CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Call for Papers:

The Rights to Privacy and Data Protection in Times of Armed Conflict

CONCEPT NOTE:

Personal data is being collected and stored for military purposes during peacetime, before and during an armed conflict and in the post-conflict phase. While the law of armed conflict contains very few, if any, *lex specialis* rules on the requirements and conditions of lawful data processing, other regimes such as international human rights law continue to apply during armed conflict and contain specific provisions concerning the protection of information privacy and data integrity. This edited volume sets out to offer the first holistic account of the relationship between these governing bodies as they relate to the respect and protection of digital rights in wartime.

In the light of the technological advances in the fields of electronic surveillance, social engineering, predictive algorithms, big data analytics, artificial intelligence, automated processing, biometric analysis, and targeted hacking, this study is more relevant today than ever before. In this research we seek to explore the way these technologies and others are currently being developed and employed in military operations, and the existing international law regimes that apply to their development and deployment.

The outcome of the planned research is an edited volume which will be published by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and launched during the 14th International Conference on Cyber conflict (CyCon) in May 2022. The book-length anthology will contain works from internationally renowned scholars as well as emerging voices. The project is jointly funded by NATO CCDCOE and the Indiana University Ostrom Workshop.

Submissions may address any aspect of the governance of the rights to privacy and data protection during times of armed conflict and we welcome theoretical, empirical, and doctrinal contributions. While not an exhaustive list, we would particularly appreciate contributions in the following areas:

1. Nature and Scope of Application: What role do the rights to privacy and data protection play in armed conflict? What doctrines ground their concurrent and extraterritorial application? Are digital rights the *lex generalis*? Can the legal obligations be identified within existing IHL treaty and customary law?
2. Relevant Actors: Does the application of these rights in wartime introduce legal obligations to non-state actors, and if so in what ways? Particularly, how do these rights apply in relations with military contractors, tech giants, internet service providers, cloud providers, third-party vendors and suppliers of software and hardware, armed groups (especially those that occupy territory), international fact-finding missions, courts and tribunals, journalists, and humanitarian actors.
3. Specific IHL Regimes:
    a. *Detainees, POWs, and Refugees:* Legal obligations associated with surveillance of detainees, interrogations, access to information on detainees, and the transfer of them (see e.g. principle 11 of the Copenhagen principles or special surveillance of detainees under GCIII).
    b. *The Law of Occupation:* Interpreting Article 43 of the Hague Regulations in the light of the human rights to privacy and data protection.
    c. *The Law of Peacekeeping:* Legal obligations associated with the rights to privacy and data protection as they relate to de-mobilization, election monitoring, meditation and negotiation.
    d. *The Law of Targeting:* What obligations may be derived from human rights to privacy and data protection to constrain certain types of attacks in cyberspace.

e. *Weapons Acquisition:* What role do the rights to privacy and data protection play in constraining weapons acquisition, particularly in the context of cyber weapons, and where such acquisition is done through collaborations with private commercial partners.

f. *The Law of Neutrality:* What legal obligations are imposed on third-party neutral states in connection with the protection of digital rights during the ongoing conflict. Specifically, what obligations apply to the sharing of data or the control over the tech sector's indirect involvement in the conflict.

g. *Coalition Operations:* How do the rights to privacy and data protection apply in the context of multilateral campaigns, especially in the context of regional and subregional security regimes and their specific arrangements around cyber defenses, data protection, information sharing, and intelligence collaboration.

h. *Specific Vulnerable Groups:* How should we conceive of the rights to privacy and data protection in the context of protecting the most vulnerable in war – civilian populations, journalists, humanitarian workers, UN staff, health professionals, etc.

i. *Jus Post Bellum:* As criminal investigations and other *jus post bellum* mechanisms rely heavily on data and information collection and dissemination, how should their confidential data be evaluated, processed, and stored, and how do the rights to privacy and data protection impact the end of war and the memory of war.

4. Specific military applications of emerging technologies and their interaction with the rights to privacy and data protection in war: e.g. health tracking and monitoring, facial recognition, the use of smartphones and tablets, autonomous weapon systems, cryptography, quantum computing, artificial intelligence, and the prospect of enhanced soldiers.

THE SUBMISSION PROCESS:

Both established and early-career legal scholars (including graduate students) are invited to submit proposals addressing the project's themes. Anyone wishing to offer a paper should submit a working title and an abstract of no more than 750 words, along with a CV, by email to: digitalrightsproject@ccdcoe.org by 19 April 2021.

The selection of abstracts will be communicated by 17 May 2021. Each selected contributor will be asked to prepare a 5000-7500 words first draft by 17 August 2021, in preparation for a September workshop of all papers in Berlin, Germany. Selected contributors will be eligible for some travel and accommodation support, depending on ability to conduct an in-person event and their specific needs. In addition, an honorarium will be awarded to authors on the completion of the project. Final drafts will then be due by 1 November 2021.

TENTATIVE TIMELINE:

1 March 2021:
Call for Papers is Released

19 April 2021:
Deadline to submit proposals

17 May 2021:
Paper Contributions Selected

17 August 2021:
Full First Drafts Expected

September 2021:
Workshop in Berlin (depending on the coronavirus situation and individual contributors needs, might be in-person, a hybrid event, or fully online)

1 November 2021:
Final Drafts Due.

November 2021-May 2022:
Editorial Work.

May 2022:
Book Launch during CyCon 2022.

CO-EDITORS-IN-CHIEF:

Dr. Asaf Lubin
(Associate Professor of Law, Indiana University Maurer School of Law). To contact: lubina@iu.edu.

Dr. Russell Buchan
(Senior Lecturer in International Law, University of Sheffield). To contact: R.J.Buchan@sheffield.ac.uk.