

# 7SSWM326 HACKING DEFENCE PROBLEMS

## General Information

<b>Module Convenors</b>	Dr Geoffrey Chapman and Prof Matthew Moran
<b>Office Hours</b>	Please see KEATS or webpage
<b>Contact Details</b>	Dr Geoffrey Chapman <a href="mailto:geoffrey.chapman@kcl.ac.uk">geoffrey.chapman@kcl.ac.uk</a> Office: (TBD) Prof Matthew Moran <a href="mailto:matthew.moran@kcl.ac.uk">matthew.moran@kcl.ac.uk</a> Office: K4U.05
<b>Module Credit</b>	30
<b>Semester</b>	Two

**The module convenors will host an online Q&A session about this module on Wednesday, 18 August at 15.00 BST.**

Join Zoom Meeting:

<https://us02web.zoom.us/j/86569729787?pwd=d2libjB5UFlGbENIeU44N3NnSVcvdz09>

**Meeting ID:** 865 6972 9787

**Passcode:** 49p7cN

## Contents

- Module Description
- Aims
- Learning Outcomes
- Employability Skills
- Teaching Methods
- Assessment
- Student handbook
- Module Requirements
- Teaching Schedule
- Class details and reading
- Weighting scheme for team portfolio

# 7SSWM326 HACKING DEFENCE PROBLEMS

## Module Description

Hacking Defence Problems (HDP) is not about computer hacking; 'hacking' here refers to finding a solution to a problem. HDP is an interdisciplinary and entrepreneurial module that provides students the opportunity to work with the Ministry of Defence (MoD) to better address the nation's emerging threats and security challenges. This is an 'applied' module where students form teams that engage directly with complex, real world problems proposed by UK government sponsors. HDP covers policy, economics, technology, national security, and any area needed to address the problem sponsor's challenge.

In the module, students will be assigned to a team and to a problem, and then be provided with a range of relevant methodological tools and techniques drawn from the business/start-up world (Lean start-up). As the module progresses, student teams will be required to discover and validate customer needs and to continually gather feedback on their understanding of the problem and their proposed solution. Teams take a hands-on approach requiring close engagement with military personnel, Ministry of Defence officials, and private-sector companies.

The goal, within the constraints of a 30-credit, one-semester module with a limited amount of time, is to give students a framework to test problem understanding and possible solutions while creating all of the pressures and demands of the real world in an early stage start-up. Students gain experience in working as part of a team, coming to grips with a complex, real-world problem, and developing and analysing possible solutions.

It is important to bear in mind that this module aims to simulate what start-ups and entrepreneurship is like in the real world: the need to take conceptually-sound decisions amidst uncertainty, challenging deadlines, and often conflicting input.

The module is based on the Hacking for Defense™ (H4D) programme initially developed at [Stanford University](#) and is now offered at many other universities as part of the [Common Mission Project](#). In the US it is an education initiative sponsored by the U.S. Department of Defense's Defense Accelerator, MD5. In the UK it is sponsored by the Ministry of Defence, under the name of [Hacking for the Ministry of Defence](#).

Note that your team may be assigned a problem that you do not find immediately interesting. Student teams at King's have worked on problems that involved intelligence, reservist attendance at training, safety systems at RAF airfields, and the delivery of opportunities for sport. It is important to remember that the aims and learning objectives of this module are focussed on developing a set of skills that you will be able to apply in a variety of professions, not on the development of substantive knowledge in a particular area. All of the problems assigned to students are curated by Hacking for MoD and by the module convenors to ensure that they provide the scope needed for the module.

### **IMPORTANT NOTE FOR STUDENTS CONSIDERING TAKING THIS MODULE**

**Workload of this module:** Because of the nature of this module, which requires working with the government sponsor of your assigned problem and gathering primary data on it, this module involves a significant time commitment beyond scheduled class time. This is reflected in the fact that it is a 30-credit module in a single term. In addition to classroom time, the module's demands include engagement with the flipped lecture and other on-line resources, course reading, preparing for presentations and coordination with their teams and an average of 10 hours of interviews per week per student team. The module also requires some preparatory work in Term 1. For more details on the workload, see the sections on 'How this Module Works' and 'Module Requirements' below.

