



Note: a detailed discussion of this model is at:
 Rid, T and B Buchanan, "Attributing Cyber Attacks,"
Journal of Strategic Studies, vol 39, no 1, February 2015,
<http://dx.doi.org/10.1080/01402390.2014.977382>

© Thomas Rid and Ben Buchanan, King's College London

Post-Publication
 How did the intruders respond to the publicity?
 Was the response professional?
 Did the intrusions continue?
 If no, did they stop permanently?
 Did tactics and methods change?
 When was the response initiated?
 How long did it take?
 Was infrastructure dismantled?
 If so, how?

What are the "terms and conditions" of releasing signatures and technical indicators?

Will adversaries be able to adapt their behaviour?
 If yes, how?
 And who?

Will operations be harmed as a result of the release?

Will capabilities be harmed as a result of the release?

How much detail should be released?
 What is the most appropriate estimative language?