



CANVAS – Constructing an Alliance for Value-driven Cybersecurity

Commented Literature lists

CANVAS Briefing Packages

Compiled by

Eva Schlehahn

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

The CANVAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540.

This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

Content

Brief introduction to the CANVAS literature lists.....	3
1. Cybersecurity and Ethics	4
2. Cybersecurity and Law	22
Cybersecurity delimitation and regulation challenges, controversies.....	22
Cybersecurity and criminal justice	26
Cybersecurity, privacy and the European data protection framework.....	27
Academic sources.....	27
Legislation.....	28
Case law and policy documents	28
Non-European and national legislation, case law and policy documents.....	29
3. Attitudes and Options regarding cybersecurity	31
Books and articles.....	31
EU projects	32
Other surveys	34
Legislation and Policy Documents.....	34
European Union.....	34
Other (non-EU)	36
4. Technological challenges in cybersecurity	37
Author recommendations for further reading.....	37
References of White Paper 4.....	38



Brief introduction to the CANVAS literature lists

The commented literature lists provided by the CANVAS project is a vast, cybersecurity focused collection of resources e.g. from academia, case law, and policy/legislation.

These resources were collected by the CANVAS consortium during the creation of four different White Papers as output of the project's research work. Derived from the White Paper's references sections, the literature collection is provided as a stand-alone set in this document for the public, and for free use. Moreover, they have been enriched by more recent publications which became available after the submission of the White Papers.

The complete literature material has been sorted according to these four research topics:

1. Cybersecurity and Ethics
2. Cybersecurity and Law
3. Attitudes and Options regarding cybersecurity
4. Technological challenges in cybersecurity

These topics correspond to the full CANVAS White Papers, which can be found on the project website here: <https://canvas-project.eu/results/whitepapers.html>.

1. Cybersecurity and Ethics

The references in this chapter come from the full CANVAS White Paper 1 (Cybersecurity and Ethics), section A.2 (List of Papers), pages 52 ff. In the following, the authors have also explained the means by which those references have been sorted to enable an easily digestible provision of the various literature resources.

Papers recommended for readers to get an introduction are marked with a *.

Papers in the top 10th decile for citations (for each domain) are marked with (two) **.

Papers which were not used for the bibliographic analysis are marked with a “x”.

Different font colours were used to indicate relevance to specific domains. The colour codes are as follows:

	Health domain
	Business domain
	National Security domain

Abbas, Assad, and Samee U. Khan. “A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds.” *IEEE Journal of Biomedical and Health Informatics* 18, no. 4 (July 2014): 1431–41. doi:10.1109/JBHI.2014.2300846.

Abdul Ghani Azmi, I.M., S. Zuhuda, and S.P. Wigati Jarot. “Data Breach on the Critical Information Infrastructures: Lessons from the Wikileaks.” In *Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012*, 306–11. Kuala Lumpur, Malaysia: IEEE, 2012. doi:10.1109/CyberSec.2012.6246173.

Abreu, Rute, Liliane Segura, Fatima David, Henrique Formigoni, Jelena Legcevic, and Flavio Mantovani. “Ethics and Fraud in E-Banking Services.” In *2015 10th Iberian Conference on Information Systems and Technologies (Cisti)*, edited by A. Rocha, G. P. Dias, A. Martins, L. P. Reis, and M. P. Cota. New York: IEEE, 2015.

Abreu R, David F, Segura L. E-banking services: Why fraud is important? *Journal of Information Systems Engineering & management*. 2016;1(2):120 x

Adeel, M., A.A. Chaudhry, R.A. Shaikh, and S.I. Shah. “Taxonomy of Cyber Crimes and Legislation in Pakistan.” In *Proceedings of 1st International Conference on Information and Communication Technology, ICICT 2005*, 2005:350. Karachi, Pakistan: IEEE, 2005. doi:10.1109/ICICT.2005.1598625.

Ahmad, Nehaluddin. “Privacy and the Indian Constitution: A Case Study of Encryption.” *Communications of the IBIMA* 2009 (2009): Article ID 455684.

Ali, Azman, David Hutchison, Plamen Angelov, and Paul Smith. “Adaptive Resilience for Computer Networks: Using Online Fuzzy Learning.” In *RNDM 2012 - 4th International Workshop on Reliable Networks Design and Modeling*, 791–97. St. Petersburg, Russia: IEEE, 2012.

Alouane, Meryeme, and Hanan El Bakkali. “Security, Privacy and Trust in Cloud Computing: A Comparative Study.” *2015 International Conference on Cloud Technologies and Applications (Cloudtech 15)*, 2015, 1-8.

Alqahtani, A. “Towards a Framework for the Potential Cyber-Terrorist Threat to Critical National Infrastructure.” *Information and Computer Security* 23, no. 5 (2015): 532–69. doi:10.1108/ICS-09-2014-0060.

- Alqahtani, Abdulrahman. "The Potential Threat of Cyber-Terrorism on National Security of Saudi Arabia." In *Proceedings of the 8th International Conference on Information Warfare and Security (Iciw-2013)*, edited by D. Hart, 231–39. Reading (UK): Academic Conferences and Publishing International Limited, 2013.
- Altawy, Riham, and Amr M. Youssef. "Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices." *IEEE Access* 4 (2016): 959–79. doi:10.1109/ACCESS.2016.2521727.
- Árnason, Vilhálmur "Coding and Consent: Moral Challenges of the Database Project in Iceland." *Bioethics* 18, no. 1 (February 2004): 27–49. doi:10.1111/j.1467-8519.2004.00377.x.**
- Arquilla, John, and David Ronfeldt, eds. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, 239–88. Santa Monica (CA): Rand Corporation, 2001.
- Asllani, A., C.S. White, and L. Ettkin. "Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals." *Journal of Legal, Ethical and Regulatory Issues* 16, no. 1 (2013): 7–14.
- Ayatollahi, Haleh, Peter A. Bath, and Steve Goodacre. "Accessibility versus Confidentiality of Information in the Emergency Department." *Emergency Medicine Journal* 26, no. 12 (December 2009): 857–60. doi:10.1136/emj.2008.070557.
- Bahsi, Hayretdin, and Olaf Manuel Maennel. "A Conceptual Nationwide Cyber Situational Awareness Framework for Critical Infrastructures." In *Secure It Systems, Nordsec 2015*, edited by S. Buchegger and M. Dam. Stockholm, Sweden, 2015. https://link.springer.com/chapter/10.1007/978-3-319-26502-5_1.
- Barnard-Wills, David, and Debi Ashenden. "Securing Virtual Space: Cyber War, Cyber Terror, and Risk." *Space and Culture* 15, no. 2 (May 2012): 110–23. doi:10.1177/1206331211430016.**
- Barrett, Edward T. "Warfare in a New Domain: The Ethics of Military Cyber-Operations." *Journal of Military Ethics* 12, no. 1 (2013): 4–17.
- Barros-Bailey, Mary, and Jodi L. Saunders. "Ethics and the Use of Technology in Rehabilitation Counseling." *Rehabilitation Counseling Bulletin* 53, no. 4 (July 2010): 255–59. doi:10.1177/0034355210368867.
- Barrows, Randolph C., and Paul D. Clayton. "Privacy, Confidentiality, and Electronic Medical Records." *Journal of the American Medical Informatics Association* 3, no. 2 (April 1996): 139–48.**
- Batchelor, Rachel, Ania Bobrowicz, Robin Mackenzie, and Alisoun Milne. "Challenges of Ethical and Legal Responsibilities When Technologies' Uses and Users Change: Social Networking Sites, Decision-Making Capacity and Dementia." *Ethics and Information Technology* 14, no. 2 (June 2012): 99–108. doi:10.1007/s10676-012-9286-x.
- Bendrath, Ralf. "From Cyberterrorism to Cyberwar, Back and Forth : How the United States Securitized Cyberspace." In *International Relations and Security in the Digital Age*, edited by Johan Eriksson and Giampiero Giacomello, 57–82. London: Routledge, 2007. <http://www.diva-portal.org/smash/record.jsf?pid=diva2:404792>.
- "The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection." *ISIJ Information & Security: An International Journal* 7 (2001): 80–103.
- Bennasar, Hanane, Mohammad Essaaidi, Ahmed Bendahmane, and Jalel Ben-othman. "State-of-The-Art of Cloud Computing Cyber-Security." In *Proceedings of 2015 Third Ieee World Conference*

- on *Complex Systems (Wccs)*, edited by M. Essaïdi and M. Nemiche. Marrakech, Morocco: IEEE, 2015. doi:10.1109/ICoCS.2015.7483283.
- Betz, David J, and Tim Stevens. *Cyberspace and the State toward a Strategy for Cyber-Power*. Abingdon: Routledge, 2011. <http://www.tandfonline.com/toc/tadl20/51/424>.
- Bodle, Robert. "Regimes Of Sharing: Open APIs, Interoperability, and Facebook." *Information Communication & Society* 14, no. 3 (2011): 320–37. doi:10.1080/1369118X.2010.542825.
- Bonner, Steven, and Eleanor O’Higgins. "Music Piracy: Ethical Perspectives." *Management Decision* 48, no. 9 (2010): 1341–54. doi:10.1108/00251741011082099.
- Bourret, Christian, and Olivia Pestana. "Information Systems and Patients’ Empowerment around Patients’ Pathways: The French and the Portuguese Scenarios." *Qualitative & Quantitative Methods in Libraries* 4 (December 2015): 767–73.
- Brey, Philip. "Ethical Aspects of Information Security and Privacy." In *Security, Privacy, and Trust in Modern Data Management*, 21–36. Data-Centric Systems and Applications. Berlin/Heidelberg: Springer, 2007. <http://link.springer.com/content/pdf/10.1007/978-3-540-69861-6.pdf#page=36>.
- Brumnik, Robert, and Iztok Podbregar. "How Terrorists Use the Internet." In *Policing in Central and Eastern Europe—Social Control of Unconventional Deviance*, edited by G. Mesko, A. Sotlar, and J. Winterdyk, 157–74. Maribor: University of Maribor, Faculty of Criminal Justice and Security, 2011.
- Bucci, Steven. "Joining Cybercrime and Cyberterrorism: A Likely Scenario." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S Reveron. Washington, DC: Georgetown University Press, 2012. <http://www.jstor.org/stable/j.ctt2tt6rz>.
- ×
- Buckovich, Suzy A., Helga E. Rippen, and Michael J. Rozen. "Driving Toward Guiding Principles: A Goal for confidentiality, and Security of Health Information." *Journal of the American Medical Informatics Association* 6, no. 2 (April 1999): 122–33.
- Bunnik, Eline M., Maartje H. N. Schermer, and A. Cecile J. W. Janssens. "Personal Genome Testing: Test Characteristics to Clarify the Discourse on Ethical, Legal and Societal Issues." *BMC Medical Ethics* 12 (June 2011): 11. doi:10.1186/1472-6939-12-11.
- Caldicott, Dame F., Kingsley Manning: "A Guide to Confidentiality in Health and Social Care: Treating Confidential Information with Respect." Health & Social Care Information Center (September 2013). Accessed August 4, 2017. <http://content.digital.nhs.uk/media/12822/Guide-to-confidentialityin-health-and-socialcare/pdf/HSCIC-guide-to-confidentiality.pdf>.
- Camara, Carmen, Pedro Peris-Lopez, and Juan E. Tapiador. "Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey." *Journal of Biomedical Informatics* 55 (June 2015): 272–89. doi:10.1016/j.jbi.2015.04.007.
- Cambon-Thomsen, Anne, Emmanuelle Rial-Sebbag, and Bartha M. Knoppers. "Trends in Ethical and Legal Frameworks for the Use of Human Biobanks." *European Respiratory Journal* 30, no. 2 (August 2007): 373–82. doi:10.1183/09031936.00165006.**
- Capek, Jan, and Jana Hola. "Cybersecurity Within Cyberspace." In *Idimt-2016- Information Technology, Society and Economy Strategic Cross-Influences*, edited by D. Petr, C. Gerhard, and O. Vaclav, 325–32. Linz: Trauner Verlag, 2016.
- Carr, Madeline. "Public-Private Partnerships in National Cyber-Security Strategies." *International Affairs* 92, no. 1 (January 2016): 43–62. doi:10.1111/1468-2346.12504.**

