Cyber Civil Disobedience

A Frontier of Legal and Ethical Challenges

Doug Himberger, Ph.D.

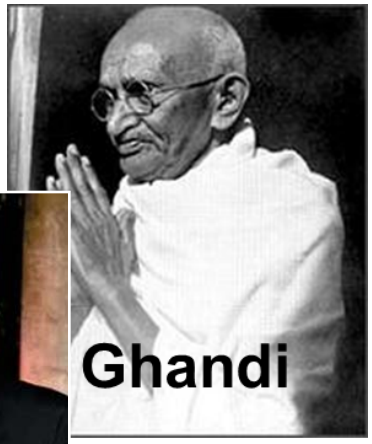
Don Goff, Ph.D.

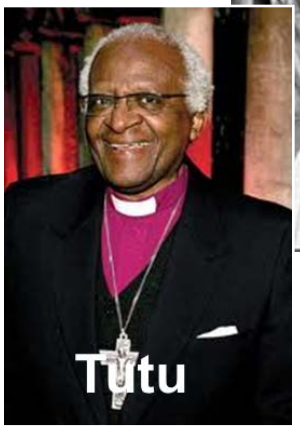
John Lickfett

Agenda

- Classic Framework for Understanding Civil Disobedience
  - Historic perspectives of a controversial social strategy
- Cyber Civil Disobedience
  - Exploring a vague new concept
- Mapping Civil Disobedience to the Digital World
  - Looking for analogies and gaps between the classic framework and the cyber context
- Liberty vs. Security: A Tipping Point
  - Risk and consequence: balancing ethics and enforcement
- Finding the Answers
  - Future research to inform protestors and enforcers

Classic Civil Disobedience





- Definitions of civil disobedience come from multiple philosophical sources, e.g., Thoreau, Gandhi, King. However, an academic definition was created by Carl Cohen (University of Michigan, Professor of Philosophy)

- Caveats: “Absolute precision in definition and the use of categories in this area is out of the question;” and others…

- “An act of civil disobedience is an illegal public protest, non-violent in character”

