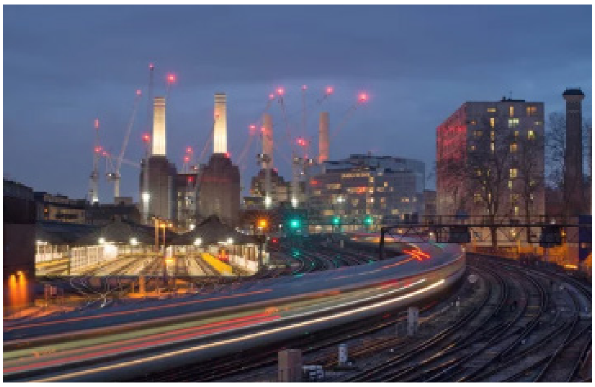
Improving the Cybersecurity of Critical National Infrastructure using Modelling and Simulation

Uchenna D Ani[1], Jeremy D McK Watson[2], Nilufer Tuptuk[3], Steve Hailes[4], Madeline Carr[5], Carsten Maple[6].

Summary

This briefing note aims to improve cybersecurity by raising awareness of the importance of adopting cybersecurity modelling and simulation techniques in Critical National Infrastructure (CNI) that embody integrated socio-technical factors. It is based on research and synthesis following a state-of-the-art literature survey and engagement workshop with critical infrastructure stakeholders hosted by the Department for Transport (DfT) in February 2019 and a desk-based study in the ongoing (2020-2022) PETRAS Modelling for Socio-technical Security (MASS) project. Participants from academia, business and industrial sectors, and government came together to discuss the effectiveness of modelling and simulation to support the protection of modern critical infrastructure systems. The discussion also covered how government effort can support the National Cyber Security Strategy 2016-2021, and beyond. Though the focus of the initial workshop was the transport sector, the recommendations made can be applied to other CNI sectors such as Energy, Water, Defence, Chemicals, and Food.



Who should read this?

This policy briefing is targeted at government departments and agencies with management and regulatory roles linked to critical infrastructure sectors such as Transport, Water, Energy, Defence, Chemicals, Food & Agriculture. The advice may be particularly relevant to DfT, Cabinet Office, BEIS, Home Office, DCMS, DEFRA, and GO-Science.

Overview

The UK's Critical National Infrastructure (CNI) is critically dependent on digital technologies that are progressively enhancing efficiency, productivity, reliability, and availability of infrastructure and services, and enabling new benefits not previously available. These can introduce vulnerabilities through the connectivity enabled by the digital systems, thus, making it easier for attackers to break in and sabotage an organisation.

1 School of Computing and Mathematics, Keele University, UK
2 Department of Science Technology Engineering and Public Policy, University College London
3 Department of Security and Crime Science, University College London
4, 5 Department of Computer Science, University College London
6 Cybersecurity Centre, WMG, University of Warwick, UK

Therefore, policies and strategies that manage risks must include an understanding of operator and corporate behaviours, as well as technical elements and the interfaces between them and humans.

Challenges

- Gaps exist in organisational understanding within the least aware critical infrastructure organisations.
- Operators may not understand the degrees of systems vulnerability or the types and subtlety of attacks.
- More aware infrastructure organisations tend to deal with cybersecurity at a purely technical level and sparsely consider and include behavioural and other social factors.

Recommendations

Best in class cybersecurity approaches use a holistic socio-technical viewpoint and are moving towards modelling and simulation (M&S) as a means of testing and assuring cybersecurity measures for securing modern critical infrastructure systems. Better CNI security via socio-technical security M&S can be achieved if backed by government effort, including appropriate policy interventions. The UK Government can contribute by sign-posting and shaping the decision-making environment concerning cybersecurity M&S approaches and tools, showing how they can contribute to enhancing security in Modern Critical Infrastructure Systems.

The Government can:

1. Encourage wider awareness and adoption of a socio-technical approach to security, from system M&S to implementation in CNIs.
2. Promote the use of critical infrastructure security open-source M&S approaches – tools and techniques.
3. Establish policies and platforms that encourage evaluating the credibility of security M&S approaches – tools and techniques.
4. Create and maintain governance for security M&S.
5. Support open, continuous cross-sector collaboration and knowledge exchange.
6. Promote team-based collaborative development of security M&S tools amongst academic/research, industry, and government organisations.
7. Incentivise and/or reward the dissemination of security M&S research outcomes.

Conclusion

Given the growing need to find ways of addressing the problem of security risk management in CNIs, M&S offers practical pathways, with techniques and tools to develop or improve security in the CNI domain. Besides encouraging the development of technologies and methodologies, policymakers can also contribute in other ways including leading by example and by shaping and signposting the environment under which decisions and actions are initiated, in favour of M&S to support effective security.

