Tales from the Security Field: Safety Online for Researchers and OSINT Practitioners

A NABS+ SEMINAR

Speakers: Professor Martin Innes and Diyana Dobreva

PRACTICAL OPSEC TIPS

- Security should be **led by your institution** and tailored to your **adversaries**
- Create **Alias Accounts**
  - Use non-attributable email, verification, and media items
  - Check your aliases are not traceable to your real identity – search with Bing, DuckDuckGo, Grok (Google search is not effective)
- Use a **VPN**
  - A VPN will mask your real IP address
  - Not all university networks are VPNs
  - A University VPN can flag your activity as legitimate research, but external trusted services are preferred for high-risk anonymity e.g., Nord, PIA, Proton
- Use a **Virtual Machine (VM)** or an isolated operating system for research
  - A VM will Isolate any malware and maintain a separate digital fingerprint
  - Imagine a secure house (personal computer) with a temporary disposable research lab in a garage (VM for research)
- Provide information to **Ethics Committees** on a **'need to know basis'**
  - Balance research transparency & accountability with researcher safety
- Seek **support** if you are subject to **interference**
  - There are resources to help manage pressures and personal toll e.g., institutional security officers, psychological first aid courses
  - Reach out to networks e.g., ESRC postgraduate or institutional networks

DEFINITION

Operational Security (OpSec) is a military term for a process that identifies critical information to determine if friendly actions can be learned or observed by enemy intelligence, and if the information obtained by the enemy could be useful to subvert operations.

- Consider ways to **protect your family**
  - If you have social media, ensure family accounts are not linked to you (in case of compromise.)
- Plan for unintentional discoveries of **illegal material**
  - Report CSAM to Internet Watch Foundation
  - Use institutional reporting channels to security services, hotlines etc.

PUBLISHING RESEARCH

- Go beyond descriptive accounts of data to conceptualise patterns – use social science theories
- Research should be immaculate to avoid 'own goals' e.g., don't conflate invidious information with misinformation or disinformation, don't publish information that helps hostile actors
- Remember influence doesn't just happen through publication, use resources such as NABS+ to network with policymakers

> **OpSec is much more than a process – it is a mindset: 'Have you got your OpSec on?'**

HOSTILE ACTORS

- War in Europe has changed the context for research
- State actors have greater capabilities for hostile action against researchers but are more predictable in terms of who, why, and how.
- Non-state actors have fewer capabilities but are less predictable.

KEY TAKEAWAY

Defend forward – think at the outset 'have you got your OpSec on?' How can I manage all the different risks for my particular kinds of research? Be aware that risks might materialise in the field or downstream.

READ MORE

- Van Maanen, J. (2011). Tales of the Field : On Writing Ethnography (2nd ed.). University of Chicago Press
- NPSA guidance for High-Risk Individuals
- Internet Watch Foundation

NABS+ (NetworkPlus for Analytical Behavioural Science in security and defence) is funded by UKRI and administered by the Economic and Social Research Council (ESRC Award ES/Z502716/1). The views expressed by the researchers and team members are their own and should not be taken as representative of views held by those who fund NABS+. For more information, visit: www.crestresearch.ac.uk/nabs