Session 2: Air Law and the aviation industry of the future

International Cyber Norms and Cybersecurity Discussions

Danielle Yeow
Deputy Director-General, International Affairs Division
Attorney-General's Chambers
Singapore

AGC SINGAPORE | ATTORNEY-GENERAL'S CHAMBERS

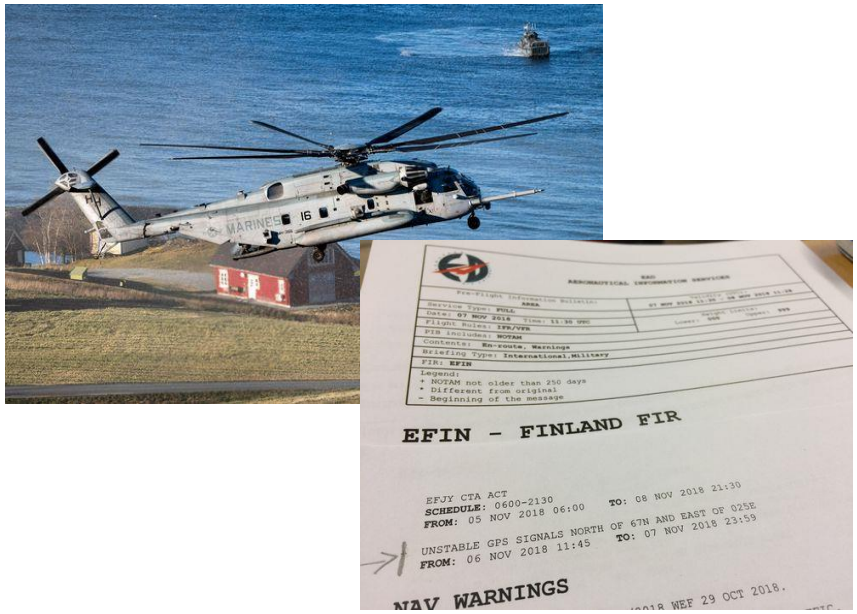
Organised by: ICAO

Supported by: CAAS Civil Aviation Authority of Singapore

International cyber norms and cybersecurity discussion

Examples of cyber attacks

- Nov 2018 Alleged Russian **disruption of GPS signals** during recent NATO exercises (affecting navigation of civilian air traffic)
- 2017 – Wannacry attack – crippled hospitals across the UK -
- 2017 NotPetya attack on critical infrastructure providers eg Ukraine (shutdown of airport), global shipping disrupted
- 2017 – BadRabbit attack – compromised systems at Odessa International Airport, causing flight delays
- 2015 Cyber attack against Ukraine's **power grid** (leaving western part of country without electricity)
- 2012 and 2016 cyber attack on Saudi Arabian aviation authority and Ministry of Transportation
- 2016 large-scale cyberattack on **ICAO**



Current discussions – UN

from Net Politics and Digital and Cyberspace Policy Program

The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased

Russia and the United States proposed two competing resolutions, possibly expecting one to prevail over the other. Instead, the General Assembly approved both.

Blog Post *by* Guest Blogger for Net Politics

November 15, 2018

A vote at the UN General Assembly Shannon Stapleton/Reuters

Current discussions – UN

- 6th UNGGE (UN Group of Government Experts on Developments in the Field of Information and Telecommunications in the context of International Security)
  - 1st UNGGE established in 2004, 6th UNGGE to meet in late 2019
  - Examine existing and potential threats in cyber sphere and possible cooperative measures to address them
  - Limited membership
  - Consensus based reports
  - Report back to GA in 2021

- OEWG (Open- Ended Working Group)
  - Open to all UN members
  - Industry consultations
  - To be convened for the 1st time in 4Q2019 and to report back to UNGA in 2020


Norms, rules and principles for the responsible behavior of States
Existing and emerging threats
Confidence-building measures
2015 GGE Repo rt
International cooperation and capacity-building
Applicability of international law
Recommendations for future work

- 11 voluntary, non-binding norms
  - limiting norms and positive good practices
  - *eg. not conduct or knowingly support ICT activity that intentionally damages critical infrastructure or otherwise impairs use and operation of critical infrastructure to provide services to the public*
  - *eg. consider how best to cooperate to exchange information, to assist each other, and to prosecute terrorist and criminal uses of ICTs and implement other cooperative measures to address such threats*
  - *eg encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT dependent infrastructure*

