Assignment Cover Sheet



* The information on this coversheet will be included in Turnitin’s similarity analysis; however, your lecturers are aware of this and will disregard it.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Student Details | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Student Number | 1 | 0 | 4 | 9 | 8 | 7 | 4 | | 3 |  | |
|  | | | | | | | | | | | |
| Family Name | David Selvam | | | | | | | GivenName | | | Visahl Samson |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| UnitDetails | | | | | | | | | | | |
|  | | | | | | | | | | | |
| UnitCode | CSI2104 | | | UnitTitle | | Introduction to Information Warfare | | | | | |
| Name of Lecturer | | | Kang Leng | | | | Due Date | | | 21 June 2019 | |
| Topic of Assignment | | | A Case Study about an Arms Manufacturer | | GrouporTutorial(if applicable) | | |  | | | |
| Course | | Bachelors of Science in Cyber Security (FT) | | | | | | | Campus | | Singapore |
| I certify that the attached assignment is my own work and that any material drawn from other sources has been acknowledged. This work has not previously been submitted for assessment in any other unit or course.  Copyrightin assignments remains my property .I grant permission to the University to make copies of assignments for assessment, review and/or record keeping purposes. I note that the University reserves the right to check my assignment for plagiarism .Should there production of all or part of an assignment be required by the University for any purpose other than those mentioned above, appropriate authorisation will be sought from me on the relevant form. | | | | | | | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ManualSubmission | | | | |
| If handing in an assignment in a paper or other physical form,sign here to indicate that you have read this form, filled it in completely and that you certify as above. | | | | |
| Signature |  | Date |  | ***Office Use Only*** |
| ElectronicSubmission | | | |
| **OR,**ifsubmitting thispaper electronically as per instructions for the unit, place an ‘X’ in the box below to indicate that you have read this form and filled it in completely and that you certify as above. Please include this page with your submission. Any responses to this submission will be sent to your ECU email address. | | | |
| Agreement | X☐select checkbox | Date | 21 June 2019 |
| For procedures and penalties on late assignments please refer to the [University Admission, Enrolment and Academic Progress](http://intranet.ecu.edu.au/__data/assets/pdf_file/0005/378320/Admission-Enrolment-and-Academic-Rules.pdf)  [Rules](http://intranet.ecu.edu.au/__data/assets/pdf_file/0005/378320/Admission-Enrolment-and-Academic-Rules.pdf)- rule 24, and the ECU Course and Unit Delivery and Assessment Policy | | | | |

Contents

[Assignment Cover Sheet 1](file:///C:\Users\Samson\Downloads\Assignment-Cover-Sheet-Electronic%20(1).docx#_Toc12002665)

[Introduction 3](#_Toc12002666)

[Players 4](#_Toc12002667)

[Offensive player 4](#_Toc12002668)

[Defensive player 4](#_Toc12002669)

[Vital Player 4](#_Toc12002670)

[Actors 4](#_Toc12002671)

[Mind Map 6](#_Toc12002672)

[British Aerospace 6](#_Toc12002673)

[CAAT 7](#_Toc12002674)

[Purpose 7](#_Toc12002675)

[Information gathering and passing 8](#_Toc12002676)

[Conclusion 8](#_Toc12002677)

[References 9](#_Toc12002678)

# Introduction

In current scenario information warfare is growing rapidly. Information warfare consists of actions taken to take over control of the information while protecting one’s own information. The given case study explains how a Private Intelligence Company used information warfare strategies to take over control on an activist group to profit its client. Furthermore, this case study introducing the concept Corporate Espionage where a corporate/organization use improper actions against the competitor to gain commercial advantage. Besides it explains the offensive and defensive strategies applied by both the parties. Also, it explains the corporate espionage and need of threat intelligence in details.

In this scenario the British Aerospace used a private intelligence agency established by the Evelyn le Chêne for performing corporate espionage of its competitor CAAT. CAAT is just known as the Campaign against Arms Trade. Here the author analysed the spy documents and explains what can be learned from this case.