- Caudle, Daryl. "Improving Cyber Warfare Decision-Making by Incorporating Leadership Styles and Situational Context into Poliheuristic Decision Theory." In *Proceedings of the 8th International Conference on Information Warfare and Security (Iciw-2013)*, edited by D. Hart, 240–47. Reading (UK): Academic Conferences Ltd., 2013.
- Caulfield, Timothy, Amy L. McGuire, Mildred Cho, Janet A. Buchanan, Michael M. Burgess, Ursula Danilczyk, Christina M. Diaz, et al. "Research Ethics Recommendations for Whole-Genome Research: Consensus Statement." *PLoS Biology* 6, no. 3 (March 2008): 430–35. doi:10.1371/journal.pbio.0060073.**
- Caulfield, Timothy, Ross EG Upshur, and Abdallah Daar. "DNA Databanks and Consent: A Suggested Policy Option Involving an Authorization Model." *BMC Medical Ethics* 4 (January 2003): 1. doi:10.1186/1472-6939-4-1.
- Cavelty, Myriam Dunn. "Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology and Politics* 4, no. 1 (2008): 19–36. doi:10.1300/J516v04n01_03.
- "The Militarisation of Cyberspace: Why Less May Be Better." In *2012 4th International Conference on Cyber Conflict, CYCON 2012 - Proceedings*. Tallinn, Estonia: IEEE, 2012. <http://ieeexplore.ieee.org/document/6243971/>.
- "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse." *International Studies Review* 15, no. 1 (March 2013): 105–22. doi:10.1111/misr.12023.**
- "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities." *Science and Engineering Ethics* 20, no. 3 (September 2014): 701–15. doi:10.1007/s11948-014-9551-y.**
- Dunn Cavelty, M., V. Mauer, and S. Krishna-Hensel, eds. "Concluding Remarks: The Role of the State in Securing the Information Age—challenges and Prospects." In *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace.*, 130–51. Aldershot, England: Ashgate, 2007.
- Chang, Betty L., Suzanne Bakken, S. Scott Brown, Thomas K. Houston, Gary L. Kreps, Rita Kukafka, Charles Safran, and P. Zoe Stavri. "Bridging the Digital Divide: Reaching Vulnerable Populations." *Journal of the American Medical Informatics Association* 11, no. 6 (December 2004): 448–57. doi:10.1197/jamia.M1535.**
- Chaturvedi, Manmohan, Aynur Unal, Preeti Aggarwal, Shilpa Bahl, and Sapna Malik. "International Cooperation in Cyber Space to Combat Cyber Crime and Terrorism." In *2014 IEEE Conference on Norbert Wiener in the 21st Century (21cw)*, edited by M. Gibbs. Boston (MA): IEEE, 2014. <http://ieeexplore.ieee.org/document/6893915/>.
- Chen, Yasha, Xinjie Zhao, Wen Li, and Jianpeng Zhao. "A New Architecture for Cloud Computing System Protection." In *2013 International Conference on Advanced Cloud and Big Data (Cbd)*, 46–50. Nanjing, China: IEEE, 2013. doi:10.1109/CBD.2013.6.
- Chow-White, Peter A., Maggie MacAulay, Anita Charters, and Paulina Chow. "From the Bench to the Bedside in the Big Data Age: Ethics and Practices of Consent and Privacy for Clinical Genomics and Personalized Medicine." *Ethics and Information Technology* 17, no. 3 (September 2015): 189–200. doi:10.1007/s10676-015-9373-x.
- Christen M, Fischer J, Huppenbauer M, Tanner C, van Schaik C (eds.) (2014): Empirically Informed Ethics. Morality between Facts and Norms. Library of Ethics and Applied Philosophy. Springer, Berlin (349 pp.) x

- Christen M, Ineichen C, Tanner C (2014b): How moral are the principles of biomedical ethics? *BMC Medical Ethics* 15: 47 x
- Christen M, Narvaez D, Tanner C, Ott T (2016): Mapping Values: Using Thesauruses to Reveal Semantic Structures of Cultural Moral Differences. *Cognitive Systems Research* 40: 59-74 x
- Christensen, S., W.J. Caelli, W.D. Duncan, and E. Georgiades. "An Achilles Heel: Denial of Service Attacks on Australian Critical Information Infrastructures." *Information and Communications Technology Law* 19, no. 1 (2010): 61–85. doi:10.1080/13600831003708059.
- Conger, Sue, Joanne H. Pratt, and Karen D. Loch. "Personal Information Privacy and Emerging Technologies." *Information Systems Journal* 23, no. 5 (September 2013): 401–17. doi:10.1111/j.1365-2575.2012.00402.x.
- Creasey, J.C. "Protecting Critical National Infrastructure through Collaborative Cyber Situational Awareness." In *8th IET International System Safety Conference Incorporating the Cyber Security Conference 2013*, Vol. 2013. IET Conference Publications, 2013. doi:10.1049/cp.2013.1708.
- Cutts, Andrew. "Warfare and the Continuum of Cyber Risks: A Policy Perspective." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by C. Czosseck and K. Geers, 66–76. Amsterdam: IOS Press, 2009.
- Czosseck, Christian, Rain Ottis, and Anna-Maria Talihaerm. "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security." In *Proceedings of the 10th European Conference on Information Warfare and Security*, edited by R. Ottis, 57–64. Estonia 7-8 July 2011.
- D’Arcy, John, and Anat Hovav. "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures." *Journal of Business Ethics* 89 (2009): 59–71.
- Da Veiga, Adele. "A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument." In *Proceedings of the 2016 SAI Computing Conference (SAI)*, 1006–15. London, UK: IEEE, 2016.
- Davis, Gaye. "State Security in Charge of Cybercrime Plans | Dailynews." *Independent Media Online*. February 20, 2012, Daily News edition. <https://www.iol.co.za/dailynews/news/state-security-in-charge-of-cybercrime-plans-1238243>.
- Dawson, M. "A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism." In *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, edited by M. Dawson and O. Marvan, 1–7. Hershey PA, USA: Igi Global, 2015. doi:10.4018/978-1-4666-8345-7.ch001.
- De Abajo, Francisco J., Lydia F. Grande, Javier J. Gutiérrez, Mara C. M. Arribas, Benedetto Terracini, Teresa P. Ros, Jaime C. Castelló, Amelia M. Uranga, Moisés A. Alonso, Joaquin H. Carranza and Maria J. S. Martinez. "Ethical Guidelines Governing the Creation and Use of Registries for Biomedical Research Puposes." Ethics Committee of the Rare Disease Research Institute, 2007.
- De Vries, Jantina, Muminatou Jallow, Thomas N. Williams, Dominic Kwiatkowski, Michael Parker, and Raymond Fitzpatrick. "Investigating the Potential for Ethnic Group Harm in Collaborative Genomics Research in Africa: Is Ethnic Stigmatisation Likely?" *Social Science & Medicine* 75, no. 8 (October 2012): 1400–1407. doi:10.1016/j.socscimed.2012.05.020.
- Dean, Matthew D., Dinah M. Payne, and Brett J. L. Landry. "Data Mining: An Ethical Baseline for Online Privacy Policies." *Journal of Enterprise Information Management* 29, no. 4 (2016): 482–504. doi:10.1108/JEIM-04-2014-0040.

- Deibert, Ronald J. "Cyber-Security and Threat Politics: US Efforts to Secure the Information Age." *International Studies Review* 11, no. 2 (June 2009): 373–75.
- Deibert, Ronald. Tracking the Emerging Arms Race in Cyberspace." *Bulletin of the Atomic Scientists* 67, no. 1 (February 2011): 1–8. doi:10.1177/0096340210393703.
- Demchak, C.C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens and London: The University of Georgia Press, 2011.
- Dennis, A., R. Jones, D. Kildare, and C. Barclay. "Design Science Approach to Developing and Evaluating a National Cybersecurity Framework for Jamaica." *Electronic Journal of Information Systems in Developing Countries* 62, no. 1 (2014).
- Devillier, Nathalie. "Ageing, Well-Being and Technology: From Quality of Life Improvement to Digital Rights Management: A French Perspective." *Proceedings of the 2016 ITU Kaleidoscope Academic Conference - ICTs for a Sustainable World (ITU WT)*, 2016, 41–47.
- Dillon, Gurpreet, Tiago Oliveira, Santa Susarapu, and Mario Caldeira. "Deciding between Information Security and Usability: Developing Value Based Objectives." *Computers in Human Behavior* 61 (August 2016): 656–66. doi:10.1016/j.chb.2016.03.068.
- Docherty, Annemarie B., and Nazir I. Lone. "Exploiting Big Data for Critical Care Research." *Current Opinion in Critical Care* 21, no. 5 (October 2015): 467–72. doi:10.1097/MCC.0000000000000228.
- Dodig-Crnkovic, Gordana. "On the Importance of Teaching Professional Ethics to Computer Science Students." In *Computing and Philosophy Conference, E-CAP*. London: College Publications, 2004. <http://www.idt.mdh.se/personal/gdc/work/TeachingProfEthics.pdf>.
- Dong, L.N. *Design of Computer Information Network Security System*. Vol. 539. Applied Mechanics and Materials. Zurich: Trans Tech Publications Inc., 2014. doi:10.4028/www.scientific.net/AMM.539.305.
- Dong, Naipeng, Hugo Jonker, and Jun Pang. "Challenges in eHealth: From Enabling to Enforcing Privacy." In *Foundations of Health Informatics Engineering and System*, 195–206. Springer, 2011. Accessed August 4, 2017. <http://link.springer.com/content/pdf/10.1007/978-3-642-32355-3.pdf#page=205>.
- Dunn Cavelty, M. (2014). "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", *Science and Engineering Ethics*, Volume 20, Issue 3, September 2014, Pages 701-715, DOI: 10.1007/s11948-014-9551-y.
- Elkhannoubi, H., and M. Belaissaoui. "A Framework for an Effective Cybersecurity Strategy Implementation: Fundamental Pillars Identification." In *International Conference on Intelligent Systems Design and Applications, ISDA 2015*. Marrakech, Morocco, 2016. doi:10.1109/ISDA.2015.7489156.
- Eun, Yong-Soo, and Judith Sita Amann. "Cyberwar: Taking Stock of Security and Warfare in the Digital Age." *International Studies Perspectives* 17, no. 3 (August 2016): 343–60. doi:10.1111/insp.12073.
- Faqir, R.S.A. "Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010." *International Journal of Cyber Criminology* 7, no. 1 (2013): 81–90.
- Fayomi, Oluyemi, Oly Nelson Ndubisi, Charles Ayo, Felix Chidozie, Lady Ajayi, and Uchechukwu Okorie. "Cyber-Attack as a Menace to Effective Governance in Nigeria." Edited by C. Adams. *Proceedings of the 15th European Conference on Egovernment*, 2015, 107–16.

- Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. "Cybersecurity and US Legislative Efforts to Address Cybercrime." *Journal of Homeland Security and Emergency Management* 10, no. 1 (2013). doi:10.1515/jhsem-2012-0007.
- France, Francis H. Roger. "Ethics and Biomedical Information." *International Journal of Medical Informatics* 49, no. 1 (March 1998): 111–15. doi:10.1016/S1386-5056(98)00018-5.
- Garvie C., Bedoya A. M., and Frankle J. 2016. The perpetual line-up. Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology. x
- Gattiker, U. E., and H. Kelley. "Morality and Computers: Attitudes and Differences in Moral Judgments." *Information Systems Research* 10, no. 3 (September 1999): 233–54. doi:10.1287/isre.10.3.233.**
- Geers, K. "The Challenge of Cyber Attack Deterrence." *Computer Law and Security Review* 26, no. 3 (2010): 298–303. doi:10.1016/j.clsr.2010.03.003.
- "The Cyber Threat to National Critical Infrastructures: Beyond Theory." *Journal of Digital Forensic Practice* 3, no. 2–4 (2010): 124–30. doi:10.1080/15567281.2010.536735.
- Ghernouti-Helie, Solange. "A National Strategy for an Effective Cybersecurity Approach and Culture." *Fifth International Conference on Availability, Reliability, and Security: Ares 2010, Proceedings*, 2010, 370–73. doi:10.1109/ARES.2010.119.
- Ghioni, F. "National Security and Threat Awareness." In *Data Mining VI: Data Mining, Text Mining and Their Business Applications*, edited by A. Zanasi, C. A. Brebbia, and N. F. F. Ebecken, 381–87, 2005.
- Godard, Béatrice, Sandy Raeburn, Marcus Pembrey, Martin Bobrow, Peter Farndon and Ségolène Aymé. "Genetic Information and Testing in Insurance and Employment: Technical, Social and Ethical Issues." *European Journal of Human Genetics* 11, no. 2 (December 2003): 123–42. doi: 10.1038/sj.ejhg.5201117.
- Goldman, H., R. McQuaid, and J. Picciotto. "Cyber Resilience for Mission Assurance." In *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, 236–41. Waltham, MA, USA: IEEE, 2011. doi:10.1109/THS.2011.6107877.
- Grabosky, P. "Organised Crime and the Internet: Implications for National Security." *RUSI Journal* 158, no. 5 (2013): 18–25. doi:10.1080/03071847.2013.847707.
- Granado, N., and G. White. "Cyber Security and Government Fusion Centers." Waikoloa, HI, USA: IEEE, 2008. doi:10.1109/HICSS.2008.111.
- Grant, Jeremy A. "The National Strategy for Trusted Identities in Cyberspace Enhancing Online Choice, Efficiency, Security, and Privacy through Standards." *Ieee Internet Computing* 15, no. 6 (December 2011): 80–84.
- Greenbaum, Dov, Andrea Sboner, Ximeng Jasmine Mu, and Mark Gerstein. "Genomics and Privacy: Implications of the New Reality of Closed Data for the Field." *PLoS Computational Biology* 7, no. 12 (December 2011): e1002278. doi:10.1371/journal.pcbi.1002278.
- Greiman, Virginia. "To Catch a Thief in the Cloud: A Paradigm for Law Enforcement." In *Proceedings of the 9th International Conference on Cyber Warfare and Security (Iccws-2014)*, edited by S. Liles, 77–83. London: Academic Conferences and Publishing International Limited, 2014.
- Grobler, M., J.J. Van Vuuren, and L. Leenen. "Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward." In *ICT Critical Infrastructures and Society. Proceedings.*, Vol. 386 AICT. IFIP Advances in Information and Communication Technology. Berlin: Springer, 2012. doi:10.1007/978-3-642-33332-3_20.

