzoeksconsequenties voor de beleidsvorming. *Secondant*, *25*(1), 42-45.
- Leukfeldt, E.R., Kleemans, E.R. & Stol, W.Ph. (2016). Cybercriminal Networks, Social Ties and Online Forums: Social Ties versus

Digital Ties Within Phishing and Malware Networks. *British Journal of Criminology*, *57*(3), 704-722.

- Leukfeldt, E.R. & Yar, M. (2016). Applying Routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.
- Levy, S. (1984). *Hackers heroes of the information age.* New York: Double Day.
- Leys, M., Zaitch, Z. & Decorte, T. (2016). De Gevalstudie. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve Methoden en Technieken in de Criminologie* (pp. 161-186). Leuven/Den Haag: Acco.
- Lindgren, S-A. (2005). Social Constructionism and Criminology. Traditions, Problems and Possibilities. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *6*(1), 4-22.
- Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal (Canadian Edition)*, *7*(1), 35-49.
- Lupton, D. (1999). Monsters in Metal Cocoons: 'Road Range' and Cyborg bodies. *Body & Society, 5*(1), 57-72.
- Lyng, S. (2004). Crime, Edgework and Corporeal Transaction. *Theoretical Criminology, 8*(3), 359-375.
- Mähring, M., Holmström, J., & Montealegre, R. (2004). Trojan Actor-Networks and Swift Translation: Bringing Actor-Network Theory to Project Escalation Studies. *Information Technology & People*, *17*(2), 210-238.

- Maimon, D. *et al*. (2015). On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents. *British Journal of Criminology*, *55*(3), 615-634.
- Maimon, D., Kamerdze, A., Cukier, M. & Sobesto, B. (2013). Daily Trends and Origins of Computer-Focused Crimes against a Large University Network. An Application of the Routine-Activities and Lifestyle Perspective. *British Journal of Criminology*, *53*(2), 319-343.
- Mann, D. & Sutton, M. (1998). >>NETCRIME: More Change in the Organization of Thieving. *The British Journal of Criminology, 38*(2), 201-229.
- Martin, A. (2005). Agency in Inter-Action: Bruno Latour and Agency. *Journal of Archaeological Method and Theory*, *12*(4), 283-311.
- Masys A.J. (2014). Critical Infrastructure and Vulnerability: A Relational Analysis Through Actor Network Theory. In Masys A. (eds), *Networks and Network Analysis for Defence and Security* (pp. 265-280). Lecture Notes in Social Networks. Springer, Cham.
- Masys A.J. (2015). The Cyber-Ecosystem Enabling Resilience Through the Comprehensive Approach. In Masys A. (eds) *Disaster Management: Enabling Resilience. Lecture Notes in Social Networks* (pp. 143-154). Springer, Cham
- Matza, D. (1964). *Delinquency and Drift*. New York: John Wiley.

- Matza, D. (1969). *Becoming Deviant.* Englewood Cliffs: Prentice Hall.
- Mead, G.H. (1934). *Mind, Self and Society: From the Standpoint of a Social Behaviorist*. Chicago: Chicago University Press.
- McGuirre, M. (2008). *From hyperspace to hypercrime: Technologies and the geometries of deviance and control* (British Criminology Conference 8). Londen: British Society of Criminology.
- McLean, C. & Hassard, J. (2004). Symmetrical Absence/Symmetrical Absurdity: Critical Notes on the Production of Actor-Network Accounts*, Journal of Management Studies*, *41*(3), 493-519.
- McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice*, *31*(1), 30-52.
- Michalowski R.J. & Kramer, R.C. (2007). State-Corporate Crime and Criminological Inquiry. In H.N. Pontell & G. Geis (Eds.), *International Handbook of White-Collar and Corporate Crime* (pp. 200-219). Springer, Boston, MA.
- Mielke, C. J. & Chen, H. (2008). Botnet and the cybercriminal underground. In *International Conference on Intelligence and Security Informatics 2008* (pp. 206-211). IEEE.
- Milward, H.B. & Raab, J. (2006). Dark Networks as Organizational Problems. Elements of a Theory. *International Public Management Journal*, *9*(3), 333-360.

