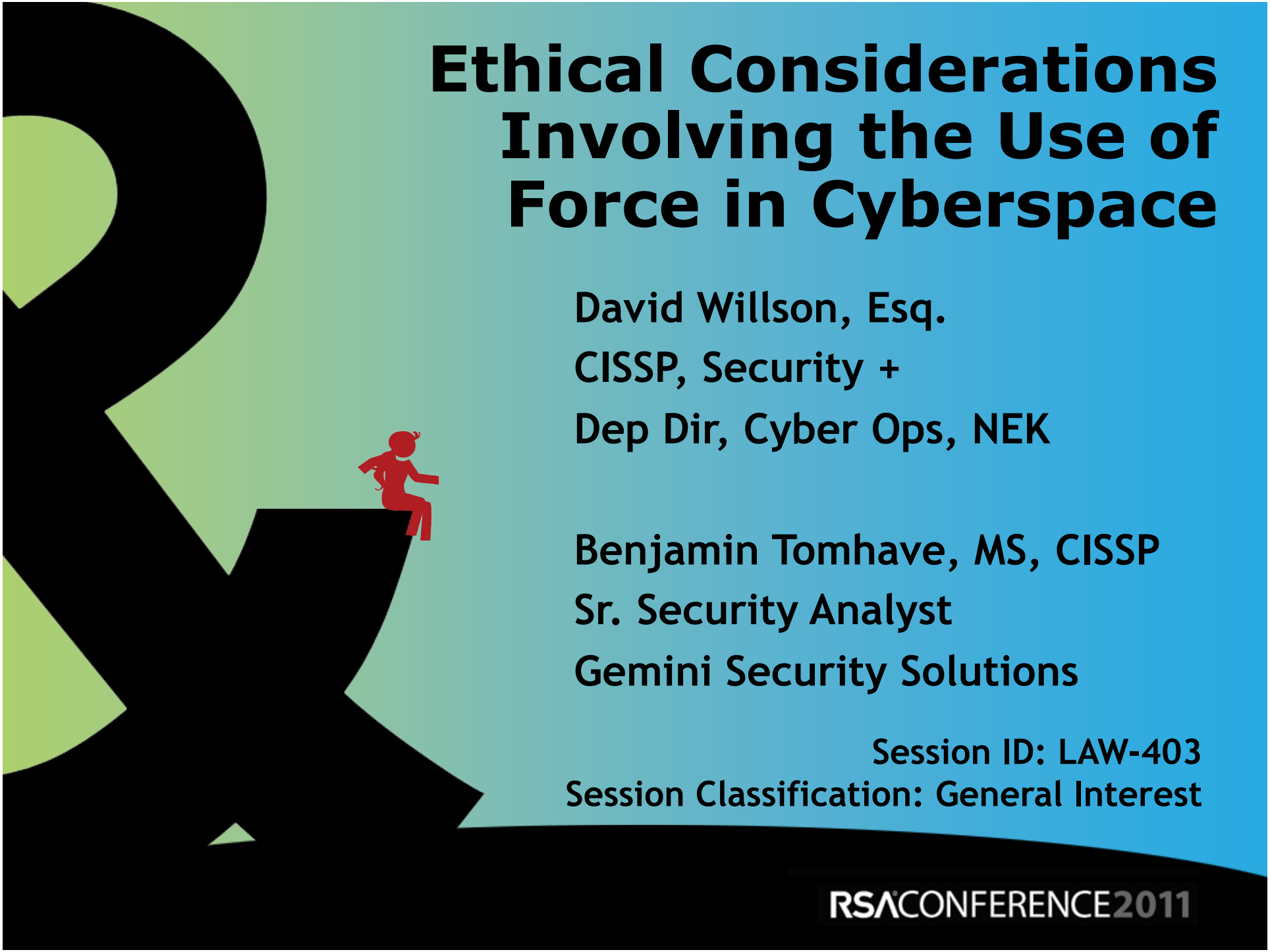
Ethical Considerations Involving the Use of Force in Cyberspace



David Willson, Esq.
CISSP, Security +
Dep Dir, Cyber Ops, NEK

Benjamin Tomhave, MS, CISSP
Sr. Security Analyst
Gemini Security Solutions

Session ID: LAW-403
Session Classification: General Interest

Question A:
Is it legal to initiate an offensive response to a cyber attack?

