ISS European Union Institute for Security Studies

CYBER NORMS BUILDING

Nathalie Van Raemdonck
Associate Analyst
EUISS

“Cyberattacks are here to stay. They are Effective, Affordable, and Deniable ”

- Mikko Hypponen

THREAT ACTORS: NATION STATES

- 2007 Estonian attack (DDoS)
- 2008 Natanz nuclear facility (Stuxnet)
- 2012 Saudi Aramco (Shamoon)
- 2015 Sony Hack (Guardians of Peace)
- 2015 Ukrainian power plant (Darkenergy)
- 2016 Bangladesh Bank Heist (Lazarus Group)
- 2016 DNC hack (Fancy Bear/ Cosy Bear)
- 2017 Vault 7 (Shadowbrokers)
- 2017 Wannacry (Eternalblue Lazarus)
- 2017 NotPetya (Fancy Bear/ Cosy Bear)
- 2018 OPCW hack (GRU)

INTERNATIONAL LAW & NORMS

UN Group of Governmental Experts Developments in the field of information and telecommunications in the context of international security (UNGGE):

- UNGGE 2015 : **International Law is Applicable in Cyberspace**. Suggests norms & CBM’s, recommends that states ‘cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security’

INTERNATIONAL LAW

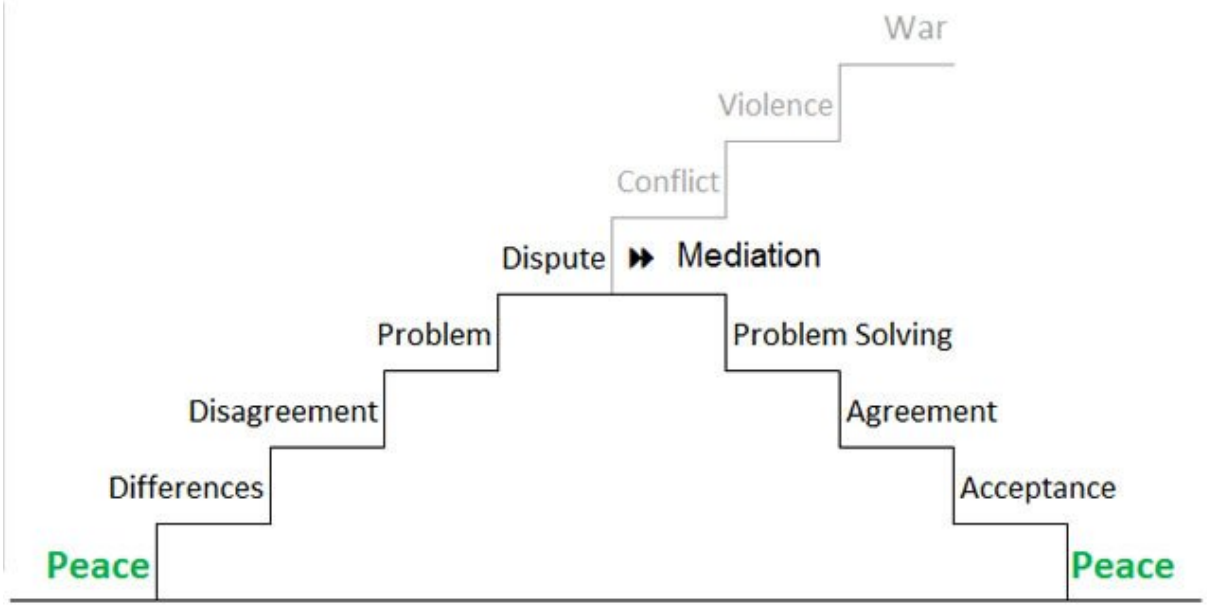
Article 2(4): all states shall **refrain** in their international relations from the **threat or use of force** against the territorial integrity or political independence of any state.

Possible response: diplomatic condemnation, sanctions, criminal prosecution, countermeasures, military response (Article 51)

”Almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time.”

- Louis Henkin

NORMS



a norm exist if its violation is denied, hidden or minimised

2015 UNGGE NORMS

States should cooperate in developing and applying measures to **increase stability and security in the use of ICTs** and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

In case of ICT incidents, States should **consider** all relevant information, including the larger context of the event, the **challenges of attribution** in the ICT environment and the nature and extent of the consequences;

States should not knowingly allow their **territory to be used** for internationally wrongful acts using ICTs (due dilligence)

States should consider how best to **cooperate** to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats.

States, in ensuring the secure use of ICTs, should **respect Human Rights** Council resolutions on the promotion, protection and enjoyment of human rights on the Internet, and the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression

2015 UNGGE NORMS (II)

A State should not conduct or knowingly support ICT activity that intentionally damages **critical infrastructure** or otherwise impairs the use and operation of critical infrastructure to provide services to the public

States should take appropriate measures to **protect their critical infrastructure** from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global **culture of cybersecurity** and the protection of critical information infrastructures, and other relevant resolutions;

States should respond to appropriate **requests for assistance** by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State **emanating from their territory**, taking into account due regard for sovereignty;

States should take reasonable steps to ensure the **integrity of the supply chain** so that end users can have confidence in the security of ICT products. States should seek to prevent the **proliferation of malicious ICT tools** and techniques and the use of harmful hidden functions;

2015 UNGGE NORMS (III)

States should 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

States should not conduct or knowingly support activity to harm the information systems of the authorized **emergency response teams** (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

INTERNATIONAL LAW & NORMS

Failure UNGGE 2017:

- No agreement on application of **International Humanitarian Law**
- Differing interpretations on **Self-defense threshold**
- **SCO Code of Conduct**
  - an emphasis on sovereignty
  - **rights of an individual** in the offline environment must also be protected in the **online environment**, but these rights are subject to **certain restrictions**, which will be provided by law and necessary for **respect of the rights or reputations of others and for the protection of national security or of public order**, or of public health or morals.

INTERNATIONAL LAW & NORMS

2018 UN resolutions:

(OEWG) Developments in the field of information and telecommunications in the context of international security (UN document A/C.1/73/L.27.Rev.1)
proposed by 31 States, including China and Russia
approved by a vote of 109 in favour to 45 against, with 16 abstentions

(**UNGGE**) **Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN document A/C.1/73/L.37)**
proposed by 36 States, including the United States and European States
approved by a vote of 139 in favour to 11 against, with 18 abstentions

INTERNATIONAL LAW & NORMS

New norms by Global commission on the stability of cyberspace (GCSC)

- protecting the public core of the internet
- protecting electoral infrastructure
- norm against commandeering of ICT devices into Botnet
- vulnerability equities processes (prevent stockpiling vulnerabilities)

INTERNATIONAL LAW & NORMS

Do we need a treaty?

INCIDENT RESPONDER PARTICIPATION

Participation:
OEWG intersessional multistakeholder meeting
Internet Governance Forum Best Practice Forum on cybersecurity (IGF BPF)
Global Forum of Cyber Expertise (GFCE)

norms:
mutually agreed norms for routing security (MANRS)
FIRST code of ethics