- Mol, A. (2010). Actor-Network Theory: sensitive terms and enduring tensions. *Kölner Zeitschrift für Soziologie und Sozialpsychologie, 50*(1), 253-269.
- Monsma, E., Buskens, V., Soudijn, M. & Nieuwbeerta, P. (2010). Partners in cybercrime: An online forum evaluated from a social network perspective. *ISCORE papers, 285*, 1-28.
- Moszkowicz, Y. (2009). Een kritische noot bij "Runescape" en "Habbo-hotel"-uitspraken: een illusie is geen goed. *Strafblad*, 495-503.
- Mythen, G & McGowan, W. (2018). Cultural victimology revisited. Synergies of risk, fear and resilience. In S. Walklate (Ed.), *Handbook of Victims and Victimology* (pp. 364-378). London/New York: Routledge.
- Nikitina, S. (2012). Hackers as Trickster of the Digital Age: Creativity in Hacker culture. *Journal of Popular Culture, 45(1)*, 133- 152.
- Nissen, J. (1998). Hackers: Masters of Modernity and Modern Technology. In J. Sefton-Green (Ed.), *Digital Diversions: Youth Culture in the Age of Multimedia* (pp. 149–171). London: UCL Press.
- Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media* Society, *6*(2), 195-217.
- O'Brien, M. (2005). What is Cultural about Cultural Criminology? *British Journal of Criminology*, *45*(5), 599-612.
- Odinot, G., Verhoeven, M.A., Pool, R.L.D & De Poot, C.J. (2016). Chapter II. Cyber-OC in the Netherlands. In G. Bulanova-Hristova

et al. (Eds.), *Cyber-OC-Scope and manifestations in selected EU member states* (pp. 15-99). Bundeskriminalamt Criminalistic Institute.

- O'Neil, M. (2006). Rebels for the system? Virus writers, general intellect, cyberpunk and criminal capitalism, *Continuum: Journal of Media & Cultural studies*, *20*(2), 225-241.
- Overill, R.E. (1998). Trends in Computer Crime. *Journal of Financial Crime*, *6*(2), 157-162.
- Paxton, N.C. Ahn, G-J. & Shehab, M. (2011). Master-Blaster: Identifying Influential Players in Botnet Transactions. In *The 35th Annual Computer Software and Applications Conference* (pp. 413-419). IEEE.
- Pease, K. (2001). Crime futures and foresight. Challenging criminal behavior in the information age. In D. Wall (Ed.), *Crime and the Internet* (pp. 18-28). London: Routlegde.
- Pinch, T. (2010). The Invisible Technologies of Goffman's Sociology From the Merry-go Round to the Internet, *Technology and Culture*, *51*(2), 409-424.
- Pratt, T.C. & Turanovic J.J. (2015). Lifestyle and Routine Activity Theories Revisited: The Importance of "Risk" to the Study of Victimization. *Victims & Offenders*, *11*(3), 335-354.
- Preda, A. (1999). The turn to things: Arguments for A Sociological Theory of Things. *The Sociological Quarterly*, *40*(2), 347-366.
- Reyns, B.W. (2013). Online routines and identity theft victimization further expanding routine activity theory beyond

direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238.