The beginning of the article discussed how the infiltrators collected the information and transfer it to BAe. Afterward it is moving to how BAe used the information to stop CAAT’s plans against them. After that it explaining what are all the defensive and offensive operations done by the infiltrates. Afterwards, it continues to explain how effectively BAe used the information against its target CAAT by stopping their plans. Then how CAAT reacted to the incident happened. After that the case study explains Evelyn’s intelligence link and the remaining unanswered question then concluded with pros and cons of corporate intelligence.

# Players

## Offensive player

Offensive player is the one who launch an operation against the target using various strategies and tactics. Here the Aerospace of British is the one who started the information warfare operation against CAAT to acquire the information. Basically Aerospace of British is one of largest in defence contractor which is in Europe and also one of the well-known aerospace companies in globe ("British Aerospace UK", n.d.). So, British Aerospace is offensive player in this scenario.

## Defensive player

Defensive player is the one who protect the information from the offensive player’s operations. Here the Campaign against Arms Trade was the defensive player. CAAT is basically a United Kingdom based organization which functioning to end a trade of arms around the world

### Vital Player

The vital player in this operation without whom, the operation is not possible is Evelyn le Chêne the founder of the Threat response international which advised corporations on security threats.

Another notable person in this project is Andrian Franks son of Evelyn Le Chêne also owned a company called Risk and crisis analysis.

## Actors

In this threat response case study apart from offensive and defensive player there are Non-state actors available. Non-state actors are generally has influence in politics but not connected with any particular country/state. The non-state actors played major roles in this operation. They are follows,

**Sunday Times**

The primary Non-state actor here is David Connett from the Sunday times. He is the one who found this spying incident online and released in the media. Also, Sunday times known for its quality reporting and covering about British politics. ("The Sunday Times | British newspaper", n.d.)

**Dutch Grass roots**

The organization which involves here is Dutch Grass roots buro Jansen & Janssen. This Buro Jansen & Janssen is a specialist in monitoring police en secret services. The reason the organization involves in this case is it was approached by ASEED (Action for Solidarity Environment Equality and Diversity) to investigate about Andrian frank and exposed about him. (schrijft, 2004)