- Affirmed that international law applies to the use of ICTs. Non-exhaustive views :
  - *States have jurisdiction over the ICT infrastructure within their territory*
  - *In use of ICTs, States must observe State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs.*

Current discussions – UN

2016-2017 UNGGE

- No consensus report
- No consensus on how principles of international law apply
- Some progress on CBMs and capacity building

Current discussions – UN

UNGGE	OEWG
OP3 – … study … possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States..	**OP5:** …further develop the rules, norms and principles of responsible behaviour of States … and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and to … study, … existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building…

Current discussions – other platforms

ASEAN

- ASEAN Leaders Statement on Cybersecurity Cooperation (April 2018) – affirming needs for rules based international order in cyberspace
- 3rd ASEAN Ministerial Conference on Cybersecurity (Sept 2018)
- agreed to subscribe in principle to the UNGGE 11 voluntary, non-binding norms
- focus on regional capacity building in implementing these norms

OSCE

- 16 voluntary cyber/ICT security CBMs (3 clusters)
  - Posturing
  - Communication
  - Preparedness

Current discussions – other platforms

EU

- EU Cyber Diplomacy Toolbox
- To develop Framework for Joint EU Diplomatic response to malicious cyber activities

G7

- Declaration on Responsible Behaviour in Cyberspace 2017

Shanghai Cooperation Forum

- Meeting of SCO National Security Council Secretaries (2018)

African Union

- Convention on Cyber Security and Personal Data Protection (2014)

Current discussions – other platforms

Financial Sector

- CPMI-IOSCO Principles for Financial Market Infrastructure
- G7 Fundamental Elements of Cybersecurity for the Financial Sector
- G20 Finance Ministers and Central Bank Governors meeting, March 2017 Communique

Multistakeholder

- Global Commission on Stability in Cyberspace
- Paris Call for Trust and Security in Cyberspace (Nov 2018) –

Current discussions – other platforms

IMO

- ISM Code incorporated maritime cyber risk management (June 2017)
- require shipowners and managers to incorporate cyber risk management into ship safety

Bilateral MOUs

Private Sector initiatives

- Cybersecurity Tech Accord (April 2018)
- Microsoft proposals

Observations – international aviation

Observations – international aviation

- rules based multilateral international order in cyberspace grounded on UNGGE norms
- inclusive discussions – ensure coherence, avoid fragmentation and divisiveness
- intersect between norms, technology and policy
- pragmatic approach – non-binding norms, recommendations, guidelines, best practices
- robust CMBs - confidence and trust building
- capacity building
- multi-stakeholder approach - private sector, academia and NGOs engagement

Observations - international aviation

- highly connected and mutually reliant industry
- convergence of IT and operational technology
- formerly closed operational technology environment subject to digital transformation (IoT landscape)
- tension between robust multi-layered security and open platforms for collaboration and seamlessness
- different stakeholders – different proprietary systems, separate global connectivity, interdependence

Observations – international aviation

Preventive aspects

- need to protect critical infrastructure (including airports)
- complexity: transboundary nature of cyber activities
  - e.g. regulation of overseas service providers
    - obligation to regulate service-providers based in their jurisdiction?
    - setting global standards applicable for all operators?
    - Harmonised, inter-operable technical standards to be adopted by service providers?
    - Extraterritorial reach of legislation aimed at cyber security?
    - Technology neutral approach in interpretation and implementation international conventions eg definition of hijacking?
  - Need for multi-stakeholder approach

Observations – international aviation

Preventive aspects

- sharing of cyber threat indicators, identification and information
- sharing of mitigation strategies
- Sharing of best practices

Observations – international aviation

Post-incident aspects

- Cyber attack detection and incident response

- Coherence, non-duplication of discussions at UN forum

- Issues
  - Assessment / categorisation of the “cyber attack” (Art 2 UN Charter)
  - Principle of non-intervention
  - Attribution (State Responsibility)
  - Self Defence (Art 51 UN Charter)

Q & A

danielle_yeow@agc.gov.sg