

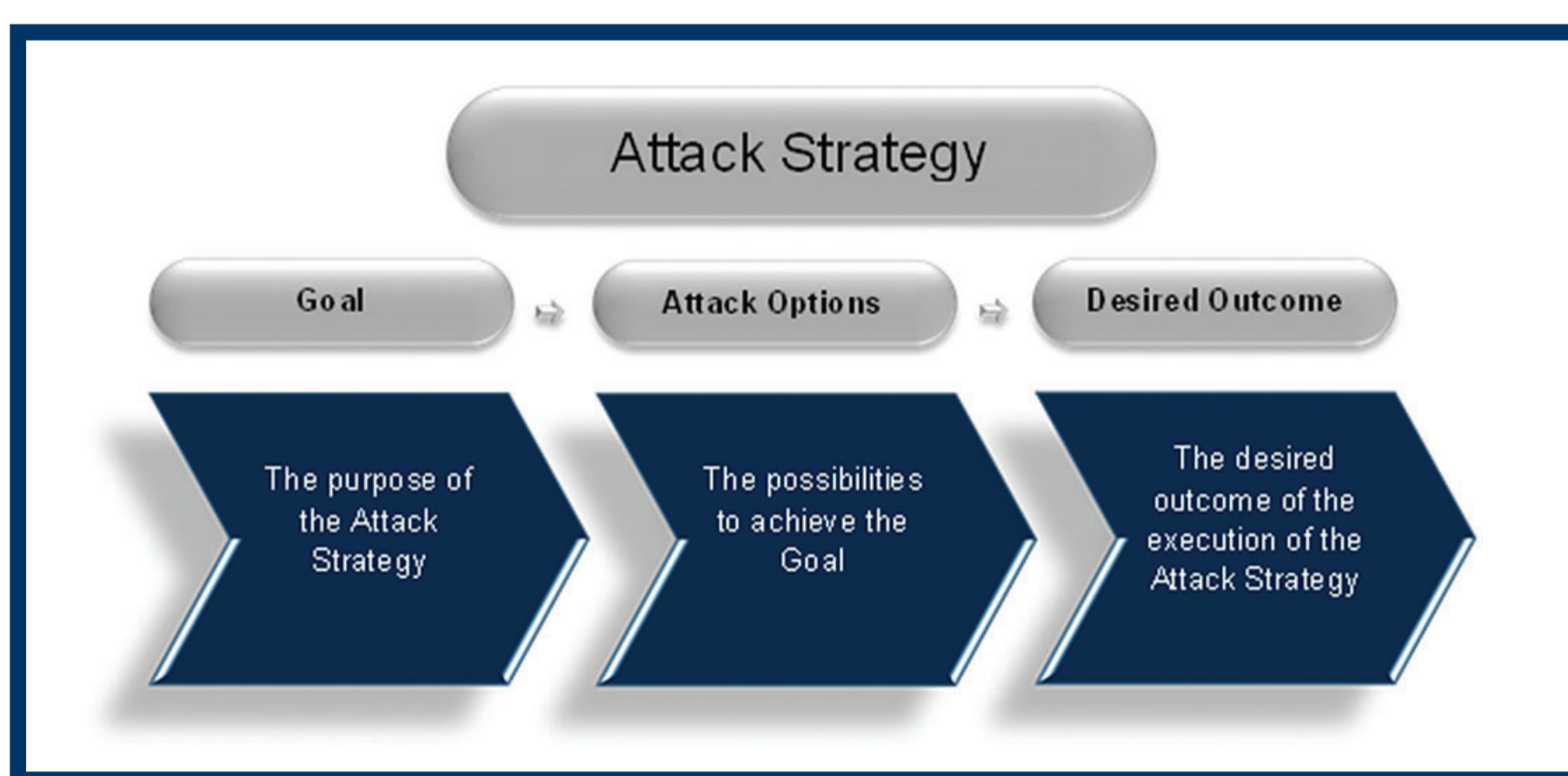
A study of mobile botnets: analysis of attack strategies

H PIETERSE
 CSIR Defence, Peace, Safety and Security, PO Box 395, Pretoria, South Africa, 0001
 Email: hpieterse@csir.co.za – www.csir.co.za

