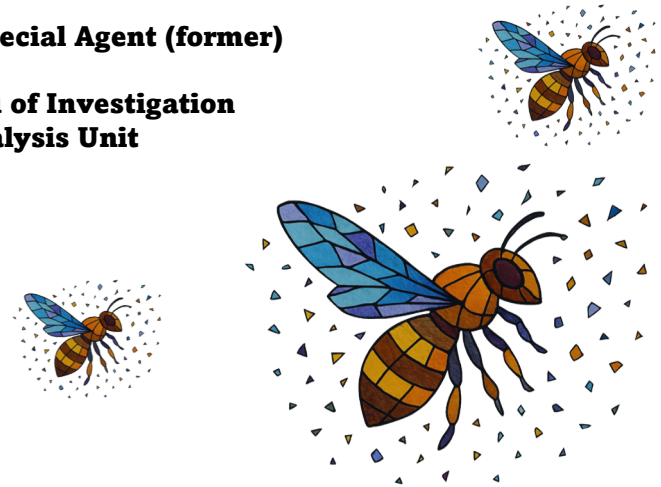
'Welcome to the Party, Pal': How *Die Hard* Can Help Us Design Cyber Deception Influence Models Built on Signaling More Than Infrastructure

Honeynet Workshop Prague 2 June 2025

Tim Pappa
Incident Response Engineer – Cyber Deception Strategy, Content Development, and Marketing
Walmart Global Tech
Cyber Deception Operations

Supervisory Special Agent (former)
Profiler
Federal Bureau of Investigation
Behavioral Analysis Unit

