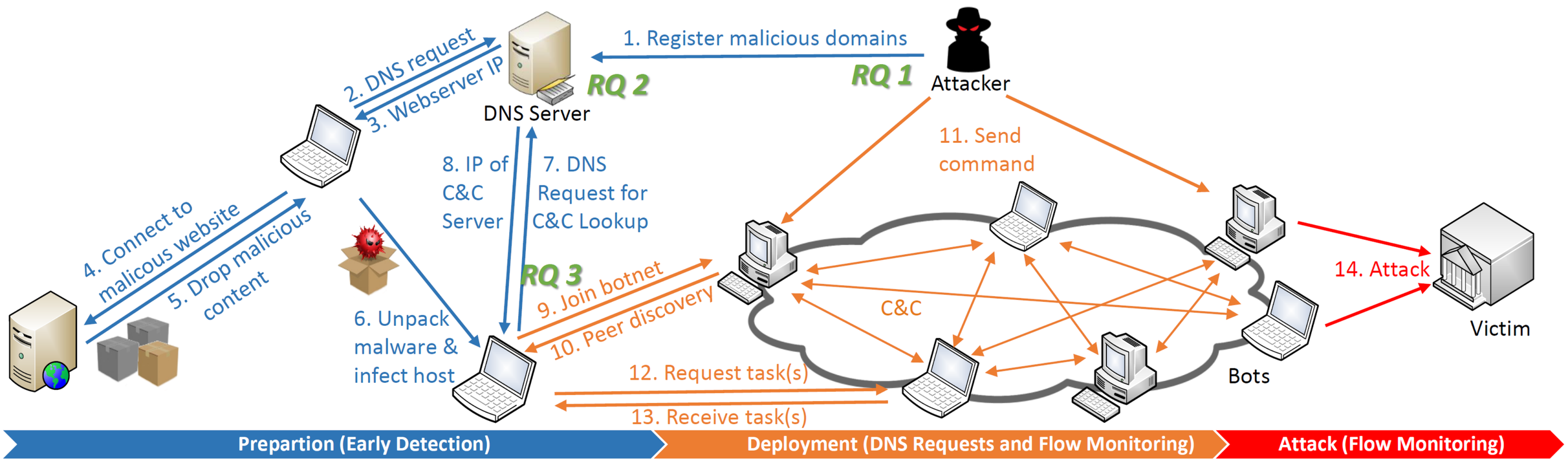
Proactive Botnet Detection and Defense at Internet scale

A collaborative approach

Problem: Botnets enable various cyber-criminal activities[1,2].



