BACKGROUND PAPER:

Security Council (SC)

New Frontiers in Digital Sovereignty

Introduction:

**Delegates will benefit from reading the GA and SCT background papers in order to prepare for this topic, focusing most upon the opening pages (1-4), data extinction discussion (12-13), and geo-political challenges (15), and the implications for data extinction (20-23).*

> Today's militaries and paramilitary groups are just as active in the datasphere as any other actor. There is no denying that war has been digitally transformed and that a growing volume of information is now "sensed, collected, stored, analyzed, and disseminated every day" to advance wartime efforts.
>
> - "Data in War" (2022)

As cyberwarfare scales up, so too do its applications, and while the UN has debated whether "cyber" attacks or activities constitute "armed" conflict, it is nevertheless true that every active military (state-led or paramilitary) desires and employs data, including the types of private data previously discussed. More, this data is used during conflict, post-conflict periods, and in peacetime.

In the war in Ukraine, for instance, business-owned satellites gather images and data for military surveillance; citizen cell services gather and send data on human rights abuses; cyber militias gather data to find weaknesses in Russian targets; Russian communications networks are intercepted to control data movement; and social media platforms are manipulated for purposes of propaganda ("Data in War"). Beyond spyware and video surveillance (with machine learning prediction software to anticipate behavior), militaries use biometric data and facial recognition at checkpoints.

Unsurprisingly, conversations about responsible use of this data collection are still in their initial stages, and few to none include all of the various players involved in gathering, moving, studying, storing, and disposal of it.

Worse, data breaches in the military are nearly as common as anywhere else, perhaps a larger target due to the value of such data. In November 2023, a Duke University study discovered the personal records of thousands of US servicemen available for sale online (including their current posts via GPS), along with the records of their families and friends.

If the stakes for data privacy are higher in the military (both for the damages incurred from loss and the strategic advantages gained from retention), what impact a Web3 ability for users to eliminate personal data?

Current Uses of Data for Military

The list of uses is nearly inexhaustible and fast-growing as AI and machine learning technologies demand data for their analyses and prediction models. However, we can list a few general categories where personal data is routinely valued in the world's militaries:

- Of a nation's own servicepeople
    - For the routine business of military employment
    - For biometric and GPS tracking
    - For operations in control of military hardware and software
    - For behavioral records related to security
- Intelligence Gathering
    - To identify potential threats
    - To determine behavioral patterns and anomalies in small groups and larger societies
    - Of communications for threat analysis and evidence gathering
- Site security (IP addresses, user profiles, biometrics, etc.)
    - To protect military data and measure activity
    - To log and track inventories
    - To trace browser histories and patterns
- Operational advantages
    - For autonomous weapons systems data-driven prediction
    - For surveillance
    - For fast, data-driven strategic and tactical decision-making
- For cyberwarfare defense and counter-measures
    - Too numerous to list here

Militaries know that too heavy a reliance on digital data itself is a vulnerability, but for nations that are resource-challenge, data use and cyberwarfare are inexpensive ways to compete on the international strategic stage when conventional methods are stretched.

The Stakes

Buchan and Lubin edited a book on *The Rights to Privacy and Data Protection in Times of Armed Conflict* in 2022. In it, several writers balance the call for data privacy against the strategic need for data, covering everything from occupation and prisoners of war to facial recognition and drone surveillance, and from “third party” nations in conflict to war criminal data retention. In addition, 2022 saw the CyCon (cyberwar conference) which addresses more technological challenges to data used, including ransomware threats, cyber-deception and misidentification challenges, and the military’s implied “responsibility to detect” (Jancarkova).

The field is awash in possibilities and threats! And it is one thing when an enemy force works against military objectives, but what are we to think of a citizen-level interference with those goals? *In brief, are strategic military needs (including those by UN-mandates) greater than the rights of private citizens? In what circumstances might a military force actively counter data-extinction tags?*

But after all, how troublesome might simple “personal data sets” be if they were suddenly unavailable for security operations?

“Actively Seized of the Matter” in Yemen

The Security Council, in reviewing the current situation in Yemen and making directives and resolutions, continues to be “actively seized” (continually monitoring and responding to) the complex conflict in that region. Its most recent resolution in July 2024 extended (again) the UN Mission to Support the Hodeidah Agreement (UNMHA), a civilian observer mission which called for a ceasefire in that port city, a withdrawal of active troops, and the resuming of humanitarian aid.

Earlier this year (in June and January), the Security Council passed resolutions demanding that Houthi forces end all attacks on nearby merchant and commercial ships in the region. Houthi attacks have made the Red Sea a highly dangerous region and as a result trade ships largely avoid it and take longer routes around southern Africa. For their part, Houthis have vowed to continue their attacks until the war on Gaza ends and humanitarian aid reaches the area. In August, a Greek oil tanker was attacked, causing a catastrophic oil spill in the Red Sea. US & UK forces have been bombing Houthi targets in Yemen for the past year. The Houthi forces are Iranian-backed. In the meantime, the UN Secretary-General’s Special Envoy to Yemen (OSESGY) continues to work for peaceful solutions in the region.