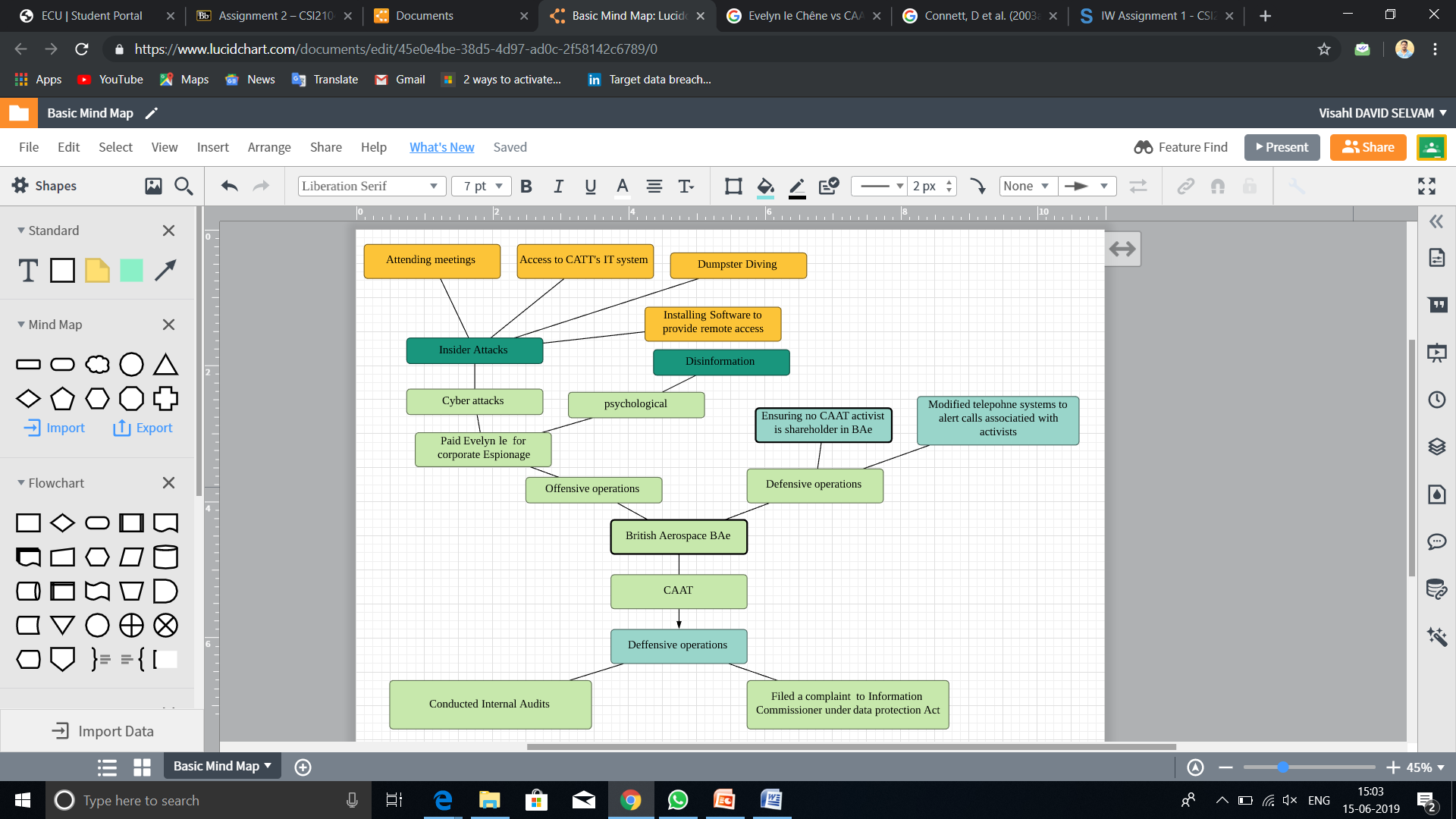
**Corporate watch**

Corporate watch is an another non-state actor involved in this case. It is said that this organization used Andrian Frank to spy on ASEED in 1998. Since, Corporate watch and BAe’s motives looks as same and involves a same person this organization comes under non-state actor category.

**John Major's Government**

Government is the best example for actor role in information warfare. The reason John Major’s government listed here is because at the time of operation this government was deciding authority to grant permission to BAe ‘s Hawk contract (£500m sale of the British Aerospace to Indonesia). But at the same occasion Evelyn was performing inside fence actions to acquire and pass the information.

# Mind Map



Screenshot Mind map of offensive and defensive operations from BAe and CAAT

## British Aerospace

* British Aerospace started it’s operation with paying Evelyn Le Chene. The various operations performed by her are explained below,
* In order to gather details from CAAT Evelyn has done several defensive actions. All those attacks executed under Insider the fence and the approach here is Corporate Espionage. The main offensive operations performed by Evelyn include attending meetings, accessing CAAT’s IT system.
* By attending CAAT’s meetings Evelyn’s agents gathered sensitive information such as upcoming plans, political supports. Once, these details gathered they have been forwarded to BAe. Also, by accessing CAAT’s IT system BAe was able to get all the information about CAAT’s activists also BAe was able to download the entire list. By installing remote access in Evelyn’s computer made BAe’s work easy.
* By performing dumpster driving Evelyn was able to find out all CAAT’s funding, bank transactions, internal plans, etc. All the defensive operations come under corporate espionage category. Also, as Psychological actions Evelyn provided false information to CAAT whenever required and advised BAe not to release the news through BBC.
* As Adrian Frank’s part he had done provocateur work very well. His actions includes irritating other activists by suggesting radical approaches. Where these action lead CAAT to grow issues with Amnesty International which is a human rights NGO.
* As offensive approaches, BAe started to check the activist names in their computer systems to ensure their stackholders are not CAAT activists. Also, BAe modified their phone systems to alert calls associated with activists. By doing these offensive actions BAe ensured their information is secured.
* From Evelyn part she had asked BAe to arrange arrest warrant for her own agents who were part of CAAT’s incursion of BAe’s plant.