- Gunarto, Harry. "Ethical Issues in Cyberspace and IT Society." Paper given at the Symposium on Whither The Age of Uncertainty, Ritsumeika Asia Pacific University, 2003/01/23. <http://www.apu.ac.jp/~gunarto/it1.pdf>
- Gutmann, A. W., J. W. Wagner, Y. Ali, A. L. Allen, J. D. Arras, B. F. Atkinson, N. A. Farahany, et al. "Privacy and Progress in Whole Genome Sequencing." Washington, D.C.: Presidential Commission for the Study of Bioethical Issues, October 2012.
- Hadlington, Lee. 2017. "Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours." *Heliyon* 3 (7): e00346. <https://doi.org/10.1016/j.heliyon.2017.e00346>.
- Harrington, S. J. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions." *Mis Quarterly* 20, no. 3 (September 1996): 257–78. doi:10.2307/249656.**
- Harrop, W., and A. Matteson. "Cyber Resilience: A Review of Critical National Infrastructure and Cyber Security Protection Measures Applied in the UK and USA." *Journal of Business Continuity & Emergency Planning* 7, no. 2 (2013): 149–62.
- Hashim, M.S., M.N. Masrek, and Z. Yunos. "Elements in the Cyber Security Framework for Protecting the Critical Information Infrastructure against Cyber Threats." *Information (Japan)* 19, no. 7B (2016): 2989–94.
- Hens, Kristien, Emmanuelle Lévesque, and Kris Dierickx. "Children and Biobanks: A Review of the Ethical and Legal Discussion." *Human Genetics* 130, no. 3 (September 2011): 403–13. doi:10.1007/s00439-011-1031-8.
- Hiller, Janine S., and Roberta S. Russell. "The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison." *Computer Law & Security Review* 29, no. 3 (June 2013): 236–45. doi:10.1016/j.clsr.2013.03.003.**
- Hoedemaekers, Rogeer, Bert Gordijn, and Martien Pijnenburg. "Solidarity and Justice as Guiding Principles in Genomic Research." *Bioethics* 21, no. 6 (July 2007): 342–50. doi:10.1111/j.1467-8519.2007.00562.x.
- Horton, Joe. 2017. "Aggregation, Complaints, and Risk." *Philosophy & Public Affairs* 45 (1): 54–81. <https://doi.org/10.1111/papa.12084>.
- Hui, Lucas C. K., K. P. Chow, and S. M. Yiu. "Tools and Technology for Computer Forensics: Research and Development in Hong Kong (Invited Paper)." In *Information Security Practice and Experience, Proceedings*, edited by E. Dawson and D. S. Wong, 11–19. LNCS 4464. Berlin/Heidelberg: Springer, 2007.
- Hunton, Paul. "A Rigorous Approach to Formalising the Technical Investigation Stages of Cybercrime and Criminality within a UK Law Enforcement Environment." *Digital Investigation* 7, no. 3–4 (April 2011): 105–13. doi:10.1016/j.diin.2011.01.002.
- Ienca, Marcello, and Pim Haselager. "Hacking the Brain: Brain-Computer Interfacing Technology and the Ethics of Neurosecurity." *Ethics and Information Technology* 18, no. 2 (June 2016): 117–29. doi:10.1007/s10676-016-9398-9.

- Ikonen, Veikko, and Eija Kaasinen. "Ethical Assessment in the Design of Ambient Assisted Living." In *Assisted Living Systems - Models, Architectures and Engineering Approaches*, edited by Arthur I. Karshmer, Jürgen Nehmer, Hartmut Raffler, and Gerhard Tröster. Dagstuhl Seminar Proceedings. Dagstuhl, Germany: Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Germany, 2008. <http://drops.dagstuhl.de/opus/volltexte/2008/1462>.
- Introna L., Wood D. 2004. "Picturing algorithmic surveillance: the politics of facial recognition systems." In: *Surveillance & Society* 2 (2/3): 177-198. URN: <http://nbn-resolving.de/urn:nbn:de:0168-ssoar-200675> ×
- Jain, N., D.R. Kalbande, and P. Sharma. "Empirical Relationship between Victim's Occupation and Their Knowledge of Digital Forensic," 21-22-March-2016:61–65, 2016. doi:10.1145/2909067.2909077.
- Jakobson, G., and M.N. Schmitt. "Proceedings: Foreword." In *2012 4th International Conference on Cyber Conflict, CYCON 2012 - Proceedings*. Tallinn, Estonia: IEEE, 2012. <http://ieeexplore.ieee.org/document/6243959/>
- Jasmontaite, Lina, Gloria González Fuster, Serge Gutwirth, Florent Wenger, David-Olivier Jaquet-Chiffelle, and Eva Schlehahn. 2017. "Canvas White Paper 2 – Cybersecurity and Law." SSRN Scholarly Paper ID 3091939. Rochester, NY: Social Science Research Network. <https://papers.ssrn.com/abstract=3091939>.
- Jica, H. "Cyber Security and National Security Awareness Initiatives in Albania: A Synergy Approach." *Mediterranean Journal of Social Sciences* 4, no. 10 (2013): 614–22. doi:10.5901/mjss.2013.v4n10p614.
- Kaminski, Ryan T. "Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions." In *Conference on Cyber Conflict. Proceedings 2010*, edited by C. Czosseck and K. Podins, 2010. <https://ccdcoe.org/multimedia/conference-cyber-conflict-proceedings-2010.html>.
- Kaplan, Bonnie, and Sergio Litewka. "Ethical Challenges of Telemedicine and Telehealth." *Cambridge Quarterly of Healthcare Ethics* 17, no. 4 (Fall 2008): 401–16. doi:10.1017/S0963180108080535.
- Karabacak, Bilge, and Unal Tatar. "Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection." In *Critical Infrastructure Protection*, edited by M. Edwards, 116:63–73, 2014.
- "Regulatory Approaches for Cyber Security of Critical Infrastructures: The Case of Turkey." *Computer Law & Security Review* 32, no. 3 (June 2016): 526–39. doi:10.1016/j.clsr.2016.02.005.
- Karabacak, Bilge, Sevgi Ozkan Yildirim, and Nazife Baykal. "A Vulnerability-Driven Cyber Security Maturity Model for Measuring National Critical Infrastructure Protection Preparedness." *International Journal of Critical Infrastructure Protection* 15 (December 2016): 47–59. doi:10.1016/j.licip.2016.10.001.
- Kask, R.J. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." In *Strategies for Trusted Identities and Infrastructure in Cyberspace*, by R. J. Kask, 49–127. New York: Nova Science Publishers, 2011.
- Kasper, A. "The Fragmented Securitization of Cyber Threats." In *Regulating Etechnologies in the European Union: Normative Realities and Trends*, edited by Tanel Kerikmäe, 157–88. Cham: Springer International Publishing, 2014. doi:10.1007/978-3-319-08117-5_9.

- Kiggins, R.D. "Us Leadership in Cyberspace: Transnational Cyber Security and Global Governance." In *Cyberspace and International Relations: Theory, Prospects and Challenges*, edited by Jan-Frederik Kremer and Benedikt Müller, 161–80. Berlin: Springer, 2014. doi:10.1007/978-3-642-37481-4_10.
- Kim, J., S. Park, and T. Hyun. "An Inquiry into International Countermeasures against Cyberterrorism." In *The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005*. Phoenix Park, South Korea: IEEE, 2005. doi:10.1109/ICACT.2005.245895.
- Kittinger, R., L. Kittinger, and G.E. Avina. "Job Analysis and Cognitive Task Analysis in National Security Environments." In *Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience*, 341–47. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9743. Berlin/Heidelberg: Springer, 2016. doi:10.1007/978-3-319-39955-3_32.
- Kjaerland, M. "Profiling Coordinated Cyber Incidents towards the Critical Infrastructure in Norway." *International Journal of Critical Infrastructures* 4, no. 4 (2008): 335–52. doi:10.1504/IJCIS.2008.020155.
- Klare B.F., Burge M.J., Klontz J.C., Vorder Bruegge R.W., and Jain A.K. 2012. "Face Recognition Performance: Role of Demographic Information." *IEEE Transactions on Information Forensics and Security* 7 (6): 1789-1801. ×
- Kluge, Eike-Henner W. "E-Health Promises and Challenges: Some Ethical Considerations." In *International Perspectives in Health Informatics*, edited by E. M. Borycki, J. A. BartleClar, M. S. Househ, C. E. Kuziemy, and E. G. Schraa, 148–53. Studies in Health Technology and Informatics 164. Amsterdam: IOS Press, 2011.
- Knoppers, Bartha Maria. "Framework for Responsible Sharing of Genomic and Health-Related Data." *The HUGO Journal* 8 (2014): 3.
- Kotsopoulou, Anastasia, Athanasios Melis, Violetta-Irene Koutsompou, and Christina Karasarlidou. "E-Therapy: The Ethics behind the Process." *Procedia Computer Science* 65 (2015):492–99.
- Kouatli, Issam. "Managing Cloud Computing Environment: Gaining Customer Trust with Security and Ethical Management." In *Promoting Business Analytics and Quantitative Management of Technology: 4th International Conference on Information Technology and Quantitative Management (Itqm 2016)*, edited by H. Lee, Y. Shi, J. Lee, F. Cordova, I. Dzitac, G. Kou, and J. Li, 91:412–21. Amsterdam: Elsevier Science Bv, 2016.
- Kramer, Franklin D. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." In *Cyberpower and National Security*, edited by Franklin D Kramer, Stuart H Starr, and Larry K Wentz, 1–23. Lincoln NE: University of Nebraska Press, 2009.
- Kugler, Richard L. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, edited by Franklin D Kramer, Stuart H Starr, and Larry K Wentz. Lincoln NE: University of Nebraska Press, 2009.
- Lane, Julia, and Claudia Schur. "Balancing Access to Health Data and Privacy: A Review of the Issues and Approaches for the Future." *Health Services Research* 45, no. 5 (October 2010): 1456–67. doi:10.1111/j.1475-6773.2010.01141.x.
- Laur, Audrey. "Fear of E-Health Records Implementation?" *Medico-Legal Journal* 83, no. 1 (March 2015): 34–39. doi:10.1177/0025817214540396.
- Lawson S. "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States." *First Monday* 17, no. 7 (2012).

<http://firstmonday.org/ojs/index.php/fm/article/view/3848>

- Lee, Daeseob, and Dongho Won. "A Study on Security Management Service System for Wireless Network Environment." *Applied Mathematics & Information Sciences* 6 (January 2012): 209–20.
- Lee, K.-B., and J.-I. Lim. "The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-Terror Attack on the Korea Hydro & Nuclear Power Co., Ltd." *KSII Transactions on Internet and Information Systems* 10, no. 2 (2016): 857–80. doi:10.3837/tiis.2016.02.023.
- Lehto, M. "The Ways, Means and Ends in Cyber Security Strategies." In *European Conference on Information Warfare and Security, ECCWS*, 182–90. London: Academic Conferences and Publishing International, 2013.
- Leiwo, J., and S. Heikkuri. "An Analysis of Ethics as Foundation of Information Security in Distributed Systems." In *Proceedings of the Thirty-First Hawaii International Conference on System Sciences, Vol Vi: Organizational Systems and Technology Track*, edited by H. J. Watson, 213–22. Los Alamitos: IEEE Computer Soc, 1998.
- Leukfeldt, R., S. Veenstra, and W. Stol. "High Volume Cyber Crime and the Organization of the Police: The Results of Two Empirical Studies in the Netherlands." *International Journal of Cyber Criminology* 7, no. 1 (2013): 1–17.
- Li, X. "Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime." *International Journal of Cyber Criminology* 9, no. 2 (2016): 185–204. doi:10.5281/zenodo.56225.
- Liu, E.C., G. Stevens, K.A. Ruane, A.M. Dolan, and R.M. Thompson. "Cybersecurity: Selected Legal Issues." In *Cybersecurity and Related Federal Laws: Revision Proposals*, 81–141. New York: Nova Science Publishers, 2012.
- Lowrance, William W. "Privacy, Confidentiality, and Identifiability in Genomic Research: Discussion document for workshop convened by the National Human Genome Research Institute, Bethesda, October 3-4, 2006." Accessed August 4, 2017. <https://www.genome.gov/pages/about/od/reportspublications/identifiabilityworkshopwhitepaper.pdf>.
- Lowry, Paul Benjamin, Clay Posey, Tom L. Roberts, and Rebecca J. Bennett. "Is Your Banker Leaking Your Personal Information? The Roles of Ethics and Individual-Level Cultural Characteristics in Predicting Organizational Computer Abuse." *Journal of Business Ethics* 121, no. 3 (2014): 385–401.
- Lupton, Deborah. "Quantified Sex: A Critical Analysis of Sexual and Reproductive Self-Tracking Using Apps." *Culture Health & Sexuality* 17, no. 4 (April 2015): 440–53. doi:10.1080/13691058.2014.920528.
- Mascalzoni, Deborah, Edward S. Dove, Yaffa Rubinstein, Hugh J. S. Dawkins, Anna Kole, Pauline McCormack, Simon Woods, et al. "International Charter of Principles for Sharing Bio-Specimens and Data." *European Journal of Human Genetics* 23, no. 6 (June 2015): 721–28. doi:10.1038/ejhg.2014.197.
- Matwyszyn, Andrea M. "CSR and the Corporate Cyborg: Ethical Corporate Information Security Practices." *Journal of Business Ethics* 88 (September 2009): 579–94. doi:10.1007/s10551-009-0312-9.
- McClanahan, Kitty. "Balancing Good Intentions: Protecting the Privacy of Electronic Health Information" *Bulletin of Science, Technology & Society* 28 no. 1 (2007): 69–79. ×
- McCormack, Pauline, Anna Kole, Sabina Gainotti, Deborah Mascalzoni, Caron Molster, Hanns

