

Crisis Cyber Decision Making

The OODA “Loop”

Allen Forbes

President, Certico Corporation

afortbes@certicoconsulting.com

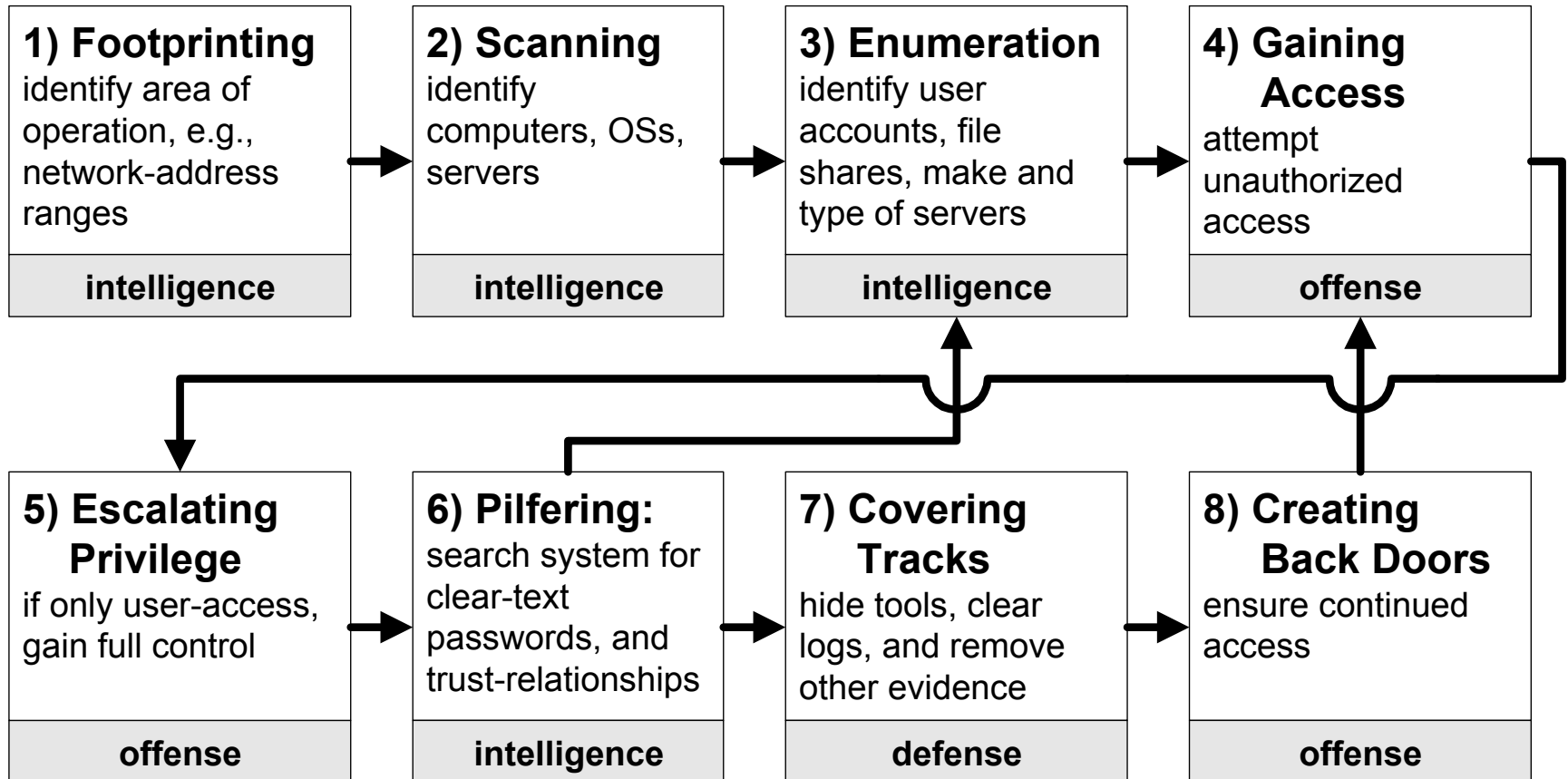
(480) 502-2258

Overview

- Attacker Methodology & Points of Detection
- OODA Loop
 - Observe
 - Orient
 - Decide
 - Act
- Critical Connections

