

# The Darknet Mesh Project

David Ford, OxCERT (University Of Oxford)  
Project is a collaboration between several UK  
Universities

- Concept of a Darknet will be familiar to many
- Address space assigned to yourselves that is unused
- Can be used to detect various forms of malicious traffic



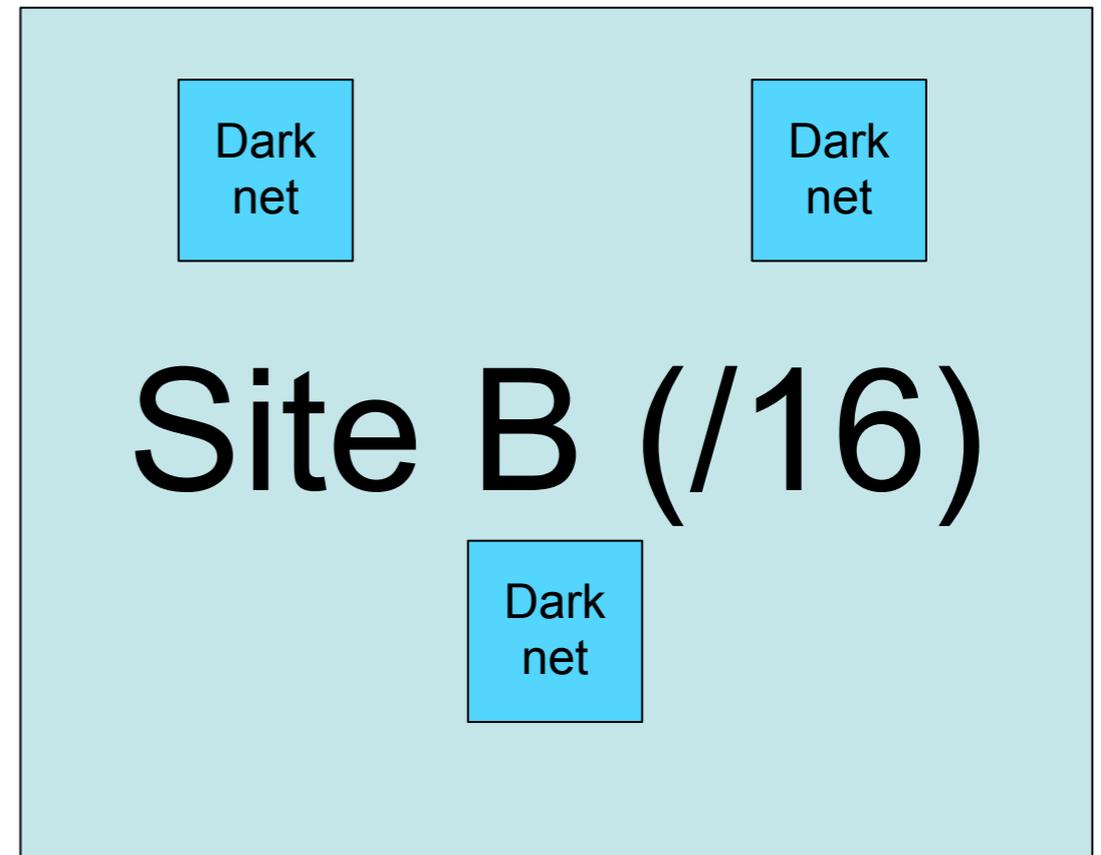
- Per site/organisation Darknet usage brings benefits

