United Nations Office of Information and Communications Technology

CHMUN XIX

General Assembly

Committee Background:

The United Nations Office of Information and Communications Technology, or OICT for short, was set up in 2007 to provide the technology tools and services needed across the entire UN Secretariat. Their goal is to make sure the UN can use information and communication technology (ICT) in an efficient, effective, and innovative way to support the substantive and administrative work of the UN. At the head of OICT is the Chief Information Technology Officer, or CITO, who reports directly to the Under-Secretary-General for Management. The CITO is responsible for providing the strategic vision and leadership for carrying out ICT strategy across the Secretariat and making sure all the systems fit together smoothly. OICT is based at the UN headquarters in New York but also has offices in Geneva, Vienna, Nairobi, and other locations where the UN has duty stations. The team is around 300 people strong, with staff in roles like software development, infrastructure management, information security, business analysis, project management, and IT support. OICT's goal is to tap into the potential of digital technologies, so the UN can achieve its global mission more efficiently and effectively. As the UN continues adopting more innovative ICT solutions and digital platforms, OICT's role has become increasingly critical.

Topic A: Defending Against Data Breaches in the Private Sector

Introduction

Nowadays, data breaches have become a huge problem that every private company needs to take seriously. A data breach is when hackers or bad actors get their hands on private info or data that should've been kept confidential. In recent years, we've seen some massive breaches impact millions of customers - big names like Equifax, Yahoo, Marriott, and more have been hit hard. The fallout from these attacks can be severe, totally shaking customer trust, damaging company finances, and trashing reputations. So defending against breaches has to be a top priority for any business today. The truth is, there's no silver bullet. Companies need to put together a layered defense with the right mix of policies, tech tools, training, and best practices. They absolutely need strong cybersecurity like encryption and access controls to lock down systems. Carefully monitoring for threats and having an incident response plan is crucial too. But even with all the right tech, human mistakes can still leave gaps. That's why everyone in a company has to be trained on security protocols and staying vigilant. Bringing in ethical hackers to test systems is a smart, proactive move too. If businesses make data defense a total company effort, they can reduce the chances of an attack and minimize the damage if one happens. However, even with strong technical defenses, human error is often the weakest link. Companies must train employees in security protocols and exercise vigilance company-wide. Partnering with ethical hackers to test systems is another proactive tactic. With a proper understanding of the risks and a commitment to defense at all levels, companies can reduce the likelihood and impact of data breaches. This introduction has provided an overview of the importance and elements of effective data breach defense for the private sector.

Current Events

Data breaches remain a major threat to companies and consumers alike. Recent years have seen massive breaches like the Equifax incident in 2017 which exposed nearly 150 million Americans' personal information. As a result, Equifax agreed to pay $700 million to settle legal claims in July 2019.

Ransomware attacks have also surged, where hackers encrypt organizations' data until ransom demands are paid. High-profile cases include the Colonial Pipeline attack in 2021 disrupting gasoline supplies. New data privacy regulations like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are forcing companies to devote more resources to security. However, cyber insurance is getting more expensive as breaches rise. Experts recommend multi-factor authentication, encryption, network segmentation, and robust backup systems to better defend data. But debates continue around imposing stricter government security regulations on companies, with business groups arguing this could be burdensome. In summary, private sector data breaches have prompted legal settlements, insurance changes, investments in technology, and ongoing debates over regulations. But risks remain high, demanding continued vigilance and response.

Relevant UN Action

The United Nations has woken up to the growing threat of data breaches and cyberattacks that are plaguing private companies. In 2015, the UN adopted a resolution calling on member states to think about preventative measures to guard against data breaches. It pushed for cooperation between governments and private companies to share info and best practices. The resolution also made clear that international law applies in cyberspace - states have a responsibility not to conduct or support cyber operations that intentionally damage critical systems or private sector computer networks. More recently, in 2021, the UN General Assembly passed another resolution focused on "Promoting responsible Behavior by States in cyberspace." This outlined norms and principles for how states should responsibly behave online, including not doing or supporting malicious cyber activities that purposefully wreck critical infrastructure providing services to the public. It also pushed states to take reasonable steps to ensure the integrity of supply chains so end users can trust the technology products and services they use. The UN has also created space for different stakeholders to come together and discuss these issues by organizing expert working groups and hosting events on topics like cyber

stability and data protection. While these UN resolutions aren't legally binding per se, they show political will by member states to uphold cybersecurity and counter the threat of data breaches, however more UN action may be required to turn high-minded principles into concrete improvements in cybersecurity.

Questions to Consider

1. How can collaboration with government agencies, industry peers, and cybersecurity experts enhance private sector organizations' ability to defend against data breaches?
2. What strategies and technologies can private sector organizations implement to protect sensitive information and prevent unauthorized access by cybercriminals?
3. What are the ethical and human rights considerations that private sector organizations should take into account when addressing data breaches?
4. How can private sector organizations ensure they have effective redress mechanisms in place for individuals affected by data breaches?

