GOVERNANCE OF CYBER SECURITY NORMS – THE ROLE OF INTERNATIONAL CONFERENCES AND INITIATIVES

PRESENTATION

BY LEONHARD SIMON FOR THE „MEETING ON INTERNET GOVERNANCE AND CYBERSECURITY NEXUS”

BEIRUT, DECEMBER 4-7
Table of Contents

1. Layers of Cyber Security
2. Stakeholder
3. Norms and Trust
4. Platform MSC
5. Challenges
6. Conclusion
Stakeholder

Governments

Non-State Actors

Military

Society
Governments

- Acknowledging the nature of cyber space as
  - ungoverned
  - non-national
  - “real”
  - of strategic importance

- Monopoly of power contested
Non-state actors

- Digital technologies as backbone of global order
- Primacy of private companies (access and content)
- Public-Private Partnerships needed
- Engagement in offensive cyber operations?
Military

- Understanding offensive cyber capabilities
- Development of “cyber weapons”
- Developing strategies countering threats by cooperation
Society

- Including non-profit and non-governmental efforts into the debate
- Involvement of civil rights groups and initiatives
Norms and Trust

- Military
- Non-State Actors
- Governments
- Society

Norms

Leonhard Simon // Twitter: @_LSimon
Platform MSC

- Global Commission on the Stability of Cyberspace
  - EastWest Institute
  - The Hague Institute

- Charter of Trust
  - Siemens
  - MSC
  - Other partners, mainly from private sector

- Paris Call
  - Governmental initiative
Challenges

■ Why is a political agreement difficult?
  – *Fragmentation of players*
  – *Missing common standards*
  – *Role of private companies*
  – *Lack of understanding*
  – *Unwillingness for sharing information*
Conclusion

- Stronger Public-Private cooperation
- Recommendation: Creation of Regional Cyber Security Bodies
- Greater emphasis on cyber-education on political level needed → role for cyber experts on political conferences

Leonhard Simon // Twitter: @_LSimon
Thank you very much for your attention!

Let’s stay in touch!

simon@securityconference.de

Twitter: @_Lsimon