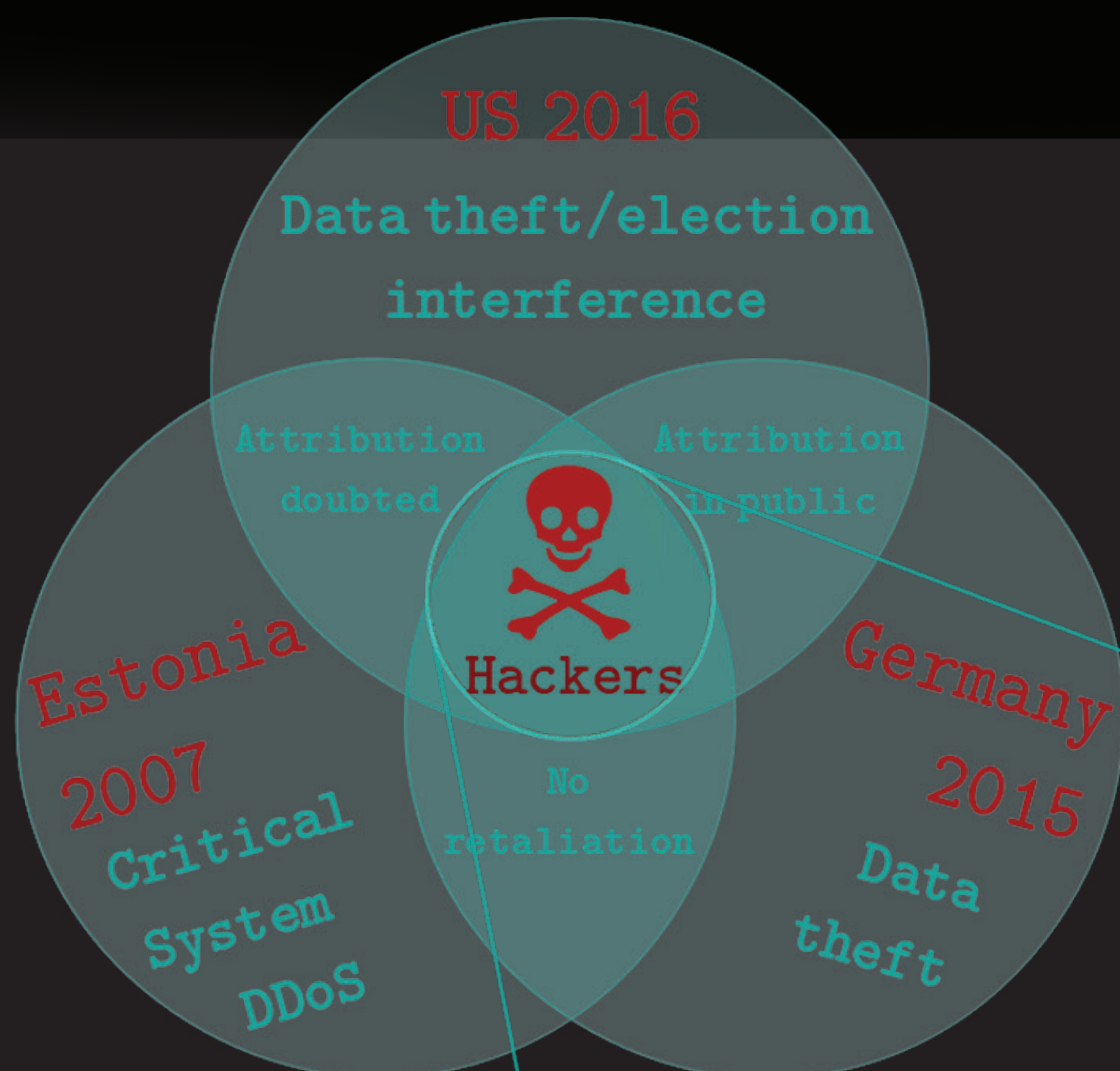


A Disruptive Approach to Law Enforcement on the Dark Web

Introduction

Cybercriminals have played a key role in high profile attacks and **disruptive state level operations**. For law enforcement agencies, tracking down and mitigating the threat these groups pose has a **high resource cost**. The dark web is the part of the deep web (sites that cannot be found via search engines like Google) where criminals trade in products and services. We explore how authorities have been able to **stop criminal activity** simply due to the **human error** of those acting on the dark web.



Taking down the Dark Web



Alphabay
Administrator left his personal email in the welcome message to new users.

Silk Road
Administrator boasted about his position on LinkedIn and used photos of himself on various accounts.

Silk Road 2.0
Administrator used his name to rent servers.

Finishing thoughts

Cybercrime is **not infallible**. It is important to remember that humans are central to cybercrime operations because **humans make mistakes** and being able to target a "weak link" is often key to taking down the wider operation. A **targeted approach by law enforcement** focusing on individuals will disrupt the trust holding these criminal networks together.