

Module Specification

Module Summary Information

1	Module Title	Security in the Digital Age
2	Module Credits	20
3	Module Level	7
4	Module Code	CRI7031

5	Module Overview
<p>This module will examine the intersection between digital technology and security in the contemporary era bringing together a range of topics and issues subsumed under the heading “cybersecurity”. Innovation in the field of digital technology has enhanced how security is performed but has also created opportunity for security breaches and the eroding of international norms and civil liberties. The module offers a comprehensive overview of the capabilities of digital security and the improved operationalisation of security. For instance, most if not all CCTV footage is digitally recorded, is easily digitally stored and can be transferred or shared instantly over digital networks. Such an example presents the efficiency and impact of the digital on security. However, with this comes considerations of how such data is managed and protected, as well as its potential to be exploited. Likewise, more and more of the management of national critical infrastructure is being housed on computer networks across the private and public sphere. Such developments aid the speed, efficiency and reliability of critical functions and process but also potentially provide a more accessible point of attack for a range of nefarious state and sub-state actors. The module will examine a range of different debates including the security and insecurity brought on by innovation in the field of digital technologies and the tensions that exist between how security is performed and how we can begin to understand freedoms and liberties and how these may be affected by particular security agendas.</p>	

6	Indicative Content
<ul style="list-style-type: none"> • Security in the Digital Age • History of Cybersecurity • Privacy and Security in the Digital Age • Dataveillance • Race and Surveillance • Bank Fraud and Money Laundering • The Dark Net • Corporate and Governmental Responsibility • Cyberattack : Means and Methods • Cyberwar: The fifth domain? • Cyberterrorism • Cyberattack : Attribution and Response • Constructing Cyberthreats • (Re)considering Security in the Digital Age 	

7	Module Learning Outcomes On successful completion of the module, students will be able to:
1	Demonstrate an applied knowledge of security in the digital environment that recognises both the theoretical and practical elements of this domain.
2	Demonstrate an understanding of and critically evaluate the tensions that exist between security and privacy in the digital domain.
3	Exhibit and utilise appropriate evidence from a range of academic sources to construct critical and original arguments.
4	Exhibit and apply a range of transferable skills including clear communication, effective independent and group based work and an ability to translate complex ideas to a wide audience.

8	Module Assessment		
Learning Outcome			
	Coursework	Exam	In-Person
1-4	X		

9	Breakdown Learning and Teaching Activities	
Learning Activities	Hours	
Scheduled Learning (SL) includes lectures, practical classes and workshops, peer group learning, Graduate+, as specified in timetable	24	
Directed Learning (DL) includes placements, work-based learning, external visits, on-line activity, Graduate+, peer learning, as directed on VLE	24	
Private Study (PS) includes preparation for exams	152	
Total Study Hours:	200	