- Lochmüller, and Simon Woods. "‘You Should at Least Ask’. The Expectations, Hopes and Fears of Rare Disease Patients on Large-Scale Data and Biomaterial Sharing for Genomics Research." *European Journal of Human Genetics* 24, no. 10 (October 2016): 1403–8. doi:10.1038/ejhg.2016.30.
- McCormack, Pauline, Simon Woods, Annemieke Aartsma-Rus, Lynn Hagger, Agnes Herczegfalvi, Emma Heslop, Joseph Irwin, et al. "Guidance in Social and Ethical Issues Related to Clinical, Diagnostic Care and Novel Therapies for Hereditary Neuromuscular Rare Diseases: ‘Translating’ the Translational." *PLoS Currents* 5 (January 2013). doi:10.1371/currents.md.f90b49429fa814bd26c5b22b13d773ec.
- McGraw, Deven, James X. Dempsey, Leslie Harris, and Janlori Goldman. "Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange." *Health Affairs* 28, no. 2 (April 2009): 416–27. doi:10.1377/hlthaff.28.2.416.**
- McGraw, Gary, Richard Clarke, Silver Bullet, and Gary McGraw. "Silver Bullet Talks with Richard Clarke." *Ieee Security & Privacy* 8, no. 4 (August 2010): 5–11.
- McNally, Julie. "Improving Public-Private Sector Cooperation on Cyber Event Reporting." Edited by D. Hart. *Proceedings of the 8th International Conference on Information Warfare and Security (Iciw-2013)*, 2013, 147–53.
- McReynolds, Phillip. "How to Think About Cyber Conflicts Involving Non-State Actors." *Philosophy & Technology* 28, no. 3 (September 1, 2015): 427–48. doi:10.1007/s13347-015-0187-x.
- Meinrath, Sascha D., and Sean Vitka. "Crypto War II." *Critical Studies in Media Communication* 31, no. 2 (June 2014): 123–28. doi:10.1080/15295036.2014.921320.
- Mittelstadt, Brent. 2017. "Designing the Health-Related Internet of Things: Ethical Principles and Guidelines." *Information* 8 (3). <http://www.mdpi.com/2078-2489/8/3/77htm>.
- Moore, T., A. Friedman, and A.D. Procaccia. "Would a ‘Cyber Warrior’ Protect Us? Exploring Trade-Offs between Attack and Defense of Information Systems," 85–94, 2010. doi:10.1145/1900546.1900559.
- Motti, Vivian Genaro, and Kelly Caine. "Users’ Privacy Concerns About Wearables: Impact of Form Factor, Sensors and Type of Data Collected." In *Financial Cryptography and Data Security (FC 2015)*, edited by M. Brenner, N. Christin, B. Johnson, and K. Rohloff, 8976:231–44. Berlin: Springer, 2015.
- Mulligan, Deirdre K., and Fred B. Schneider. "Doctrine for Cybersecurity." *Daedalus* 140, no. 4 (FAL 2011): 70–92.
- Mulvenon, J. "Toward a Cyberconflict Studies Research Agenda." *Ieee Security & Privacy* 3, no. 4 (August 2005): 52–55. doi:10.1109/MSP.2005.110.
- Myhre, Sonja L., Jane Kaye, Lee A. Bygrave, Margunn Aanestad, Buthaina Ghanem, Patricia Mechael, and J. Frederik Frøen. "eRegistries: Governance for Electronic Maternal and Child Health Registries." *BMC Pregnancy and Childbirth* 16 (September 2016): 279. doi:10.1186/s12884-016-1063-0.
- Newman, Lily Hay. 2017. "Medical Devices Are the Next Security Nightmare." *Wired*, March 2, 2017. <https://www.wired.com/2017/03/medical-devices-next-security-nightmare/>.
- Nissenbaum, H. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7, no. 2 (2005): 61–73. doi:10.1007/s10676-005-4582-3.
- O’Shea, P. "Cyber War from a Living Room." *Electronic Products (Garden City, New York)* 52, no. 10 (2010).

- Olmsted, Murrey G., Barbara L. Massoudi, and Yuying Zhang. "What Consumers Want in Personal Health Applications: Findings from Project HealthDesign." *Personal and Ubiquitous Computing* 19, no. 1 (January 2015): 79–83. doi:10.1007/s00779-014-0811-2.
- Olvingson, Christina, Jonas Hallberg, Toomas Timpka, and Kent Lindqvist. "Ethical Issues in Public Health Informatics: Implications for System Design When Sharing Geographic Information." *Journal of Biomedical Informatics* 35, no. 3 (June 2002): 178–85. doi:10.1016/S1532-0464(02)00527-0.
- Organisation for Economic Co-operation and Development. "Cybersecurity Policy Making at a Turning Point." OECD Digital Economy Papers. Paris: OECD Publishing, 2012.
- Ottis, R. "Proactive Defense Tactics against On-Line Cyber Militia," 233–37, 2010. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84873105908&partnerID=40&md5=0f7b0212912c9ccde5b71fc044ac2ef7>.
- Ozair, Fouzia F., Nayer Jamshed, Amit Sharma, and Praveen Aggarwal. "Ethical Issues in Electronic Health Records: A General Overview." *Perspectives in Clinical Research* 6, no. 2 (2015): 73–76. doi:10.4103/2229-3485.153997.
- Pearson, Siani. "Privacy, Security and Trust in Cloud Computing." In *Privacy and Security for Cloud Computing*, by Siani Pearson and George Yee, 3–42. London: Springer, 2013.
- Peddicord, Douglas, Ann B. Waldo, Marc Boutin, Tina Grande, and Luis Gutierrez. "A Proposal To Protect Privacy Of Health Information While Accelerating Comparative Effectiveness Research." *Health Affairs* 29, no. 11 (November 2010): 2082–90. doi:10.1377/hlthaff.2010.0635.
- Peng, C., M. Xu, S. Xu, and T. Hu. "Modeling and Predicting Extreme Cyber Attack Rates via Marked Point Processes." Article in Press, 2016. Scopus. doi:10.1080/02664763.2016.1257590.
- Phahlamohlaka, Jackie. "Globalisation and National Security Issues for the State: Implications for National ICT Policies." In *Social Dimensions of Information and Communication Technology Policy*, edited by C. Avgerou, M. L. Smith, and P. VandenBesselaar, 95–107. IFIP International Conference on Human Choice and Computers 282. Berlin: Springer, 2008.
- Phahlamohlaka, L. J., J. C. Jansen van Vuuren, and A. J. Coetzee. "Cyber Security Awareness Toolkit for National Security: An Approach to South Africa's Cyber Security Policy Implementation," 2011. <http://researchspace.csir.co.za/dspace/handle/10204/5162>.
- Pieters, Wolter. "Security and Privacy in the Clouds: A Bird's Eye View." In *Computers, Privacy and Data Protection: An Element of Choice*, 445–457. Springer, 2011. http://link.springer.com/chapter/10.1007/978-94-007-0641-5_21.
- Piotrowski, Rafal, and Joanna Sliwa. "Cyberspace Situational Awareness in National Security System." *2015 International Conference on Military Communications and Information Systems (Icmcis)*, 2015.
- Posey, Clay, Becky Bennett, Tom Roberts, and Paul Benjamin Lowry. "When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse," 2011. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1958530.
- Prislan, Kaja, and Igor Bernik. "From Traditional Local to Global Cyberspace - Slovenian Perspectives on Information Warfare." Edited by V. Lysenko. *Proceedings of the 7th International Conference on Information Warfare and Security*, 2012, 237–44.
- Qian, Li. "Study of Information System Security of Government Data Center Based on the Classified Protection." In *8th International Conference on Computer Science & Education (ICCSE)*, 2013.

- Colombo, Sri Lanka: IEEE, 2013.
- Rahim, Fiza Abdul, Zuraini Ismail, and Ganthan Narayana Samy. "Information Privacy Concerns in Electronic Healthcare Records: A Systematic Literature Review." In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 504–9. New York: IEEE, 2013.
- Read, O. "How the 2010 Attack on Google Changed the Us Government's Threat Perception of Economic Cyber Espionage." In *Cyberspace and International Relations: Theory, Prospects and Challenges*, 9783642374814:203–30, 2014. doi:10.1007/978-3-642-37481-4_12.
- Reddy, D.S., and G. Dietrich. "Identifying Multiple Categories of Cybersecurity Skills That Affect User Acceptance of Protective Information Technologies." In *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*, 2016. <http://aisel.aisnet.org/amcis2016/ISSec/Presentations/37/>.
- Reddy, D.S., and S.V. Rao. "Cybersecurity Skills: The Moderating Role in the Relationship between Cybersecurity Awareness and Compliance." In *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*, 2016. <http://aisel.aisnet.org/amcis2016/ISSec/Presentations/23/>.
- Rifaut, Andre, Christophe Feltus, Slim Turki, and Djamel Khadraoui. "Analysis of the Impact of Ethical Issues on the Management of the Access Rights." In *Proceedings of the 8th International Conference on Security of Information and Networks*, 12–19. ACM, 2015. <http://dl.acm.org/citation.cfm?id=2799996>.
- Rigoni, Andrea, and Salvatore Di Blasi. "A Proposal for Domain Name System (DNS) Security Metrics Framework." Edited by R. Ottis. *Proceedings of the 10th European Conference on Information Warfare and Security*, 2011, 333–36.
- Robertson, Christopher J., Anna Lamin, and Grigorios Livanis. "Stakeholder Perceptions of Offshoring and Outsourcing: The Role of Embedded Issues." *Journal of Business Ethics* 95, no. 2 (August 2010): 167–89. doi:10.1007/s10551-009-0353-0.
- Rock, Barry, and Elaine Congress. "The New Confidentiality for the 21st Century in a Managed Care Environment." *Social Work* 44, no. 3 (May 1999): 253–62.
- Rodrigues, Paulo, and Henrique Santos. "Health Users' Perception of Biometric Authentication Technologies." Edited by Pedro P. Rodrigues, Mykola Pechenizkiy, João Gama, Ricardo C. Correia, Jiming Liu, Agma Traina, Peter Lucas, and Paolo Soda. *2013 IEEE 26th International Symposium on Computer-Based Medical Systems (CBMS)*, 2013, 320–25.
- Rollins, J., and A.C. Henning. "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations." In *Internet Policies and Issues*, 6:65–89, 2010.
- Ross, David A. "Foreword". In *Public health informatics and information systems*, edited by Patrick W. O'Carroll, William A. Yasnoff, M. Elizabeth Ward, Laura H. Ripp and Ernest L. Martin, v-vi. New York: Springer, 2003. x
- Rothenpieler, Peter, Claudia Becker, and Stefan Fischer. "Privacy Concerns in a Remote Monitoring and Social Networking Platform for Assisted Living." In *Privacy and Identity Management for Life*, edited by Jan Camenisch, Bruno Crispo, Simone Fischer-Hübner, Ronald Leenes, Giovanni Russello, 352 (2011): 219–30.
- Rüger, Korbinian. 2018. "On Ex Ante Contractualism." *Journal of Ethics and Social Philosophy* 13 (3). <https://doi.org/10.26556/jesp.v13i3.323>.
- Saigí-Rubió, Francesc, Ana Jiménez-Zarco, and Joan Torrent-Sellens. "Determinants of the Intention to Use Telemedicine: Evidence from Primary Care Physicians." *International Journal of Tech-*

