AiS/BCGE-Training
Digital Repression Across Borders: Methods, Risks and Responses

Online training 14.-15. September 2023, 9:00-13:00

Digital technologies have given authoritarian governments new tools to control, silence and punish dissidents in other countries. These governments use surveillance, malware attacks, online harassment, and defamation campaigns to threaten political exiles and diaspora communities. International scholars can also fall into the surveillance practices of authoritarian governments even though not being explicit political exiles. Digital threats are now a key method of cross-border repression – and they are often intertwined with other, more direct tactics such as pressure on home-country families, threats from embassy staff and even physical assaults. Digital transnational repression can spread uncertainty, stress and social isolation among exiles and academics abroad, and it clearly affects their personal security and basic human rights. The two-day workshop introduces prevalent methods of digital transnational repression and highlights some of the security risks that scholars originating from repressive contexts may be exposed to while working in Germany and other countries. The workshop aims to help participants assess potential threats to their personal safety and information security, and develop strategies to mitigate those risks. Through a series of exercises and group discussions, participants will gain a better understanding of what security means to them, brainstorm potential threats to their personal safety and information security, and map out their information ecosystem to identify vulnerabilities and develop strategies to protect their data.

Workshop objectives:

- Build knowledge on digital threats, their connection to physical security and wellbeing
- Stimulate reflections on risk perception and risk mitigation in daily routines
- Find practical solutions for improving digital hygiene and information security

When? 14.-15. September 2023, from 9:00-13:00 CET.

Where? Online, via **Webex**, a link will be provided some days bevor the event.

Target group: International, displaced and at-risk scholars of the AiS-network as well as international scholars who are members of the Berlin University Alliance (FU Berlin, TU Berlin, HU Berlin, Charité) and researchers affiliated in research projects at BUA (postdoc and PhDs)

Trainers:

Marcus Michaelsen, PhD, is a researcher studying digital technologies, human rights activism and authoritarian politics. He currently works for the Citizen Lab at the University of Toronto in a project on digital transnational repression. Previously, he was a researcher in the Law, Science, Technology and Society (LSTS) research group at Vrije Universiteit Brussel as well as in the Political Science Department of the University of Amsterdam.

Damian Paderta is a digital consultant and web geographer working on the topics of Open Knowledge, Civic Technology and Smart City. As the founder of the OK.NRW Institute, he is committed to open government and works with clients in government, non-profit organizations, and the private sector to help them use technology to promote transparency, open access to information and privacy protection. He is a private lecturer at the Studieninstitut Ruhr.

Gefördert im Rahmen der Exzellenzstrategie von Bund und Ländern

How to Register
The training is organized by AiS in collaboration with BCGE. **To register**, please send to AiS your intent to join and a brief description of your interests, motivation, and institutional affiliation. Applications should be sent to ais@fu-berlin.de with the subject line: Application - Training "Digital Repression" until **18 August 2023**.

PROGRAMM

Day 1: Understanding and Identifying Digital Threats

The first day of the workshop will be dedicated to enhancing participants' understanding of the complex world of digital transnational repression.

Topics Covered

- What is Digital Transnational Repression?
  Participants will learn the key aspects of digital transnational repression and how it manifests in different scenarios.
- Cyber Threat Landscape
  In this section, we will delve into the types of digital threats commonly used by authoritarian regimes, including surveillance, malware attacks, online harassment, and defamation campaigns.
- Definitions and Meanings of Security
  The discussion will shift to the broader concept of security, covering both physical and digital domains, to foster a holistic understanding of the term.

Day 2: Assessing Risks and Developing Mitigation Strategies

The second day of the workshop will focus on equipping participants with the necessary skills and tools to identify potential threats and develop strategies for reducing risks.

Topics Covered

- Mapping Your Information Ecosystem & Risk Assessment
  Participants will be guided through the process of analyzing their digital footprint and identifying potential vulnerabilities within their information ecosystem.
  Participants will learn how to assess the risks associated with digital threats and how these could impact their personal safety and information security.
- Digital Hygiene and Information Security
  The focus will shift to practical ways of improving digital hygiene and information security. We will discuss tools, best practices, and strategies to protect data and reduce vulnerability to digital threats.
- Developing Mitigation Strategies
  The final section of the workshop will be a hands-on session where participants will work on creating personalized mitigation strategies against potential digital threats.

Benefits:
The workshop will equip participants with practical strategies to safeguard against digital threats, helping to ensure their safety and the security of their information. This knowledge and these skills will be beneficial in both their professional and personal lives, minimizing the impact of digital transnational repression.

- **Digital Transnational Repression:** Understand what digital transnational repression is, its implications, and how it is utilized by authoritarian regimes to control, silence, and punish dissidents, even those residing abroad.
- **Security Concepts:** Grasp the definitions and meanings of both digital and physical security. Develop a holistic understanding of security as it pertains to personal safety, well-being, and information protection.
- **Mapping Information Ecosystem:** Learn how to assess your digital footprint, identify vulnerabilities in your information ecosystem, and understand how these vulnerabilities could be exploited.
- **Risk Assessment:** Acquire the ability to assess and analyze digital risks to your personal safety and information security.
- **Digital Hygiene and Information Security:** Learn practical ways to improve digital hygiene and information security. Understand which tools, best practices, and strategies can be used to protect your data and minimize your digital vulnerabilities.
- **Mitigation Strategies:** Develop the skills to create personalized strategies to protect against potential digital threats. Understand how to respond effectively to threats, and ensure both your personal safety and information security.

Gefördert im Rahmen der Exzellenzstrategie von Bund und Ländern