German Review on the United Nations | Abstracts

Volume 64 | 2016 | No. 2

United Nations in Cyberspace

Tim Maurer pp. 51–55

Cybersecurity in a Complex Environment

Transatlantic Divergences and Diplomatic Achievements

In December 2015, a cyber-attack caused a blackout in Western Ukraine. It was the first known blackout during a conflict to have been caused by malware. However, this is only the latest in a series of high-profile incidents in recent years that illustrate the deteriorating cybersecurity environment. The international community has become increasingly alarmed by these developments and has ramped up diplomatic efforts to address the problem. One of the key forums for these discussions is the United Nations. Dating back to a first draft resolution introduced in 1998, the First Committee has been discussing this issue for the past eight years, reaching several important diplomatic agreements along the way. This article outlines the history of this discussion by breaking it up into four different phases. As the Obama administration is nearing its end, it also examines which direction this agenda will take in the future.

Tatiana Tropina · Nicolas von zur Mühlen pp. 56–60

Crimes in the Digital Sphere

The United Nations' Fight against Cybercrime

Effective prevention, disruption and investigation of cybercrime require a wide variety of technical, organizational and legal measures. Due to the transnational nature of information and communications networks, the harmonization of legislation and procedural frameworks is necessary to avoid safe havens for cybercriminals, carry out cross-border investigations and collect electronic evidence. Therefore, international standard-setting and efforts to facilitate international cooperation in criminal investigations have become some of the central issues on the agenda of many international organizations. This article aims to provide an analysis of the role the United Nations has played, and still does play, in the efforts to build capacity and set standards to tackle the problem of cybercrime.

Anja Mihr pp. 61–66

Threatened Human Rights in Cyberspace

The Internet is a tool for the implementation of fundamental civil and political rights as well as social and economic human rights, particularly in the context of the realization of the Sustainable Development Goals (SDGs). But the international community has thus far not been able to protect and fully promote human rights offline or online. In the light of these challenges, the UN General Assembly has passed a resolution concerning the multi-stakeholder approach as a mechanism to implement, realize and protect globally agreed human rights norms and standards in cyberspace.

Wolfgang Kleinwächter pp. 67–72

Who Governs the Internet?

Internet Governance Being Tested

Cyberspace, with its 3.2 billion Internet users, has become a main subject of political controversy in recent years. On the one hand, a number of governments want to regulate all Internet-related issues through a multilateral, legally-binding instrument. On the other hand, the concept of 'multistakeholderism' gains more and more support. In the 'Internet Governance Ecosystem', numerous governmental and non-governmental players coexist and work hand in hand to manage various technical and non-technical issues. The UN-based Internet Governance Forum (IGF), established in 2005, is the main platform for discussion of those issues. In December 2015, the 70th UN General Assembly renewed its mandate until 2025.

Markus Wagner pp. 73–78

The Future of Warfare?

Autonomous Weapon Systems as a Challenge for International Law

The question of how to deal with autonomous weapon systems (AWS) is no longer academic. Indeed, there are contemporary challenges with respect to their compliance with international law. The article outlines the applicable international humanitarian law framework concerning AWS, specifically the principle of distinction and the principle of proportionality. It concludes that at this point, and despite impressive technological advances in autonomous technology, the deployment of autonomous weapon systems would be impermissible only for circumstances in which they are not needed. The article embeds the legal debate in the larger policy debate concerning AWS. Finally, it describes the current regulatory approaches under discussion and assesses their viability.