References

1. NCSC. CNI Hub. Website Article (2021).
2. Pescaroli G, Alexander D. Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Nat Hazards* 2016; 82: 175–192.
3. Ani UD, Watson JDM, Nurse JRC, et al. A Review of Critical Infrastructure Protection Approaches: Improving Security Through Responsiveness To the Dynamic Modelling Landscape. In: *PETRAS/IET Conference Living in the Internet of Things: Cybersecurity of the IoT - 2019 system*. London, UK: IET, pp. 1–16.
4. Ani UPD, He H (Mary), Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *J Cyber Secur Technol* 2017; 1: 32–74.
5. Davis J, Magrath S. A Survey of Cyber Ranges and Testbeds. Edinburgh South Australia (2013).
6. Ani UPD, Watson JM, Green B, et al. Design Considerations for Building Credible Security Testbeds : Perspectives from Industrial Control System Use Cases Design Considerations for Building Credible Security Testbeds : Perspectives from Industrial Control System Use Cases ABSTRACT. J *Cyber Secur Technol* 2020; 00: 1–49.
7. Government Office for Science. *Computational Modelling: Technical Futures*. London (2018).
8. Piggin R. *Cyber security and Critical National Infrastructure*. 2015; 1–4.
9. Ani UD, Watson JMK, Carr M, et al. A review of the use and utility of industrial network-based open-source simulators: functionality, security, and policy viewpoints. *J Def Model Simul* 2020; 9: 11–20.
10. Watson J, Ani UD. *Critical Infrastructure Protection Approaches: Analytical Outlook on Capacity Responsiveness to Dynamic Trends*. 2019; 1–41.
11. Newsweek Vantange. WEATHERING THE PERFECT STORM: SECURING THE CYBER-PHYSICAL SYSTEMS. London, UK (2020).
12. Department for Digital Culture Media & Sports (DCMS). *A safe and secure cyberspace - making the UK the safest place in the world to live and work online* (2017).
13. Oliva G, Panzieri S, Setola R. Modeling and simulation of critical infrastructures. *WIT Trans State Art Sci Eng* 2012; 54: 39–56.
14. Wynn DC, Kreimeyer M, Clarkson PJ, et al. Dependency modelling in complex system design. *J Eng Des* 2012; 23: 715–718.
15. Amélie G, Aurélia B, Emmanuel L. The Challenge of Critical Infrastructure Dependency Modelling and Simulation for Emergency Management and Decision Making by the Civil Security Authorities. In: Rome E, Theocharidou M, Wolthusen S (eds) *Critical Information Infrastructures Security. CRITIS 2015. Lecture Notes in Computer Science*. Cham: Springer Cham, pp. 255–258.
16. University of Cambridge. Centre for Digital Built Britain. *National Digital Twin Programme* (2020, accessed 11 December 2020).
17. National Infrastructure Commission. Data for the public good. London, UK (2017).
18. Watson JM, Ani UD. Review of Open Source Simulators in ICS/IIoT Security Context - ALIoTT Technical Report. *PETRAS Cybersecurity Research Hub, UK*.
19. 19. Lewis JA. Government Open Source Policies (2010).
20. Watson JM, Ani UD. Critical Infrastructure Protection Approaches: Analytical Outlook on Capacity Responsiveness to Dynamic Trends. Analytical Lenses for Internet of Things Threats (ALIoTT) Report, *PETRAS Cybersecurity Research Hub*.
21. DoD. Department of Defense Modeling and Simulation Best Practices Guide (2010).
22. McLean C, Lee YT, Jain S, et al. Modeling and Simulation of Critical Infrastructure Systems for Homeland Security Applications. *NIST Special Publications* 2011; 86.
23. SISO. Reference for Generic Methodology for Verification and Validation (GM-VV) to Support Acceptance of Models , Simulations and Data. 2013; 3: 1–48.
24. Nottinghamshire NHS Commissioning organisations. *Information Governance Management Framework*. 2019; 1–14.
25. Ohori KA, Ledoux H, Stoter J. Modeling and manipulating spacetime objects in a true 4D model. *J Spat Inf Sci* 2017; 14: 61–93.
26. Watson JM, Ani UD. Review of Open Source Simulators in ICS / IIoT Security Context PETRAS Project : Analytical Lenses for Internet of Things Threats (ALIoTT). 2018; 1–49.
27. The Cabinet Office. Open Source, Open Standards and Re-Use: Government Action Plan. *Policy Paper: An open source strategy for government* 2010; 1–9.