- nology Assessment in Health Care* 32, no. 1–2 (2016): 29–36.
doi:10.1017/S0266462316000015.
- Salman, Ali, Suhana Saad, and Mohd Nor Shahizan Ali. “Dealing with Ethical Issues among Internet Users: Do We Need Legal Enforcement?” *Asian Social Science* 9, no. 8 (2013): 3.
- Sekgwathe, Virginia, and Mohammad Talib. “Cyber Crime Detection and Protection: Third World Still to Cope-Up.” In *E-Technologies and Networks for Development*, edited by J. J. Yonazi, E. Sedoyeka, E. Ariwa, and E. ElQawasmeh, 171:171–81, 2011.
- Sevis, Kamile Nur, and Ensar Seker. “Cyber Warfare: Terms, Issues, Laws and Controversies.” *2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2016.
- Shakib, Javad, and David Layton. “Interaction between Ethics and Technology.” *2014 IEEE International Symposium on Ethics in Science, Technology and Engineering*, 2014.
- Shannon, J., and N. Thomas. “Human Security and Cyber-Security: Operationalising a Policy Framework.” In *Cyber-Crime*, 327–46, 2005.
- Shkëmbi, A., and D. Sina. “Cybercrime in the Perspective of the European Legal Framework.” *Mediterranean Journal of Social Sciences* 4, no. 9 (2013): 327–31.
doi:10.5901/mjss.2013.v4n9p327.
- Simshaw, Drew, and Stephen S. Wu. “Ethics and Cybersecurity: Obligations to Protect Client Data.” In *National Symposium on Technology in Labor and Employment Law*. San Francisco, CA, 2015.
- Spafford, Eugene H. “Cyber Security: Assessing Our Vulnerabilities and Developing an Effective Defense.” In *Protecting Persons While Protecting the People*, edited by C. S. Gal, P. B. Kantor, and M. E. Lesk, 5661:20–33, 2009.
- Spitalewsky, K., J. Rochon, M. Ganzinger, and P. Knaup. “Potential and Requirements of IT for Ambient Assisted Living Technologies: Results of a Delphi Study.” *Methods of Information in Medicine* 52, no. 3 (2013): 231–38. doi:10.3414/ME12-01-0021.
- Spriggs, Merle, Michael V. Arnold, Christopher M. Pearce and Craig Fry. “Ethical questions must be conserved for electronic health records.” *Journal of Medical Ethics* 39, no. 9 (May 2012): 635-39. doi: 10.1136/medethics-2011-100413.
- Stahl, Bernd Carsten, Neil F. Doherty, Mark Shaw, and Helge Janicke. “Critical Theory as an Approach to the Ethics of Information Security.” *Science and Engineering Ethics* 20, no. 3 (September 2014): 675–99. doi:10.1007/s11948-013-9496-6.
- Taddeo, Mariarosaria. “Cyber Security and Individual Rights, Striking the Right Balance.” *Philosophy and Technology* 26, no. 4 (2013): 353–356. doi:10.1007/s13347-013-0140-9.
- “The Struggle Between Liberties and Authorities in the Information Age.” *Science and Engineering Ethics* 21, no. 5 (October 2015): 1125–38. doi:10.1007/s11948-014-9586-0.
- Tatar, Unal, Bilge Karabacak, and Adrian Gheorghe. “An Assessment Model to Improve National Cyber Security Governance.” *Proceedings of the 11th International Conference on Cyber Warfare and Security (Iccws 2016)*, 2016, 312–19.
- Tatar, Unal, Orhan Calik, Minhac Celik, and Bilge Karabacak. “A Comparative Analysis of the National Cyber Security Strategies of Leading Nations.” In *Proceedings of the 9th International Conference on Cyber Warfare and Security (Iccws-2014)*, edited by S. Liles, 211–18, 2014.
- Tatarinova, L.F., K.N. Shakirov, and D.V. Tatarinov. “Criminological Analysis of Determinants of Cyber-crime Technologies.” *Mathematics Education* 11, no. 5 (2016): 1127–34.
- The Academy of Medical Sciences. “Personal Data for Public Good: Using Health Information in Med-
- Horizon 2020 Grant Agreement No 700540

- ical Research.” London: Academy of Medical Sciences, January 2006. Accessed August 4, 2017. <https://acmedsci.ac.uk/policy/policy-projects/personal-data>.
- Thilakanathan, Danan, Rafael A. Calvo, Shiping Chen, Surya Nepal, and Nick Glozier. “Facilitating Secure Sharing of Personal Health Data in the Cloud.” *JMIR Medical Informatics* 4, no. 2 (June 2016): 56–73. doi:10.2196/medinform.4756.
- Thuraisingham, B. *Dependable Computing for National Security: A Position Paper*, 2003.
- *Data Mining for Security Applications*. Edited by M. Kantardzic, O. Nasraoui, and M. Milanova, 2004.
- Tieu, Lina, Urmimala Sarkar, Dean Schillinger, James D. Ralston, Neda Ratanawongsa, Rena Pasick, and Courtney R. Lyles. “Barriers and Facilitators to Online Portal Use Among Patients and Caregivers in a Safety Net Health Care System: A Qualitative Study.” *Journal of Medical Internet Research* 17, no. 12 (December 2015): e275. doi:10.2196/jmir.4847.
- U. K. Biobank. “UK Biobank Ethics and Governance Framework: Version 3.0.” 2007. Accessed August 4, 2017. <https://www.ukbiobank.ac.uk/wp-content/uploads/2011/05/EGF20082.pdf>.
- Van Allen, Jason, and Michael C. Roberts. “Critical Incidents in the Marriage of Psychology and Technology: A Discussion of Potential Ethical Issues in Practice, Education, and Policy.” *Professional Psychology-Research and Practice* 42, no. 6 (December 2011): 433–39. doi:10.1037/a0025278.
- Van der Linden, Helma, Dipak Kalra, Arie Hasman, and Jan Talmon. “Inter-Organizational Future Proof EHR Systems: A Review of the Security and Privacy Related Issues.” *International Journal of Medical Informatics* 78, no. 3 (March 2009): 141–60. doi:10.1016/j.ijmedinf.2008.06.013.
- van Vuuren, Joey Jansen, Jackie Phahlamohlaka, and Louise Leenen. “Governance of CyberSecurity in South Africa.” Edited by E. Filiol and R. Erra. *Proceedings of the 11th European Conference on Information Warfare and Security*, 2012, 135–44.
- van Vuuren, Joey Jansen, Jackie Phahlamohlaka, and Mario Brazzoli. “The Impact of the Increase in Broadband Access on South African National Security and the Average Citizen.” Edited by E. L. Armistead. *Proceedings of the 5th International Conference on Information Warfare and Security*, 2010, 171–81.
- van Vuuren, Joey Jansen, Louise Leenen, Jackie Phahlamohlaka, and Jannie Zaaiman. “Development of a South African Cybersecurity Policy Implementation Framework.” Edited by D. Hart. *Proceedings of the 8th International Conference on Information Warfare and Security (Iciw-2013)*, 2013, 106–15.
- van Vuuren, Joey Jansen, L. Leenen, J. Phahlamohlaka, and J. Zaaiman. “An Approach to Governance of Cybersecurity in South Africa.” In *Cyber Behavior: Concepts, Methodologies, Tools, and Applications*, 3–4:1583–97, 2014. doi:10.4018/978-1-4666-5942-1.ch082.
- van Vuuren, Joey Jansen, Marthie Grobler, and Jannie Zaaiman. “Cyber Security Awareness as Critical Driver to National Security.” *International Journal of Cyber Warfare and Terrorism (IJCWTT)* 2, no. 1 (2012): 27–38.
- “The Influence of Cyber Security Levels of South African Citizens on National Security.” Edited by V. Lysenko. *Proceedings of the 7th International Conference on Information Warfare and Security*, 2012, 138–47.
- van Vuuren, Joey Jansen, Marthie Grobler, Louise Leenen, and Jackie Phahlamohlaka. “Proposed Model for a Cybersecurity Centre of Innovation for South Africa.” In *Ict and Society*, edited by K. Kimppa, D. Whitehouse, T. Kuusela, and J. Phahlamohlaka, 431:293–306, 2014.

- Vayena, Effy, Urs Gasser, Alexandra Wood, David O'Brien, Micah Altman: "Elements of a New Ethical Framework for Big Data Research." *Washington and Lee Law Review Online* 72, Issue 3 (March 2016): 420-441.
- Venkatraman, Sitalakshmi, and Indika Delpachitra. "Biometrics in Banking Security: A Case Study." *Information Management & Computer Security* 16, no. 4 (2008): 415-430.
- Verheul, E., B.-J. Koops, and H. Van Tilborg. "Binding Cryptography - A Fraud-Detectible Alternative to Key-Escrow Proposals." *Computer Law and Security Report* 13, no. 1 (1997): 3-14. doi:10.1016/S0267-3649(97)81186-7.
- Visvanathan, Akila, Alan P. Gibb, and Richard R. W. Brady. "Increasing Clinical Presence of Mobile Communication Technology: Avoiding the Pitfalls." *Telemedicine and E-Health* 17, no. 8 (October 2011): 656-61. doi:10.1089/tmj.2011.0018.
- Wallace, Ilse M. "Is Patient Confidentiality Compromised With the Electronic Health Record? A Position Paper." *CIN: Computers, Informatics, Nursing* 33, no. 2 (February 2015): 58-62. doi:10.1097/CIN.0000000000000126.
- Walters, Gregory J. "Privacy and Security: An Ethical Analysis." *SIGCAS Comput. Soc.* 31, no. 2 (June 2001): 8-23. doi:10.1145/503345.503347.
- Wang, Jin, Zhongqi Zhang, Kaijie Xu, Yue Yin, and Ping Guo. "A Research on Security and Privacy Issues for Patient Related Data in Medical Organization System." *International Journal of Security and Its Applications* 7, no. 4 (2013): 287-98.
- Warren, Matthew, and Shona Leitch. "Australian National Critical Infrastructure Protection: A Case Study." Edited by R. Ottis. *Proceedings of the 10th European Conference on Information Warfare and Security*, 2011, 275-80.
- Weber, Karsten, Michele Loi, Markus Christen, and Nadine Kleine. 2018. "Digital Medicine, Cybersecurity and Ethics: An Uneasy Relationship." *American Journal of Bioethics* 18 (9): 52-53.
- White, G.B., and D.J. DiCenso. "Information Sharing Needs for National Security." In *Proceedings of the Annual Hawaii International Conference on System Sciences*. Big Island, HI, USA, USA: IEEE, 2005. <http://ieeexplore.ieee.org/document/1385491/>.
- Williams, Patricia A. H. "In a 'Trusting' Environment, Everyone Is Responsible for Information Security." *Information Security Technical Report* 13, no. 4 (2008): 207-15. doi:10.1016/j.istr.2008.10.009.
- Wilson, Clay, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress." *Focus on Terrorism* 9 (2003): 1-42.
- "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues." In *Electronic Warfare*, 161-80. New York: Nova Science Publishers, 2010
- "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress." Report for Congress. Washington, D.C.: Congressional Research Service, 2005
- "Cyber Threats to Critical Information Infrastructure." In *Cyberterrorism: Understanding, Assessment, and Response*, 123-36. Berlin/Heidelberg: Springer, 2014. doi:10.1007/978-1-4939-0962-9_7.
- Wjst, Matthias. "Caught You: Threats to Confidentiality Due to the Public Release of Large-Scale Genetic Data Sets." *BMC Medical Ethics* 11 (December 2010): 21. doi:10.1186/1472-6939-11-21.
- World Medical Association. "Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects." *Journal of the American Medical Association* 310, no. 20 (November 2013):

- 2191–94. doi:10.1001/jama.2013.281053.
- Wright, Galen E. B., Pieter G. J. Koornhof, Adebowale A. Adeyemo, and Nicki Tiffin. “Ethical and Legal Implications of Whole Genome and Whole Exome Sequencing in African Populations.” *BMC Medical Ethics* 14 (May 2013): 21. doi:10.1186/1472-6939-14-21.
- Wynia, Matthew K., Steven S. Coughlin, Sheri Alpert, Deborah S. Cummins, and Linda L. Emanuel. “Shared Expectations for Protection of Identifiable Health Care Information: Report of a National Consensus Process.” *Journal of General Internal Medicine* 16, no. 2 (February 2001): 100–111. doi:10.1046/j.1525-1497.2001.00515.x.
- Xiao, Liang, Paul Lewis, and Alex Gibb. *Developing a Security Protocol for a Distributed Decision Support System in a Healthcare Environment*. New York: ACM, 2008.
- Yaghmaei, Emad, Ibo van de Poel, Markus Christen, Bert Gordijn, Nadine Kleine, Michele Loi, Gwennyth Morgan, and Karsten Weber. 2017. “Canvas White Paper 1 – Cybersecurity and Ethics.” SSRN Scholarly Paper ID 3091909. Rochester, NY: Social Science Research Network. <https://papers.ssrn.com/abstract=3091909>.
- Yang, Bian. “What Make You Sure That Health Informatics Is Secure.” In *Inclusive Smart Cities and Digital Health*, edited by C. K. Chang, L. Chiari, Y. Cao, H. Jin, M. Mokhtari, and H. Aloulou, 9677:443–48. Cham: Springer, 2016.
- Young-do, Kim, Kim Jin-sung, and Lee Kyung-ho. “Major Issues of the National Cyber Security System in South Korea, and Its Future Direction.” *Korean Journal of Defense Analysis* 25, no. 4 (2013): 435–55.
- Young, Rachel, Erin Willis, Glen Cameron, and Mugur Geana. “‘Willing but Unwilling’: Attitudinal Barriers to Adoption of Home- Based Health Information Technology among Older Adults.” *Health Informatics Journal* 20, no. 2 (June 2014): 127–35. doi:10.1177/1460458213486906.
- Zheng, A.-K., P. Song, B.-X. Han, and M.-J. Zheng. *Reflection of the Nation Cybersecurity’s Evolution*. Vol. 347–350. Applied Mechanics and Materials, 2013. doi:10.4028/www.scientific.net/AMM.347-350.2553.

2. Cybersecurity and Law

The references used to compile White Paper 2 (Cybersecurity and Law) are available in several places of the full paper. Therefore, this derived literature list is also multi-partial, sorted by the topics for which the respective research sources have been used.

Cybersecurity delimitation and regulation challenges, controversies

These references have been derived chapter 5, pages 34 ff.

