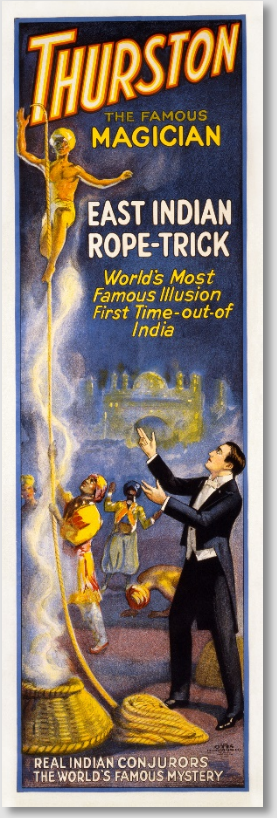
“The Devil Does Not Exist”—The Role of Deception in Cyber

Mark Mateski
Red Team Journal

Matt Devost
FusionX



Blackhat 2014

Introduction

Why study deception?

At the end of the day, your attacker/adversary is not a one or a zero.

Attackers are good at exploiting human factors (e.g. spearphishing) because we are wired to want to believe the lie.

Attackers are wired the same way.

Need to overcome cultural bias against deception.

Bridging the cyber gap

We have long-standing disciplines of gaming human/entity interaction that can be applied to our domain.

Spent time interacting with intel community to understand the deception elements of espionage.

There is direct applicability to attack/defense.

Applying Deception to Cyber

Misdirection

Get the attacker to go after the wrong target through public (e.g. announce wrong product code name) or private (network architecture) manipulation

Observation/ surveillance

- Passive monitoring for attribution
- Implied monitoring to influence attacker behavior
- Intentionally attribute to wrong class of attacker

Outright deception

- Impact the attacker’s OODA Loop
- Plant false data (example)
- Divert or attract to honeypot

As an attacker?

- Feign false level of sophistication
  - E.g. inability to hack *nix systems
- Deception in internal targeting
- Egress Deception

East and West

East and West

Historically, Westerners have often viewed trickery in war as less-than-noble.

- They are generally most willing to employ cunning when their backs are against the wall (the Allies in World War II, for example).

In the East, the practice of cunning is generally much more accepted.

East and West

Historically, Westerners have often viewed trickery in war as less-than-noble.

- They are generally most willing to employ cunning when their backs are against the wall (the Allies in World War II, for example).

In the East, the practice of cunning is generally much more accepted.

Tension in the West

“ … in the history of the Western military tradition from Homer to the present, a tension exists in military ethics between the advocates of what I call the Achilles ethos and the Odysseus ethos.” (Wheeler, xiii–xiv)

Achilles vs. Odysseus

“The Achilles ethos promotes chivalry, face-to-face confrontation, open battle, and the use of force, while the Odysseus ethos asserts the superiority of trickery , deceit, indirect means, and the avoidance of pitched battle, although not the denial of the use or force or battle if advantageous.” (Wheeler, xiv)

The 36 stratagems

"Stratagems are used everywhere, by people in all walks of life. But Western civilization has never produced anything remotely resembling the highly condensed catalog of devious tactics known as the '36 Stratagems.' The entire catalog consists of a mere 138 Chinese characters. Yet into these terse 36 Stratagems the Chinese have compressed much of their thousands of years of experience in dealing with enemies (both internal and external) and overcoming difficult and dangerous situations." (von Senger, *The Book of Stratagems*, 1)

A linguistic tag

"Most of the cunning behaviors advocated by the 36 stratagems were, and still are, used outside China as well. However, they are generally used spontaneously, in an unconsidered way, and without the benefit of there being a linguistic tag to name the cunning behavior, as is the case with the catalog of the 36 stratagems. As a result of a lack of awareness of cunning, tricks generally remain unnoticed and unanalyzed." (von Senger, *The 36 Stratagems for Business*, 30)

No tags

“Since Europe came into being, a European has never asked the question ‘What stratagem?’ either in a novel or in real life. This is a question that Europeans cannot ask, because they do not have the terminology for the various trick techniques.” (von Senger, *The 36 Stratagems for Business*, 27)

The lexicon of cons

Interestingly enough, an informal vocabulary of trickery *did* emerge in the West among con artists.

Many of the tricks con artists employ have names, allowing con artists to employ them in much the same way Eastern strategists employ the “linguistic tags” inherent in the 36 stratagems.