Nation vs. Nation

Law of War

Article 51

Fear of Reprisal

Escalation

(Picture Source: http://www.inquisitr.com/10599/us-army-to-setup-camp-on-second-life/)

Company/Individual vs. Hacker(s)

CFAA & ECPA

Wiretap Act

Pen Trap & Trace Law

State laws

Self-Defense

Question B:
Is it ethical to initiate an offensive response to a cyber attack?

Considerations

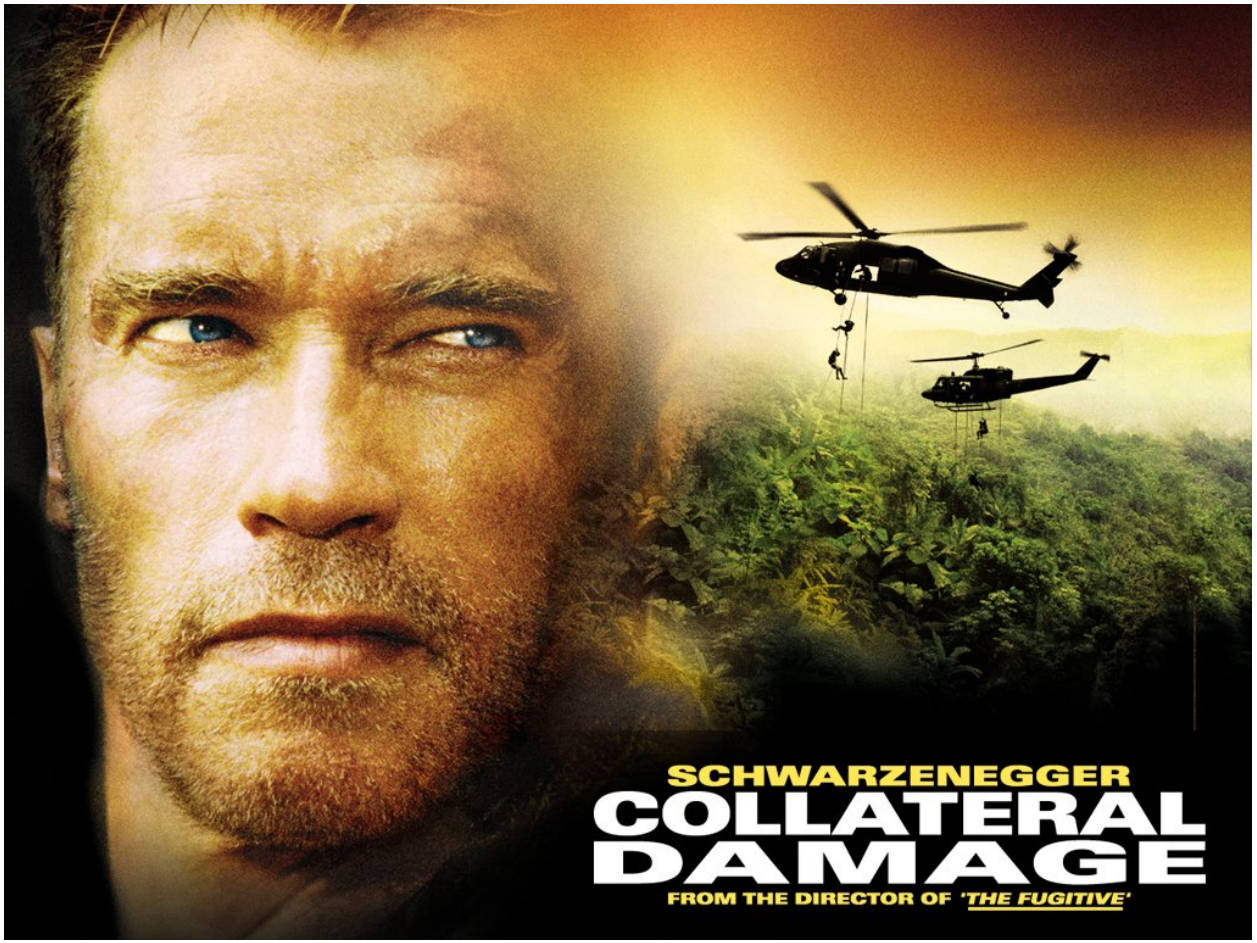
Nation v. Nation

Article 51

Company/Individual v. Hacker(s)

Self-Defense

Attribution: A Key Challenge



RSA 2011 CONFERENCE

GEMINI SECURITY SOLUTIONS

NEK

Is Traceback/Hackback, or Offensive Use of Cyberspace, Legal or Ethical?

