Topic Guide

Data Collection as a Threat to International Security

Disarmament and International Security Commission
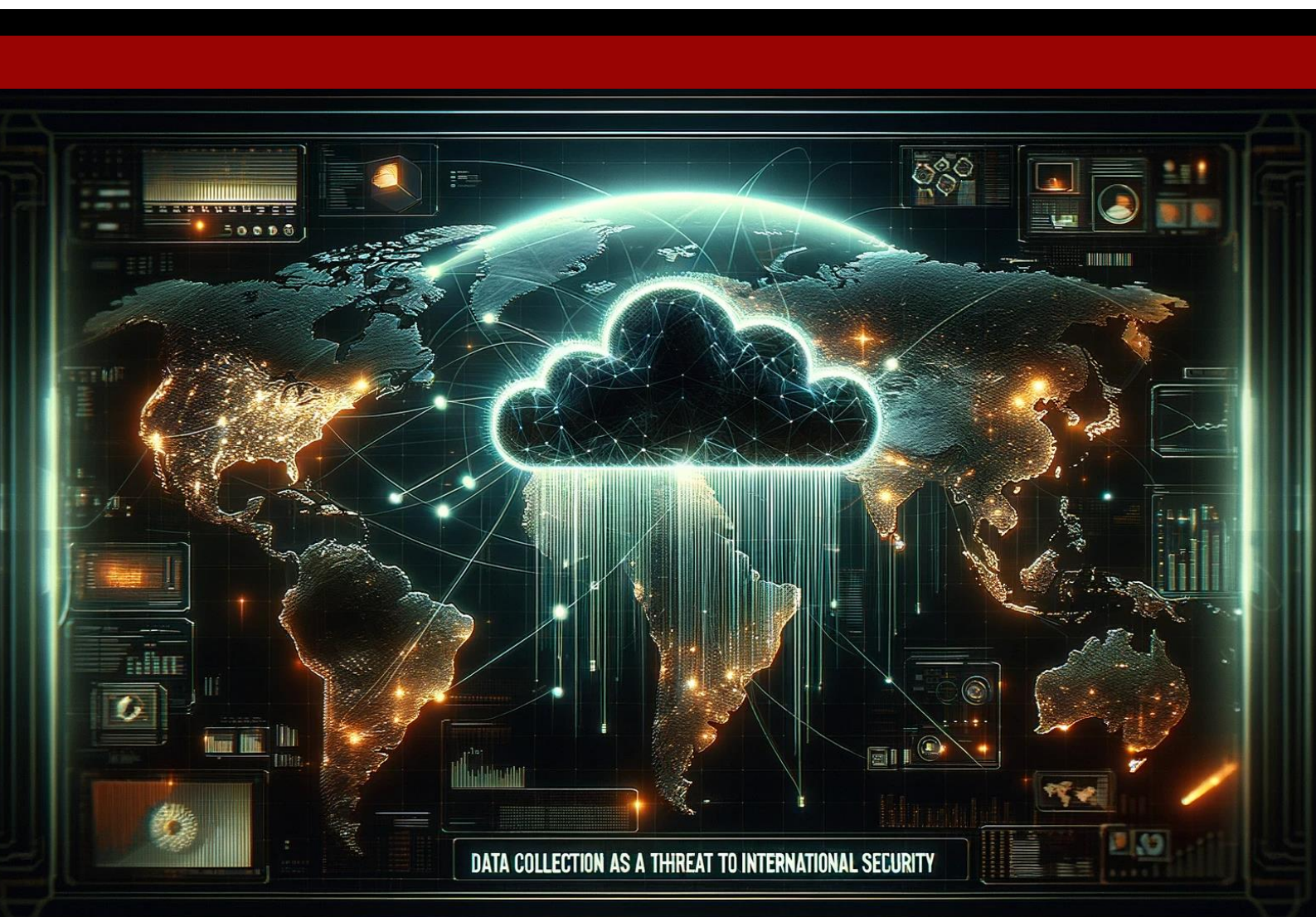
DATA COLLECTION AS A THREAT TO INTERNATIONAL SECURITY

Data Collection as a Threat to International Security

Topic Overview

This topic addresses the growing concern over how data collection impacts international security. It involves understanding the implications of data localization, the challenges posed by digital surveillance, and the balance between national security, privacy, and global data governance.

Topic Background

- **The Rise of Data Localization**: The increased need to control where and how data is stored and accessed for reasons ranging from national security to data privacy has led to data localization mandates. These mandates vary by country and are influenced by each country's digital governance approach.

- **Data Localization and National Security**: These mandates impact national security in several ways:
  - Digital Sovereignty: Efforts to maintain control over data can be seen as thinly veiled attempts to assert domestic digital domain control, impacting human rights and economic interests.
  - Fragmented Global Data Governance: The uneven enforcement of data localization results in a patchwork of international data flow restrictions, leading to internet fragmentation.

- **Recent Developments in Data Privacy and Security Laws**: The EU's GDPR has been vigorously enforced, with significant fines. There have been key developments in the EU's regulatory landscape for digital services and data sharing, notably the Digital Services Act (DSA) and the Digital Markets Act (DMA). Internationally, countries like Indonesia, Tanzania, and Oman have been adopting new data protection laws, reflecting a global trend toward tighter data governance.

Points of Debate

1. National Security Implications:
   a. Authoritarian Threats: Data localization can enable digital authoritarianism, threatening democracy and human rights.
   b. Security Collaboration Limits: These policies can hinder international collaboration between security agencies and create safe havens for malicious actors.
   c. Cybersecurity Risks: Data localization increases cybersecurity risks due to the need for more data centers, which can be more vulnerable to attacks.

2. Economic and Privacy Concerns: The debate over whether data localization measures truly enhance privacy or simply serve to exert government control over citizens and suppress minority communities.

3. Global Policy Responses: The need for a balanced approach in international data governance, recognizing the legitimate national security concerns while ensuring the free flow of data, privacy, and economic growth.

4. Balancing Benefits with Risks and Interests: The challenge lies in balancing the benefits of enhanced data access and sharing against the risks and legitimate private, national, and public interests. This includes the need to reduce barriers to cross-border data flows while maintaining data security and protecting intellectual property rights (IPRs) and privacy. This balance is crucial in cases involving sensitive data, where the risk of confidentiality breaches can lead to a systemic risk with wide-ranging societal effects.

5. Digital Security Threats and Personal Data Breaches: Enhanced data access and sharing can expose organizations to digital security threats, potentially disrupting the availability, integrity, or confidentiality of critical data and information systems. These threats can affect not just individual organizations but entire supply chains and essential services. Personal data breaches, resulting from such increased access and sharing, can cause significant harm to individuals' privacy and lead to substantial economic losses for businesses, affecting their competitiveness and reputation.

References

1. CSIS (n.d.) The Real National Security Concerns over Data Localization. Available at: https://www.csis.org (Accessed 24 November 2023).

2. Haverford College (n.d.) Impact of Data Localization on National Security. Available at: https://pols.sites.haverford.edu (Accessed 24 November 2023).

3. Gibson Dunn (2023) International Cybersecurity and Data Privacy Outlook and Review – 2023. Available at: https://www.gibsondunn.com (Accessed 24 November 2023).