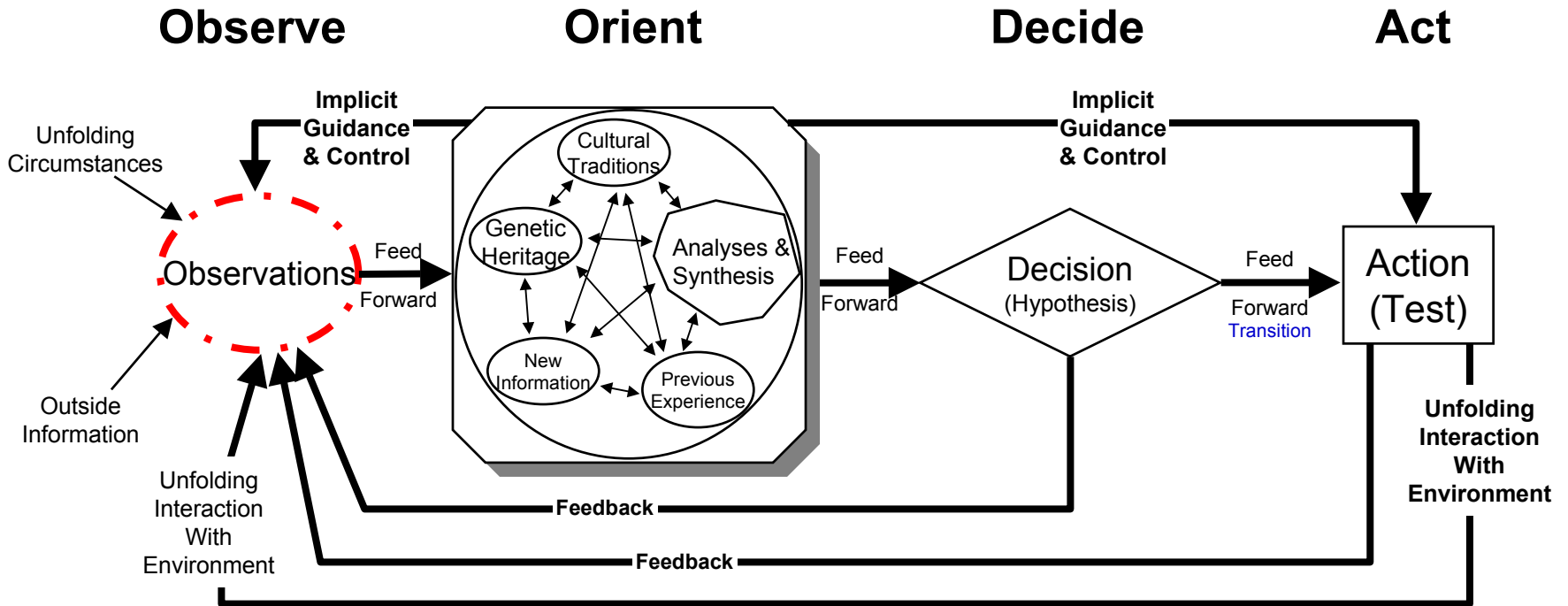
Model of the incident hacking-process

(adapted from *Hacking Exposed*)



Boyd's OODA "Loop"

