1. **Title of the module**

POLIR8114 Governance and War in Cyberspace

1. **School or partner institution which will be responsible for management of the module**

Politics and International Relations

1. **The level of the module (Level 4, Level 5, Level 6 or Level 7)**

Level 7

1. **The number of credits and the ECTS value which the module represents**

20 credits (10 ECTS)

1. **Which term(s) the module is to be taught in (or other teaching pattern)**

Autumn or Spring

1. **Prerequisite and co-requisite modules**

None

1. **The programmes of study to which the module contributes**

This optional module contributes to all programmes offered by, and with, the School of Politics and International Relations.

1. **The intended subject specific learning outcomes.
On successfully completing the module students will be able to:**

1. Understand and critically assess various definitions of cyberspace, confidently dividing these into social and technical forms.

2. Demonstrate a rigorous comprehension of the existing structures for the governance of cyberspace, and the challenges of progressing this governance regime further.

3. Critique the manner in which cyberspace can be used as a means of power projection by both state and non-state actors.

4. Demonstrate a keen critical understanding of cyber weaponry and its potential effects, confidently distinguishing between ‘costly nuisances’ and ‘cyber disasters’.

5. Critically analyse the role of identity and representation in the formulation of a ‘Politics of Cybersecurity’, with reference to relevant case studies.

6. Rigorously apply knowledge gained in the module to assess cases of both ‘online’ and ‘offline’ conflagration.

1. **The intended generic learning outcomes.
On successfully completing the module students will be able to:**

1. Gather, organise and deploy evidence, data and information from a variety of secondary and some primary sources.

2. Identify, investigate, analyse, formulate and advocate solutions to problems.

3. Develop reasoned arguments, synthesise relevant information and exercise critical judgement.

4. Be self-reflective and critical of their own work.

5. Effectively use online bibliographic search engines, online resources, and conduct research.

6. Engage in academic and professional communication with others in both verbal and written format.

1. **A synopsis of the curriculum**

This module provides an overview of the degree to which cyberspace continues to revolutionise the operations of both state and non-state actors, and the challenges of governing this ‘fifth sphere’ of power projection. Whilst this module is not entrenched in International Relations or Security Studies theory, students will have the opportunity to apply both traditional and non-traditional approaches to the politics of cyberspace. Key themes include: 21st century technology, cyber warfare, espionage, surveillance, deterrence theory, cyberterrorism, and representation of threatening cyber-entities. Students will develop a toolkit to critique the existing state and NGO-based governance regime for cyberspace, and will convey arguments both for and against a ‘Geneva Convention’ for cyberspace.

1. **Reading list (Indicative list, current at time of publication. Reading lists will be published annually)**

Thomas Chen, Lee Jarvis and Stuart Macdonald, (2014) Cyberterrorism: Understanding, Assessment, and Response, New York: Springer

Nazli Choucri et al., (2019) Cyberspace and International Relations: The Co-Evolution Dilemma, Cambridge MA: MIT Press

Lucas Kello, (2018) The Virtual Weapon and International Order, New Haven CT: Yale University Press

Jan-Frederick Kremer and Benedikt Muller, (2014) Cyberspace and International Relations: Theory, Prospects and Challenges, New York: Springer

David Sanger, (2018) The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age, London: Scribe

Damien Van Puyvelde and Aaron Brantly, (2019) Cybersecurity: Politics, Governance and Conflict in Cyberspace, Cambridge: Polity Press

1. **Learning and teaching methods**

Total contact hours: 22

Private study hours: 128

Total study hours: 150

1. **Assessment methods**
	1. Main assessment methods

Policy paper, 1,500 words (40%)
Individual essay, 3,500 words (60%)

13.2 Reassessment methods

Reassessment instrument: 100% coursework

1. ***Map of module learning outcomes (sections 8 & 9) to learning and teaching methods (section12) and methods of assessment (section 13)***

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Module learning outcome** | 8.1 | 8.2 | 8.3 | 8.4 | 8.5 | 8.6 | 9.1 | 9.2 | 9.3 | 9.4 | 9.5 | 9.6 |
| **Learning/teaching method** |  |  |  |  |  |  |  |  |  |  |  |  |
| Lectures | **X** | **X** | **X** | **X** | **X** | **X** |  | **X** |  |  |  | **X** |
| Seminars | **X** | **X** | **X** | **X** | **X** | **X** | **X** | **X** | **X** |  |  | **X** |
| Private study | **X** | **X** | **X** | **X** | **X** | **X** | **X** | **X** | **X** | **X** | **X** |  |
| **Assessment method** |  |  |  |  |  |  |  |  |  |  |  |  |
| Policy paper | **X** | **X** | **X** | **X** |  | **X** | **X** | **X** | **X** | **X** | **X** |  |
| Essay | **X** | **X** | **X** | **X** | **X** | **X** | **X** | **X** | **X** | **X** | **X** |  |

1. **Inclusive module design**

The School recognises and has embedded the expectations of current equality legislation, by ensuring that the module is as accessible as possible by design. Additional alternative arrangements for students with Inclusive Learning Plans (ILPs)/declared disabilities will be made on an individual basis, in consultation with the relevant policies and support services.

The inclusive practices in the guidance (see Annex B Appendix A) have been considered in order to support all students in the following areas:

a) Accessible resources and curriculum

b) Learning, teaching and assessment methods

1. **Campus(es) or centre(s) where module will be delivered**

Canterbury

1. **Internationalisation**

Cyberspace, by default, is an international realm. Notwithstanding the technical considerations of the technology itself, from a legal perspective, one of the most significant dilemmas facing policymakers is the difficulty of extending overarching legal frameworks across many sovereign jurisdictions. When viewed through a North-South lens, cyberspace can serve as a fundamentally empowering realm; however, cyberspace can also serve to entrench existing power imbalances in terms of economy, military and culture. With encouragement, students will be invested with a toolkit with which they can critique these issues.

**FACULTIES SUPPORT OFFICE USE ONLY**

**Revision record – all revisions must be recorded in the grid and full details of the change retained in the appropriate committee records.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date approved | Major/minor revision | Start date of delivery of revised version | Section revised | Impacts PLOs (Q6&7 cover sheet) |
|  |  |  |  |  |
|  |  |  |  |  |