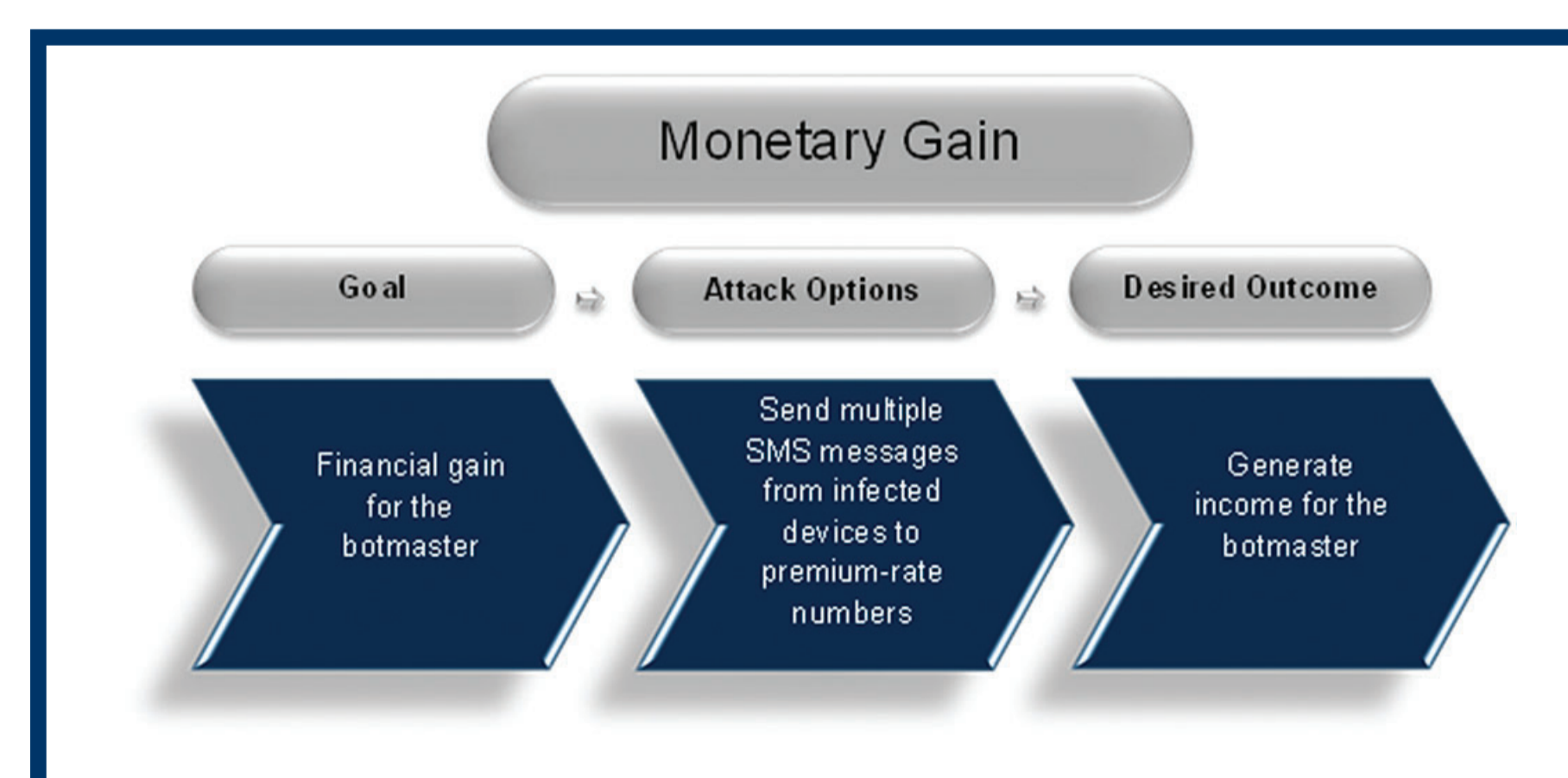