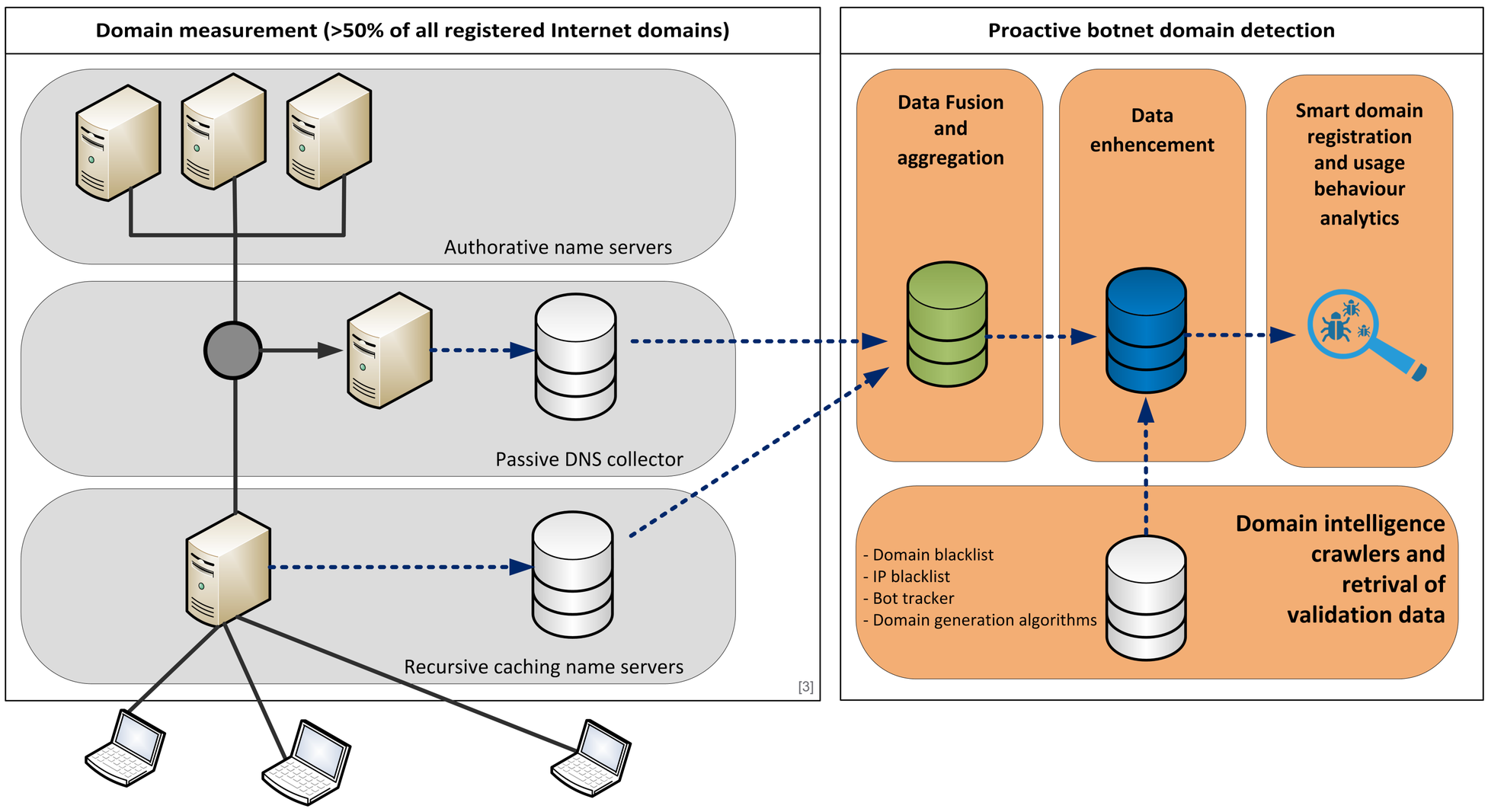
Research Questions:

RQ 1: What do bots need to be deployed and to form a new or join an existing botnet?

RQ 2: How do bots interact with central internet services, like the domain name service (DNS)?

RQ 3: How can the interacation with central services be used for detection before botnets can evolve their full size an power?

Approach: Detection and mitigation of botnets before they evolve their full size and attack power.



References:

[1] Christian Dietz, Anna Sperotto, Gabi Dreo, Aiko Pras: How to achieve early botnet detection at the provider level? In Proceedings of Autonomous Infrastructure, Management and Security (AIMS) Conference, June 2016 ,Springer, DE

[2] van der Wagen, Wytske, and Wolter Pieters: From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. British Journal of Criminology 55.3 (2015): 578-595.

[3] Roland van Rijswijk-Deij, Mattijs Jonker, Anna Sperotto and Aiko Pras: The Internet of Names: A DNS Big Dataset. In Proceedings of ACM SIGCOMM 2015, 17-21 August 2015, London, UK

Research Center Cyber Defence

der Bundeswehr Universität München

UNIVERSITY OF TWENTE.

Contact:

Christian Dietz[1,2]
Anna Sperotto[2]
Gabi Dreo Rodosek[1]
Aiko Pras[2]

[1] CODE - Research center cyber defense, Universität der Bundeswehr München, München, Germany {christian.dietz, gabi.dreo}@unibw.de

[2] Design and Analysis of Communication Systems (DACS), University of Twente, Enschede, The Netherlands {c.dietz, a.sperotto,a.pras}@utwente.nl