TENTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

THE RIPPLE EFFECT

The Cascading Impacts of Cyber Security

OCTOBER 26–28, 2020

cybersecuritysummit.org

10 YEAR ANNIVERSARY

Corporations and Governance:

Harbinger or Promise?

David Mussington PhD CISSP
School of Public Policy
University of Maryland College Park

27 October 2020

Biographical Details – David Mussington

Dr. David Mussington is Professor of the Practice and Director of the Center for Public Policy and Private Enterprise at the University of Maryland's School of Public Policy. Prior to joining UMD in 2016 he was Assistant Director of the Information Technology and Systems Division at the Institute for Defense Analyses (IDA). David is also a Senior Fellow at the Center for International Governance Innovation (CIGI).

David has extensive public and private sector experience in cybersecurity. In 2010 he was selected for the Senior Executive Service and assigned to the Office of the Secretary of Defense in the role of Senior Advisor for Cyber Policy, later joining the National Security Council Staff as Director for Surface Transportation Security Policy. Since leaving the White House David has directed cybersecurity studies for the Department of Homeland Security, the Office of the Director of National Intelligence, the Federal Communications Commission, and NATO. In 2014 Dr. Mussington led a cybersecurity risk assessment and gap analysis at the request of the Bank of Canada and partner financial services' oversight agencies in Canada. Most recently his research focus is on adversary cyber operations, military cyber doctrine, election cyber security, and countering mis- and dis-information.

Abstract

While previously corporations were commonly acknowledged to be the owner/operators of critical infrastructures, and the providers of digital services, today their contributions are both broader and deeper. No one can doubt the expertise and operational experience possessed by private corporations in capitalist economies. Less highlighted, but nonetheless as important are the important strides in risk awareness and risk management efficacy also achieved by private corporations - both domestic and global. Not only are these entities increasingly operating sensor infrastructures that deliver near - real time insights on the risk exposure of key cyber physical systems, but the risk experience of consumers are increasingly known to corporate actors before coming to the attention of governments. This superior risk - contact has potential importance for the future of governance.

(From David Mussington, “Corporations and Governance: Promise or Harbinger”. *Cyber Security Summit – Trust & Security in Cyberspace – The Changing Role of Corporations*) 27 October 2020

Overview and a Bottom Line

- Risk Assumptions
- Who is Accountable? And How might that work?
- Priorities and Decision Making: 3 Cases
- Dilemmas
- Implications

A Bottom Line

- Corporate knowledge, risk management capacity, analytic tools and and situational awareness rival those of many governments
- These advantages have fostered global growth and supply chains, linking economies together – creating interdependence and shared interests. However, common interests and infrastructures also propagate common vulnerabilities in critical systems and digital services.
- These infrastructures can be used by adversaries as vectors to exploit risks to key parts of the economy and to public services. Such a potential requires oversight. Yet the oversight authorities may lack the knowledge and risk information to conduct effective policy interventions, should the need arise.
- The Challenge: How can effective oversight be designed – achieving effective risk mitigation -- without diminishing technological and economic innovation?
    - And what redress opportunities will civil society have for influencing the distribution of harms that may result whichever decisions are taken?

Risk Assumptions

- Partnerships involving the public and private sector in cybersecurity assume complementarity of factual awareness, insight, and risk
- Despite differences of domain expertise, access to facts, risk information – and to analytic methodologies – risk mitigation efforts are considered to be mutually reinforcing;
- What if these assumptions are mistaken? What if important information asymmetries exist, and analytical capabilities are unequal? And what if differences in knowledge reinforce self-interested rather than strategic behavior? What is the impact on risk management practices and efficacy in critical infrastructure protection and cyber defense?

Who is accountable? (and How?)

- Differences of interest are expected, but differences of capacity can skew outcomes if not properly managed;
- For governance, this can mean that risk decisions made by those in control of key systems and updated risk exposure information dominate operational judgments and longer-term investment prioritization;
- Externalities of such decisions can place at risk – or shift risk – to stakeholders more *distant* from direct infrastructure control – customers, dependencies, and homeland security;
- …yet the choices involved in risk prioritization are commonly viewed as basic aspects of public policy.