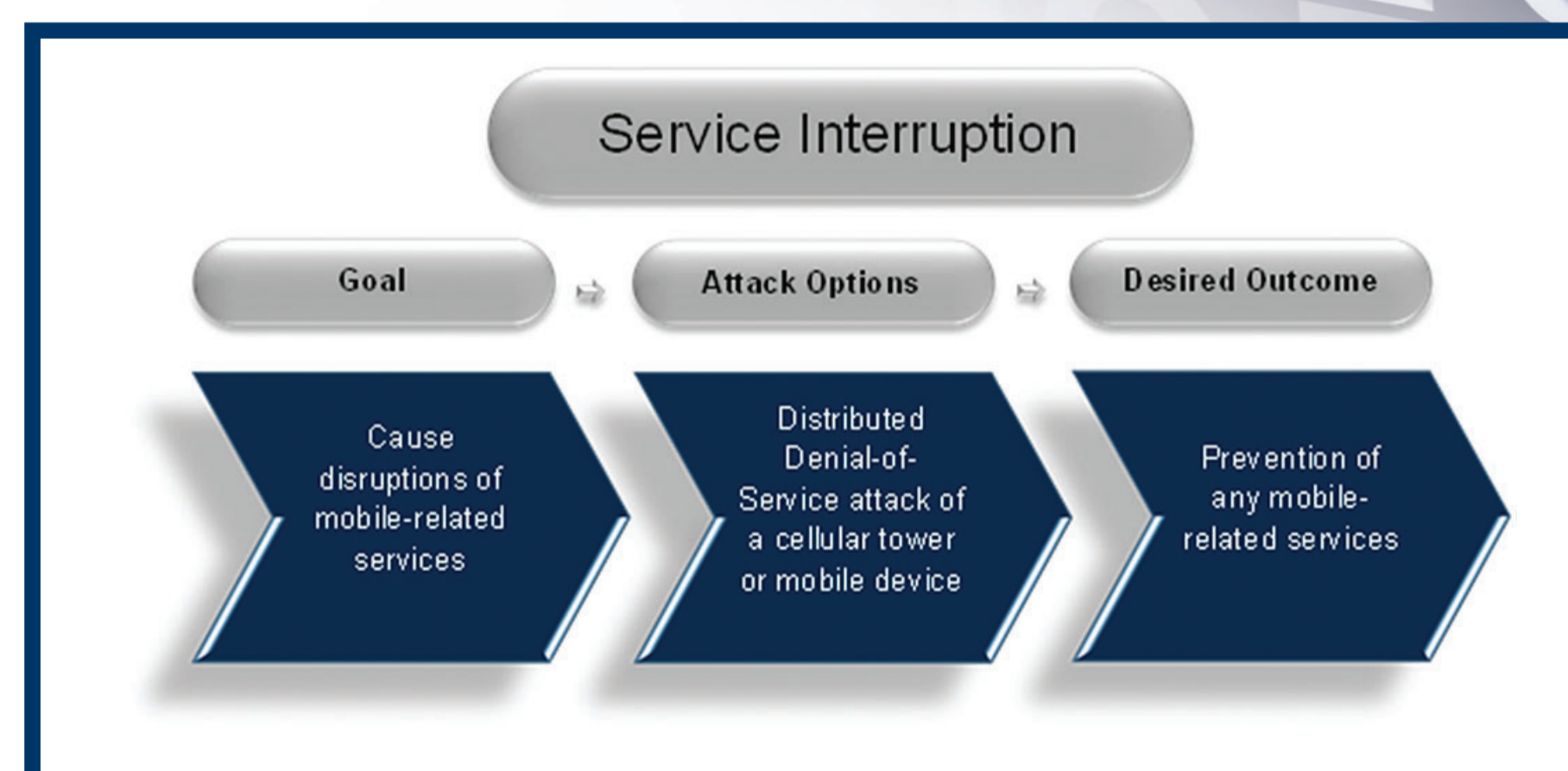
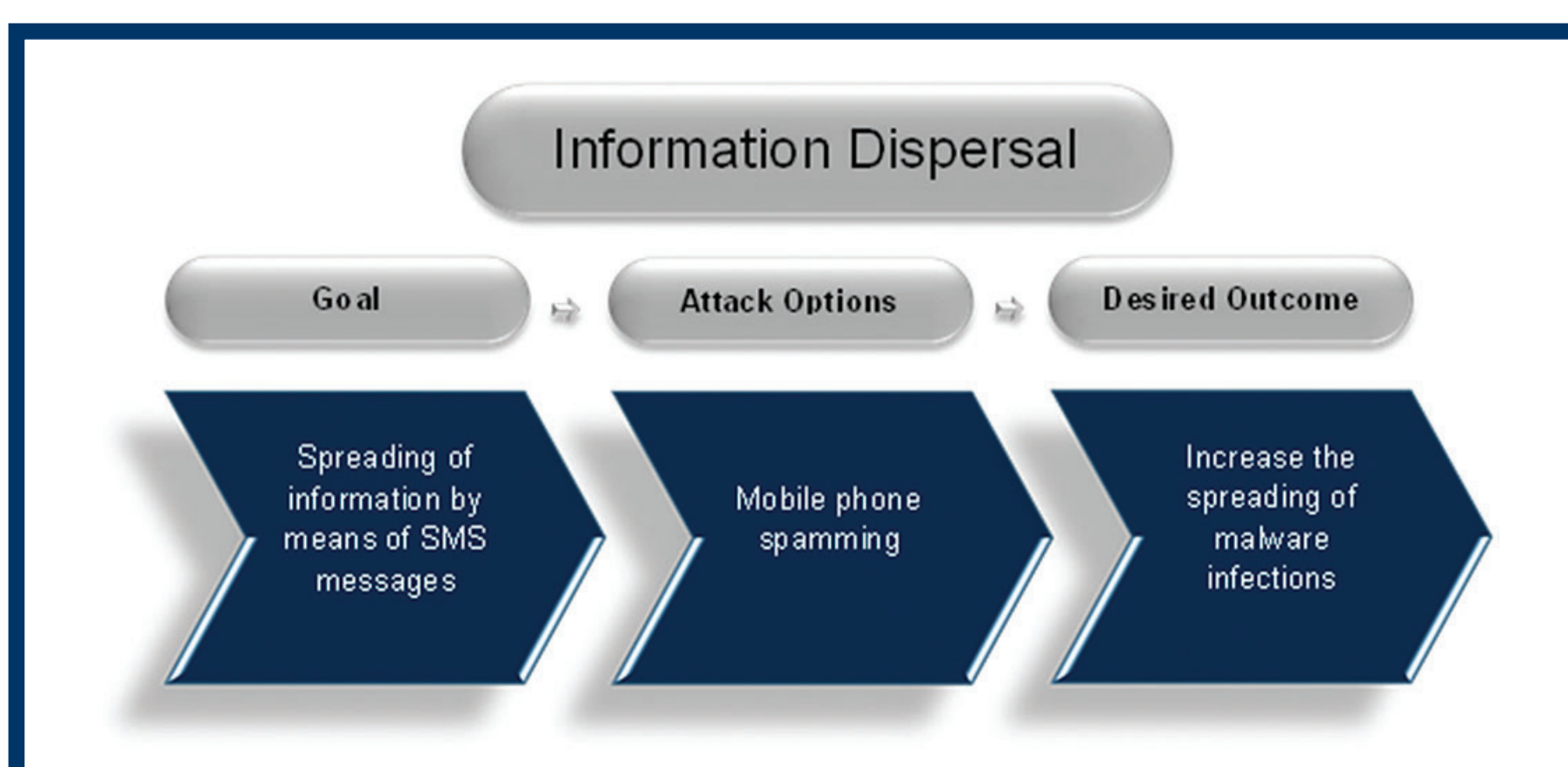