- Rock, P. (2007). Theoretical perspectives on victimization. In S. Walklate, *Handbook of Victims and Victimology* (pp. 37-61). Willan Publishing.
- Sandywell, B. (2010). On the globalization of crime: the Internet and new criminality. In Y. Jewkes & M. Yar (Eds.), *Handbook of Internet Crime* (pp. 38-66). London/New York: Routledge.
- Schinkel, W. (2007). Sociological discourse of the relational: the cases of Bourdieu & Latour. *The Sociological Review*, *55*(4), 707-729.
- Schless, T. & Vranken, H. (2013). Counter Botnet Activities in the Netherlands. A study on organization and effectiveness. In *the 8th International Conference for Internet Technology and Secured Transactions* (pp. 437- 442). IEEE.
- Schuilenburg, M.B. (2015). *The Securization of Society: Crime, Risk and Social Order*. New York: New York University Press.
- Silva, S.S.C., Silva, R.M.P, Pinto, R.C.G. & Salles, R.M. (2012). Botnets: A Survey. *Computer Networks*, *30*, 378-403.
- Silvast, A. & Reunanen, M. (2014). Multiple Users, Diverse Users: Appropriation of Personal Computers by Demoscene Hackers. In G. Alberts & R. Oldenziel (Eds.), *Hacking Europe. From Computer Cultures to Demoscenes* (pp. 151-163). Springer.
- Skibell, R. (2002). The Myth of the Computer Hacker. *Information, Communication and Society*, *5*(3), 336-356.

- Skoudis, E. & Zeltser, L. (2004). Malware Fighting Malicious Code. New Jersey: Prentice Hall.
- Smith, G.J.D., Bennet Moses L & Chan, J. (2017). Challenges of doing criminological research in the big data area: towards a digital and data-driven approach. *British Journal of Criminology*, *57*, 259-274.
- Sørensen, M. H. & Ziemke, T. (2007). Agents Without Agency? *Cognitive Semiotics (special issue)*, 102–124.
- Soudijn, M.R.J. & Zegers, B.C.H.T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, *15*(2-3), 111-129.
- Speer, D.L (2000). Redefining Borders. The Challenges of Cybercrime. *Crime Law & Social Change*, *34*(3), 259-273.
- Stake, R.E. (2008). Qualitative case studies. In N.K. Denzin & Y.S. Lincoln (Eds.), *Strategies of qualitative inquiry* (pp. 119-150). Thousand Oaks, CA: Sage.
- Staring, R. & Van Swaaningen, R. (2016). Kwalitatief onderzoek en criminologische theorie. Over de relatie tussen theorie, onderzoeksvragen en methode. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve Methoden en Technieken in de Criminologie* (pp. 33-80). Leuven/Den Haag: Acco.
- Steinmetz, K.F. (2014). The Greatest Crime Syndicate Since the Gambino's: A Hacker Critique of Government, Law, and Law Enforcement. *Deviant Behavior, 35*(3), 243-261.
- Steinmetz, K.F. (2015) Craft(y)ness. An Ethnographic Study of Hacking. *British Journal of Criminology*, *55*(1), 125-145.

- Steinmetz, K.F. & Gerber, J. (2015). "It Doesn't Have Be This Way": Hacker Perspectives on Privacy. *Social Justice, 41*(3), 29-51.
- Steinmetz, K.F. & Nobles, M.R. (2017). *Technocrime and Criminological Theory*. Routledge.
- Sterling, B. (1993). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Viking: London.
- Strikwerda, L. (2012). Theft of virtual items in online multiplayer computer games: an ontological and moral analysis. *Ethics and Information Technology, 14*(2), 89-97.
- Strikwerda, L. (2015). Present and Future Instances of Virtual Rape in Light of Three Categories of Legal Philosophical Theories on Rape. *Philosophy & Technology*, *28*(4), 491-510.
- Stryker, C. (2012). *Hacking the future: Privacy, Identity and Anonymity on the web*. New York: Cole Stryker.
- Suarez, J.R.P. (2015). *We are Cyborgs: Developing a Theoretical Model for Understanding Criminal Behaviour on the Internet*. Dissertation, University of Huddersfield.
- Suler, J. (2004). The online disinhibition effect. *CyberPsychology and Behavior*, 7(3), 321-326.
- Tarde, G. (1999). *Monadologie et sociologie*, re-edition. Paris: Les empêcheurs de penser en rond.
- Taylor, P.A. (1999). *Hackers. Crime in the digital sublime.* London and New York: Routledge.
- Taylor, P.A. (2005). From Hackers to Hacktivists: Speed bumps on the Global Superhighway? *New Media Society, 7*(5), 625-646.

