

Global cybersecurity governance

Young Women in Non-Proliferation and Disarmament (YWNPD) Mentorship Programme

Vienna Center for Disarmament and Non-Proliferation (VCDNP)
International Affairs Institute (IAI)

Stella Blumfelde

PhD Security, Risk, and Vulnerability

Security and Strategic Studies

Contact: stella.blumfelde@edu.unige.it

2022, April 29

01 Cyber disarmament

02 Project 1: *IOs and cybersecurity governance*

03 Project 2: *AI and Digital sovereignty*
























04 Questions to the audience

Disarmament for cyber?

- Cyber-attack effects
- Limited possibility of arms control
- Issue of attribution
- WHO is the responsible?
- Definitions?

UN Secretary-General's *Agenda for Disarmament* (2018)

DISARMAMENT FOR FUTURE GENERATIONS

Action 24	Raise awareness on new weapon technologies		
Action 25	Facilitate information exchanges on new weapon reviews		
Action 26	Produce studies of new weapon technologies		
Action 27	Convene dialogue on emerging technologies	 	
Action 28	Encourage responsible innovation of science and technology		
Action 29	Keep humans in control at all times over the use of force	 	
Action 30	Prevention and peaceful settlement of malicious activity in cyberspace	 	
Action 31	Foster accountability and adherence to emerging norms in cyberspace	     	



Regional cybersecurity governance: AU, OAS, ASEAN, SCO, EU

Stella Blumfelde

University of Genova

Regional cybersecurity governance

“...a partnership between the United Nations and regional and other intergovernmental organizations should be developed if peace and security are to be maintained” (UNSC Secretary-General, 2006)

Greater role in security governance provision; expansion of mandates (Kirchner and Dominguez, 2011)

Increased variance between regions in defining and addressing security (Fawcett, 2013)

How do OAS, AU, EU, SCO, and ASEAN provide regional cybersecurity?

WHAT?

Regional IGOs

Official policy and strategic documents

HOW?

Cybersecurity governance literature

Security governance theory and regionalism

Qualitative thematic analysis

Quantitative analysis with *Wordfish*

Preliminary conclusions and further development

IOs provide security through the collective use of force or the non-use of force. Do other means exist?

Possibly. Resilience as a concept of security -> capacity building.

Differences between countries and regions in:

- a) technological advancements,*
- b) cybersecurity capacities,*
- c) knowledge and awareness of cyber risks.*



Artificial Intelligence and EU Digital Sovereignty

The EU pathway to Digital Autonomy

Strategic Autonomy

(Conclusions of the European Council of 19/20 December 2013, European External Action Services 2016, , European External Action Services 2021)

European Sovereignty (Juncker 2018)

Digital Sovereignty

1. Dependency from non-EU digital intermediaries
2. A strategy to reduce dependency on foreign technology (European Parliament 2019)
3. Three pillars of Digital Sovereignty: computing power, control over data, secure connectivity (Breton 2020)
4. Becoming Global Leader in Artificial Intelligence (European Commission 2021)

The EU as a global AI regulatory actor

- Treaty of Lisbon 2007: EU principles and values
- 2017, UN debate on Lethal Autonomous Weapon Systems
- Ethical application of dual-use technologies

(European Parliament 2015, Committee on International Trade 2017)

- European Defence Fund ⁽²⁰¹⁹⁾: “no funds can be allocated on R&D on LAWS ”
- European Parliament ⁽²⁰²¹⁾ guidelines for military and non military use of AI

Questions for the audience

- 1) Can other international treaties serve as examples in the creation of an international organization for cyber issues?
- 2) How can an international cyber treaty deal with the more challenging cyber weapons features, such as unpredictability, accountability and attribution?



www.stellablumfelde.com



[@SBlumfelde](https://twitter.com/SBlumfelde)