Digital Diplomacy, ICTs and Cyber-Security in the United Nations

This document reproduces the abstract of the following article, published with Emerald:

Pauletto, Christian (2020), "Information and telecommunications diplomacy in the context of international security at the United Nations", *Transforming Governments: People Practice and Policies* (Emerald), 14(3):351–380. <https://www.emerald.com/insight/content/doi/10.1108/TG-01-2020-0007/full/html, for subscribers>.

This article was published in 2020 and explores the functioning, work and challenges of the United Nations "Group of Governmental Experts (GGE) on developments in the field of information and telecommunications in the context of international security", and also proposes some directions for future work. The UN General Assembly first addressed the issue of ICTs and international security in 1981 and, starting in 2004, it established six Groups of Governmental Experts (GGEs) and two Open-Ended Working Groups (OEWGs) to debate on this issue. The last OEWG – the "open-ended working group on security of and in the use of information and communications technologies 2021–2025" – was established pursuant to UNGA resolution 75/240 (https://docs.un.org/en/A/RES/75/240), with a mandate extending from 2021 to 2025 (OEWG 2021–2025), and successfully concluded its work in 2025. The "Final report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025" has been published in document A/80/257 of 24 July 2025 under the agenda item "Developments in the field of information and telecommunications in the context of international security" of the UNGA (https://digitallibrary.un.org/record/4087789?v=pdf). Through resolution A/RES/80/16 (https://docs.un.org/en/A/RES/80/16), the UNGA adopted the report of the OEWG and decided to establish a "Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour in the Use of ICTs". Since then, work proceeds under the auspices of the Global Mechanism.

The abstract reproduced below may be found also on the publisher's web site (as indicated above) and in the article itself.

Abstract

Purpose

The development of technologies for the conduct of cyber operations represents an opportunity for states to defend their interests in international relations but also bears risks and challenges. Since the early 2000s, the United Nations "group of governmental experts (GGE) on developments in the field of information and telecommunications in the context of international security" debates on this issue. This paper aims to investigate how states are challenged in the development of international cyber norms and where capacity to act is idle, i.e. to assess how much has been reached in the international community's debate on cyber threats and malicious behaviors in the international security context and to identify directions to move GGE work further.

Design/methodology/approach

The methodology uses an extensive text-based desk research and relies on a thorough collection, analysis and interpretation of the United Nations (UNs) documents. When specific substantial topics are addressed in the GGE, the content of the debate was confronted with issue-specific academic literature on those matters.

Findings

The results highlight that the GGE managed to gather consensus on a number of cooperation and normative measures in this politically highly sensitive topic and more deliverables are expected during this and next year. The paper identifies a weakness in terms of operational implementation though. The paper proposes a few examples of concrete headways that could complement existing consensus, especially on the implementation side.

Originality/value

Because of its political sensitivity, the GGE has worked with discretion and has attracted little academic attention. This paper is an original and timely attempt to assess the achievements and possible outlook of this endeavor of the international community, including the incipient work of a recently established open-ended working group. It also attempts to connect the subject matter discussed in the UN with related academic literature, including in respect of definitional and conceptual issues.

Keywords:

United Nations; Information security; Cyber diplomacy; Digital diplomacy; International security; Cyber law; Cyber-security; Information and communication technology (ICT)

Acknowledgements

The author expresses his grateful thanks to Jon A. Fanzun, Special Envoy of the Swiss Federal Council to Cyber, Foreign and Security Policy, to Daniel Stauffacher, former Ambassador of Switzerland for the World Summit on the Information Society (WSIS) and founder of ICT4Peace, and to the anonymous peer-reviewers, for their highly valued comments. All remaining errors are the author's own.