## 7SSWM326 HACKING DEFENCE PROBLEMS

**Distribution of your course load:** Note that because this module comprises 30 credits in a single term, choosing this module has implications for the distribution of your course load. For further information, see the section on Distribution of Course Load on p.8 below.

**Implications for switching out of this module:** Because this course is run as a 30-credit model in Term 2, if you are allocated the module and then decide in December or January that you want to change modules, your options will be limited. You will not be able to choose from the other 30 credit modules that started in September, so your choice of replacement modules will be restricted to the 15 credit modules available in Term 2 and/or Term 3.

If you have questions about what the module will require and whether you will be able to commit the time necessary, please contact Prof Matthew Moran or Dr Geoffrey Chapman before you list this module on your module preference form. Note that the number of students on the module is limited, as we will have four or five teams with four, five or six students each.

Once you list the module on your preference form, you are **making a commitment** to the government agencies that are sponsoring problems for the module as well as to your fellow team members. **Dropping the module once modules have been allocated is unfair to your fellow students (who did not get into the module or who are on the module and will be down a team member) and also appears unprofessional to the government sponsors involved.**

See below for more information on what is required for students. **Any student who requests this module through the option module allocation process is agreeing to make the time necessary to fulfil the module's requirements.** We will host an online session on Wednesday, 18 August at 15.00 BST. You can also ask questions by email.

**GROUP WORK:** Students work in teams throughout this module, including on weekly presentations and the assessed Team Portfolio. The learning outcomes (see below) require assessment through the Team Portfolio, which collects and reflects on the work of the student team over the course of the module. This means alternative assessments that do not involve group work are not practical for this module. If you have or may need a King's Inclusion Plan that encourages the substitution of alternative assessment for group work, please talk to us before you select this as one of your module options. We can discuss whether there is support that we can provide that will enable you to participate in the group work that is embedded throughout this module. It is vital that any issues in regard to your ability to participate in group work are brought to our attention as soon as possible, ideally before you select this module as one of your choices.

### Aims

- To provide students with a deep knowledge and understanding of some of the most pressing security challenges facing the UK
- To provide students with insights into some of the constraints and opportunities facing government as it seeks to address these challenges
- To equip students with a range of methodological tools focused around Lean Start-up principles (see <https://hbr.org/2013/05/why-the-lean-start-up-changes-everything>) that can be applied to real-world security problems
- To provide students with the means to critically assess the value and relevance of methodological tools as they relate to specific problems
- To help students develop a repeatable model for problem-solving that can be used in a range of other contexts

# 7SSWM326 HACKING DEFENCE PROBLEMS

## Learning Outcomes

By the end of the module, students will have demonstrated:

- A sophisticated and empirically-grounded understanding of pressing security challenges facing UK government;
- An ability to engage critically with a range of methodological tools and approaches commonly deployed to address security-related challenges;
- A deep understanding of the practical dynamics underpinning team-based approaches to addressing security-related challenges and solutions;
- The development of critical analysis, independent judgment, complex problem solving, team coordination and oral and written presentation to a level commensurate with taught post-graduate study.

## Employability Skills

The skills acquired over the course of this module are many and will prove valuable in a range of different workplace positions.

1. Students will be equipped with a range of methodological tools and approaches that can be deployed to address complex problems. While in this module the skillset is developed in the security context, it is transferable to other areas.
2. Students will gain valuable real-life experience working with government sponsors and we expect that this experience will prove attractive to employers.
3. Students will forge valuable contacts with government and industry stakeholders that may prove valuable in your future.
4. Students will be exposed to with some of the challenges and pressures that are commonly encountered in post-university employment. This will help students prepare for similar, future scenarios.
5. The team-based approach that is at the heart of this module directly replicates real-life work practices and will provide students with valuable communication, leadership and team-working skills.

## How the Module Works/Teaching Methods

The module is taught through a combination of in-person and online delivery.