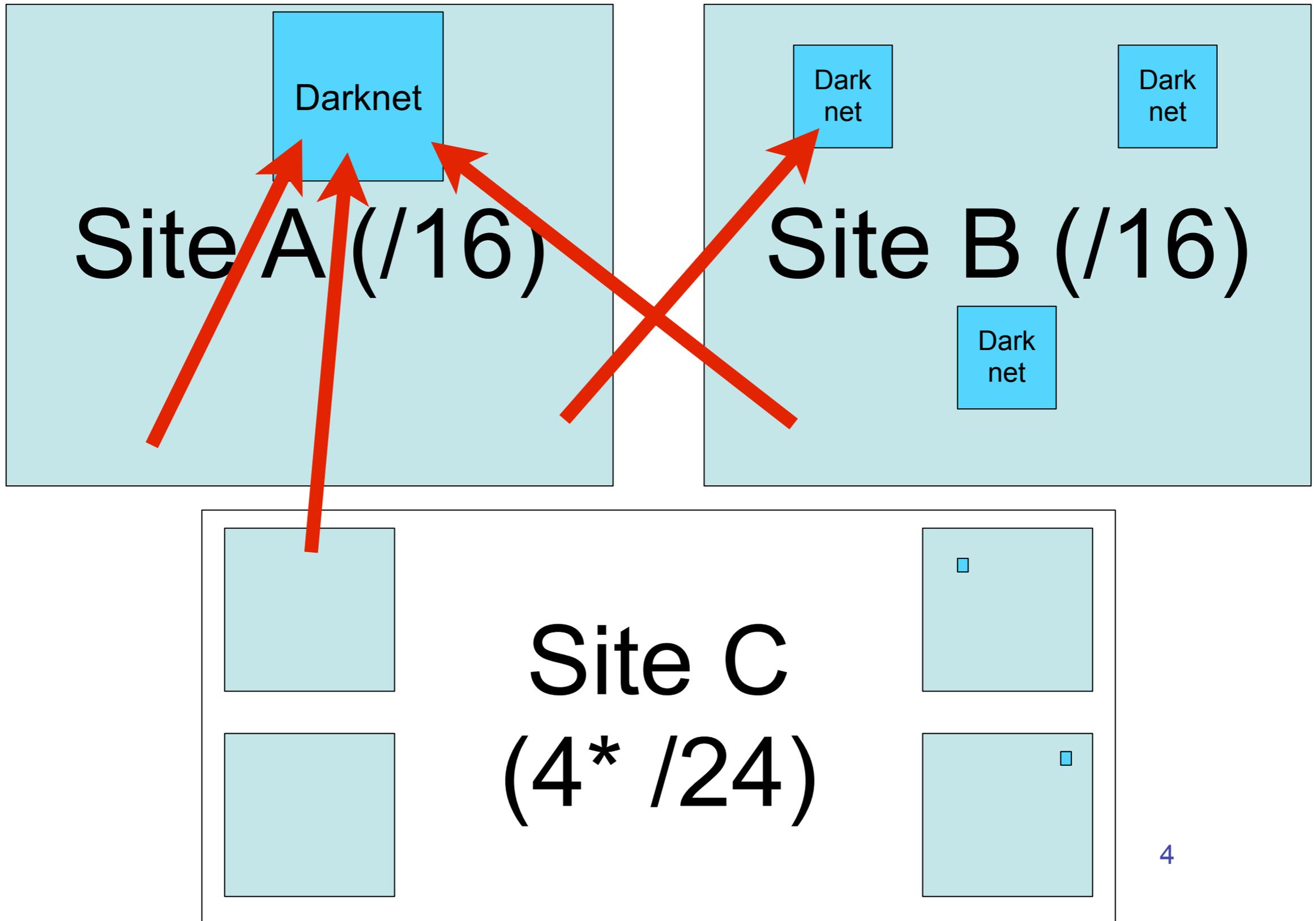
However...

- IPv4 Exhaustion makes obtaining “virgin” IP Space Hard
- Scanners tend not to confine themselves to your IP space any more - random scanning more likely than systematic