Committee Mission

The Security Council should review the situation in the Red Sea and the current state of UNMHA in Yemen. However, it will soon become obvious that the topic of data extinction in the Special Committee on Technology has an immediate international security dimension, necessitating one or more responses by the Security Council.

The resolutions emerging from the Security Council will deal less with the complete Yemeni conflict than they will the various parties involved around the data crisis and determinations around the topic of ***digital sovereignty****: who has the unassailable right to data use and under what circumstances?*

Preparation

Security Council delegates should review the basic nature of the conflict in Yemen (see the separate bibliography on possible sources). They might also review the issues and sources relevant from the other committees. Finally, the Security Council bibliography references the pdfs from Buchan and Lubin and Jancarkova which may prove interesting reading.

Finally, in preparing committee responses, delegates might address the various uses military forces make of personal data (p. 25) and consider which seem reasonable to their governments and which may be regulated in the name of data privacy. Are citizens always within their rights to destroy their own data?

Questions to Consider:

Like the GA and SCT, identifying your own nation's position on data use is a good first step. In the face of (nearly) inevitable user-defined data extinction, are there any data uses that your country would consider limiting?

1. Is there any difference in a military's right to data between peacetime, active war, and post-conflict operations?
2. Are there any limits to the partners (businesses or civilian or partner nations) the military may employ in gathering, analyzing, storing, and deleting data?
3. If nations weigh the answers to these questions differently, does this give privacy-denying nations a strategic advantage militarily? How could this be reconciled?
4. Are there any circumstances where a civilian's data extinction decision might re-categorize them as combatant, terrorist, or political dissident?

5. Are developing nations and combatant forces within their rights to protect data collection when it means their own security power is enhanced against more advanced foes?
6. What role in a military's data security and collection (gathering, analyzing, storing, or deleting) might make a non-combatant person or agency a legitimate military target?

Security Council Additional Bibliography

"Adopting Resolution 2739 (2024) on Yemen, Security Council Demands Houthis Immediately Cease All Attacks against Merchant, Commercial Vessels." Meetings Coverage and Press Releases, 27 June 2024, https://press.un.org/en/2024/sc15750.doc.htm.

Blanchard, Christopher M. "'Yemen: Conflict, Red Sea Attacks, and U.S. Policy.'" CRS Reports, IF12581, Aug. 2024, https://crsreports.congress.gov/product/pdf/IF/IF12581.

Buchan, Russell, and Asaf Lubin, editors. "The Rights to Privacy and Data Protection in Times of Armed Conflict." CCDCOE, NATO CCDCOE Publications, 2022, https://ccdcoe.org/uploads/2022/06/The-Rights-to-Privacy-and-Data-Protection-in-Armed-Conflict.pdf.

"Data in War." The Datasphere Initiative, 13 Oct. 2022, https://www.thedatasphere.org/news/data-in-war/.

"Data Protection and Privacy Legislation Worldwide." UNCTAD, 2024, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

Hadi, Abd Rabbou Mansour. "Law 13 of 2012 Regarding The Right to Access to Information." President of the Yemeni Republic , 2012. https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/ye/ye026en.pdf.

Jancarkova, T., and et al, editors. "14th International Conference on Cyber Conflict: Keep Moving." CCDCOE Publications, 2022. https://ccdcoe.org/library/publications/cycon-2022-book/.

Lyngaas, Sean. "How Cyberwarfare Is Playing into Yemen's Civil War." CyberScoop, 28 Nov. 2018, https://cyberscoop.com/yemen-civil-war-cyberwarfare-recorded-future-cyberwarcon/.

McThenia, Noah. "Yemeni Civil War Spans Cyberspace, Too." American Grand Strategy, 16 Jan. 2019, https://ags.duke.edu/2019/01/16/yemen-conflict-spans-cyberspace-too/.

Mishra, Vibhu. “UN Warns of Escalating Conflict in Yemen amid Humanitarian Crisis, Regional Tensions.” UN News, 12 Sept. 2024, https://news.un.org/en/story/2024/09/1154271.

Muggah, Robert. “Yemen’s Parallel War in Cyberspace.” Foreign Policy, 6 Jan. 2022, https://foreignpolicy.com/2022/01/06/yemen-war-internet-media-houthis-iran-saudi-arabia/.

Starks, Tim. “Researchers Catch Yemeni Hackers Spying on Middle East Military Phones.” CyberScoop, 9 July 2024, https://cyberscoop.com/researchers-catch-yemeni-hackers-spying-on-middle-east-military-phones/.

“UN in Yemen.” OSESGY, 18 Sept. 2024, https://osesgy.unmissions.org/un-yemen.

UN. Security Council (79th year : “Resolution 2722 (2024) / Adopted by the Security Council at Its 9527th Meeting, on 10 January 2024.” United Nations Digital Library System, 10 Jan. 2024, https://digitallibrary.un.org/record/4033392?ln=en&v=pdf.

“Yemen.” DataGuidance, 2012, https://www.dataguidance.com/jurisdiction/yemen.