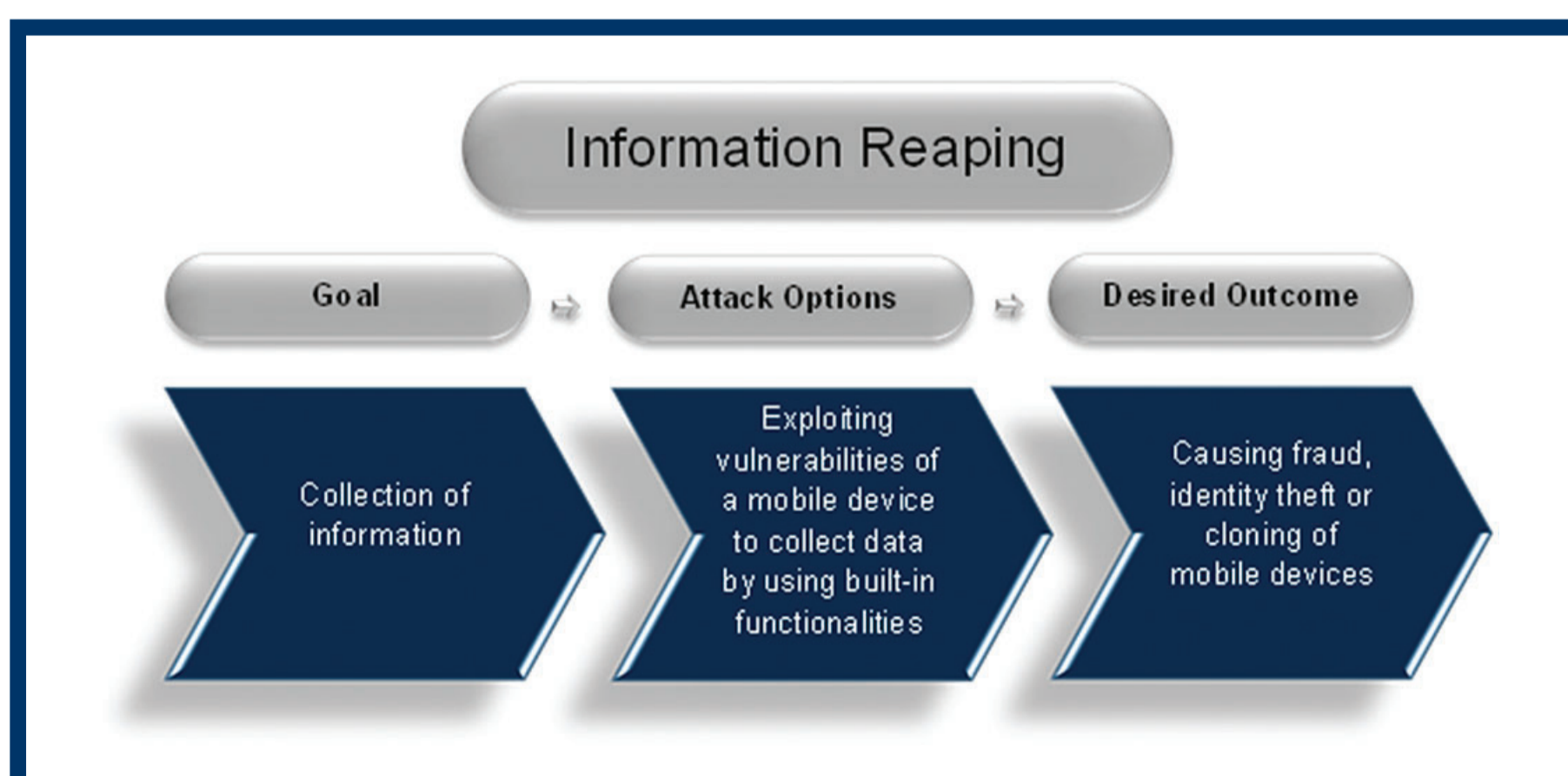
INTRODUCTION