1105 MEDIA

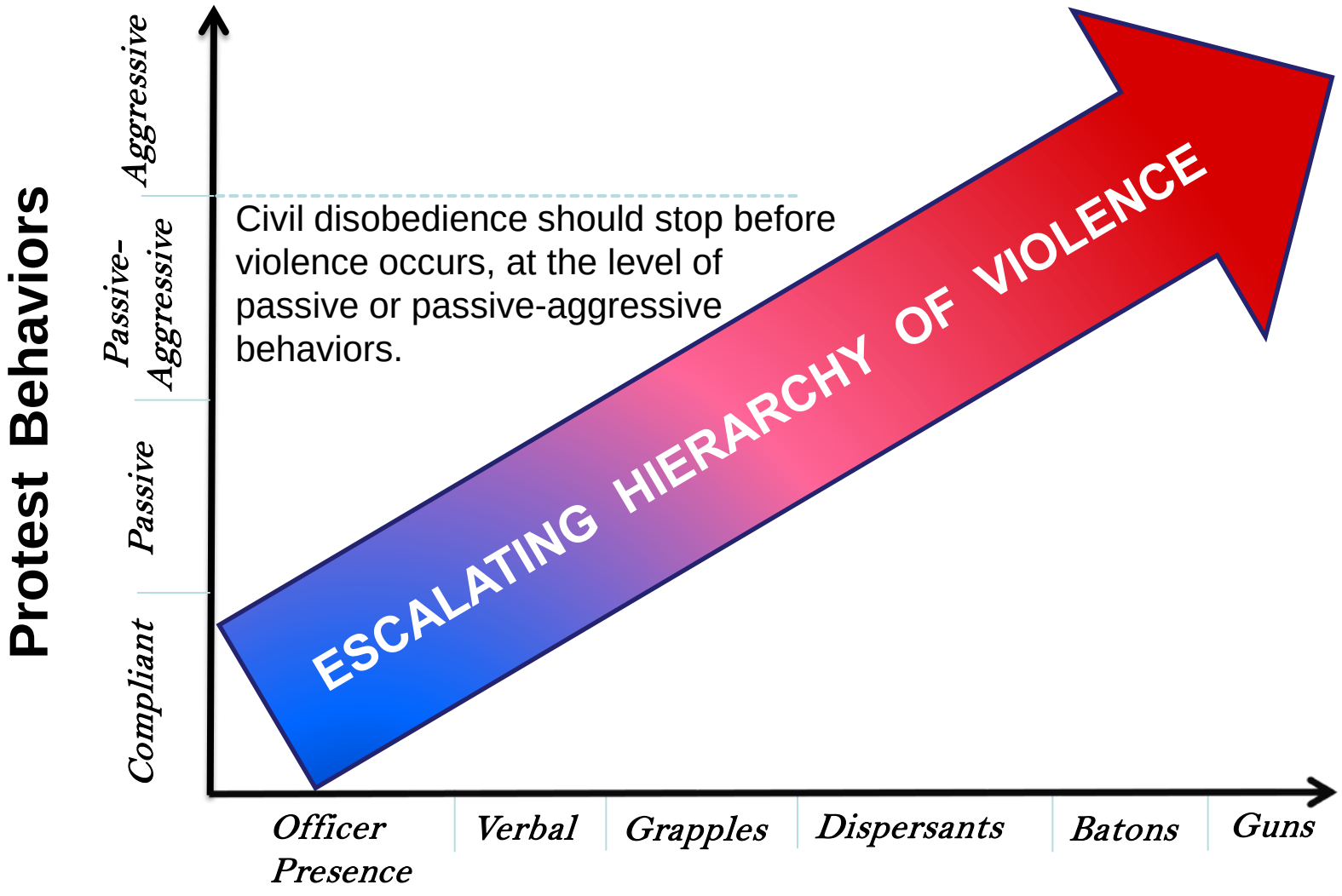
www.govsecwest.com

GOVSEC WEST
THE GOVERNMENT SECURITY CONFERENCE & EXPO

Civil Disobedience: A Classic Framework – Cohen (1966)

Framework Component	Classic Framework Characteristic
Definition of “Civil Disobedience”	An act of civil disobedience is an illegal public protest, non-violent in character
Requirements	Must break the law
	Must be public
	Must be an act of protest
	Non-violence is a factor
Caveats	No absolute precision in definition or categories
	No absolute generality forming conclusions

Dissent and Violence



Agenda

- Classic Framework for Understanding Civil Disobedience
  - Historic perspectives of a controversial social strategy
- Cyber Civil Disobedience
  - Exploring a vague new concept
- Mapping Civil Disobedience to the Digital World
  - Looking for analogies and gaps between the classic framework and the cyber context
- Liberty vs. Security: A Tipping Point
  - Risk and consequence: balancing ethics and enforcement
- Finding the Answers
  - Future research to inform protestors and enforcers

Electronic Civil Disobedience

Defined in 1996

"As hackers become politicized and as activists become computerized, we are going to see an increase in the number of cyber-activists who engage in what will become more widely known as Electronic Civil Disobedience. The same principals of traditional civil disobedience, like trespass and blockage, will still be applied, but more and more these acts will take place in electronic or digital form. The primary site for Electronic Civil Disobedience will be in cyberspace."

- Stefan Wray (Author of "Electronic Civil Disobedience and the World Wide Web of Hacktivism")

Hacktivism: Goals and Behaviors

- Hacktivism = Hacking + Activism. Hacktivism is the use of computers and computer networks as a means of protest to promote political ends.

Anonymous

- Goals of hacktivism include some not yet identified in the literature—focus has been on the method for putting out the message:
  - Technology as an organizing tool, e.g., “flash mobs”
  - Exploitation of non-attribution to protect dissidents
  - Use of technology to inform media and distribute message globally
  - “Doxing”—digging up personal information to harass specific individuals.

OCCUPY

- Examples of disobedient hacktivist behaviors include:
  - Web site defacement
  - Distributed denial of service (DDOS)
  - Data manipulation
  - Disruption of infrastructure
  - Denial of service
  - Distribution of extruded data
  - Extortion and blackmail
  - Data extrusion—theft
  - Malware

Agenda

- Classic Framework for Understanding Civil Disobedience
  - Historic perspectives of a controversial social strategy
- Cyber Civil Disobedience
  - Exploring a vague new concept
- Mapping Civil Disobedience to the Digital World
  - Looking for analogies and gaps between the classic framework and the cyber context
- Liberty vs. Security: A Tipping Point
  - Risk and consequence: balancing ethics and enforcement
- Finding the Answers
  - Future research to inform protestors and enforcers