For example, some famous cons of yesteryear (and today) include “three-card monte, banco, chuck-a-luck, green goods, the gold brick, the country send, [and] the Spanish prisoner.” (Nash, 1)

Short vs. long cons

When considering trickery and deceit in the world of the con artist, it is especially useful to distinguish between the short and the long con.

“If the short con is an anecdote, the long con is a novel. Essentially, a short con involves taking the pigeon for all the money he has on his person, while the big [or long] con sends him home to get more.” (Sante in Maurer, x)

Our goal

Our goal is to introduce you to a simple “LexiCon” of trickery.

The purpose of the LexiCon is to improve our ability to talk about perception and misperception, particularly in the context of cybersecurity.

The LexiCon

The LexiCon

The LexiCon framework consists of three games and two perceptual states.

We can combine the games and states to describe a variety of possible situations involving perception, misperception, and deception.

We illustrate and explore these situations using examples.

Understanding the games and states can help security analysts anticipate risks and exploit opportunities.

Three games, two states

The three games are …

1. eye-to-eye,
2. the con, and
3. the hypercon.

The two perceptual states are …

1. awareness and
2. false confidence.

Game 1: Eye-to-eye

Both players see the same game. There are no secrets, although this doesn't mean one player knows what the other will do.

- Chess and checkers are good examples.

Game 2: The con

The first player seeks an advantage by playing the game while withholding a relevant secret. The second player doesn't know the secret.

- Rigged games and street hustles are good examples.
- A honeypot is another example of a con.

Game 3: The hypercon

The second player perceives and attempts to leverage the con (without the first player knowing).

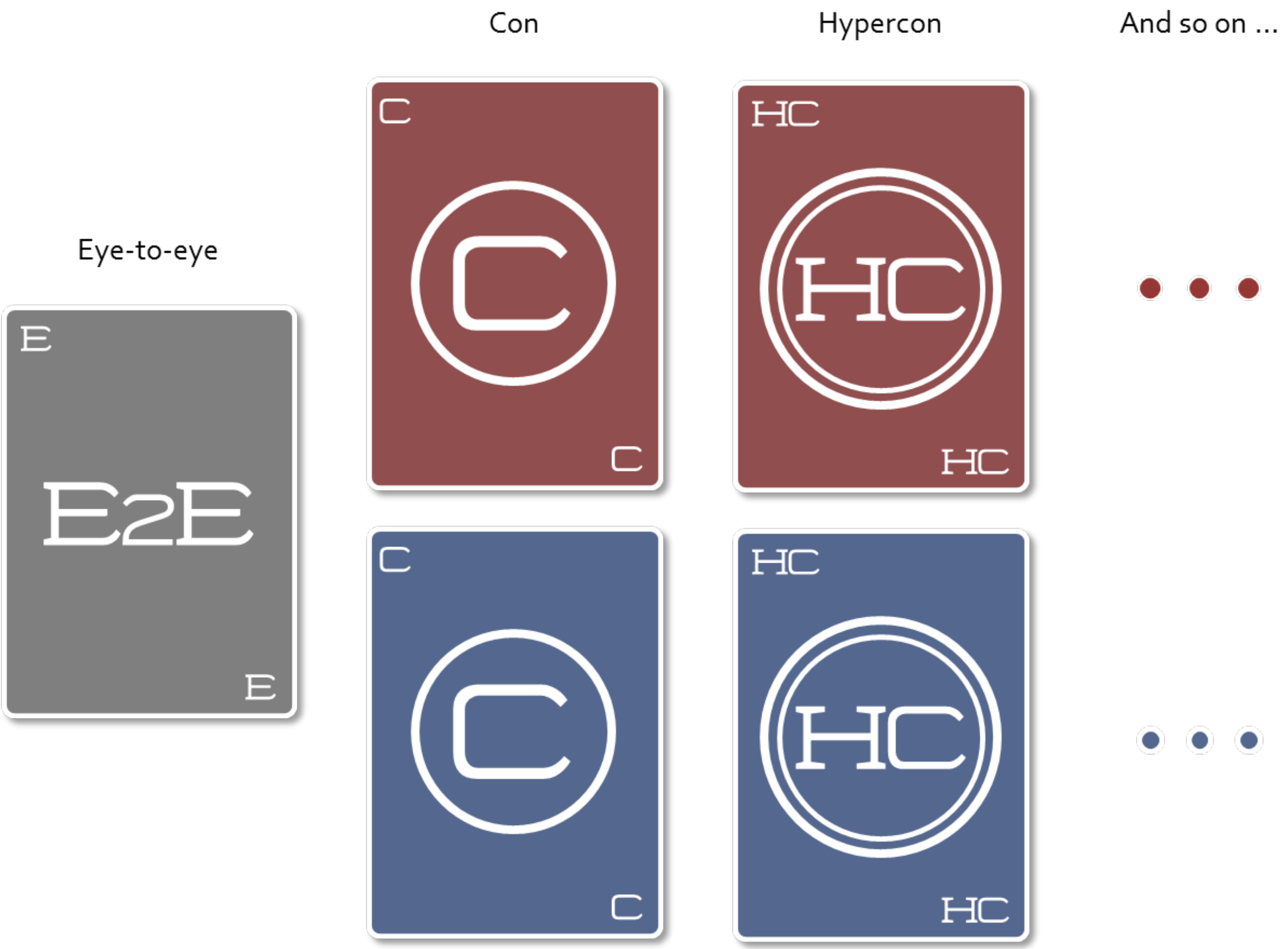
- A sting is a good example of a hypercon.
- A honeypot the attacker perceives and exploits is another example.