- Alheit, K., 'The applicability of the EU Product Liability Directive to Software', *Comparative and International Law Journal of Southern Africa*, Volume 34, Issue 2, Jul 2001.
- Article 29 Working Party, Guidelines on the right to data portability, April 2017.
- Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", February 2010.
- Benedek, W., Kettemann, M.C., Freedom of expression and the Internet, Council of Europe, 15 Jan 2014.
- Black, J., 'The role of risk in regulatory processes' in R. Baldwin, M. Lodge and M. Cave, *Oxford Handbook of Regulation*, Oxford University Press, 2010.
- Bryman, A., *Social Research Methods*, Oxford University Press, 2008.
- Cf. Note 14711/16 from the Council of the European Union Presidency to the Permanent Representatives Committee/Council on the subject title 'Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report', Brussels, 23 November 2016.
- Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union (2010/C 83/01).
- Council of the EU, Presidency Progress report: Encryption: Challenges for criminal justice in relation to the use of encryption - future steps, LIMITE CYBER 137, JAI 976, 14711/16, Brussels, 23 November 2016.
- Council of the EU, The Stockholm Program: An open and secure Europe serving the citizen, 17024/09.
- Craig, P., *The Lisbon Treaty: law, politics, and Treaty reform*, Oxford University Press, 2013.
- Daley, J., 'Insecure software is eating the world: Promoting cybersecurity in an age of ubiquitous software-embedded systems', 19 *The Stanford Technology Law Review* 533 (2016).
- Darmois, E. and Schméder, G., Cybersecurity: a case for a European approach, Paper commissioned by the Human Security Study Group SiT/WP/11/16, 2016.
- De Hert, P., Jasmontaite, L., Internet Content Suppression, in De Gruyter et al. *Culture and Human Rights: The Wroclaw Commentaries*, 2016.
- De Schutter, O., The Implementation of the Charter of Fundamental Rights in the EU institutional framework, Study for the AFCO Committee, 2016.
- Digital Economy and Society Index, Results of the study are available at: <https://ec.europa.eu/digital-single-market/en/desi>.
- Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

- EDPS, Guidance on Security Measures for Personal Data Processing Article 22 of Regulation 45/2001.
- EDPS, Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation).
- EDPS, Opinion 8/2015 Dissemination and use of intrusive surveillance technologies.
- EDPS, The EDPS as Supervisor of Large-Scale IT Systems and Member of Supervision Coordination Groups, 2015.
- ENISA, Definition of Cybersecurity: Gaps and overlaps in standardization, December 2015.
- ENISA, Principles and opportunities for a renewed EU cyber security strategy, ENISA contribution to the Strategy review, May 2017.
- Eriksson, J., Giacomello, G., 'The information Revolution, Security and international Relations; (IR)relevant theory?' International Political Science Review, Vol. 27, No. 3, 2006.
- European Commission and High Representative of the EU for Foreign Affairs and Security Policy (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final.
- European Commission, Commission Staff Working document 'Comprehensive Assessment of EU Security Policy accompanying the document Communication to the European Parliament, the European Council and the Council: Ninth progress report towards an effective and genuine Security Union' (Part 1), Brussels, 26.7.2017 SWD(2017) 278 final.
- European Commission, Commission Staff Working Document, Better Regulation Guidelines, Strasbourg, 19.5.2015 SWD(2015) 111 final.
- European Commission, Communication - A strategy for a Secure Information Society - 'Dialogue, partnership and empowerment' {SEC(2006) 656} /* COM/2006/0251 final.
- European Commission, Communication 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM(2000) 890.
- European Commission, Communication on Seventh progress report towards an effective and genuine Security Union, 16.5.2017 COM(2017) 261 final.
- European Commission, Communication to the European Parliament, the European Council and the Council, Seventh progress report towards an effective and genuine Security Union COM(2017) 261 final.
- European Commission, Communication, 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM(2000) 890.
- European Commission, Communication, eEurope Benchmarking Report - eEurope 2002 /* COM/2002/0062 final.
- European Commission, Communication, The Digital Agenda for Europe - Driving European growth digitally, COM(2012) 784 final.
- European Commission, Legal study on ownership and access to data, 2016, 978-92-79-62181-9.
- European Commission, Reflection Paper on the Future of European Defence, June 2017.
- European Commission, Study on Product liability in the European Union, February 2003, Contract No. ETD/2001/B5-3001/D/76.



- European Communication, Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All, Brussels, 10.5.2017 COM(2017) 228 final.
- European Criminal Policy Initiative, 'Manifesto II'.
- European Parliament, Report on the fight against cybercrime, 2017/2068, A motion for a European Parliament Resolution.
- European Union Agency for Network and Information Security, 'ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards our Digital Identity', December 2016.
- European Union Agency for Network and Information Security, ENISA's Opinion Paper on Encryption Strong Encryption Safeguards our Digital Identity, December 2016.
- German CCC publication: 'Chaos Computer Club analyzes government malware', published October 8th 2011.
- Gordon, L. A., Loeb M.P., Zhou L., Investing in Cybersecurity: Insights from the Gordon-Loeb Model, Journal of Information Security Vol.7 No.2, 2016.
- Hildebrandt, M., Tielemans, L., 'Data protection by design and technology neutral law' Computer law & Security Review 29 (2013) 509-521.
- Irish National Cyber Security Centre within the Department of Communications, Energy and Natural Resources, National Cyber Security Strategy 2015-2017.
- ITU, Recommendation, ITU-T X.1205.
- Kuner, C., 'Data Nationalism and Its Discontents', 2014, 64 Emory Law Journal 2089-2098.
- Kuner, C., 'The Internet and the Global Reach of EU Law' (February 1, 2017). Forthcoming, Collected Courses of the Academy of European Law (Oxford University Press); LSE Legal Studies Working Paper No. 4/2017; University of Cambridge Faculty of Law Research Paper No. 24/2017. Available at: <http://dx.doi.org/10.2139/ssrn.2890930>.
- Nagurney, A. & Nagurney, L.S., Netnomics, A game theory model of cybersecurity investments with information asymmetry (2015) 16: 127. doi:10.1007/s11066-015-9094-7.
- Opinion No. 28 of the European Group on Ethics in Science and New Technologies, 'Ethics of Security and Surveillance Technologies', Brussels, 20 May 2014.
- Outcome of the 3508th Council meeting, document 15391/16 and press release 67 by the Justice and Home Affairs department, section 'Criminal justice in Cyberspace', Brussels, 8th and 9th December 2016.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L119/1, 4.5.2016.
- Regulation (EU) No 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) repealing Regulation (EC) No 460/2004.
- Schuman Declaration, 9 May 1950, available at: https://europa.eu/european-union/about-eu/symbols/europe-day/schuman-declaration_en.
- Special Eurobarometer 390, Cyber security, Wave EB77.2 – TNS Opinion & Social, 2012.
- Speech by Vice-President Ansip at the Chatham House annual cyber conference: Evolving norms, improving harmonisation and building resilience, 26 June, 2017.

Steiner, J., Woods, L. *EU Law*, Oxford University Press, 2012.

Summers et al., *The Emergence of EU Criminal Law*, Hart Publishing, 2014.

Treaty Constituting the European Coal and Steel Community, available at:

<http://www.consilium.europa.eu/uedocs/cmsUpload/Treaty%20constituting%20the%20European%20Coal%20and%20Steel%20Community.pdf>.

Van der Meulen Nicole, Eun A. Jo and Stefan Soesanto (RAND Europe), *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses* (2015), available at:

[http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU\(2015\)536470](http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)536470).

Wensink, W. et al, *The European Union's Policies on Counter-Terrorism Relevance, Coherence and Effectiveness*, 2017.

Wiewiórowski Wojciech, *Privacy, security and technology: the Annual Privacy Forum 2017*, available at: https://edps.europa.eu/press-publications/press-news/blog/privacy-security-and-technology-annual-privacy-forum-2017_en.

Jurisprudence

Court of Justice of the European Union, *Aklagaren v Hans Akerberg Fransson* (C-617/10) 23 February 2013.

Court of Justice of the European Union, *Breyer v Bundesrepublik Deutschland* (C-582/14), 19 October 2016.

Court of Justice of the European Union, *Joined Cases Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General* (C-293/12) and *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* (C-594/12), 8 April 2014.

Court of Justice of the European Union, *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14), 6 October 2015.

Court of Justice of the European Union, *Opinion 1/15 Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data from the European Union to Canada*, 26 July 2017.

Court of Justice of the European Union, *SABAM v Netlog NV* (C-360/10), 16 February 2012.

Court of Justice of the European Union, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (C-70/10), 24 November 2011.

Cybersecurity and criminal justice

These references have been derived Annex 3, after section A3.3.3, pages 63 ff.

- Boutayeb, Chahira. *Droit et Institutions de l'Union Européenne: La Dynamique Des Pouvoirs*. Systèmes. Paris: LGDJ, 2011.
- Choraś, Michał, and Rafał Kozik, eds. *Comprehensive Roadmap (Research Agenda) for Fight against Cybercrime and Cyber Terrorism*. CAMINO Project, 2016. http://www.fp7-camino.eu/assets/files/Book-CAMINO_roadmap_250316.pdf.
- 'CYBERROAD D-3.1: Social, Economic, Political, and Legal Landscape Report', 31 May 2015. http://www.cyberroad-project.eu/m/filer_public/2016/05/02/d31_social_economic_political_and_legal_landscape_report.pdf.
- 'E-CRIME D-3.2: Final Report on Counter-Measures Including Policy and Enforcement Responses', 31 March 2015. <http://ecrime-project.eu/wp-content/uploads/2015/02/E-CRIME-Deliverable-3-2-FINAL.pdf>.
- European Criminal Policy Initiative. 'A Manifesto on European Criminal Policy'. *Zeitschrift Für Internationale Strafrechtsdogmatik* 4, no. 12 (2009): 707–16.
- . 'A Manifesto on European Criminal Procedure Law'. *Zeitschrift Für Internationale Strafrechtsdogmatik* 8, no. 11 (2013): 430–46.
- 'EVIDENCE D-3.1: Overview of Existing Legal Framework in the EU Member States', 30 October 2015.
- 'FIDUCIA D-9.2: Report Conceptualising and Classifying Cybercrime', 3 October 2013. <http://www.fiduciaproject.eu/page/45>.
- 'FIDUCIA D-9.3: Paper on Current Domestic and Supranational Policies on Cybercrime', 28 April 2014. <http://www.fiduciaproject.eu/page/45>.
- Ghernaouti-Hélie, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. EPFL Press, 2013. <http://www.epflpress.org/product/51/9782940222667>.
- Internet Rights & Principles Coalition. 'The Charter of Human Rights and Principles for the Internet'. Accessed 13 December 2016. http://internetrightsandprinciples.org/site/wp-content/uploads/2014/08/IRPC_Booklet-English_4thedition.pdf.
- Klip, André. *European Criminal Law: An Integrative Approach*. 3rd edition. Cambridge: Intersentia, 2016.
- Koops, Bert-Jaap, and Tessa Robinson. 'Cybercrime Law: A European Perspective'. In *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd edition. Waltham, MA: Academic Press, 2011.
- Pavone, Vincenzo, Elvira Santiago Gomez, and David-Olivier Jaquet-Chiffelle. 'A Systemic Approach to Security: Beyond the Tradeoff between Security and Liberty'. *Democracy and Security* 12, no. 4 (1 October 2016): 225–46. doi:10.1080/17419166.2016.1217776.
- Summers, Sarah, Christian Schwarzenegger, Gian Ege, and Finlay Young. *The Emergence of EU Criminal Law: Cybercrime and the Regulation of the Information Society*. Oxford: Hart Publishing, 2014. <http://www.bloomsburycollections.com/book/the-emergence-of-eu-criminal-law-cybercrime-and-the-regulation-of-the-information-society>.



United Nations Office on Drugs and Crime. 'Comprehensive Study on Cybercrime'. Draft, February 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Cybersecurity, privacy and the European data protection framework

These references originate from Annex 4, pages 73 ff. They had been sorted by academic sources, European and non-European legislation, as well as case law and policy documents.

Note from the author: URL addresses listed in the references section to point to the respective document sources originate from those which could be found on the Internet at the time of writing this White Paper, i. e. were valid links at the appointed date of August 7th 2017. No guarantee was given that those URLs still function at the time of any recipient reading this document.

Academic sources

Amnesty International (2017): *Dangerously disproportionate: The ever-expanding national security state in Europe*. January 17th 2017. Available at: <https://www.amnesty.org/en/documents/eur01/5342/2017/en/>

Austin, L. M. (2015): *Surveillance and the Rule of Law*. Debate article published in the *Surveillance & Society Journal* Vol 13, No 2 (2015). Available at: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/viewFile/law_rule/law_rul

Bellovin, S. M.; Blaze, M.; Clark, S.; Landau, S. (2014): *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*. 12 Nw. J. Tech. & Intell. Prop. 1 (2014). Available at: <http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1>

Chaos Computer Club (2011): *Chaos Computer Club analyzes government malware*. October 8th 2011. Available at: <https://www.ccc.de/en/updates/2011/staatstrojaner>

Marks, Joseph (2017): *Obama's Cyber Legacy: He Did (Almost) Everything Right and It Still Turned Out Wrong*. Article published at nextgov.com January 17th 2017. Available at: <http://www.nextgov.com/cybersecurity/2017/01/obamas-cyber-legacy-he-did-almost-everything-right-and-it-still-turned-out-wrong/134612/>

Nakashima, E. (2016): *Powerful NSA hacking tools have been revealed online*. The Washington Post Online, August 16th 2016. Available at: https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html?utm_term=.61735c899442

Pietrosanti, F. and Aterno, S. (2017): *Italy unveils a legal proposal to regulate government hacking*. February 15th 2017. Available at: <https://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html>

The H Security blog (2012): *Federal Commissioner unable to audit Federal Trojan source*. Article published September 11th 2012. Available at: <http://www.h-online.com/security/news/item/Federal-Commissioner-unable-to-audit-Federal-Trojan-source-1704460.html>

Rannenber, K.; Royer, D.; Deuker A. (ed.) (2017): *The Future of Identity in Information Society - Challenges and Opportunities*. Pages 292 ff. (section 7.3 - When Idem meets Ipse: The Identity of

the European Citizen)World Economic Forum ‘*Global Risks Report 2017*’ Insight Report, 12th Edition by the Global Competitiveness and Risks Team. Available at: http://www3.weforum.org/docs/GRR17_Report_web.pdf