### Semester One

- Although the module is taught in Semester Two, it requires that students do some work in Semester One:
  - By **21 October 2021**, students who have been allocated to the module are required to submit a CV to module convenors that includes previous degrees and work experience. This will allow the module convenors to assign students to interdisciplinary teams. If there is a possibility that you will not be in the UK for either or both Semester One and Two, please specify this and indicate the time zone you may be in. We will endeavour to assign teams and schedule online sessions to accommodate students in various time zones.
  - There will be some preparatory work to do in Semester One, including the completion of the on-line 'Foundation Course' produced by the Common Mission Project, which provides an introduction to Lean Start-up methods for mission driven organisations. Timely completion of this as well as other intro material (readings/videos, interview training) allows you to 'hit the ground running' at the start of Semester Two.

## 7SSWM326 HACKING DEFENCE PROBLEMS

- A session on interview training will be recorded and posted on KEATS in early November. In the week of **8 November** (precise date and time TBC), we will have a Q &A session on conducting interviews with an opportunity to ask other questions.
- A meet and greet session will be held the week of **13 December** (revision week) after teams have been assigned, where you will meet your teammates. You will also have your first opportunity to meet your government problem sponsor. At this meeting, you should also receive from your sponsor a list of contacts for your first set of interviews.
- Students are encouraged to coordinate with their team as soon as teams are assigned, so that they can begin interviews as soon as the module begins in January.

### Semester Two

#### Each week will involve the following components:

- **Online lectures and other course materials.** Each week students are required to engage with the online materials, which may include a combination of podcasts, readings, blogs and videos as part of their preparation for class. These provide the Lean Start-up methods that you will apply to your problem through your interviews and weekly presentations and evaluate in your individual essay.
- **Weekly Team Presentations (2 hours session).** Each team will present and receive feedback on its updated Mission Model Canvas. (The Mission Model Canvas is a visual tool and framework Hacking for Defence developed to rapidly test hypotheses against solutions for government issues.) Presentations should also demonstrate an understanding and application of the Lean Start-up methodology. There will be an opportunity to discuss questions about the online lecture material (some asked by the lecturers, some raised by the students) and to engage with supplemental material.
- **Weekly Team Hackathon (2 hour session).** In response to student feedback, we will use these sessions to provide dedicated time for teams to work together on their problem. Instructors will also use these sessions to provide further feedback and suggestions to each team. This session should not be used for interviews, unless unavoidable.
- **Interviews and Research** Outside of class time, each team will conduct interviews and other research to understand the problem they have been assigned and to identify and test possible solutions. Each student team will be expected to conduct an average of ten interviews per week. Teams will work with the government sponsor and their industry mentor throughout the term, with the government sponsor providing information and feedback, facilitating interviews, etc.
- **Team Blog** Each team will also keep a 'team blog,' which allows them to track their thinking and progress. Weekly updates to the blog can cover new hypotheses, interviews conducted, lessons learned, next steps, and ideas for potential solutions. Each student is expected to contribute to the blog over the course of the semester.

In addition to the standard KEATS page, MS Teams will be used to facilitate communication between team members, as well as between the team and its government sponsor. Through their MS Teams Channel, each team will also have a SharePoint site to facilitate each team's work, including the Team and where all documents should be stored. Because MS Teams is MOD compliant, it is also the preferred online communication tool.

Office hours will be held either on campus or online, and you can arrange to meet with us by email/sign up for them in advance.

## 7SSWM326 HACKING DEFENCE PROBLEMS

### Assessment

Type of Assessment	Word Limit / Duration	Deadline Date	Deadline Time	% of Final Mark
Team Portfolio	5000-8000 Words	14 April 2022	13:00 UK Time	60%
Individual Essay	2500 Words	28 April 2022	13:00 UK Time	40%

The Team Portfolio brings together the work your team has done over the course of the module. For example, it includes an analysis of your weekly Mission Model Canvases and the Team Blog. The portfolio will be assessed and then each student will receive that mark as weighted by their contribution to the team's work over the course of the term. For more information, see the explanation at the end of the module handout. The individual essay asks you to reflect critically on the Lean Start-up methodology and your team's use of it.