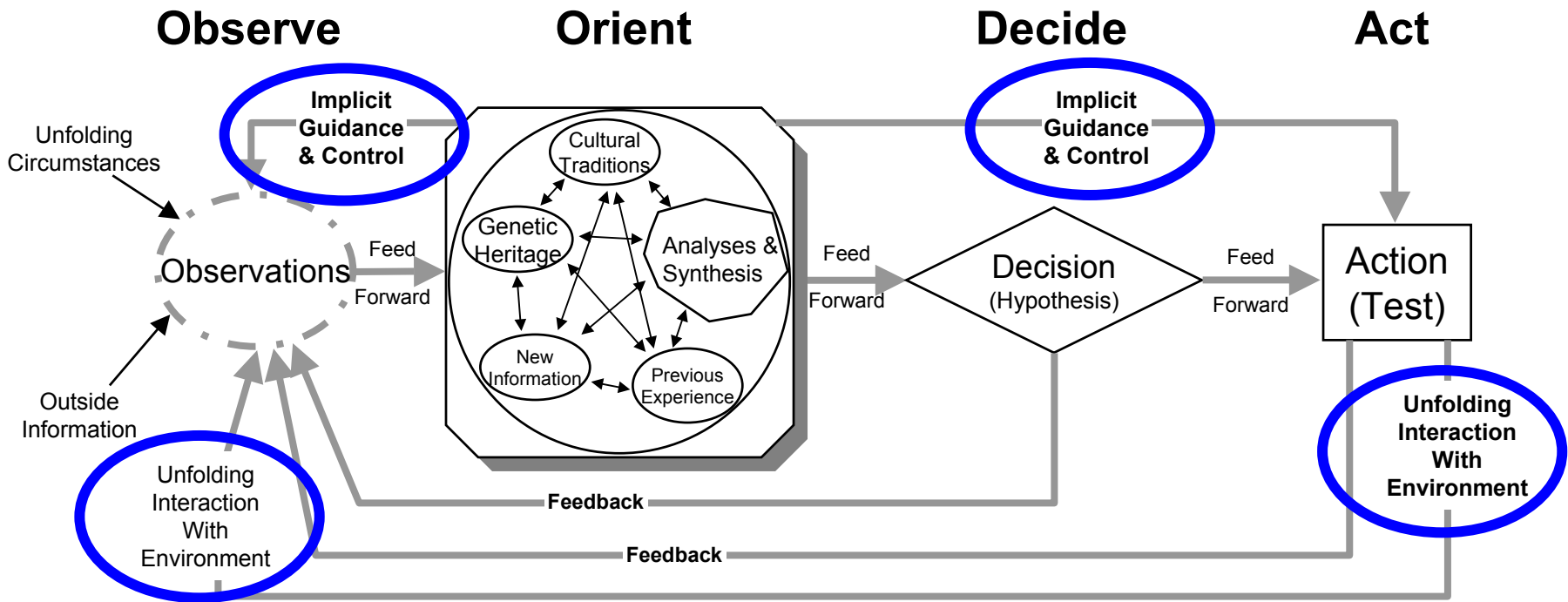
Sketch



Orientation shapes observation, shapes decision, shapes action, and in turn is shaped by the feedback and other phenomena coming into our sensing or observing window.

Also note how the entire "loop" (not just orientation) is an ongoing many-sided implicit cross-referencing process of projection, empathy, correlation, and rejection.

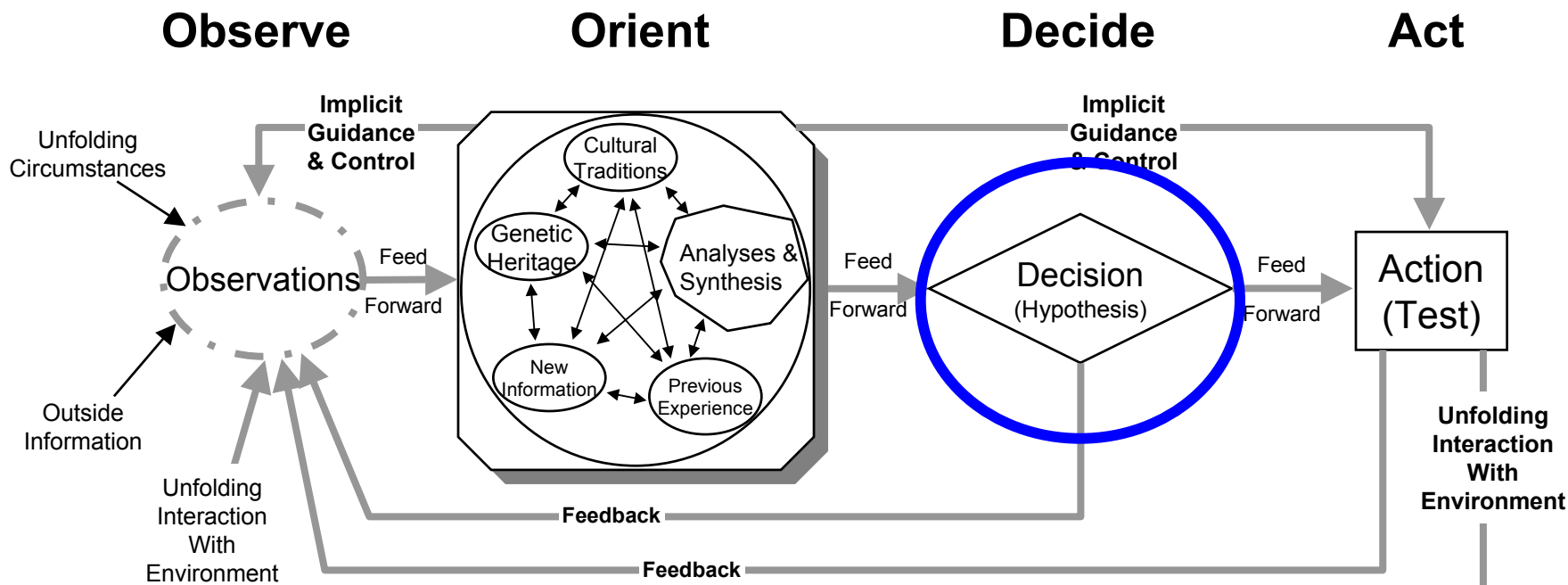
Critical Connections



Emphasizing implicit guidance accounts for organizational friction and maximizes available time. *Soccer game.*

Constant interaction guides the organization, ensures communications, and flows expectations.

Critical Connections



Decisions are *explicit*. Make them when you need to align or re-orient the actions of your team.

Decision making and re-orientation take time.

Implicit guidance and controls influence the teams actions until they re-orient.

Questions

Allen Forbes

President, Certico Corporation

aforbes@certicoconsulting.com

(480) 502-2258