CYBER-DETERRENCE

Boston Global Forum
December 12, 2016

Kim Taipale
Stilwell Center

Overview

Deterrence seeks to prevent someone from doing something by shaping their perception of costs and benefits to influence their decision-making

Deterrence strategies

- Deterrence by denial
  - Defense (goal denial) – success uncertain
  - Resilience (benefit denial) – success futile
- Deterrence by imposing costs
  - Penalty/Consequences/Punishment – success costly
  - Dependency/entanglement - success counter-productive

Deterrence strategies

- General deterrence
  - Dissuade any potential attacker
  - Obama – Dec 2015
- Specific deterrence
  - Keep a specific adversary from acting
  - Biden Aug 2016
- Tailored deterrence
  - Tailored to specific actors, situations, capabilities, and communications
  - Obama – Nov 2016

Targets of deterrence

- Potentially subject to direct deterrence – first party
  - Nation states (peers, near-peers, lesser states)
  - Legitimate/identifiable organizations/group
- Potentially subject to indirect deterrence – second party
  - Proxies/hybrids/sponsors, terrorists/funders, criminals/home jurisdiction, individuals/ISPs,
- Not easily subject to deterrence
  - untraceable/ephemeral
  - "useful idiots"

Actions

- Cyber Attacks (syntactic)
  - Break systems or networks
  - Availability of Critical Infrastructure
- Malicious Cyber Actions
  - Unauthorized access (espionage)
  - Confidentiality of information
- Semantic/outcome (cf. information war)
  - "Weaponized information"
  - Integrity of systems for decision making

US policy is "effects" based

- CA/MCA intended to cause casualties
- CA/MCA "intended to cause significant disruption to the normal functioning of US society or government, including attacks against CI … used to provide key services"
- CA/MCA threatens military C&C, other assets
- MCA that undermines economic security, economic espionage or sabotage

Deterrence by imposing cost

- Requires:
  - Consequential threat
  - Adequately signaled
  - That is credible
  - And relatively incontestable
- Impacts:
  - Discloses victim (disincentive)
  - Punishes attacker (second party)
  - Warns others (third parties)

Consequential threat

- All instrument of national power DIME-LE
  - Whole Government/Whole Nation
- Cross-domain
- Escalation (proportionality)
  - Name and shame (Russia)
  - Law enforcement (China, Iran)
  - Diplomatic/economic sanctions (North Korea)
  - Cyber-attacks (disclosure problem)
  - Kinetic attacks (declared policy but …)

Clear statement

- "Whole point of a doomsday device is lost if you keep it a secret!" Dr. Strangelove 1964
- Signaling dilemma
  - Too precise trigger/red line becomes safe-harbor
  - Elicits precisely calibrated challenges
  - Obliged to respond
  - So, maintain strategic ambiguity for flexibility
  - Cf, US policy (too vague for declaration? CYA?)

Credibility

- Consequences likely to be imposed
  - Known/proven capability
  - Demonstrated intention or will
  - Political environment (bayonet)
- Credible on its face
  - "Kill people who kill bits?"

Contestability

- Effectiveness of deterrence based on its Certainty, Celerity and Severity
  - Probability of being held accountable
  - Swiftness of the punishment
  - Magnitude of the cost
  - ~what are chances of being quickly identified and punished?
- Contestability
  - Challenge (political, legal, normative) (JP Morgan hack)
  - Resistance (counter-force) (Russian banks)

Cyber-domain issues

- Scalability –
  - non-linear/can't calibrate blast radius
- Temporality –
  - instantaneous, no time for early warning or ladders of escalation
- Attribution –
  - ambiguous attribution and motivation (proof discloses sources & methods)
- Digital economics –
  - zero marginal cost of attack, no predictable ROI on offense or defense
- Contestability –
  - no testing, demonstration

Cyber response issues

- Can't disclose sources and methods of attribution
- Can't demonstrate capabilities
- Payloads/attacks have to be customized thus arms race (and everyone is "prepping")
- Duality – civilian/military, offense/defense, probe/attack
- Infinitely asymmetrical (zero day exploit > any defense)

Case Studies

Russia