Mapping Civil Disobedience to the Cyber World

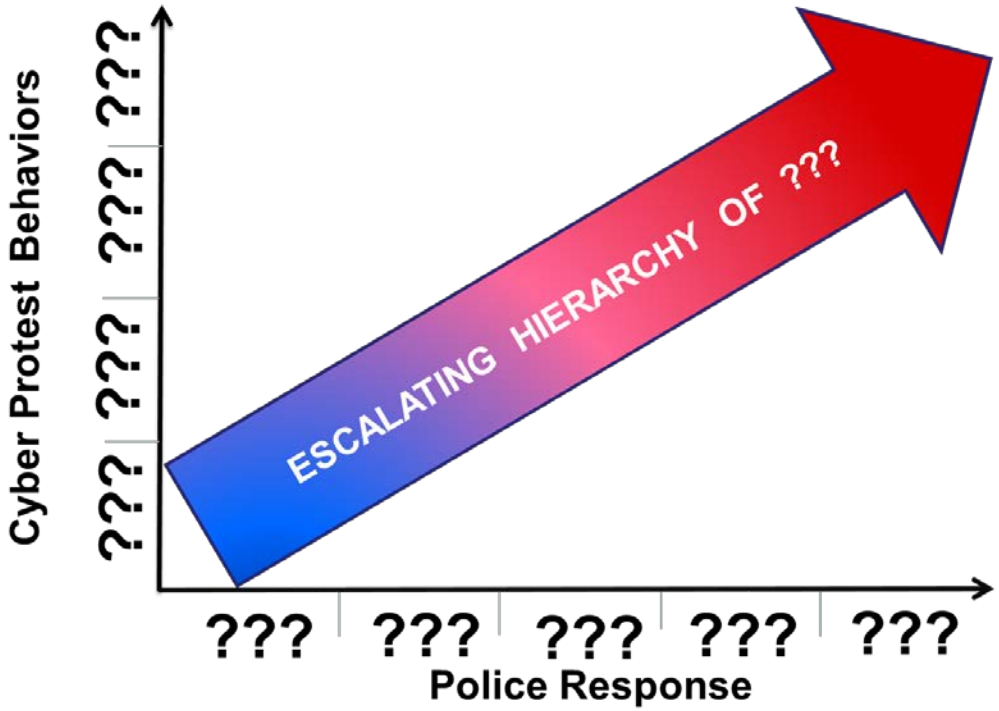
- Can classical civil disobedience case studies offer lessons about cyber disobedience?
- Has new technology provided new ways to perform old actions?

- Is the influence of technology more nuanced (faster and more effective communications)?
- Can the technology protect individuals from reprisal?

- Are there varying degrees of cyber civil disobedience?

A Digital Analogy?

- How do cyber protest behaviors relate to those in the physical world?
- Can we map the behavior vs. response continuum to the cyber world?
- Are physical and cyber civil disobedience analogous?



Cyber Framework: An Uncharted Concept

Framework Component	Classic Framework Characteristic	Cyber Framework Characteristic
Definition of “Civil Disobedience”	An act of civil disobedience is an illegal public protest, non-violent in character	???
Requirements	Must break the law	???
	Must be public	???
	An act of protest	???
	Non-violence is a factor	???
Caveats	No absolute precision in definition or categories	???
	No absolute generalizations	???

Agenda

- Classic Framework for Understanding Civil Disobedience
  - Historic perspectives of a controversial social strategy
- Cyber Civil Disobedience
  - Exploring a vague new concept
- Mapping Civil Disobedience to the Digital World
  - Looking for analogies and gaps between the classic framework and the cyber context
- Liberty vs. Security: A Tipping Point
  - Risk and consequence: balancing ethics and enforcement
- Finding the Answers
  - Future research to inform protestors and enforcers?

Liberty vs. Security: A Tipping Point?

- **U.S. Institute of Peace funded conference at Stanford University: Social Media and the Struggle for Political Change**

From Wikileaks revelations to claims of "Twitter revolutions," the role of new media in shaping global political action is one of the most discussed but least understood phenomena confronting scholars, policymakers, advocates, and the private sector. Secretary of State Hillary Clinton has made "digital democracy" a cornerstone of U.S. diplomacy; grassroots organizations like Ushahidi are crowdsourcing everything from protest to disaster relief; and corporations like Cisco and Google are increasingly making news for their role in international development and commerce. Everyone seems to agree new and social media matter. Less clear is how, when, and why. (February 2011)

At what point does cyber civil disobedience threaten national security?

At what point does enforcement threaten first amendment rights to free speech?

Agenda

- Classic Framework for Understanding Civil Disobedience
  - Historic perspectives of a controversial social strategy
- Cyber Civil Disobedience
  - Exploring a vague new concept
- Mapping Civil Disobedience to the Digital World
  - Looking for analogies and gaps between the classic framework and the cyber context
- Liberty vs. Security: A Tipping Point
  - Risk and consequence: balancing ethics and enforcement
- Finding the Answers
  - Future research to inform protestors and enforcers

The Hard Questions…

- Legal issues
  - Legality of cyber protest vs. legality of enforcement
  - Protest/Response continuum for the digital world?
- Technical Issues
  - The attribution problem: chasing the bit stream
  - Reduced accountability
- Risk and Consequence
  - The cost of inaction
  - “On the fly” policy decisions - decisions made without evidence
  - Widespread implications: national and international

Finding the Answers: Audience Discussion

- What are the gaps between the physical framework and the cyber framework?
- What are some other legal, technical, or risk issues?
- Comments and discussion?

Thank You!

Doug Himberger, Ph.D.

himberger-douglas@norc.org

Don Goff, Ph.D.

dgoff@cstarsystems.com

John Lickfett

Lickfett-john@norc.org