The need for a “Digital Geneva Convention” in Times of Cyber(In)Security

EC High Level Internet Governance Meeting
Brussels, October 3, 2017

Jan Neutze
Director of Cybersecurity Policy
Europe/Middle East/Africa (EMEA)
Microsoft
[Alleged] Nation State Cyberattacks contribute to Rising Cyber Insecurity

- DDoS against Estonia
- Russo-Georgian war
- ‘Cast Lead’ and ‘Pillar of Defense’ (Israel/Palestine)
- Stuxnet
- Jasmine Revolution
- Operation Aurora
- GhostNet
- India – Pakistan cyber war
- Sony
- Saudi Aramco and RasGas
- North Korea – South Korea
- OPM
- Sony
- Heartbleed security bug
- Yahoo!
- Japan Pension Service
- North Korea
- Pyongyang
- Ukrainian power grid
- WannaCry/NotPetya
- North Korea
- South Korea
- Saudi Aramco and RasGas
- ADP
- Montenegro
- Czech MFA
- Russian banks

Timeline:
- 2007
- 2008
- 2009
- 2010
- 2011
- 2012
- 2013
- 2014
- 2015
- 2016
- 2017

Events:
- 2007: Russo-Georgian war
- 2008: DDoS against Estonia
- 2009: ‘Cast Lead’ and ‘Pillar of Defense’ (Israel/Palestine)
- 2010: Stuxnet
- 2011: Operation Aurora
- 2012: GhostNet
- 2013: India – Pakistan cyber war
- 2014: Sony
- 2015: Heartbleed security bug
- 2016: WannaCry/NotPetya
- 2017: North Korea – South Korea
Governments heavily involved in cyberspace

50+ Countries with Defensive Capabilities
30+ Countries with Offensive Capabilities
95+ Countries Developing Cyber Legislation

ESTIMATED SPENDING ON CYBER OPERATIONS

USA <$6.7bn
China ~$1.5bn
Germany ~$1.1bn
Russia <$300m

France ~$1bn
UK ~$2bn
N. Korea ~$200m
Iran ~$1bn

USER
PROTECTOR
EXPLOTIER
LEGISLATOR
International Cybersecurity Debates: Current State of Play
Existing intergovernmental discussions and fora

- UNGGE
- G7
- G20
- SCO
- EU
- OSCE
- FIRST
- NATO
- UNODC
- UNIDIR
Limited number of public-private platforms on cyber

- **Governments**
- **Private Sector**
- **Civil Society & Non-Governmental Groups**

**Global Conferences on Cyberspace**

aka **The London Process**

(GCCS)

**Internet Governance Forum**

(IGF)

**Global Forum on Cyber Expertise**

(GFCE)

**Global Commission for the Stability of Cyberspace**

(GCSC)
A “Digital Geneva Convention”

Peacetime rules & mechanisms to help protect civilians in cyberspace
Addressing a critical gap in international law

No binding international agreement to protect civilians from cyber attacks that are not constitute "armed conflict"
Three proposals

DIGITAL GENEVA CONVENTION

BINDING GOVERNMENT AGREEMENTS

TECH SECTOR ACCORDS

ATTRIBUTION ORGANIZATION
Cybersecurity Norms – Proposals for Protecting Civilians in Cyberspace

**DO NOT:**

1) Attack systems whose destruction would adversely **impact safety & security** of civilians
2) Attack systems whose destruction could **impact the global economy**
3) Insert **backdoors** into mass-market commercial technology products
4) Steal the **intellectual property** of private companies
5) Hack personal accounts or private data held by **journalists**

**ACT IN ORDER TO:**

1) Limit engagement in cyber offense
2) Exercise **restraint in developing cyber weapons**
3) Agree to **limit proliferation** of cyber weapons and sanction those who do proliferate
4) Agree to a clear policy for acquiring, securing, using and **reporting vulnerabilities** – with strong mandate for reporting to vendors
5) **Assist private sector efforts** to detect, contain, respond and recover from significant attacks
Proposals for a Global Tech Accord

1) 0% Offense – 100% Defense

2) Assist customers everywhere

3) Collaborate to bolster first-response efforts

4) Support governments response efforts

5) Coordinate vulnerability handling and reporting

6) Fight the proliferation of vulnerabilities
The importance of cyber attack attribution

**TECHNICAL ATTRIBUTION**
- Non-governmental organization missing
- Opportunity to leverage specialized knowledge existing in private sector & academia today
- Develop common methodology & confidence levels

**POLITICAL ATTRIBUTION**
- Prerogative of nation states
- Often based on all-source intelligence
- Rarely sharing technical attribution details
- Consequences not well defined
JanNeutze
Director of Cybersecurity Policy
Europe, Middle East, Africa
Microsoft