Please note that the department policy is that assessment must be submitted on KEATS before 13:00 UK Time, i.e. by 12:59:59. If you submit at 13:00, it will be counted as a late submission. Please note that the department does not accept computer issues as an excuse. Hence, please submit ahead of schedule and leave enough time (if you run into computer problems) to drop by the administrative office with an accessible soft copy of your essay to be uploaded to KEATS before the deadline.

### Student Handbook

You will find the Student Handbook on KEATS. It is essential that you read this carefully. In the Student Handbook, you will find important information such as:

- Penalties for missing a coursework deadline
- Penalties for exceeding the coursework word limit
- How to apply for a deadline extension
- Advice on referencing
- How to avoid plagiarism
- How your work is marked
- Generic Marking Criteria
- Exam FAQs

### Module Requirements

#### What is Required of Students

Because of the nature of this module, it requires students to commit to the following:

- Various activities in Semester One, including submitting a CV by **21 October 2021**, completion of the Common Mission Project Foundation Course for Hacking 4 MoD (hosted on Teachable, you will be enrolled in this and a link will be sent to you **mid-late October**);
- Attend meet and greet with teams, problem sponsors and convenors in week of **13 December 2021** (exact date TBC)
- During Semester Two, you commit to 10-15 hours a week of work outside of the classroom, including a target of 10 interviews a week (per team);

## 7SSWM326 HACKING DEFENCE PROBLEMS

- Two class sessions per week, including weekly team presentations on progress, including an updated Mission Model Canvas and a discussion of how you have applied the online lessons to your project;
- Weekly team blog updates that include
  - New hypotheses and ways to evaluate them
  - Interviews, lessons learned and next steps.
  - Ideas for potential solutions and ways to test them;
- Complete a mid-term peer feedback form and submit it by **10 February 2021**
- Maintain weekly contact with the government problem sponsor and regular contact with your team mentor.

Each team will make a final presentation to the class, the problem sponsors and various others during week of **21 March 2022**.

### Teaching Schedule

#### Semester One:

- a) Deadline for submission of CV to module convenors: **21 October 2021**
- b) Interview training - pre-recorded session by early November; Q and A week of **8 November 2021** (exact date TBC)
- c) Meeting with convenors, teammates and problem sponsors week of **13 December 2021**.
- d) Students will be provided their pre-reading, enrolled in the Foundation course, and are encouraged to coordinate with their team to begin interviews as soon as Semester 2 begins. Before the first week of term, teams should have:
  - Introduced themselves on their team's chat on MS Teams (the government sponsor will also be on the chat)
  - Completed the Foundation course and other pre-reading and be familiar with the terms: beneficiary, value proposition, and mission model canvas.

#### Semester Two:

1. Introduction to Module and to MoD/Defence Landscape
2. Mission Model Canvas and Beneficiaries & Stakeholders (Teams present their first Mission Model Canvas)
3. Value Proposition
4. Dual Use & Product Mission Fit
5. Mission Achievement (No team presentations this week, hackathon session still takes place)
6. Buy In & Support (In presentations this week we will focus on both mission achievement and buy in& support)
7. Deployment
8. Activities, Resources & Partners and Mission Budget & Operating Plan
9. Last weekly presentation/practice final presentation and Q and A
10. Final presentations and lessons learned at an event that includes problem sponsors, industry mentors, H4D-UK staff and a variety of people from King's.
11. Work on team portfolio (week ending 1 April)

## 7SSWM326 HACKING DEFENCE PROBLEMS

### Class Details and Reading

#### Class Textbooks:

- Blank, Steve and Bob Dorft. “*Start-up Owners Manual*” K&S Ranch Publishing (2012)
- Osterwalder, Alex *et al.* “*Value Proposition Design*” Wiley, New Jersey (2014) (e-book available through the King’s library)

#### Suggested General Reading:

- Blank, Steve. “*The Four Steps to the Epiphany.*” Steve Blank (2013)
- Osterwalder, Alex and Yves Pigneur “*Business Model Generation*” Wiley, New Jersey (2010) (e-book available through the King’s library)