Why Not?

What should an InfoSec Professional do when there is a significant public risk and a relatively easy-to-implement solution that mitigates that risk?

What would you do if you had the ability to preemptively stop the spread of a malicious worm by patching or inoculating systems in the wild (e.g., release a “white worm”)?

"You can strike back. Your enemies are not ethical hackers."
Laurent Oudot, founder and CEO of TEHTRI-Security

Unethical Behavior?

Can you distinguish between activity that is illegal but also ethical? Is hacking a system and stealing or causing damage unethical?? (That's a give me!!)

Is it ethical to use your neighbor's wireless network?

What about if your home computer gets hacked and you think you can trace back and find the hacker? Unethical??? Illegal??? (Needed to ask)

Your company gets hacked; Millions $$$ lost. From your home computer you trace and track the hacker. Unethical?? Illegal??

“The Ethics of White Worms”

Two approaches:

a) Greatest good for the greatest number.

b) Two wrongs don’t make a right.

RSA 2011 CONFERENCE

GEMINI SECURITY SOLUTIONS

NEK

Practical Application

Short-Term: Assess!

Snap Assessment: What's your true exposure?

What's your network worth?
What's your data worth?
What's availability worth?
What are the potential legal costs?
Think outside your environment!
Immediate / Downstream / Etc.

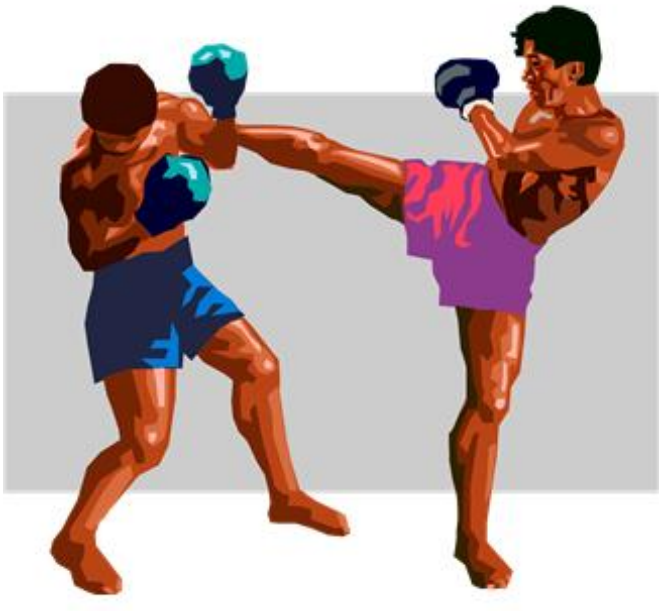
"If you cannot measure it, you cannot improve it." – Lord Kelvin

RSA 2011 CONFERENCE

GEMINI SECURITY SOLUTIONS

NEK

Mid-Term: Legal Defensibility



What are your…

…obligations?

…resources?

…liabilities & exposures?

Leverage formal analysis.

Document, document, document!

Cool-headed pre-planning.

Mid-Term: Architect

Focus on:

1. Baseline operational security.
2. Detection and response.
3. Pre-planning business responses.

"Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat." – Sun Tzu

Long-Term: Survivability

1. Continually analyze risk landscape
2. Optimize operational security
3. Maximize detection
4. Optimize response

Objective: To continue operations despite degraded conditions, including active attacks.

"An ounce of action is worth a ton of theory."
– Ralph Waldo Emerson

David Willson, Esq.
CISSP, Security +
Dep Dir, Cyber Ops, NEK

Benjamin Tomhave, MS, CISSP
Sr. Security Analyst
Gemini Security Solutions

Q & A

Thank You!