For many years, botnets have been a serious security threat to users of the internet and personal computers. Countermeasures are constantly running behind as botmasters develop new botnet techniques. Until recently, mobile phones remained free of the threat of botnets due to the isolation between mobile networks and the internet. The situation has changed significantly with the fast-growing popularity of smartphones such as Android-based phones and Apple's iPhone. Today, smartphones offer their users endless capabilities and allow communication to occur via multiple mechanisms. Due to the popularity of smartphones and the advanced capabilities offered, botnets are expected to move towards mobile networks.

A mobile botnet is a collection of compromised smartphones controlled by a botmaster through a command and control network to serve a malicious purpose^[1]. Without a clear understanding of the threats posed by such a mobile botnet, it will be difficult to defend against these rising threats. The purpose of this study is to focus on the classification of possible attacks caused by mobile botnets. It is important to realise that a botmaster develops any mobile botnet with a specific purpose in mind. This purpose is to achieve a certain goal and varies from botmaster to botmaster, but will most likely be built around the following: collection of information, stealing of money, prevention of services, sending of spam, etc. These various goals can be summarised into one of the following Attack Strategies: Information Reaping, Information Dispersal, Service Interruption and Monetary Gain. An Attack Strategy is essentially a classification of a possible mobile botnet attack according to the following generic structure:



ATTACK STRATEGIES



CONCLUSION

These Attack Strategies aid the understanding of the threats posed by mobile botnets and can lead to the improvement of defence mechanisms. The classification of the Attack Strategies will also further improve the possibility to detect and discover new developments of mobile botnets in the coming future.

REFERENCES

^[1] Geng, G., Xu, G., Zhang, M., Guo, Y., Yang, G. and Wei C. 2012. The Design of SMS Based Heterogeneous Mobile Botnet. Journal of Computers, 7(1), pp. 235 – 243.

Until recently, mobile phones remained free of the threat of botnets due to the isolation between mobile networks and the internet. The situation has changed significantly with the fast-growing popularity of smartphones such as Android-based phones and Apple's iPhone.