THE REQUIREMENT FOR BETTER DATA AND ANALYTICAL FRAMEWORKS FOR CYBER OPERATIONS ASSESSMENT AND RISK MANAGEMENT

DAVID MUSSINGTON PHD CISSP

PROFESSOR OF THE PRACTICE, SCHOOL OF PUBLIC POLICY, UNIVERSITY OF MARYLAND COLLEGE PARK

CYBER POLICY LACKS A STABLE CONSENSUS EVIDENTIARY BASE

- Standards of evidence are important, as they set the backdrop for determinations of causation, risk, and accountability;
- Analysis of complex cyber behaviors by nation states and non-state actors, and the complexity of campaigns of espionage and cyber attack, requires better data and proven data handling methods;
- Better means need to be found to communicate analytical results to decision makers and the general public;
- Oversight of critical infrastructure cybersecurity and surveillance of cyber threat actors requires improvements in academic analysis of the evidence used to justify policy conclusions and recommendations.

CORE THEMES

- Evidentiary statements used to characterize cyber threats and attribution to threat actors need clearer more compelling public rationales
- Commercial threat information providers compete with each other, governments, and the news media to name, define, and characterize the importance of particular cyber events and trends
- Private cyber threat information providers collect and report data on cyber events, from data breaches to malware outbreaks, distributed denials of service (DDOS) and cyber crime. Conclusions are reported in competing data sets with different definitions of terms and identifications of threat actors
- NIST, MITRE, CIS, ISO and other organizations each produce standards, documentation and guidance on how to create and interpret data on cyber risks
- Overall assessment of threat conditions, policy outcomes, and priorities is undertaken by public and private sector entities. Academia needs to assert itself to establish its independent and unbiased voice.

USE CASES

- Cybersecurity and the 2016 Presidential Election
  - Whether IT systems and networks were illegally accessed
  - Whether targeting information was shared by unidentified third parties
  - Whether social media platforms concealed knowledge of Russian manipulation of public opinion using social media influence activities
  - Broad metrics useful for. Understanding Impact
- Social Media and Foreign Influence in the 2016 Election
  - Understanding the sequencing, authorship and impact of influence attempts on social media
  - Whether algorithms were developed by social media platforms "solely" to manipulate the perceptions of members for political purposes
  - Ensuring metrics for assessment of impact

CONCLUSIONS

- There is a potential conflict between the collection and sharing of data for public policy and the privacy and data security expectations of private companies and the public
- Non-disclosure agreements in the private and public sectors, and classification of data by governments, impede the availability of data for academic analysis
- Private and public sector entities compete to define the shape off the cyber risk landscape; common standards for reporting, analysis; space exists, however, for academics to contribute rigor and disinterested analysis – adapting big data and data science techniques to information made available under special conditions – and in response to cyber vulnerabilities and risks of concern.