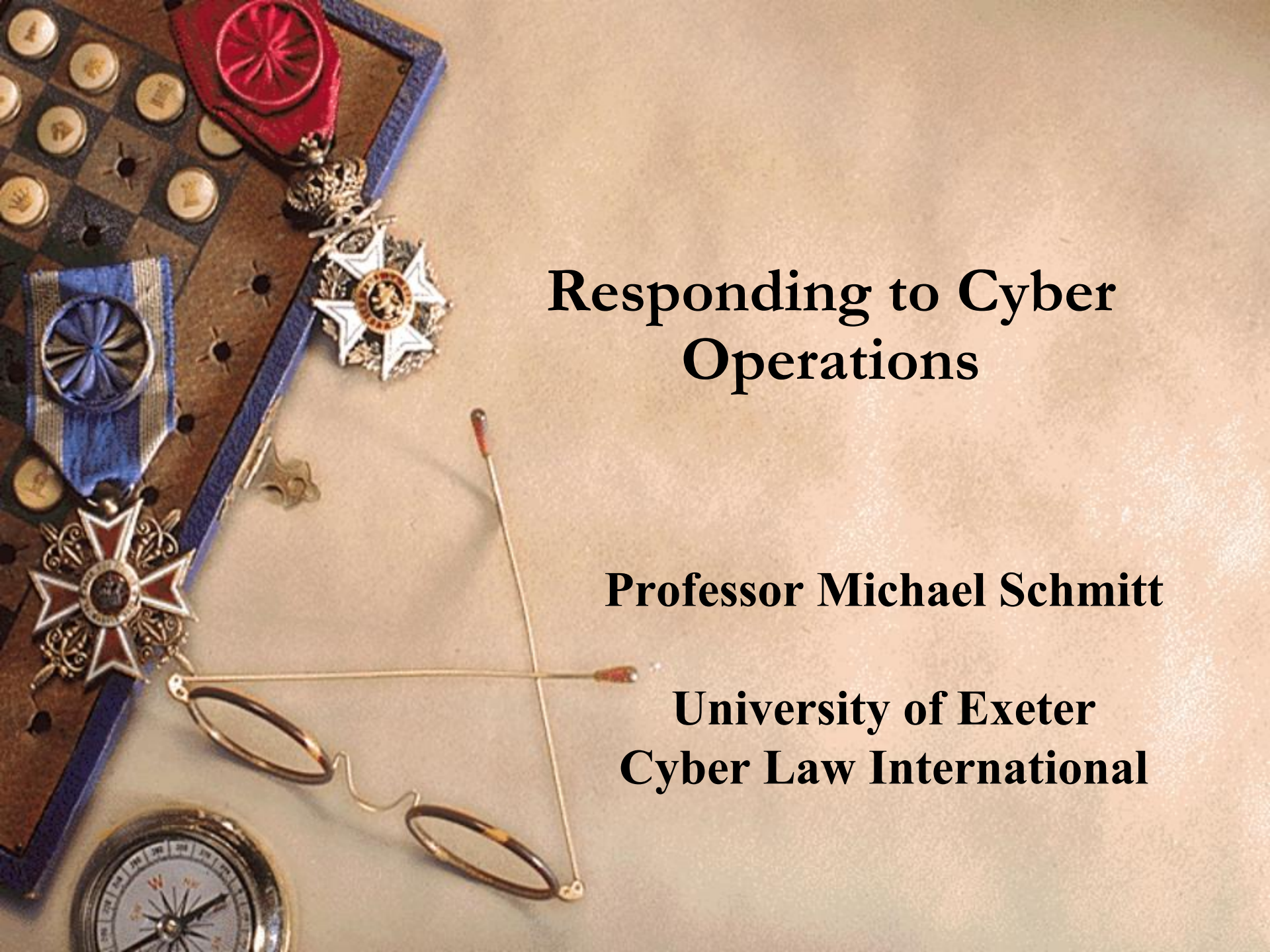

Responding to Cyber Operations

Professor Michael Schmitt

University of Exeter
Cyber Law International

Response Options

1. Traditional Lawful Responses
2. Countermeasures
3. Plea of Necessity
4. Self-defense

1. Traditional Lawful Responses

- Criminal law enforcement
- Civil remedies
- Resort to international tribunals, arbitration or mediation
- Negotiation & diplomacy
- Retorsion (unfriendly, but lawful responses)
  - E.g., shutting off access to cyber infrastructure, expulsion of diplomatic personnel, economic sanctions

2. Countermeasures

- "Internationally wrongful acts"
  - E.g., violation of sovereignty by destructive targeting of private cyber infrastructure
- Opens door to countermeasures
  - Response to cyber operation that would *otherwise be unlawful*
  - E.g., non-destructive "hack-back"

Limits

- Only in response to State cyber ops or non-State actor ops legally attributable to States
  - Attribution of private entities: "Instructions, direction or control"
- Designed only to get other side to stop
- No "in-kind" requirement OR requirement to strike only attacker
- Must be proportionate

Who May Conduct?

- No collective countermeasures
  - E.g., NATO/individual States cannot engage in countermeasures on behalf of State w/o capability
  - But … may assist if does not breach legal obligations towards the target of the countermeasures?

- Private entities not authorized to respond
  - Not vio. int'l law, but may violate domestic law
  - May implicate State's due diligence obligation
  - But State may turn to private industry
  - Actions legally attributable to State

Examples

- State A violates State B's sovereignty with cyber op damaging private cyber infrastructure
  - State B responds with cyber ops v. A's government or private sites
- Group under A's control does same
  - B responds with cyber ops v. group, A's government or private industry
- Group in A not under A's control does same
  - Is State A in violation of due diligence obligations?
  - If so, strike back at group or cyber infrastructure in A in response to breach of DD obligation

Caution: 2016 UN GGE

- June 2017: Rejected reference to right to respond to internationally wrongful acts
  - Veiled reference to countermeasures

3. Plea of Necessity

- Allows otherwise unlawful cyber or non-cyber response
- Includes response to non-State actor cyber ops OR technical attribution unreliable
- Only exceptional cases
  - Protection of essential interests of a State against grave & imminent peril
  - Shall not seriously impair essential interests of affected States
- Opens door to hack-back

4. Self-defense

Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs …"

UN Charter, art. 51

- ✓ Shoot back kinetically OR with cyber
- ✓ Unclear whether applies to non-State actors

UN GGE

- 2013: "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."
- 2015: Noted inherent right to "take measures consistent with int'l law and as recognized in the Charter"
- June 2017: Lack of consensus on using term "self-defence" in report

Application to Cyber?

- Is cyber op an "armed attack"?
  - Tallinn Manual 2.0: At least cyber op intended to directly cause significant physical damage to tangible objects or injury to humans
  - Severe, non-destructive consequences?
- Not available to non-State actors unless authorized by State
- In response to non-State actor cyber attacks?