#### Suggested Pre-Class Preparation / Reading

- Rationale for H4D: <https://steveblank.com/2016/01/26/hacking-for-defense-stanford/>
- Overview Business Model Canvas: <http://businessmodelgeneration.com/canvas/bmc>
- Overview Mission Model Canvas: <http://steveblank.com/2016/02/23/the-mission-model-canvas-an-adapted-business-model-canvas-for-mission-driven-organizations/>
- Minimum Viable Products – Blog Post: <https://steveblank.com/2013/07/22/an-mvp-is-not-a-cheaper-product-its-about-smart-learning/>
- Customer Development, An Overview: <http://giffconstable.com/2012/12/12-tips-for-early-customer-development-interviews-revision-3/>
- Beginner’s Mindset: <https://vimeo.com/78551898>
- *Start-Up Owners Manual*: pp.22-30, pp.31-50, pp.67-68

### Note on Distribution of your Course Load

You are required to take a total of 90 credits of option modules. Because this module comprises 30 credits in a single term, choosing this module has implications for the structure of your course load.

In terms of possible options, a balanced workload for your options modules could look like:

Term 1	Term 2
15 credit option	30 credits Hacking defence problems
15 credit option	n/a
30 credit full year or 2 15 credit optional modules	

Or you might choose to have fewer modules/credits in Term 1 and a higher workload in Term 2. Given the demanding nature of HDP, we do not recommend this.

Term 1	Term 2
n/a	30 credits Hacking defence problems
30 credit full year or 2 15 credit modules	
30 credit full year or 2 15 credit modules	

If you choose to take an optional module in Term 3, you have more choice of how to distribute your workload.



## 7SSWM326 HACKING DEFENCE PROBLEMS

### Weighting the team portfolio by each member's contribution to the work of the team over the course of the module:

At the end of the module, each student will be asked to distribute a nominal £1000 bonus among their fellow team members (but not to themselves). For example, with a team of six students, the result of this distribution might look like this:

Given by student:	A gives to team mates	B gives to team mates	C gives to team mates	D gives to team mates	E gives to team mates	F gives to team mates	Total bonus for each student
A	n/a	£200	£237.50	£275	£180	£200	1092.5
B	£200	n/a	£237.50	£225	£240	£200	1102.5
C	£250	£200	n/a	£200	£240	£200	1090
D	£250	£200	£237.50	n/a	£240	£200	1127.5
E	£200	£300	£237.50	£225	n/a	£200	1162.5
F	£100	£100	£50	£75	£100	n/a	425

The student with the highest bonus gets 100% of the given mark. For example, if the mark given the Team Portfolio is 72, the student with the highest total bonus receives a 72. In this example, Student E received the highest bonus, so they get a 72 on the team portfolio.

The mark of all other students is a function of the mark given the portfolio (72) multiplied by the bonus they received divided by the highest bonus received. See the table below for the calculations of the final marks for the example team.

Student	Student's total bonus:	Weight for team contribution = (student bonus divided by the highest bonus received):	Final, weighted mark (where portfolio received a mark of 72)
A	1092.5	$1092.5/1162.5=0.94$	$0.94 \times 72 = 67.68$
B	1102.5	$1102.5/1162.5=0.95$	$0.95 \times 72 = 68.4$
C	1090	$1090/1162.5=0.94$	$0.94 \times 72 = 67.68$
D	1127.5	$1127.5/1162.5=0.97$	$0.97 \times 72 = 69.84$
E	1162.5	$1162.5/1162.5=1.00$	$1 \times 72 = 72$
F	425	$424/1162.5=0.37$	$0.37 \times 72 = 26.64$

**Note:** The mark of all other students is a function of the mark given the portfolio (72) multiplied by the bonus they received divided by the highest bonus received. The module convenors will moderate the mark that results from this. This will be done in a uniform manner across all students. In exceptional circumstances (e.g. where the total bonus given to a particular student is clearly out of line with the weekly contributions), we reserve the right to adjust individual marks.