The two perceptual states

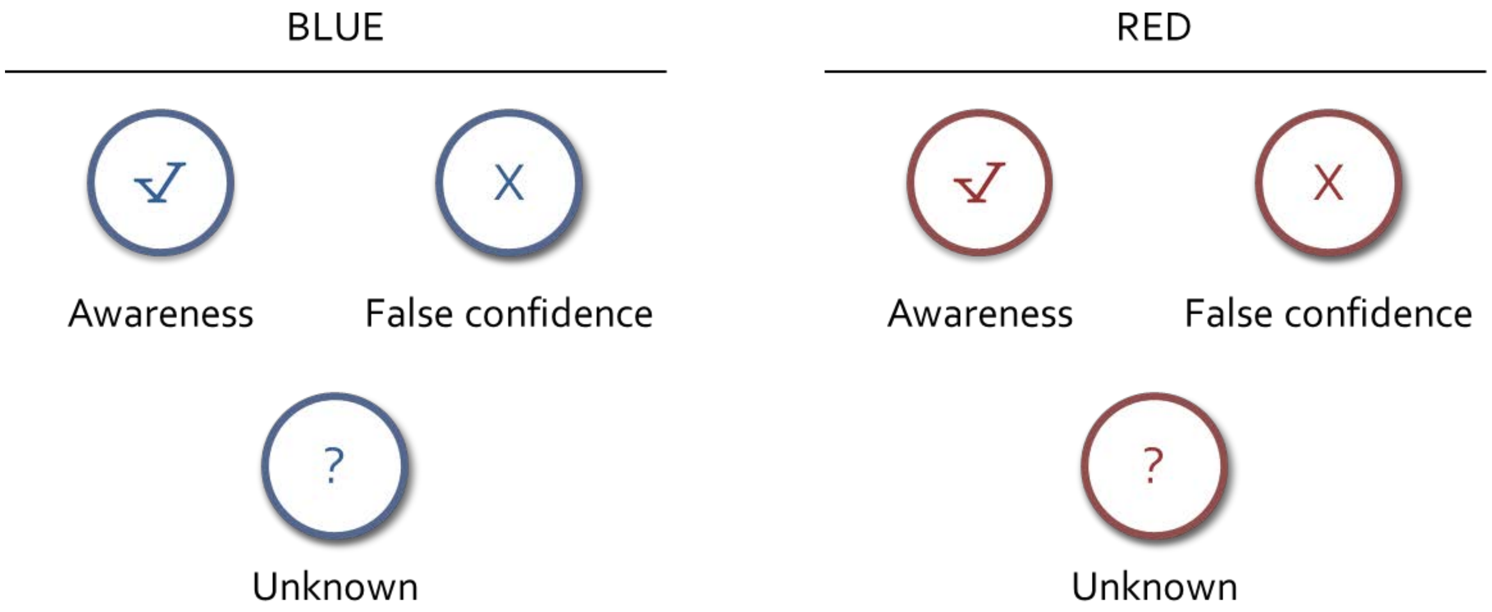
Layered atop the three games are two perceptual states:

1. Awareness: The player's perception is correct.
2. False confidence: The player's perception is incorrect (in other words, it's a misperception.)
3. Unknown.

