IMSISS Dissertation Feedback & Mark Sheet

Student Matriculation No.	**Glasgow** 2478010 **DCU** 19108796 **Charles** 42696365
Dissertation Title	Shadow Warrior: The Outsourcing of the United States' Offensive Cyber Capabilities

INDIVIDUAL INSTITUTION GRADING

Reviewer 1 Initial Grade	***Reviewer 2 Initial Grade***	***Late Submission Penalty***
Select from drop down list	*Select from drop down list*	*no penalty*
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: 22.264 ***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: A4 [19] ***After Penalty:*** A4 [19]

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	
• *Originality of topic*	Excellent
• *Coherent set of research questions and/or hypothesis identified*	Very Good
• *Appropriate methodology and evidence of effective organisation of work*	Very Good
• *Logically structured argument and flow of ideas reflecting research questions*	Excellent
• *Application of theory and/or concepts*	Very Good
B. Use of Source Material This refers to your skills to select and use relevant information and data in a correct manner	
• *Evidence of reading and review of published literature*	Excellent
• *Selection of relevant primary and/or secondary evidence to support argument*	Excellent
• *Critical analysis and evaluation of evidence*	Excellent
• *Accuracy of factual data*	Excellent
C. Academic Style This refers to your ability to write in a formal academic manner	
• *Appropriate formal and clear writing style*	Excellent
• *Accurate spelling, grammar and punctuation*	Excellent
• *Consistent and accurate referencing (including complete bibliography)*	Excellent
• *Is the dissertation free from plagiarism?*	Yes
• *Evidence of ethics approval included (if required based on methodology)*	Not required

IMSISS Dissertation Feedback & Mark Sheet

• *Appropriate word count*	Yes

ADDITIONAL WRITTEN COMMENTS

Reviewer 1

This is an ambitious work focusing on outsourcing of US offensive cyber capabilities. The main research question asks which effect the private sector has on the United States' offensive cyber capabilities. In this respect the work seeks to determine which factors contribute to outsourcing of offensive cyber capabilities in the first place, and what effects such tendency has on the ability of the United States to conduct cyber operations.

Research direction and the scope of this work provide a contribution to an important and much needed debate by discussing why offensive cyber capabilities being outsourced, if it is one of the central components of state security. What is the scope of outsourcing of such capabilities and if it includes strategic ones? The work tries to understand whether private sector, having innovating potential, is this way becoming the source of a boost for state cyber technologies by providing access to latest developments and human capital. The scope is further expanded in the analysis part of the thesis.

The work is well structured, providing a solid literature review, methodological considerations, justifying the theoretical choices. One of the key areas that this research is tackling is the blurring line between private sector and the state when it comes to the militarisation of the cyber domain. It is a much overdue discussion, as state-private partnerships are becoming increasingly popular in offensive use of technology. Literature review sets the stage for theoretical chapter and helps direct the research. It well identifies gaps in existing literature and positions research to focus on addressing those gaps. It also discusses how cyber domain adds to, and in a way expands on, a traditional domain.

Throughout the work we learn about factors that contribute to the increase in outsourcing of cyber capabilities, and identify specific capabilities being outsourced. This development is further put into context when the work contrasts it with the history of military outsourcing, such as PMCs and other means. Importantly, the work is not shying away from considering ethical side of military functions' outsourcing.

Some areas can be improved, though. There are questions related to the methodological clarity of the work as well as the depth of methodological justification. While case study is a logical choice, it is not particularly clear how exactly selected method helps identify factors contributing to outsourcing of the offensive cyber capabilities. It would be of benefit to focus on explaining how methodologically speaking the limitation of the study, which is highly analytical, can be overcome. It would also help to expand discussion on why two other examples (two states) of existing dedicated cyber departments in the military are not discussed in detail. Thus, what are the limitations of a comparative case study in this case. On another note, a more specific discussion on the role of norms would be helpful.

Overall, it is a very diligently researched work. We learn a lot about the evolution of the outsourcing and what are the business processes, not only security ones, behind decisions related to outsourcing of cyber capabilities. Even though limited amount of information is available in open sources, the work demonstrated well developed high level of research by mapping exact

IMSISS Dissertation Feedback & Mark Sheet

structure of US military presence in cyberspace and providing explanations for understanding decisions on cyber outsourcing, such as details of tendering contracts and cooperation with private entities.

Reviewer 2

This is an extremely interesting and timely piece of work that is poised to make a genuine contribution to the literature. The linkage of the private sector to US state offensive (and defensive) capabilities is a classic topic, but the shift to cyber provides it with an extra layer of novelty and interest. It is meticulously researched and well written--similarly, it benefits from an appropriate structure, which sets the dissertation on good foundations. The research design is solid, although two pages (just about) on methodology is, to my mind, a bit unsifficient for an MA dissertation. The topic is such that the analysis in chapter 5, following the empirical outline in Chapter 4, is policy-relevant; this adds weight to the effectiveness of the dissertation as a whole and compliments the very aims of the IMSISS programme. Summaires after conclusions seem somewhat unecessary, but I appreciate the effort of the student in this regard; again, it is as if a policy-relevant addition. An excellent piece of work overall, which suggests a student well suited to industry, only slightly hampered by a lack of methodological exposition.