Legislation

Charter of Fundamental Rights of the European Union. OJ C 364, 18.12.2000, p. 1–22. Available at: [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000X1218\(01\)](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000X1218(01))

Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012, p. 47–390. Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT>

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community. Signed at Lisbon, 13 December 2007. OJ C 306, 17.12.2007, p. 1–271. Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT>

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995, p. 31-50. Available at: <http://eur-lex.europa.eu/eli/dir/1995/46/oj>

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, p. 1–88. Available at: <http://eur-lex.europa.eu/eli/reg/2016/679/oj>

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. OJ L 119, 4.5.2016, p. 89–131. Available at: <http://eur-lex.europa.eu/eli/dir/2016/680/oj>

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31.7.2002, p. 37. Available at: <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002L0058>

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. OJ L 386/89, 29.12.2006, p. 89-100. Available at: http://eur-lex.europa.eu/eli/dec_framw/2006/960/oj

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. OJ L 350, 30.12.2008, p. 60–71. Available at: http://eur-lex.europa.eu/eli/dec_framw/2008/977/oj

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (EUROPOL). OJ L121/37, 15.5.2009, p. 37 – 66. Available at: <http://eur-lex.europa.eu/eli/dec/2009/371/oj>

Case law and policy documents

Article 29 Working Party: *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*. Adopted on 4 April 2017 (WP247). Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

- CNIL (2017): Commission Nationale de l'Informatique et des Libertés: Encryption: security element of information assets. 18 July 2017. Available at: <https://www.cnil.fr/en/what-cnils-position-terms-encryption>
- CNIL (2018): Commission Nationale de l'Informatique et des Libertés: Security of personal data. 4 April 2018. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf
- European Data Protection Supervisor: *Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*. April 24th 2017. Available at: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf
- High Representative of the European Union for Foreign Affairs and Security Policy: *Cybersecurity Strategy of the European Union - An Open, Safe and Secure Cyberspace*. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Brussels 7.2.2013. JOIN (2013) 1 final. Available at: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
- Council of the European Union Presidency: *Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report*. Note 14711/16 to the Permanent Representatives Committee/Council, Brussels, November 23rd 2016. Available at: <http://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf>
- Council of the European Union - Justice and Home Affairs department: *Outcome of the 3508th Council meeting*, Document 15391/16, section 'Criminal justice in Cyberspace' and Press release 67, Brussels, 8th and 9th December 2016. Available at: <http://data.consilium.europa.eu/doc/document/ST-15391-2016-INIT/en/pdf>
- European Group on Ethics in Science and New Technologies: *Ethics of Security and Surveillance Technologies*. Opinion No. 28, Brussels, May 20th 2014. Available at: <https://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologies-pbNJAJ14028/>
- European Union Agency for Network and Information Security (ENISA): *ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards our Digital Identity*. Released December 2016. Available at: <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption>
- European Union Agency for Network and Information Security (ENISA): *ENISA Threat Taxonomy - A tool for structuring threat information*. Initial Version 1.0, January 2016. Available at: <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information>

Non-European and national legislation, case law and policy documents

- Census court decision of the German Federal Constitutional Court (In German: *Volkszählungsurteil Bundesverfassungsgericht*). 15th December 1983. Az.: 1 BvR 209, 269, 362, 420, 440, 484/83. Available at: https://cdn.zensus2011.de/live/uploads/media/volkszaehlunsurteil_1983.pdf
- Court Decision of the German Federal Constitutional Court on the basic right of every citizen to have full integrity and confidentiality of his or her information technology systems (In German: 'Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme'). 27th February 2008. Az.: 1 BvR 370/07. Available at: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html



3. Attitudes and Options regarding cybersecurity

The sources in this chapter were derived from the CANVAS White Paper 3 (Attitudes and Options regarding Cybersecurity), Appendix A.4, pages 43 ff.

NB: titles of must-read references are highlighted in **bold** print (with or without *italics*).

Books and articles

- BERKNIK, Igor and Gorazd MESKO (2012): Study of the perception of cyber threats and the fear of cybercrime. *Proceedings of the 7th International Conference on Information Warfare and Security (ICIW2012)*, University of Washington, Seattle, USA, 22-23 March 2012, p. 27-35 (ISBN 978-1-908272-29-4)
- ESCHENBURG, Felix, Jani LYLKANGAS, Nicole KRÄMER, Veikko SURAKKA, Heide TROITZSCH, Kimmo VUORINEN and Gary BENTE (2005): User acceptance: the BioSec approach. *Biometric Technology Today*, 13(7), 2005, p. 8-10 ([https://doi.org/10.1016/S0969-4765\(05\)70369-6](https://doi.org/10.1016/S0969-4765(05)70369-6))
- FRIEDEWALD, Michael, J. Peter BURGESS, Johann ČAS, Walter PEISSL and Rocco BELLANOVA (eds.) (2017): ***Surveillance, privacy and security: citizens' perspectives***[#] Oxon, Routledge, 2017 (PDF version available for free) (<http://www.tandfebooks.com/doi/book/10.4324/9781315619309>)
- FURNELL, S.M. and T. KARWENI (1999): Security implications of electronic commerce: a survey of consumers and businesses. *Internet Research*, 9(5), 1999, p. 372-382 (<https://doi.org/10.1108/10662249910297778>)
- GASKELL, George, Herbert GOTTWEIS, Johannes STARKBAUM, Monica M. GERBER, Jacqueline BROERSE, Ursula GOTTWEIS, Abbi HOBBS, Ilpo HELÉN, Maria PASCHOU, Karoliina SNELL and Alexandra SOULIER (2013): Publics and biobanks: pan-European diversity and the challenge of responsible innovation. *European Journal of Human Genetics*, 21(1), 2013, p. 14-20 (<https://doi.org/10.1038/ejhg.2012.104>)
- GILES, Keir and Kim HARTMANN (2014): Socio-political effects of active cyber defence measures. 2014 6th International Conference on Cyber Conflict (CyCon 2014) (<https://doi.org/10.1109/CYCON.2014.6916393>)
- GOODSON, M. L. and B. G. VERNON (2003): A study of public opinion on the use of tissue samples from living subjects for clinical research. *Journal of Clinical Pathology*, 57(2), 2003, p. 135-138 (<https://doi.org/10.1136/jcp.2003.9886>)
- HANSEN, Marit, Meiko JENSEN and Martin ROST (2015): Protection goals for privacy engineering. Security and Privacy Workshops (SPW), IEEE, 2015, p. 159-166 (<https://doi.org/10.1109/SPW.2015.13>)
- HEGEMANN, L. (2018): 'Deutschland bekommt eine Agentur für innere Netzsicherheit'. 29 AUGUST 2018, published on Zeit Online. Available at: <https://www.zeit.de/digital/internet/2018-08/cybersicherheit-bundesregierung-innovation-cyberagentur-netzpolitik>
- KETTIS-LINDBLAD, Åsa, Lena RING, Eva VIBERTH and Mats G. HANSSON (2007): Perceptions of potential donors in the Swedish public towards information and consent procedures in relation to use of human tissue samples in biobanks. A population-based study. *Scandinavian Journal of Public Health*, 35(2), 2007, p. 148-156 (<https://doi.org/10.1080/14034940600868572>)

[#] This reference is a must read to get an overview of the most relevant findings.

- PAVONE, Vincenzo, Elvira SANTIAGO GOMEZ and David-Olivier JAQUET-CHIFFELLE (2016): A systemic approach to security: beyond the tradeoff between security and liberty. *Democracy and Security*, 12(4), 2016, p. 225-246 (<https://doi.org/10.1080/17419166.2016.1217776>)
- RILEY, Chris, Kathy BUCKNER, Graham JOHNSON and David BENYON (2009): Culture & biometrics: regional differences in the perception of biometric authentication technologies. *AI & Society*, 24(3), 2009, p. 295-306 (<https://doi.org/10.1007/s00146-009-0218-1>)
- SANCHEZ, Orestes (2005): BioSec: a European project. *Biometric Technology Today*, 13(6), 2005, p. 9 ([https://doi.org/10.1016/S0969-4765\(05\)70347-7](https://doi.org/10.1016/S0969-4765(05)70347-7))
- SNELL, K., J. STARKBAUM, G. LAUB, A. VERMEER and I. HELÉN (2012): From protection of privacy to control of data streams: a focus group study on biobanks in the information society. *Public Health Genomics*, 15(5), 2012, p. 293-302 (<https://doi.org/10.1159/000336541>)
- TUPASELA, Aaro, Sinikka SIHVO, Karolna SNELL, PA JALLINOJA, Arja R. ARO and Elina HEMMINKI (2010): Attitudes towards biomedical use of tissue sample collections, consent, and biobanks among Finns. *Scandinavian Journal of Public Health*, 38(1), 2010, p. 46-52 (<https://doi.org/10.1177/1403494809353824>)
- VON LIECHTENSTEIN, Alfred (2002): *Internet und Öffentlichkeit*. Vienna, WUV Universitätsverlag, 2002 (ISBN 978-3-85114-667-7)

EU projects

This reference section of White Paper 3 also points towards a complete EU Projects Overview in its section A.1. (see there pages 40 f.)

CANVAS: constructing an alliance for value-driven cybersecurity: <https://canvas-project.eu>

CONSENT: consumer sentiment regarding privacy: <http://www.consent.law.muni.cz/>

‘CONSENT D-7.3: Synthesised all countries report’[#]: Public deliverable, February 2013 (not available online)

PACT: public perception of security and privacy: <http://www.projectpact.eu>

‘PACT D-4.2: Survey report’[#]: Public deliverable, 20 June 2014:
<http://www.projectpact.eu/deliverables/wp4-data-analysis/d4.2/D4.2.pdf/view>

‘PACT: Final report summary’: http://cordis.europa.eu/result/rcn/181728_en.html

PRESCIENT: privacy and emerging sciences and technologies: <http://www.prescient-project.eu>

‘PRESCIENT D-3: Privacy, data protection and ethical issues in new and emerging technologies’[#]:
Public deliverable, 16 May 2012: http://prescient-project.eu/prescient/inhalte/download/PRESCIENT_Deliverable_3_Final.pdf

PRISE: privacy enhancing shaping of security research and technology: <http://www.prise.oew.ac.at>
Supported by PASR (preparatory action on the enhancement of the European industrial potential in the field of security research)

[#] This reference is a must read to get an overview of the most relevant findings.

'PRISE D-5.8: Synthesis report – interview meetings on security technology and privacy'[#]: Public deliverable, April 2008: http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf

'PRISE D-6.2: Criteria for privacy enhancing security technologies': Public deliverable, 2008: http://www.prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf

'PRISE D-7.6: Concluding conference statement paper': Public deliverable (no date): http://www.prise.oeaw.ac.at/docs/PRISE_Statement_Paper.pdf

PRISMS: privacy and security mirrors: <http://prismsproject.eu>

'PRISMS D-10.1: Report on statistical analysis of survey'[#]: Public deliverable, 16 October 2015 (not available online)

'PRISMS D-9.1: Findings from qualitative focus groups': Public deliverable, 29 October 2013: <http://prismsproject.eu/wp-content/uploads/2014/01/PRISMS-D9-1-Focus-Groups-Report.pdf>

'PRISMS: Final report summary': http://cordis.europa.eu/result/rcn/191772_en.html

RESPECT: rules, expectations and security through privacy enhanced convenient technologies: <http://respectproject.eu>

'RESPECT D-11.3: Synthesised all countries report (quantitative data)'[#]: Public deliverable, 19 May 2015 (not available online)

'RESPECT: Periodic report summary 1': http://cordis.europa.eu/result/rcn/153820_en.html

SMART: scalable measures for automated recognition technologies: <http://www.smartsurveillance.eu>

'SMART: Report summary': http://cordis.europa.eu/result/rcn/178069_en.html

SurPRISE: surveillance, privacy and security: <http://surprise-project.eu>

'SurPRISE D-6.10: Synthesis report'[#]: Public deliverable, February 2015: <http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.10-Synthesis-report.pdf>

'SurPRISE D-6.12: Workshop report': Public deliverable, December 2014: <http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.12-Workshop-report.pdf>

'SurPRISE presentation: Aligning security and privacy. En route towards acceptable surveillance'. Sara Degli Esposti, Vincenzo Pavone and Elvira Santiago: Joint conference of SurPRISE, PRISMS and PACT, Vienna, 13-14 November 2014: http://surprise-project.eu/wp-content/uploads/2014/11/Degli-Esposti_Aligning-security-and-privacy-en-route-toward-acceptable-surveillance.pdf

'SurPRISE, PRISMS and PACT: Abstract booklet' *Citizens' perspectives on surveillance, security and privacy: controversies, alternatives and solutions*. Joint final conference, Vienna, 13-14 November 2014: http://surprise-project.eu/wp-content/uploads/2014/11/Booklet_Final.pdf

'SurPRISE: Report summary': http://cordis.europa.eu/result/rcn/171903_en.html

[#] This reference is a must read to get an overview of the most relevant findings.