Cyber Risks and Events of Concern

- Nation-state cyber attacks on critical infrastructures and key government systems
- Algorithmic and application-level attacks that may impair or disrupt dependent public services and cyber security in key systems
  - (e.g., financial support, service delivery, law enforcement investigations)
- Cyber attacks and cyber crime targeting critical data and applications
  - Ransomware
  - Destructive malware
  - DDOS
  - Integrity attacks on test and efficacy data (e.g., health care, pharma)
- Cyber theft of intellectual property (IP) and personal identifying information (PII)
- Disinformation and Misinformation campaigns
- Cyber attacks on military systems

Who is accountable? (Private sector risk decision making) Case #1

Decision Making Entities*

- Federal Agencies (SSAs)
- SLTT Authorities
- Infrastructure Owners
- Infrastructure Subject Matter Experts
- Stakeholders and Civil Society

Risk Incidence Choices

- National policy and risk prioritization
- Localized risk response and emergency preparedness
- Strategic Investment and infrastructure management
- Domain expertise and risk mitigation efficacy
- Externality

Time-Phase

Long Term planning
Medium term – local incidence
Long-term feature shaping
Operations and incident response
Infrastructure effects confrontation

[Decision making entities are “proxies” for governance levels ~ making consequential risk choices which shape outcomes].

Who is accountable? (public sector risk prioritization) Case #2

Decision Making Entities

- Federal Agencies (SSAs)
- SLTT Authorities
- Infrastructure Owners
- Infrastructure Subject Matter Experts
- Stakeholders and Civil Society

Risk Incidence Choices

- National policy and risk prioritization
- Localized risk response and emergency preparedness
- Strategic Investment and infrastructure management
- Domain expertise and risk mitigation efficacy
- Externality

Time-Phase

Long Term planning
Medium term – local incidence
Medium-to-term feature shaping
Operations and incident response
Infrastructure effects confrontation

Who is accountable? (civil society risk acceptance) Case #3

Decision Making Entities

- Federal Agencies (SSAs)
- SLTT Authorities
- Infrastructure Owners
- Infrastructure Subject Matter Experts
- Stakeholders and Civil Society

Risk Incidence Choices

- National policy and risk prioritization
- Localized risk response and emergency preparedness
- Strategic Investment and infrastructure management
- Domain expertise and risk mitigation efficacy
- Externality

Time-Phase

Long Term planning
Medium term – local incidence
Long-term feature shaping
Operations and incident response
Infrastructure effects confrontation

Dilemmas

- Case #1 – Long-term cyber risk environment shaping decisions by the private sector act that reflect ROI concerns, not public policy
  - Endemic due to conflicts between sovereigns (nation states)
  - Influence of sub-national governments is significant
  - Private sector can enhance autonomy through regulatory arbitrage

- Case #2 – Public Sector priorities fail to influence cyber risk incidence due to information asymmetry, expertise deficits, and uncertainties on adversary activity
  - Impaired risk awareness and lesser domain expertise create dependence
  - Economic arguments for corporate autonomy reinforced by civil society winners and losers

- Case #3 – Demand articulation by civil society lacks access to consequential cyber risk presentation choice
  - Distribution of harms from cyber risks too diffuse to engender policy action
  - Sovereigns may balkanize cyberspace in order impose “norm-based constraint”, but transactions costs imposed may make such policies difficult to sustain over time
  - Consumer and citizen interests may conflict, impeding mobilization to activate policy influence potential – either lacks access to sovereign preferences sufficient to flip competing cues.

Priorities and Decision-making – Characterizing the "Net-Net" of Control

- Governance assumptions that see government as charged with long-term risk environment shaping are contradicted by the time horizon of technical decisions and investment choices by other actors that may be determinate.
- Assumptions that government will get to influence private sector choices through policy decisions that "flow down" from legislation can be effective only if legacy impact from private sector decisions do not contradict preferred government resource, planning, and risk incidence assumptions - on effects
- Control flows from reinforced and effective shaping decisions that govern private, public, and civil society decisions – which governance level has binding impact?
- [Decision making entities are "proxies" for governance levels ~ making consequential choices that shape outcomes].

Implications

- Cases 1, 2, and 3 suggest the potential for significant dissonance between public, civil society, and private sector risk choices and preferences
- Impediments to effective strategic risk decisions by government mean that cybersecurity and national security may appear to be competing, rather than complementary risk areas
- Under any of the three case conditions: the prospects of government imposing a stable, effective and long-term risk governance regime on cyberspace appear slight;
- This situation transfers consequential risk decision making (governance) to the private sector – but does not create or catalyze effective and nuanced oversight regimes ~ to constrain private decisions that create problematic public interest externalities;
- Policy innovation should seek to devise oversight solutions that allow the public interest to be articulated in ways that intersect with, rather than displace or dominate, private sector risk decisions.

Questions?