

IMSIS Dissertation Feedback & Mark Sheet

Student Matriculation No.	Glasgow 2399044 DCU 18114423 Charles 65102261
Dissertation Title	Cyber deterrence as a challenge to International Security: How could a conceptual framework formulate national deterrence strategies to prevent warfare actions in the cyber domain?

INDIVIDUAL INSTITUTION GRADING

Reviewer 1 Initial Grade <i>Select from drop down list</i>	Reviewer 2 Initial Grade <i>Select from drop down list</i>	Late Submission Penalty <i>no penalty</i>
Word Count Penalty (1-15% over/under = 1gr point; 15-20% over/under = 2 gr points; 20-25% over/under = 3 gr points; more than 25% over/under = 0 fail)		
Word Count: 23934 Suggested Penalty: no penalty		

JOINT GRADING (subject to agreement of the external examiner and approval at Joint Exam Board)

Final Agreed Mark. (Following correspondence reviewers should list the agreed final internal grade taking before and after any penalties to be applied).

Before Penalty: B2 [16] **After Penalty:** B2 [16]

DISSERTATION FEEDBACK

Assessment Criteria	Rating
A. Structure and Development of Answer	
This refers to your organisational skills and ability to construct an argument in a coherent and original manner	
• <i>Originality of topic</i>	Very Good
• <i>Coherent set of research questions and/or hypothesis identified</i>	Very Good
• <i>Appropriate methodology and evidence of effective organisation of work</i>	Very Good
• <i>Logically structured argument and flow of ideas reflecting research questions</i>	Very Good
• <i>Application of theory and/or concepts</i>	Very Good
B. Use of Source Material	
This refers to your skills to select and use relevant information and data in a correct manner	
• <i>Evidence of reading and review of published literature</i>	Very Good
• <i>Selection of relevant primary and/or secondary evidence to support argument</i>	Good
• <i>Critical analysis and evaluation of evidence</i>	Very Good
• <i>Accuracy of factual data</i>	Very Good
C. Academic Style	
This refers to your ability to write in a formal academic manner	
• <i>Appropriate formal and clear writing style</i>	Very Good
• <i>Accurate spelling, grammar and punctuation</i>	Very Good
• <i>Consistent and accurate referencing (including complete bibliography)</i>	Good
• <i>Is the dissertation free from plagiarism?</i>	Yes

IMSIS Dissertation Feedback & Mark Sheet

• Evidence of ethics approval included (if required based on methodology)	Not required
• Appropriate word count	Yes

ADDITIONAL WRITTEN COMMENTS

Reviewer 1

The dissertation aimed to establish a conceptual framework for deterrence strategies in cyberspace. A realistic programme of research on the topic of deterrence was devised. The main argument was embedded in relevant topical literature. The structure is coherent and easy to follow. The dissertation demonstrates good understanding of deterrence theories and conceptual vocabulary of deterrence. It also illustrates the comprehension of difficulties in translating the language of deterrence into the cyberspace and cyber domains. The dissertation discussed the deterrence mainly from the Western (and often, the US) perspective – this could have been stated more explicitly in the introduction. A section on methodological challenges would have been helpful.

Chapter 1 set a stage by providing an overview of debates on classical and modern deterrence. The dissertation identified a number of approaches to deterrence, analysing their strengths and weaknesses. However, section 1.2 is a bit difficult to follow due to the lack of an overarching analytical framework. Some works, especially employed in Chapter 1, are missing from the bibliography, e.g. Brodie or Schelling (not ‘Schillings’). The analysis of cyber strategies of the EU and the US in the section 1.4 could have been referred to and engaged with more in further parts of the dissertation.

Chapter 2 focused on how international norms might act as international cyber deterrence and discussed the examples of cyber-attacks undertaken by nation states and non-state actors.

Especially the former part seems under-employed in further parts of the dissertation.

Chapter 3 proposes a framework for cyber deterrence strategies. The distinction between different types of deterrence is the dissertation’s forte. What seems to be missing is the boundary between measures undertaken within the framework of deterrence by denial that act as deterrence and those that result to a failure of the attack, while not deterring an attack as such. This part would also have benefitted from greater engagement with theoretical and conceptual implications of the proposed framework.

Minor remarks:

- minimal deterrence policy (p. 13) could have been discussed with reference to China’s nuclear policy rather than the Soviet/Russian-American post-Cold War context
- distinguishing between the ‘Western’ and the ‘Eastern’ patterns of behaviour in cyber domains was a bit simplifying (p. 27)
- the abbreviation ‘IR’ refers to the scholarly discipline of International Relations, it is better to use the term ‘international relations’ when referring to international politics and economy (e.g. p. 40)

Reviewer 2

This is an ambitious and potentially innovative thesis, attempting to provide a general framework for national cyber-deterrence strategy aimed at preventing warfare in the domain of cyber space. The dissertation combines concepts derived from deterrence theories, classic and modern, to reach a most efficient deterrence strategy. In most parts it is well written and the argument/s are clearly thought and articulated; it is therefore easily perceived that the student has given this question some good time to reflect upon and reading. While I liked much about the thesis, some important areas seem left underdeveloped. Firstly, the literature review is very descriptive and

IMSIS Dissertation Feedback & Mark Sheet

does not engage in a deep theoretical discussion of deterrence theory/ies. The student tells us that there has been an evolution of deterrence theory since the time of the great wars and mentions key historical event, but why, how and what challenges led to deterrence strategy to evolve from the perspective of states in a context of international competition and war are only briefly mentioned in passing rather than explained. We cannot fully grasp the challenges that lie ahead of establishing a national cyber-deterrence strategy (a new domain) if a proper layout of deterrence theories is lacking along the challenges that led to its evolution. What also is a reason of concern is that it is difficult to accept that the cyber domain can be so easily separated by the other domains of warfare. That is, can we really consider the cyber realm as separate and independent from the other realms of warfare, and can we ignore other states military and non-military capabilities in a grand cyber-deterrence strategy? Finally, the new framework proposed largely resembles a combination of all the deterrence strategies available and applicable to nation-states, the only real innovative bit resting on the addition of cumulative deterrence and a mention of the need to enhance international collaboration. Being the new framework the core of the innovative bit of the dissertation, I would have also wanted to see a more engaged theoretical discussion of its functioning and limits. For instance, I would have wanted to know more about the nature of those nation states the student believes this framework would apply best and those for which it doesn't and why? What are the main challenges to international collaborations and what solutions do we have to this? Perhaps most importantly, both scholars and practitioners have by now recognised that cyber challenges are multidimensional and thus require a multidimensional approach. The fact that the model provided only considers nation-states and their military domain is a strong limitation of the model. Overall, as mentioned at the start this is an ambitious dissertation and of very good quality.