Moira Carroll-Mayer’s Project Proposals

1. Conduct a critical analysis of the BIS 27001 Standards series in the light of contemporary technologies and if/where your research indicates shortcomings in the effectiveness of the Standards make recommendations for increased effectiveness.
2. Cloud computing is increasingly dominant. Critically analyse the effectiveness of forensics or security in the cloud and where there are identifiable issue make recommendations for improvement.
3. Open Source products are increasingly favoured by defence and security entities. Critically analyse the implications for the robustness of defence and security systems.
4. For an international company numerous practical and legal issues must be addressed to ensure the security of information/data coming into, passing through and leaving its electronic systems. Create a project around the practical and related legal issues likely to arise. You will need to create a fictitious company and identify the nature of its business; the issues and possible scenarios you address are likely to be partially dictated by the nature of the company’s business.
5. Create a project that surveys and addresses the practical and associated legal issues that typically arise for an investigator of digital crime or of wrongdoing arising from involvement in a police operation or from an investigation into the concerns of a commercial entity. Note that whichever type of investigative action (police or commercial) you select for your project you will be expected to identify any differences of approach for that and the one you did not select. Regulation, legal constructs and the achievement and maintenance of systems security for critical infrastructure of states are increasingly irreconcilable; this is particularly so at the juxtaposition of state security and individual privacy. Critically analyse the foregoing statement, with regard to the US, UK and wider European efforts to achieve security for critical systems infrastructure and suggest solutions. Your research should address regulatory, legal and technological phenomena.
6. The term ‘Dark Web’ reflects the frequently impenetrable complexity of systems developed and operated often by those who wish to keep their activities beyond forensic and security efforts. Identify, critically analyse and suggest solutions to the most contemporary law enforcement issues confronted in the Dark Web. Your research should address regulatory, legal and technological phenomena.
7. Regulation, legal constructs and the achievement and maintenance of systems security are increasingly irreconcilable; this is particularly so at the juxtaposition of state security and individual privacy. Critically analyse the foregoing statement, with regard to the US, UK and wider European efforts to achieve security for systems infrastructure and suggest solutions. Your research should address regulatory, legal and technological phenomena.
8. Elliptic curve cryptography (ECC) is widely used to strengthen systems security. Critically analyse and suggest solutions for issues arising at the intersection of ECC with law enforcement efforts. Your research should address regulatory, legal and technological phenomena.
9. The European Data Protection Directive will affect the requirements of and penalties for in layman’s terms what might be described as looking after data properly. Critically analyse the likely effectiveness of the Directive and its implications for you and/ or your employer. In undertaking this research bear in mind that the UK government expects to incorporate the principles of the Directive in UK domestic law post Brexit.
10. There is much talk of quantum computing. Critically analyse the possible implications of quantum computing for cyber forensics or security. Your research should attempt to differentiate between the realm of the not yet possible and any effects that are currently being felt.