- Tenebro, G. (2009). The Bredolab Files. Symantec Corporation, available online at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_bredolab_files.pdf
- Thomas, D. (2005). Hacking the body: code, performance and corporeality. *New Media & Society*, *7*(5), 647-662.
- Thomas, D. & Loader, B. (2000). Introduction – Cybercrime: Law enforcement, security and surveillance in the information age. In D. Thomas & B. Loader (Eds.), *Cybercrime: Law enforcement, security and surveillance in the information age.* London: Routledge.
- Tombs, S. (2017). Mitigating and Responding to Corporate Violence: Beyond Crime and Criminology. In A. Amatrudo (Eds.), *Social Censure and Critical Criminology* (pp. 217-245). London: Palgrave Macmillan.
- Tropina, T. (2016). The nexus of information technologies and illicit financial flows. *ERA Forum*, DOI 10.1007/s12027-016-0435-2.
- Turgeman-Goldschmidt, O. (2005). Hacker's Accounts: Hacking as a Social Entertainment. *Social Science Computer Review, 23*(1), 8-23.
- Turgeman-Goldschmidt, O. (2008). Meanings that Hackers Assign to their Being a Hacker. *International Journal of Cyber Criminology, 2*(2), 382-396.

- Turkle, S. (1982). The Subjective Computer: A Study in the Psychology of Personal Computation. *Social Studies of Science, 12*, 173-205.
- Turkle, S. (1984). Hackers: Loving the Machine for Itself. In *The Second Self: Computers and the Human Spirit* (pp.196-238). New York: Simon & Schuster.
- Turkle, S. (1995). *Life on the screen: Identity in the age of the Internet*. New York: Simon & Schuster.
- Turkle, S. (2005). *The Second Self: Computers and the Human Spirit*. Cambridge, MA: MIT press.
- Van Baar, A. & Huisman, W. (2012). The Oven Builders of The Holocaust. A Case Study of Corporate Complicity in International Crimes. *British Journal of Criminology*, *52,* 1033-1050.
- Van de Bunt, H. (2015). Ethische dilemma's bij criminologisch onderzoek. Tijdschrift over Cultuur en Criminaliteit, *5*(1), 55-69.
- Vandenberghe, F. (2002). Reconstructing Humants: A Humanist Critique of Actant-Network Theory, *Theory, Culture Society*, *19*(5/6), 51-67.
- Van de Port, M. (2001). G*eliquideerd: criminele afrekeningen in Nederland*. Amsterdam: Meulenhof.
- Van der Hulst, R.C. & Neve, R.J.M. (2008). *High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie.* Den Haag: Wetenschappelijk Onderzoek-en Documentatiecentrum.
- Van der Wagen, W. (2018/*forthcoming*). The Cyborgian Deviant: An Assessment of the Hacker through Actor-Network Theory. *Journal of Qualitative Criminal Justice & Criminology*.

- Van der Wagen, W., M. Althoff & Van Swaaningen, R. (2016). De andere 'anderen'. Een exploratieve studie naar processen van labelling van, door en tussen hackers. *Tijdschrift over Cultuur & Criminaliteit, 6*(1), 27-41.
- Van der Wagen, W. & Dimitrova, E. (2018). *Mission Cyborg: Op naar een hybride kijk op (de bestrijding van) cybercriminele (actor)netwerken*. Driebergen: Dienst Landelijke Recherche, report.
- Van der Wagen, W. & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578-595.
- Van der Wagen, W. & Pieters, W (2018/under review). The hybrid victim: Re-conceptualizing high-tech cybervictimization through actor-network theory.
- 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.
- Van Erp. J., Stol, W. & Van Wilsem, J. (2013), Criminaliteit en criminologie in een gedigitaliseerde wereld. *Tijdschrift voor Criminologie, 55*(4), 327-341.
- Van Loon, J. (2002). *Risk and Technological Culture. Towards a sociology of virulence*. London and New York: Routledge Taylor and Francis Group.