The LexiCon game board



The perceptual states



BLUE

✓ Awareness

X False confidence

? Unknown

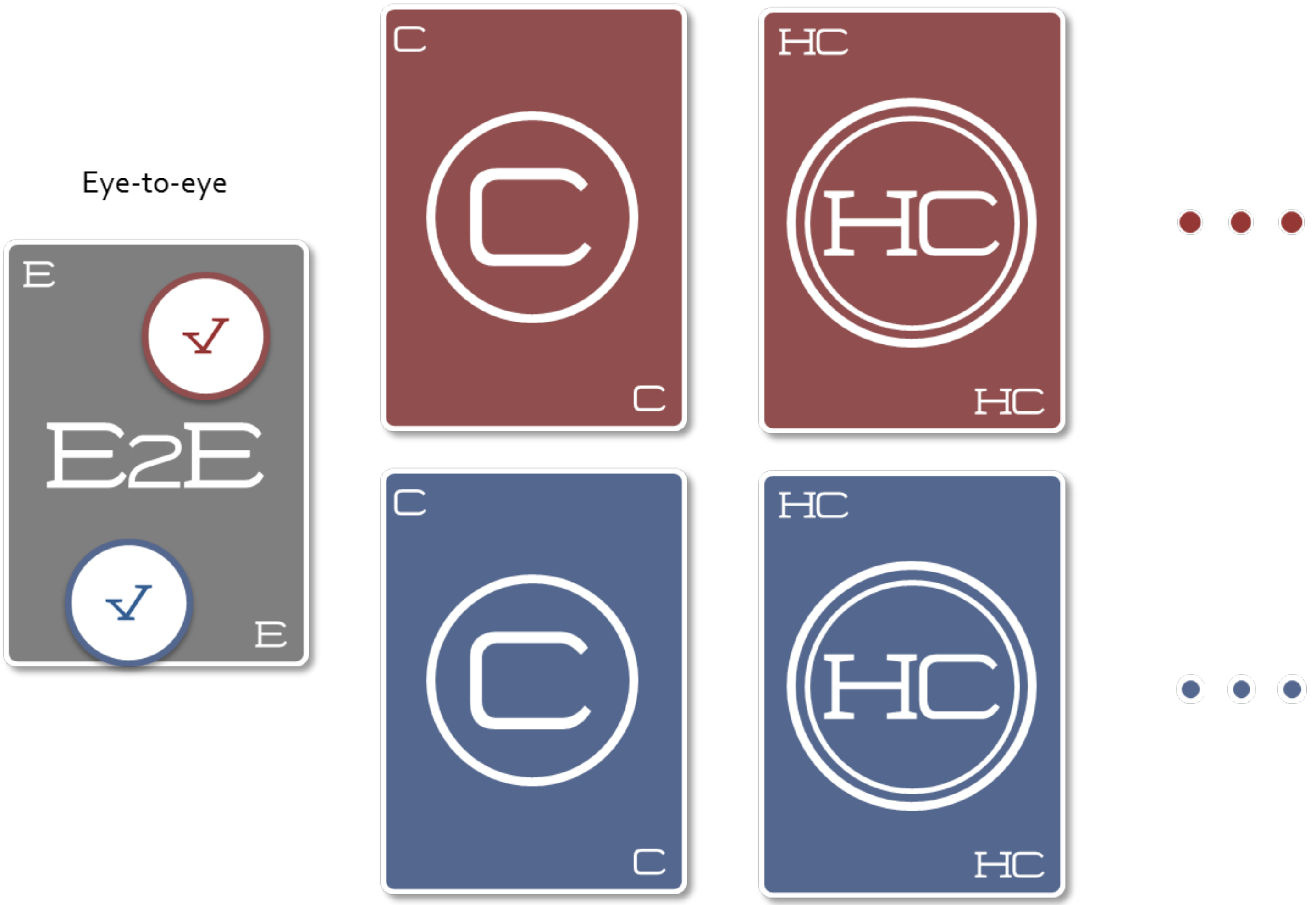
RED

✓ Awareness

X False confidence

? Unknown

Examples and cases



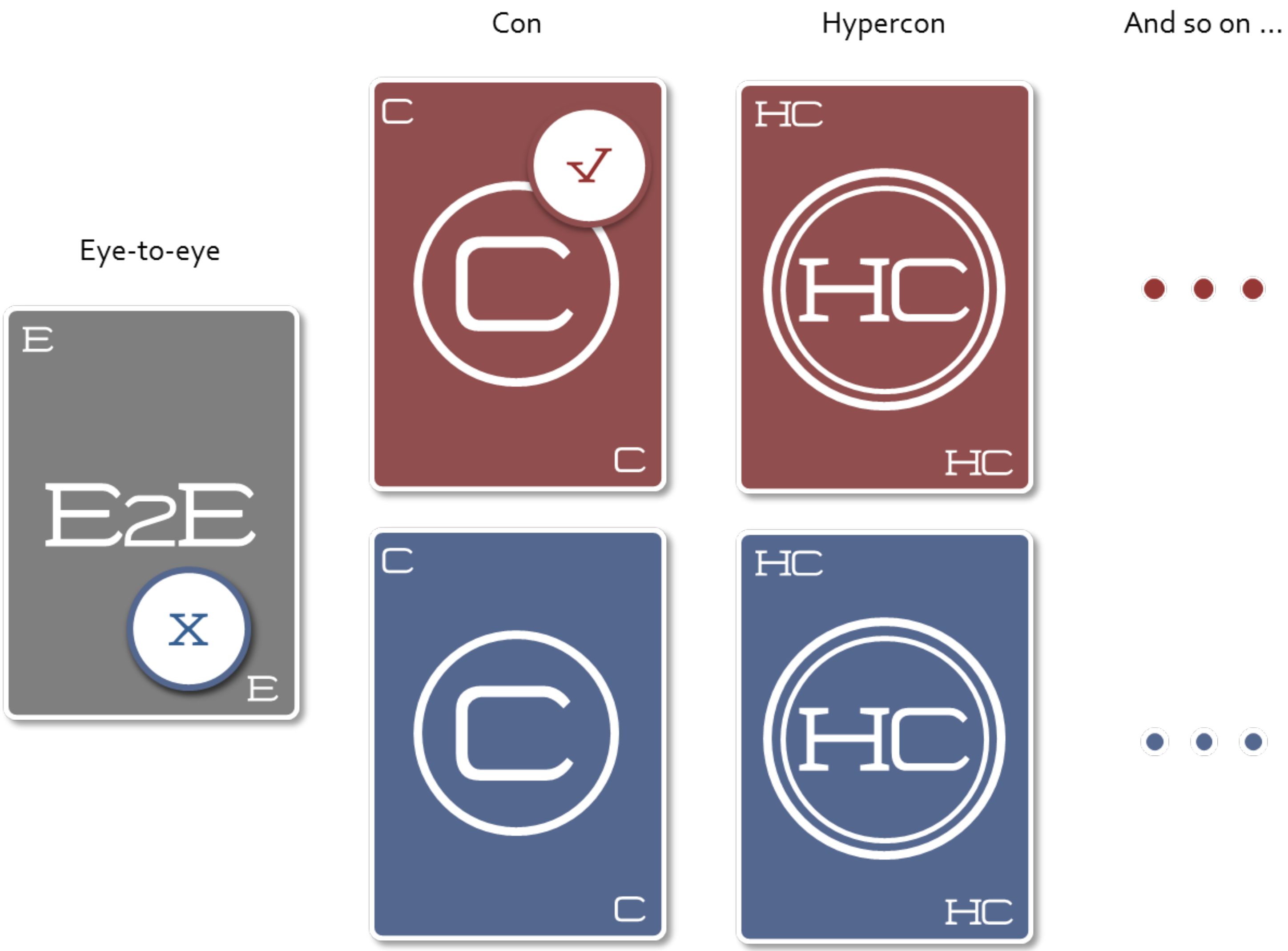
Eye-to-eye

Con

Hypercon

And so on …

Examples and cases



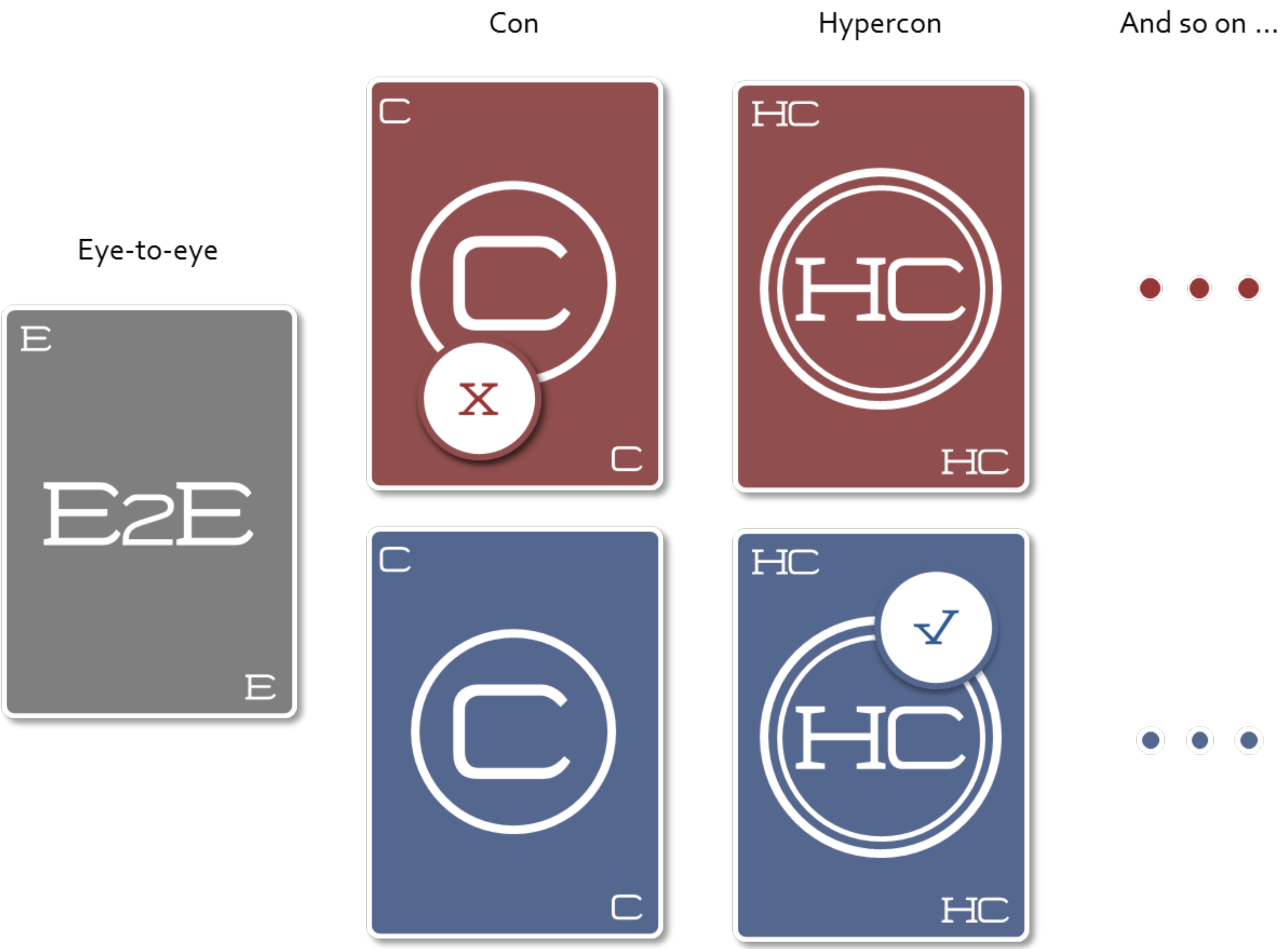
Eye-to-eye

Con

Hypercon

And so on …

Examples and cases



Eye-to-eye

Con

Hypercon

And so on …

Perceptual space

We traditionally explore the space of possible scenarios by varying elements such as capability, intent, and time.

The LexiCon framework encourages security professionals and decision makers to explore another dimension of scenario space: the perceptual.

If you explore this space systematically and your opponent does not, you hold an advantage (all other things being equal).

Questions

The LexiCon points us toward some simple but important perceptual questions:

- Is everything as it appears to be?
- Am I being conned?
- Can I turn the con into a hypercon?
- Can my opponent turn the con into a hypercon?

Note how the questions capture the trade between risk and opportunity.

Another goal

It is useful to note that the goal is not always deception. Sometimes you want to be on the same page as the other player. In these cases, you can use the LexiCon in reverse (where the goal is getting both players to meet eye-to-eye).

Sources

Maurer, *The Big Con*: *The Story of the Confidence Man* (1940/1999).

Nash, *Hustlers and Con Men* (1976).

von Senger, *The Book of Stratagems* (*Tactics for Triumph and Survival*) (1991).

von Senger, *The 36 Stratagems for Business* (2004).

Wheeler, *Stratagem and the Vocabulary of Military Trickery* (1988).