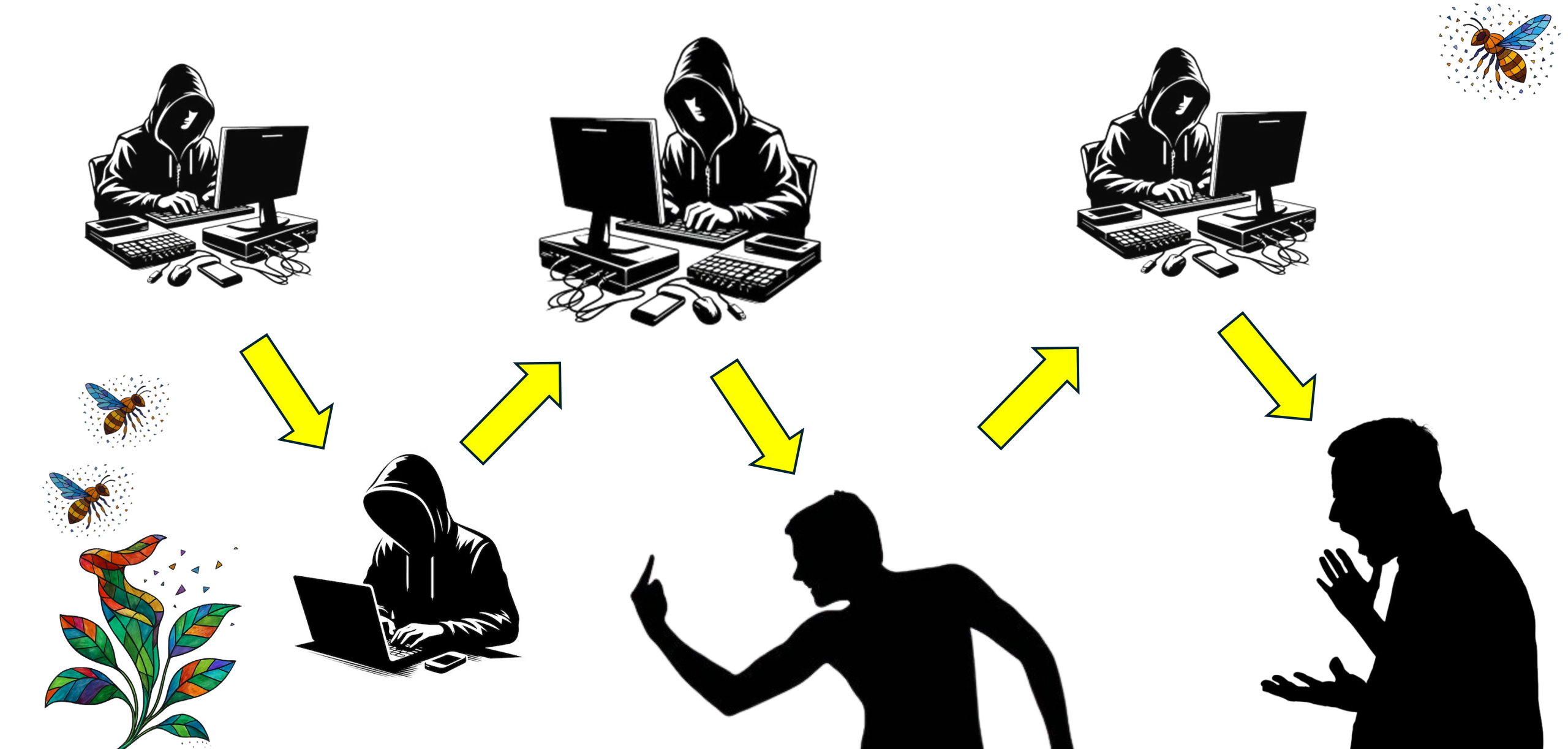


My presentation, comments, and opinions are provided in our personal capacity and not as representatives of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.

How does Die Hard help us understand deception and influence?

- The terrorist group manipulated the building's security controls and protocols using deception and influence
- Yes, NYPD Det. John McClane literally killed everyone; however, he was effective because he observed behaviors and exploited their behaviors and affect
- Det. McClane used deception to overcome the limitations of his movement and weapons, including their decision making and cognitive biases
- With each dead terrorist, Det. McClane instrumentally compounded ambiguity and uncertainty in Gruber
- Det. McClane's deception and influence was effective because it was consistent and engaging

A cyber deception experience that really shaped me



Rare experiences in government and industry cyber deception

- **Former FBI profiler, supporting adversary engagement operations and communication**
- **Design and create content supporting industry cyber deception**

Why are signaling or displays so important in cyber deception?

- Whaley was a communication researcher before he was a deception researcher
- Signaling contextualizes the “domain” costs and benefits
- We don’t want to keep waiting until an attacker gets inside

Cyber deception influence model #1:

Introduce affective storylines and content that undermine attackers' trust and certainty

- **The first dead terrorist had a brother terrorist, and they were afraid to tell him because of how he might react**
- **The terrorists who found him appeared shocked that someone had killed one of them, and appeared to have information about which floor they were on**
- **Gruber was interrupted from his plan and narrative:**
  - **"…*We are in charge*…"**
- **Gruber is contributing to the uncertainty and ambiguity:**
  - **"…*A security guard we missed?*…*No, this is something else*"**

Cyber deception influence model #1:

Introduce affective storylines and content that undermine attackers' trust and certainty

- There is a hierarchy to content sharing based on emotions and affect and humor
  - You can drive private and public content sharing.
- Inducing emotional or affective overload is an element to cognitive overload, and perhaps quicker and more effective
- This works for individuals online, but especially for groups or teams
- 'Hard targets' like hypervigilant attackers are some of the most vulnerable targets to distrust and "sinister attribution error"

Cyber deception influence model #2:

Channel attackers' attention and sensemaking to reputational and performance stages

- **Det. McClane uses the terrorists' own communication channel to talk to Gruber, but all the terrorists can hear this communication**
- **How Gruber responds perhaps changes**
  - **He expected the police response, but he did not expect Det. McClane**
- **Det. McClane mentions the deaths of various terrorists for the first time before Gruber and his terrorists can confirm those deaths, introducing further uncertainty and ambiguity**
  - **"*How does he know so much about…*"**
- **Det. McClaine misdirects the terrorists' priorities and time to confirm his claims**

