Recommended Readings

On e-governance:

Skierka, Isabel. “When Shutdown Is No Option: Identifying the Notion of the Digital Government Continuity Paradox in Estonia’s EID Crisis.” *Government Information Quarterly*, vol. 40, no. 1, Jan. 2023, p. 101781, https://doi.org/10.1016/j.giq.2022.101781.

Vassil, K., Solvak, M., Vinkel, P., Trechsel, A. H., & Alvarez, R. M. (2016). The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015. *Government Information Quarterly*, 1–7. http://dx.doi.org/10.1016/j.giq.2016.06.007

Stephany, F. (2020). It’s not only size that matters: Determinants of Estonia’s e-governance success. *Electronic Government*, *16*(3), 304–313.

Solvak, M., Unt, T., Rozgonjuk, D., Võrk, A., Veskimäe, M., & Vassil, K. (2019). E-governance diffusion: Population level e-service adoption rates and usage patterns. *Telematics and Informatics*, *36*, 39–54. https://doi.org/10.1016/j.tele.2018.11.005

Parsovs, A. (2020). *Estonian Electronic Identity Card: Security Flaws in Key Management | USENIX*. Www.usenix.org. https://www.usenix.org/conference/usenixsecurity20/presentation/parsovs

Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). The return of coppersmith’s attack: practical factorization of widely used RSA moduli. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/3133956.3133969

Kerikmäe, T., Troitino, D. R., & Shumilo, O. (2019). An idol or an ideal? A case study of Estonian e-governance: Public perceptions, myths and misbeliefs. *Acta Baltica et Philosophiae Scientarium*, *7*(1), 71–80.

Solvak, M., & Vassil, K. (2018). Could Internet Voting Halt Declining Electoral Turnout? New Evidence That E-Voting Is Habit Forming. *Policy & Internet*, *10*(1), 4-21.

Kattel, R., & Mergel, I. (2019). Estonia's digital transformation: Mission mystique and the hiding hand (pp. 143-160).

Janowski, T. (2015). Digital government evolution: From transformation to contextualization. Government information quarterly, 32(3), 221-236. https://doi.org/10.1016/j.giq.2015.07.001

D’Agostino, M. J., Schwester, R., Carrizale, T., & Melitsk, J. (2011). A study of e-government and e-governance: an empirical examination of municipal websites. *Public Administration Quarterly*, *35*(1).

On cybersecurity:

‘Shadow in the East: Vladimir Putin and the New Baltic Front,’ by Aliide Naylor (2020)

‘Cyber War Will Not Take Place,’ by Thomas Rid (2013)

‘Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries,’ by Andrei Soldatov and Irina Borogan (2015)

‘Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers,’ by Andy Greenberg (2019)

‘The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age,’ by David E. Sanger (2018)

‘The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” by Lucas Kello in International Security 38, no. 2 (2013): 7-40.

‘Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security,’ at European Conference on Information Warfare and Security, Reading, UK (2018): 57-64.

‘The Cyberspace War: Propaganda and Trolling as Warfare Tools,’ by Jessikka Aro in European View 15 (2016): 121-132.

‘Small States and Big Ideas: Estonia’s Battle for Cybersecurity Norms,’ by Matthew Crandall and Collin Allan in Contemporary Security Policy 36, no. 2 (2015): 346-368.

Georgieva, Ilina. “The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace.” *Contemporary Security Policy*, vol. 41, no. 1, 9 Oct. 2019, pp. 33–54, https://doi.org/10.1080/13523260.2019.1677389.

Giles, Keir. “Russia’s Public Stance on Cyberspace Issues.” *IEEE Xplore*, 1 June 2012, ieeexplore.ieee.org/document/6243966. Accessed 13 Aug. 2020.

Broeders, D.W.J, et al. “A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace.” *Handle.net*, The Hague Program for Cyber Norms, Nov. 2019, hdl.handle.net/1887/136465. Accessed 22 Oct. 2024.

Urgessa, Worku Gedefa. “Multilateral Cybersecurity Governance: Divergent Conceptualizations and Its Origin.” *Computer Law & Security Review*, vol. 36, Apr. 2020, p. 105368, https://doi.org/10.1016/j.clsr.2019.105368.

von Solms, Basie, and Rossouw von Solms. “Cybersecurity and Information Security – What Goes Where?” *Information and Computer Security*, vol. 26, no. 1, 12 Mar. 2018, pp. 2–9, https://doi.org/10.1108/ics-04-2017-0025.

Whyte, C. (2020). Cyber conflict or democracy “hacked”? How cyber operations enhance information warfare. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa013

Etudo, U., Whyte, C., Yoon, V., & Yaraghi, N. (2023). From Russia with fear: fear appeals and the patterns of cyber-enabled influence operations. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad016

Collier, J. (2017). Strategies of cyber crisis management: Lessons from the approaches of Estonia and the United Kingdom. In *Ethics and policies for cyber operations* (pp. 187–212). Cooperative Cyber Defence Centre of Excellence.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21.

Backman, S. (2020). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, *29*(4), 429–438. https://doi.org/10.1111/1468-5973.12347