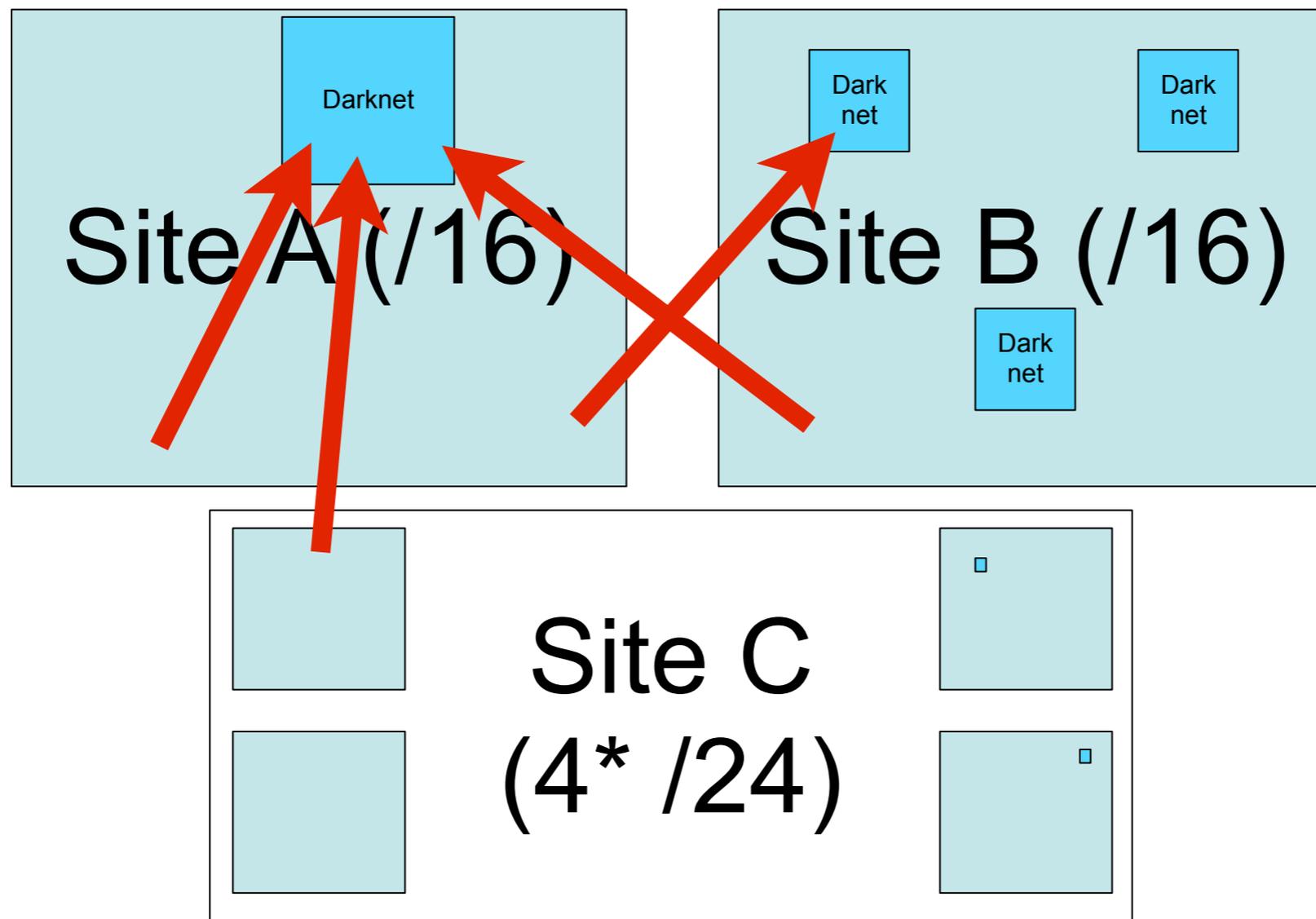


# Example (not to scale)





- With a conventional darknet setup, Site A would detect the traffic
- Sites B and C might continue in blissful ignorance of a problem
- Some other solutions exist eg. centralisation of reporting - this requires a lot of work and provides a single point of failure
- Our approach is to centralise only the registry of netblocks and contacts (and to have a failover if the update is unavailable)



- Each Site knows Sites A, B, C's address ranges and a contact, when the sensor sees traffic it contacts the site contact
- notification is near instant to the remote site

# Further Work

- Under active development, new features coming soon, next release will also be packaged for further OSes
- <http://projects.oucs.ox.ac.uk/darknet>
- Code is freely available so it is possible to either set up your own mesh, or we would consider hosting a wider mesh than currently