## CAAT

Since, CAAT had no knowledge about this corporate espionage performed by BAe on its company until the Sunday times released news about it, CAAT has nothing to do. Once, the news released in Sunday times, CAAT conducted a internal audit and found that Martin Hogbin a volunteer in CAAT had been forwarding the emails to the company with known to Evelyn and suspended Martin Hogbin from the company. ("Spying - About CAAT - Campaign Against Arms Trade", 2005) Commissioner of Information has received a case about the Martin Hogin which was filed by the CAAT. But the Commissioner of Information determined not to take the action against the Martin Hogbin since, information sent emailed by Martin doesn’t covered under 1998 Act.

So, these are the 2 defensive actions taken by CAAT in this scenario.

# Purpose

The primary aim of CAAT is, ("About CAAT - Campaign Against Arms Trade", n.d.) to conclude the arms trade of International Level, and where BAe is Britains largest arms dealer. Also CAAT is always a barrier to BAe’s project and deals. The best example is during the mid of 90’s CAAT is stepping up the campaign which was against the £500m sale of Aerospace of British jets to Indonesia. There are several cases where CAAT stands against BAe. So, it clearly shows that BAe performed this operation on CAAT for commercial advantage.

Also by doing this BAe can able to know the political support provided to CAAT and any new policy implication that can affect BAe’s Indonesia deal Furthermore, So, this operation can also intended for political purposes also.

# Information gathering and passing

As the case study explains, the primary motive of the operation is to get information about CAAT in order to gain commercial advantage and as well as political. Here, the operation was started with Evelyn le Chee who infiltrated the CAAT’s organization with her agents. The way she and her agents followed to acquire the information includes attending internal meetings, taking control over the CAAT’s IT system, installing new computer system in CAAT’s office and members homes. Reading diaries and bank statements, following CAAT’s activists,

Once, they gather all the details they have faxed them in encrypted format to BAe’s office. Later on BAe installed software on Evelyn’s computer to access the details whenever required.

By using the information gathered by Evelyn BAe stopped the several plans planned by CAAT. The plans includes 'incursion' of a BAe plant by CAAT activists. Apart from this there are several Larger protests were also managed by BAe.

# Conclusion

By analyzing this case study we come to know. Furthermore this case study briefs the protections required in today’s corporate world such as counter intelligence and intelligence gathering. Implementing these counter measures can protect the organizations from these issues.

# References

British Aerospace UK. Retrieved from <https://www.baesystems.com/en-uk/heritage/british-aerospace-uk>

The Sunday Times | British newspaper. Retrieved from <https://www.britannica.com/topic/The-Sunday-Times>

schrijft, E. (2004). The Threat Response Spy Files. Retrieved from <https://www.evel.nl/spinwatch/stuk-eng.htm>

Spying - About CAAT - Campaign Against Arms Trade. Retrieved from <https://www.caat.org.uk/about/spying>

Campaign Against Arms Trade. (n.d.). About CAAT - Campaign Against Arms Trade. [online] Available at: <https://www.caat.org.uk/about>

E, L. (2005). The Threat Response Spy Files: A Case Study about an Arms Manufacturer, a Private Intelligence Company and many Infiltrators. Journal Of Information Warfare (2005) 4, 3, ISSN 1445-3312 print/ISSN, 40 – 48.