## KentVision Code and title of the module

POLI6910 Governance and War in Cyberspace

## Division and School/Department or partner institution which will be responsible for management of the module

Division of Human and Social Sciences, School of Politics and International Relations

## The level of the module (Level 4, Level 5, Level 6 or Level 7)

Level 6

## The number of credits and the ECTS value which the module represents

15 credits (7.5 ECTS)

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

Autumn

## Prerequisite and co-requisite modules and/or any module restrictions

None

## The course(s) of study to which the module contributes

#### Optional to the following courses:

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

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

8.1 Understand and critically assess various definitions of cyberspace

8.2 Demonstrate a critical understanding of the existing structures for the governance of cyberspace, and the challenges of progressing this governance regime further

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

8.4 Demonstrate a critical understanding of cyber weaponry and its potential effects

8.5 Critically analyse the role of identity and representation in the formation of a ‘Politics of Cybersecurity’

8.6 Apply knowledge gained in the module to assess cases of both ‘online’ and ‘offline’ conflagration.

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

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

9.2 Identify, investigate, analyse, formulate and advocate solutions to problems

9.3 Develop reasoned arguments, synthesise relevant information and exercise critical judgement

9.4 Be self-reflective and critical of their own work

9.5 Effectively use online bibliographic search engines, online resources, and conduct research

9.6 Engage in academic and professional communication with others*.*

## 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.

## Reading list

The University is committed to ensuring that core reading materials are in accessible electronic format in line with the Kent Inclusive Practices.

The most up to date reading list for each module can be found on the university's [reading list pages](https://kent.rl.talis.com/index.html).

## Contact Hours

Private Study: 128

Contact Hours: 22

Total: 150

## Assessment methods

* 1. Main assessment methods

Briefing papers (x 2) of 500 words each (2 x 15% = 30%)

Essay, 3,000 words (70%)

* 1. Reassessment methods

Reassessment instrument: 100% coursework

## Map of module learning outcomes (sections 8 & 9) to learning and teaching methods and methods of assessment (section 13)

**Module learning outcomes against learning and teaching methods:**

| 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 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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** |  |

**Module learning outcomes against assessment methods:**

| 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 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Briefing papers | **x** | **x** | **x** |  |  | **x** | **x** | **x** | **x** | **x** | **x** | **x** |
| Essay | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** |

## Inclusive module design

The Division 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

## Campus(es) or centre(s) where module will be delivered

Canterbury

## 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.

**DIVISIONAL USE ONLY**

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

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