



CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

The
Cyber Policy
Initiative

Trends in Cyberwarfare

Ariel E. Levite

Presentation at the SCOR Global P&C Annual Conference

29-30 September, 2016

Systemic patterns

- Daily friction, occasional higher intensity events
- Diverse motivations (economic, ideological, strategic, operational, personal)
- Arms race and proliferation of capabilities (and a tool market)
- Rapid growth in the number and type of significant players
- Weakening control/influence of states over other entities
- Channeling of conflicts and crime into cyberspace
- Low costs/risks to those perpetrators of cyber attacks that have limited stakes in the core of the system
- Strong incentives to pre-empt (“use it or lose it”)

Instability, volatility, uncertainty, serious risks



Technical Developments

- Rising dependence on ICT for control of the physical world
- Tighter global interdependence
- Heavier reliance on institutional connectivity (including mobile) and insiders reliability
- Growing vulnerability of new devices (IOT)
- Heavier dependence on the cloud
- Considerable progress in attribution capability (partially offset by privateering)

Grave aggregation risks (operational, geographical & technological & organizational)



Recent trends in cyber attacks

- Rapidly growing attacks on data:
 - Compromising confidentiality/secretcy (more frequent)
 - Interrupting availability (ransomware becoming a menace)
 - Undermining confidence/trust (common, disconcerting)
 - Manipulating integrity (rare but increasingly worrisome)
- The effects range from temporary to permanent or recurrent. Some are even reversible
- Impact on systems' performance (including on the assets and entities they control): disruption (common), degradation (less common), disablement (infrequent); destruction (rare)
- No massive destructive attacks (for now) on critical assets




What may be holding countries back?

- Ethical considerations and legal concerns
- Vulnerability to retaliation by cyber means
- Uncertainty about the foes' identity & who stand behind them and acting on it (attribution, understanding, making public)
- Expediency and utility considerations (undershoot, overshoot)
- Fear of blowback (tools, legitimacy, incentive, systemic effects)
- Anxiety about premature compromise of unique weapons and capabilities and loss of intelligence sources



Possible remedies

- Norms on acceptable behavior in cyberspace are weak, challenging to verify, difficult to enforce, daunting to strengthen. 



A new approach to promote restraint is essential

- Passive defense measures alone are unable to provide adequate security and stability



Adding active defense is essential

- Governments are incapable of assuming sole responsibility for protection of the private sector (and its undesirable for them to try “own this risk”)




A new risk management paradigm is necessary



Insurance providers have a unique role therein



What role for insurance in the cyber domain (1)?

- Conservative
- 
- More ambitious
- Improve the understanding of cyber risks (and a data base pertaining to them) overcoming inhibitions to disclose/share). Identify trends!
 - Employ its risk underwriting potential to establish benchmarks for good cybersecurity practices
 - Incentivize compliance with these standards
 - Underwrite cyber risk beyond physical damages and loss of business due to service disruption to cover to IP and even reputational damages;
 - Help identify aggregation risks (highlighting the possible cascading effects)



What role for insurance in the cyber domain (2)?

- Harmonize behavior across nations and corporations (which no *national* regulation or legislation can do)
- Diminish the appeal of cyberattacks and cyber crime by underwriting passive and ACD and promoting their responsible/principled employment



Avant-garde



Strategic & Political Challenges to Promoting Interstate Cyber Norms

- Broad, generic, cultural divides in attitudes toward norms
- Complexity of issues, and diversity of domestic stakeholders
- Conflicting visions over utility, indispensability, and cost/risk associated with cyber weapons and warfare
- Fundamental divergence over what constitutes cyber warfare (versus information security): linkages & priorities
- Number and diversity of pertinent players internationally
- Complexity of issues associated with handling non state actors (proxies, private sector entities, NGOs, criminals)
- Weakness of enforcement options ≤

