UiT The Arctic University of Norway

Workshop: AI for Justice

Using Generative Artificial Intelligence (AI)
in War Crimes Archiving

Marie Skłodowska-Curie Project
'Hybrid Cyber Warfare and Common Security in Europe'

Artem Galushko, S.J.D., LL.M.

UiT Faculty of Law

11-12 June 2025

Oslo

Interconnected and Evolving Digital Environments

Two Major Trends:

1) Cyber operations against Critical Civilian Infrastructure (power plants, hospitals, e-networks and companies).

2) Involvement of civilians in operations during armed conflicts and the use of civilian infrastructure for military purposes (ICRC papers, 2023).

Commonalities across various conflicts:

- Risk for civilians to suffer harm (ICRC statement, 2023);
- Blurred line between what is civilian and what is military in contravention of IHL (Mačák & Rodenhäuser, 2023);
- Threat of long-term destabilization (Stoddart, 2022).

United Defence against Hybrid Threats

Project Goals:

Exemplary model of effective practices and measures as a foundation for a common response to hybrid threats in Eurasia:

- Successful digital partnerships and development of joint defence capabilities;

- Best practices, challenges, gaps and needs in digital security;

- Interdisciplinary group of security experts.

Issues and Challenges:

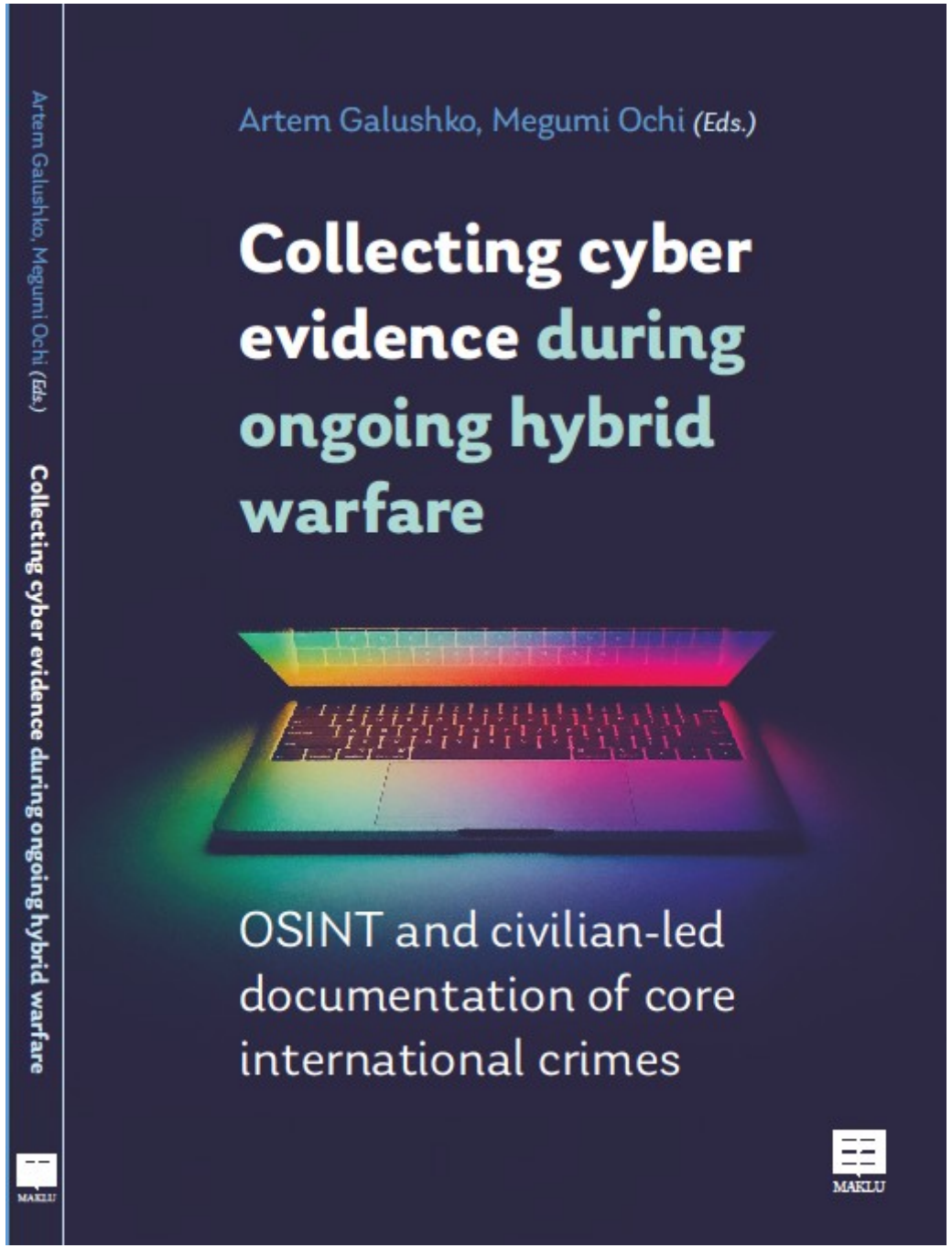
Proliferation of Armed Conflicts,

Core International Crimes and

Accumulation of Digital Materials

Importance of Archiving Data on Core International Crimes

- *2023/2024 the most violent years* since the end of Cold War (Peace Research Institute Oslo, PRIO);
- *44% increase since 2016, > 3,000 pending cases* on core crimes (Eurojust);
- International conflicts → *unprecedented amount of digital evidence*.
- Genocide, crimes against humanity, war crimes, and the crime of aggression - impact on International community.



Open-Access Book

Collecting Cyber Evidence

During Ongoing Hybrid Warfare:

OSINT and Citizen-led Documentation

of Core International Crimes

Editors: Artem Galushko and Megumi Ochi

Issues addressed:

1. Grassroots 'citizen digital initiatives'
2. Digital evidence in relation to crimes specific to ongoing hybrid warfare
3. OSINT during the Russia-Ukraine war
4. Challenges of legal compliance in data protection of digital evidence
5. Digital information and its application in court procedure in Ukraine

Why focus on Digital Evidence and Core International Crimes?

#1 – More important role internationally now

- Proposal for a *new* ***UN mechanism for evidence*** on atrocity crimes;
- ***International Digital Evidence Locker***;
- ***EU Regulation and a Directive*** on cross-border access to electronic evidence (2023);
- ***New core International Crimes Evidence Database*** by Eurojust (2023);
- ICC ***OTP Link***.

#2 – Interdisciplinary concept to facilitate international cooperation

- *Computer scientists* and *machine learning experts*;
- *Linguistics Experts*;
- *Lawyers* working on cybercrime;
- *Human rights researchers* on fact-finding missions;
- *Citizen-journalists*.

Thank you