Other surveys

- 'Flash Eurobarometer 225: Data Protection in the European Union – Citizens' Perception'
Analytical Report, The Gallup Organization (for the European Commission), 2008
http://ec.europa.eu/commfrontoffice/publicopinion/flash/fl_225_en.pdf
- 'Global State of Information Security® Survey 2017'
PricewaterhouseCoopers International Limited (PwCIL)
<http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>
- 'Special Eurobarometer 341: Biotechnology'
Report, TNS Opinion & Social (for the European Commission), 2010
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_341_en.pdf
- 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union'
Report, TNS Opinion & Social (for the European Commission), 2011
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf
- 'Special Eurobarometer 390: Cyber Security'
Report, TNS Opinion & Social (for the European Commission), 2012
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdf
- 'Special Eurobarometer 404: Cyber Security'
Report, TNS Opinion & Social (for the European Commission), 2013
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_404_en.pdf
- 'Special Eurobarometer 423: Cyber Security'**[#]
Report, TNS Opinion & Social (for the European Commission), 2015
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf
- 'Special Eurobarometer 432: Europeans' Attitudes towards Security'
Report, TNS Opinion & Social (for the European Commission), 2015
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_432_en.pdf
- 'Special Eurobarometer 464a: Europeans' Attitudes towards Security'
Report, TNS Opinion & Social (for the European Commission), 2015
<http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171>

Legislation and Policy Documents

European Union

- COM (2018): European Commission: Communication from the commission to the European Parliament, the European Council and the Council - Sixteenth Progress Report towards an effective and genuine Security Union. Brussels, 10.10.2018. COM (2018) 690 final. Available at:
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181010_com-2018-690-communication_en.pdf
- COM (2018b): European Commission: Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Brussels, 12.9.2018. COM(2018) 630 final. 2018/0328 (COD). Available at:

[#] This reference is a must read to get an overview of the most relevant findings.

https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf

‘Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime’

European Commission, Communication COM/2000/890 final, Brussels, 26 January 2001

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0890>

‘**Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace**’[#]

European Commission, Joint communication JOIN/2013/1 final, Brussels, 7 February 2013

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001>

‘Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union’

[2016] OJ L 194/1 (NIS Directive)

<http://data.europa.eu/eli/dir/2016/1148/oj>

‘**ENISA Threat Landscape Report 2016**’[#]

European Union Agency for Network and Information Security (ENISA), January 2017

<https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016>

‘European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual Public-Private-Partnership (cPPP)’

European Cyber Security Organisation (ECSO), June 2016

<http://www.ecs-org.eu/documents/ecs-cppp-sria.pdf>

‘Opinion 8/2015 on Dissemination and use of intrusive surveillance technologies’

European Data Protection Supervisor (Giovanni Buttarelli), Brussels, 15 December 2015

https://edps.europa.eu/sites/edp/files/publication/15-12-15_intrusive_surveillance_en.pdf

‘Opinion 9/2001 on the Commission Communication on “Creating a safer information society by improving the security of information infrastructures and combating computer-related crime”

Article 29 Working Party, WP 51, 5 November 2001

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp51_en.pdf

‘Opinion on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a “Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace”, and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union’

European Data Protection Supervisor (Peter Hustinx), Brussels, 14 June 2013

https://edps.europa.eu/sites/edp/files/publication/13-06-14_cyber_security_en.pdf

‘Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC’

[2016] OJ L 119/1 (General Data Protection Regulation)

<http://data.europa.eu/eli/dir/2016/1148/oj>

‘Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry’

European Commission, Communication COM/2016/410 final, Brussels, 5 July 2016

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410>

'The EDPS Strategy 2015-2019'[#]

European Data Protection Supervisor, Publications Office of the EU, Luxembourg, 2015
<https://doi.org/10.2804/35559>

Other (non-EU)

'36th Activity Report 2015'

Commission Nationale de l'Informatique et des Libertés (CNIL), France
https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_2015_gb.pdf

'Cyber Defence Pledge'

North Atlantic Treaty Organization (NATO), Press release (2016) 124, 8 July 2016
http://www.nato.int/cps/en/natohq/official_texts_133177.htm

'French National Digital Security Strategy'

République française, France, 2015
<https://www.ssi.gouv.fr/en/actualite/the-french-national-digital-security-strategy-meeting-the-security-challenges-of-the-digital-world/>

'National Cyber Security Strategy'

Gobierno de España, Spain, 2013
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf

'National Cybersecurity Strategy II'

Gouvernement du Grand-Duché de Luxembourg, 2015
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf

'Privacy: working with business – Ten corporate best practices to improve your business'

Garante per la Protezione dei Dati Personali, Italy
<http://www.garanteprivacy.it/documents/10160/2416443/Privacy%3A+working+with+business-vademecum.pdf>

'The National Cyber Security Strategy of the Republic of Croatia'

Official Gazette No 108/2015, Zagreb, 7 October 2015
<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf>

'The Standard Data Protection Model: a concept for inspection and consultation on the basis of unified protection goals'

German Data Protection Authorities, Kühlungsborn, 9-10 November 2016
https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html
See also: <https://www.datenschutzzentrum.de/sdm/>

[#] This reference is a must read to get an overview of the most relevant findings.

4. Technological challenges in cybersecurity

The sources in this chapter were derived from the CANVAS White Paper 4 (Technological challenges in cybersecurity), there in Appendix A.2 (recommendations for further reading) and A.3 (reference section of the paper), pages 34 ff.

Author recommendations for further reading

The authors recommend the following literature in order to gain deeper insights into the topics discussed in the White Paper:

ENISA Threat Taxonomy - A tool for structuring threat information. *This report by ENISA contains a taxonomy of threats to information and communication systems, both in the cyber- and physical space. The proposed taxonomy is a compilation of works carried out from 2012 to 2015 and has been used internally by ENISA as a common reference in other cybersecurity related reports.* Available at: <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information>

ENISA Privacy and Data Protection by design - from policy to engineering. *This document collects previous works on Privacy-by-design and the strategies to develop software that preserves the privacy of their users. These strategies inspire part of the GDPR and should be followed by compliant software. Next, it describes specific tools and technologies to develop said strategies.* Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

Scientific advice mechanism scoping paper: Cybersecurity. *This work provides an introduction on the cyber-security topic and the state of the policies of the EU.* Available at: https://ec.europa.eu/research/sam/pdf/meetings/hlg_sam_012016_scoping_paper_cybersecurity.pdf

Delfs, H., Knebl, H. (2015): Introduction to cryptography (Vol. 2). Springer, ISBN: 978-3-662-47973-5 (Print) 978-3-662-47974-2 (Online). *This book covers key concepts in modern cryptography, from encryption and digital signatures to more advanced cryptographic protocols. Topics on algebra, number theory, probability theory and information theory are included, so no previous background is required.*

Lecture notes on cryptography. Summer course “Cryptography and computer security” at MIT. *Collection of lecture notes from the summer course on cryptography at MIT by Shafi Goldwasser and Mihir Bellare. The notes cover most of the basic topics in cryptography, including an introduction to information theory and number theory, which are the basis of modern cryptography.* Available at: <https://cseweb.ucsd.edu/~mihir/papers/gb.pdf>

Hundepool, A., Domingo-Ferrer, J., Franconi, L., Giessing, S., Nordholt, E.S., Spicer, K., de Wolf P.-P. (2012): Statistical disclosure control. Wiley and Sons, ISBN: 978-1-119-97815-2. *This book introduces the topic of statistical disclosure control and provides several strategies for protecting the privacy of respondents in microdata databases. The work most prominently contains the definition of k-anonymity and other privacy models, along with mechanisms to achieve k-anonymity.*

References of White Paper 4

- Abril, D., Navarro-Arribas, G., & Torra, V. (2011). On the declassification of confidential documents. *Modeling decision for artificial intelligence*, 235-246.
- Ben-Or, M., Goldwasser, S., & Wigderson, A. (1988, January). Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Proceedings of the twentieth annual ACM symposium on Theory of computing* (pp. 1-10). ACM.
- Bier, E., Chow, R., Gollé, P., King, T. H., & Staddon, J. (2009). The rules of redaction: Identify, protect, review (and repeat). *IEEE Security & Privacy*, 7(6).
- Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). (Leveled) fully homomorphic encryption without bootstrapping. *ACM Transactions on Computation Theory (TOCT)*, 6(3), 13.
- Burridge, J. (2003). Information preserving statistical obfuscation. *Statistics and Computing*, 13(4), 321-327.
- Chakaravarthy, V. T., Gupta, H., Roy, P., & Mohania, M. K. (2008, October). Efficient techniques for document sanitization. In *Proceedings of the 17th ACM conference on Information and knowledge management* (pp. 843-852). ACM.
- Chaum, D., Crépeau, C., & Damgard, I. (1988, January). Multiparty unconditionally secure protocols. In *Proceedings of the twentieth annual ACM symposium on Theory of computing* (pp. 11-19). ACM.
- Chaum, D., & Van Heyst, E. (1991). Group signatures. In *Advances in Cryptology—EUROCRYPT'91* (pp. 257-265). Springer Berlin/Heidelberg.
- Cumby, C. M., & Ghani, R. (2011, August). A Machine Learning Based System for Semi-Automatically Redacting Documents. In *IAAI*.
- Diffie, W., & Hellman, M. E. (1976, June). Multiuser cryptographic techniques. In *Proceedings of the June 7-10, 1976, national computer conference and exposition* (pp. 109-112). ACM.
- Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6), 644-654.
- Domingo-Ferrer, J., & Mateo-Sanz, J. M. (2002). Practical data-oriented microaggregation for statistical disclosure control. *IEEE Transactions on Knowledge and data Engineering*, 14(1), 189-201.
- Domingo-Ferrer, J., & González-Nicolás, Ú. (2010). Hybrid microdata using microaggregation. *Information Sciences*, 180(15), 2834-2844.
- Domingo-Ferrer, J., & Torra, V. (2005). Ordinal, continuous and heterogeneous k-anonymity through microaggregation. *Data Mining and Knowledge Discovery*, 11(2), 195-212.
- Domingo-Ferrer, J., & Muralidhar, K. (2016). New directions in anonymization: Permutation paradigm, verifiability by subjects and intruders, transparency to users. *Information Sciences*, 337, 11-24.
- Douglass, M. M., Clifford, G. D., Reisner, A., Long, W. J., Moody, G. B., & Mark, R. G. (2005, September). De-identification algorithm for free-text nursing notes. In *Computers in Cardiology, 2005* (pp. 331-334). IEEE.
- ENISA (2018): European Union Agency for Network and Information Security: Looking into the crystal ball – A report on emerging technologies and security challenges. Version 1.0 31 January 2018. Available at: <https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball>

- Finkel, J. R., Grenager, T., & Manning, C. (2005, June). Incorporating non-local information into information extraction systems by gibbs sampling. In *Proceedings of the 43rd annual meeting on association for computational linguistics* (pp. 363-370). Association for Computational Linguistics.
- Gentry, C. (2009). *A fully homomorphic encryption scheme*. Stanford University.
- Gentry, C., Halevi, S., & Smart, N. P. (2012, April). Fully homomorphic encryption with polylog overhead. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 465-482). Springer, Berlin, Heidelberg.
- Goldwasser, S., Micali, S., & Wigderson, A. (1987). How to play any mental game, or a completeness theorem for protocols with an honest majority. In *Proc. of the Nienteenth Annual ACM STOC* (Vol. 87, pp. 218-229).
- Hajian, S., & Domingo-Ferrer, J. (2013). A methodology for direct and indirect discrimination prevention in data mining. *IEEE transactions on knowledge and data engineering*, 25(7), 1445-1459.
- Hajian, S., Domingo-Ferrer, J., Monreale, A., Pedreschi, D., & Giannotti, F. (2015). Discrimination-and privacy-aware patterns. *Data Mining and Knowledge Discovery*, 29(6), 1733-1782.
- Hajian, S., Domingo-Ferrer, J., & Farràs, O. (2014). Generalization-based privacy preservation and discrimination prevention in data publishing and mining. *Data Mining and Knowledge Discovery*, 28(5-6), 1158-1188.
- Jiang, W., Murugesan, M., Clifton, C., & Si, L. (2009, August). t-plausibility: Semantic preserving text sanitization. In *Computational Science and Engineering, 2009. CSE'09. International Conference on* (Vol. 3, pp. 68-75). IEEE.
- Kim, S., Sung, M. K., & Chung, Y. D. (2014). A framework to preserve the privacy of electronic health data streams. *Journal of biomedical informatics*, 50, 95-106.
- Machanavajjhala, A., Gehrke, J., Kifer, D., & Venkatasubramanian, M. (2006, April). l-diversity: Privacy beyond k-anonymity. In *Data Engineering, 2006. ICDE'06. Proceedings of the 22nd International Conference on* (pp. 24-24). IEEE.
- Muralidhar, K., Sarathy, R., & Domingo-Ferrer, J. (2014, September). Reverse mapping to preserve the marginal distributions of attributes in masked microdata. In *International Conference on Privacy in Statistical Databases* (pp. 105-116). Springer, Cham.
- Li, N., Li, T., & Venkatasubramanian, S. (2007, April). t-closeness: Privacy beyond k-anonymity and l-diversity. In *Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on* (pp. 106-115). IEEE.
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.
- Rubin, D. B. (1993). Discussion statistical disclosure limitation. *Journal of official Statistics*, 9(2), 461.
- Samarati, P., & Sweeney, L. (1998). *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression*. Technical report, SRI International.
- Sanchez, D., Batet, M., & Viejo, A. (2013). Automatic general-purpose sanitization of textual documents. *IEEE Transactions on Information Forensics and Security*, 8(6), 853-862.
- Sweeney, L. (1996). Replacing personally-identifying information in medical records, the Scrub system. In *Proceedings of the AMIA annual fall symposium* (p. 333). American Medical Informatics Association.
- Yao, A. C. C. (1986, October). How to generate and exchange secrets. In *Foundations of Computer Science, 1986., 27th Annual Symposium on* (pp. 162-167). IEEE.