- Van't Hof, C. (2015). *Helpende Hackers. Verantwoorde onthullingen in het digitale polderlandschap*. Rotterdam: Uitgeverij Tek Tok.
- Van Wilsem J.A. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2): 115-127.
- Veenstra, S., Zuursteen, R. & Stol, W.Ph. (2016). *Cybercrime among companies. Research into cybercrime victimisation among small and medium-sized enterprises and on-businesses in the Netherlands.* Eleven International Publishing.
- Verbeek P-P. (2005). *What Things Do: Philosophical Reflections on Technology, Agency and Design*. University Park: Pennsylvania State University Press.
- Verbeek, P-P (2008). De grens van de mens. Over de relatie tussen mens en techniek. In I.L. Consolie & R. Hoekstra (Eds.), *Annalen van het Thijmgenootschap* (pp. 14-36). Nijmegen: Valkhof Pers.
- Verbeek, P-P. (2014). Some Misunderstandings About the Moral Significance of Technology. In P. Kroes & P-P. Verbeek (Eds.), *The Moral Status of Technical Artefacts* (pp. 75-88). Dordrecht: Springer.
- Verschuren, P.J.M. (2003). Case study as a research strategy: some ambiguities and opportunities. *International Journal of Social Research Methodology*, *6*(2), 121-139.

- Vicini, A. & Brazal, A.M. (2015). Longing for Transcendence: Cyborgs and Trans- and Posthumans. *Theological Studies*, *76*(1), 148-165.
- Von Hentig, H. (1940). Remarks on the interaction of perpetrator and victim. *Journal of Criminal Law and Criminology, 31*(3), 303-309.
- Von Hentig, H. (1948). *The Criminal and His Victim*. Hamden, CT: Archon Books.
- Wall, D.S. (2007). *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge, UK: Polity Press.
- Wall, D.S. (2008). Cybercrime and the Culture of Fear. Social Science Fiction(s) and the Production of Knowledge about Cybercrime. *Information, Communication & Society, 11*(6), 861-884.
- Wagenaar, P. (2012). *Detecting botnets using file system indicators*, Master Thesis*,* University of Twente, Enschede.
- Webber, C. & Vass, J. (2010). Crime, film and the cybernetic imagination. In Y. Jewkes & M. Yar (Eds.), *The Handbook of Internet Crime* (pp. 120-144). London/New York: Routledge.
- Wessells, A.T. (2007). Reassembling the Social: An Introduction to Actor-Network Theory by Bruno Latour (book review). *International Public Management Journal*, *10*(3), 351-356.
- Whitson, J.R. & Haggerty, K.D. (2008). Identity Theft and the care of the virtual self. *Economy and Society*, *37*(4), 572-594.

- Wouters, K., Loyens, K., Maesschalck, J. & De Schrijver, A. (2004). Morele dilemma's bij criminologisch onderzoek. *Panopticon: Tijdschrift voor Strafrecht, Criminologie en Forensisch Welzijnswerk*, *35*(4), 313-335.
- Wood, M. (1998). Agency and Organization: Toward a Cyborg-Consciousness. *Human Relations*, *51*(10), 1209-1226.
- Wood, M.A. (2017). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's technological unconscious. *Theoretical Criminology*, *21*(2), 168-185.
- Yar, M. (2005a). The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427.
- Yar, M. (2005b). Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal, 44*(4), 387-399.
- Yar, M. (2012). Sociological and Criminological Theories in the Information Era. In E.R. Leukfeldt & W.Ph Stol (Eds.), *Cyber Safety: An Introduction* (pp. 45-55). The Hague: Eleven International Publishing.
- Yar, M. (2013). *Cybercrime and society*. Thousand Oaks, CA: Sage.
- Yip, M., Shadbolt, N. & Webber, C. (2012). Structural analysis of online criminal social networks. In *International Conference on Intelligence and Security Informatics* (pp. 60–65). IEEE.