

Introduction

Oversight in the era of ‘Snowden’ and big data: challenges and opportunities

Michael Kowalski^{1*}

Guest Editor

Chairman Netherlands Intelligence Studies Association (NISA)

Guest Researcher, Centre for Terrorism and Counterterrorism, Leiden University

m.kowalski@cdh.leidenuniv.nl

DOI: [10.1163/18750230-02404014](https://doi.org/10.1163/18750230-02404014)

1 * The views expressed in the special do not represent the position of the NISA.


Global security has been at the top of the international agenda during the last decade and is very likely to remain high-ranking in the years to come. Especially in the light of the international threat of terrorism, an additional budget and powers have been put at the disposal of nation states across the globe to counter threats and to maximize global and national security. Only recently broader attention has been generated to look into the unintended side-effects of the efforts of all those states. Especially the revelations by the American whistleblower Edward Snowden have raised questions about the scale of the efforts to maximize global security, for example, by the surveillance of global communications. The Norwegian Helsinki Committee recommends in this context to further clarify the judicial framework of internet and mobile phone surveillance and suggests that the OSCE should become a pioneer in setting standards for states to respect the right to privacy online.²

This special issue on the oversight of intelligence and security services intends to contribute to the broader debate on the role of states and their security and intelligence services in enhancing global security and their corresponding position within the global framework of human rights. In this special different perspectives on this issue are brought together. In the first article Hijzen explores the Dutch experiences with parliamentary oversight. It turns out that not only the architecture of oversight but also the political culture of a given period and the corresponding personal views of members of parliament during that period are crucial for the functioning of oversight. It is quite likely that the lessons of the Dutch context are relevant for other national oversight systems. In the second contribution Van Buuren places the issue of oversight in the context of globalization and the nodalisation of intelligence in post-democratic constellations. He concludes that there is a deterioration of the already existing problems of overseeing intelligence and views whistleblowers and investigative journalists as a real counter-power in the spirit of what oversight ought to be.

The third article in this special issue has been written by De Jonge and it provides an inside view from within the international oversight community. Although the level of cooperation between oversight bodies remains very limited, there are several important fields in which the oversight community may yet develop its cooperation. In the fourth article Kowalski tries to provide ten practical approaches to advance oversight. Core ideas are addressing the implications of the political supremacy of oversight, the integration of ethics into security research and the creation of space for applied ethics for intelligence practitioners. The final contribution by Bonilla focuses on the role of information managers as future intelligence workers. The tension between security and human rights in an age of 'big' data lies at the core of the tasks of those information workers. The way they learn to deal with these dilemmas can inform the broader field of intelligence and oversight.

All in all, it seems that the debate on the oversight of intelligence and security services is far from closed. First, national oversight mechanisms are still developing with no system of international oversight on the horizon. Second, future responses to unfolding or future threats to global and national security might challenge existing approaches and might result in a need for new arrangements of oversight. Third, what 'cyber', big data and global communication are doing to our societies still has to fully unfold and to be fully analysed. As, indeed, have the mechanisms of oversight and the framework of human rights.

² Norwegian Helsinki Committee, Internet and mobile phone surveillance must be in compliance with human rights provisions on privacy, Oslo, 2 October 2013.



This article was first published with Brill | Nijhoff publishers, and was featured on the Security and Human Rights Monitor (SHRM) website.

Security and Human Rights (formerly Helsinki Monitor) is a journal devoted to issues inspired by the work and principles of the Organization for Security and Cooperation in Europe (OSCE). It looks at the challenge of building security through cooperation across the northern hemisphere, from Vancouver to Vladivostok, as well as how this experience can be applied to other parts of the world. It aims to stimulate thinking on the question of protecting and promoting human rights in a world faced with serious threats to security.

Netherlands Helsinki Committee
Het Nutshuis
Riviermarkt 4
2513 AM The Hague
The Netherlands

© Netherlands Helsinki Committee. All rights reserved.

www.nhc.nl