Cyber deception influence model #2:

Channel attackers' attention and sensemaking to reputational and performance stages

- **If you have their attention and can hold their attention, you can directly influence their sensemaking and next steps**
- **Sensemaking is like a filter, making sense of new information**
  - **These are aspects of *reflexive control* to manipulate this filter and manage attacker behaviors**
- **Injecting into their communication and pathways of information collection and processing can significantly influence them**

Cyber deception influence model #3:

Disrupt and influence attackers' storylines with your own powerful storyline

- **The terrorists prepared to escalate if necessary and did escalate**
- **The law enforcement response was not prepared for this escalation and was generally unable to do much from outside the building**
- **Det. McClane disrupted that escalation with an escalated response, using the terrorists' C4 explosives**
  - **"*It's not the police…it's him*"**
- **The local news media were present throughout the event, providing <u>live</u> coverage**

Cyber deception influence model #3:

Disrupt and influence attackers' storylines with your own powerful storyline

- ***Privileged moments*** **of vulnerability can influence attackers and law enforcement response if revealed publicly**
- **You should not depend on law enforcement assistance during an event**
- **Attackers may prepare for law enforcement response or be familiar with law enforcement response, but they will struggle to anticipate how you will respond once you *violate* their expectations**
- **Using an attackers' tools and techniques in response just short of 'hacking back' can cause confusion and uncertainty**
- **There are other real and imagined stories you can tell powerfully**

Discussion

- **These cyber deception influence models can be demonstrated by anyone, regardless of level of training or experience.**
  - **This is not ‘hacking back’, but it is a response.**
- **The psychological underpinning of each cyber deception influence model reflects attackers’ behavioral responses.**
  - **Communication incorporating those underpinnings can effectively signal or display these cyber deception influence models in most contexts.**
  - **It costs little, too.**

Discussion

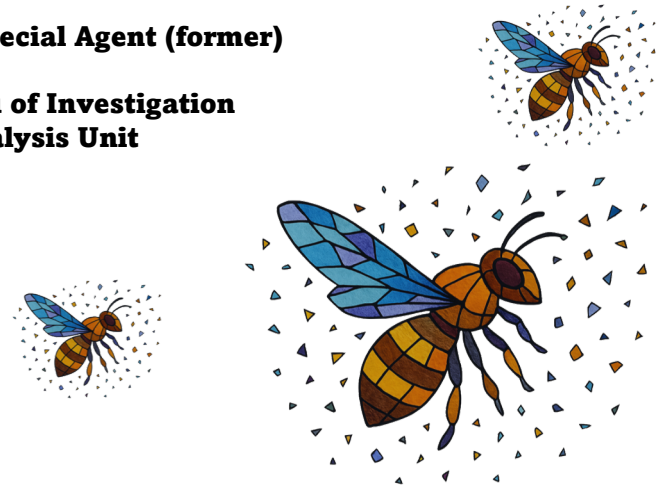
- **These cyber deception influence models can practically or instrumentally augment any existing deception infrastructure and network defense enterprise practices.**
  - **These influence models also reflect operational research into effective deception online.**
- **Even in the absence of any deception COTS or deception infrastructure, cyber deception influence models can still misdirect or deter attackers.**

'Welcome to the Party, Pal': How *Die Hard* Can Help Us Design Cyber Deception Influence Models Built on Signaling More Than Infrastructure

Honeynet Workshop Prague 2 June 2025

Tim Pappa
Incident Response Engineer – Cyber Deception Strategy, Content Development, and Marketing
Walmart Global Tech
Cyber Deception Operations

Supervisory Special Agent (former)
Profiler
Federal Bureau of Investigation
Behavioral Analysis Unit



My presentation, comments, and opinions are provided in our personal capacity and not as representatives of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.