Useful Links

1. Federal Trade Commission: "Data Breach Response: A Guide for Business"
    a. https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business
2. Cybersecurity and Infrastructure Security Agency: "Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches"
    a. https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf
3. United States Secret Service: "Preparing for a Cyber Incident"
    a. https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident

Topic 2: Utilizing Technology for Peacekeeping Efforts

Introduction

As armed conflicts evolve to span borders and involve non-state actors, the landscape of peacekeeping has become exponentially more complex. Fortuitously, recent technological advancements are equipping peacekeepers with valuable new tools to meet these multifaceted challenges. Sophisticated surveillance drones now provide aerial views of ceasefire lines and troop movements that were previously invisible. Data mining algorithms uncover early warning signs in open-source data that could predict outbreaks of violence. Encrypted mobile devices allow seamless communication between peacekeepers and commanders, facilitating better coordination. Biometric scans and digital IDs help identify ex-combatants and support disarmament processes. GPS tracking of supply trucks enables efficient logistics to remote outposts. These and other innovations are augmenting the capabilities of peacekeepers on the ground. When combined thoughtfully with political solutions, technology can create openings for conflict resolution and peacebuilding that did not previously exist. However, the use of technology is not without risks. There are real concerns surrounding data privacy, surveillance overreach, and weaponization of tech tools. With careful oversight and direction, technology can become a creative force multiplier for multilateral efforts to sustain peace and prevent conflict from erupting in the first place.

Current Events

The use of technology for peacekeeping and conflict resolution has expanded in recent years. Drones and high-resolution satellite photos are now being used to monitor conflict zones and gather evidence of human rights abuses. For example, the UN has used drones for surveillance in the Democratic Republic of Congo while groups like Amnesty International have analyzed satellite imagery to document the destruction of villages in Myanmar. The widespread availability of this kind of technology is making it easier to document atrocities. In addition, government agencies and NGOs

are utilizing software to monitor social media for signs of rising tensions and hate speech. This allows peacekeepers to identify situations at risk of violence early and try mediation and de-escalation.

Other forms of technology facilitate communication and coordination for those working in peacekeeping and conflict resolution. Secure mobile messaging apps enable mediators to stay in touch with parties in remote conflict zones. Videoconferencing and collaborative document editing platforms also assist diplomats in negotiations when in-person talks are impractical. Groups focused on peacebuilding are also crowdsourcing data from local populations to gain on-the-ground perspectives on conflicts. This helps provide a more granular view of conflict dynamics, although crowdsourced data poses risks of spreading misinformation. In addition, data scientists are developing predictive analytics models to analyze news and social media to forecast where political instability and violence are likely to occur.

Relevant UN Action

The UN has started to recognize how important it is to use technology to enhance peacekeeping missions and provide better protection for civilians in war-torn areas. In the last few years, the UN has taken some big steps to modernize peacekeeping operations through new technologies. In 2017, the UN Department of Peace Operations announced they were creating a new Technology and Innovation Section to identify technologies that could be integrated into field missions. This section has been looking at things like unmanned aerial vehicles (UAVs), geospatial data, and video analytics to improve situational awareness and threat detection on the ground. In 2018, the UN tested using UAVs in the Congo mission to provide aerial surveillance and civilian protection - one of the first major uses of drones in UN peacekeeping. The UN has also been utilizing geospatial data and intelligence more and more to strengthen operational planning and security. In 2020, they obtained high-resolution satellite imagery in over 30 UN mission areas to boost monitoring abilities. Missions like Mali have also deployed camera networks and video analytics to monitor perimeters and detect potential threats. To further speed up the adoption of new tech in peacekeeping,

Secretary-General Antonio Guterres put together an internal Working Group on Technology and Innovation in 2021. They aim to provide strategic guidance and identify emerging technologies the UN could start using.

Questions to Consider

1. In what ways can technology be utilized for peacekeeping efforts and how?
2. How can recent technological advancements be improved for peacekeepers in monitoring conflict zones and preventing violence?
3. How can technological access remain equitable and accessible for all?
4. How can nations come to a global consensus or compromise on diplomatic technology policy, and should they?
5. How can guidelines regarding technology be more clearly defined to avoid confusion?
6. What are the ethical and privacy considerations that should be taken into account when implementing technology in peacekeeping, and how can these concerns be addressed?

Useful Links

1. International Peace Institute: "New Technologies and the Protection of Civilians in UN Peace Operations"
    a. https://www.ipinst.org/wp-content/uploads/2023/09/IPI-E-RPT-New-Technologies.pdf
2. ReliefWeb: "UN Peacekeeping embraces the digital world"
    a. https://reliefweb.int/report/world/un-peacekeeping-embraces-digital-world
3. United Nations University: "Digital Peacekeeping"
    a. https://i.unu.edu/media/cs.unu.edu/attachment/4030/Peacekeeping_web.pdf

Works Cited

Duursma, Allard, et al. "UN Peacekeeping at 75: Achievements, Challenges, and Prospects." *International Peacekeeping*, vol. 30, no. 4, 2023, pp. 415–476, https://doi.org/10.1080/13533312.2023.2263178.

Loyle, Cyanne E. "Rebel Justice during Armed Conflict." *Journal of Conflict Resolution*, vol. 65, no. 1, 2020, pp. 108–134, https://doi.org/10.1177/0022002720939299.

"Myanmar's Military Struggles to Control the Virtual Battlefield." *International Crisis Group*, Crisis Group, 18 May 2021, www.crisisgroup.org/asia/south-east-asia/myanmar/314-myanmars-military-struggles-control-virtual-battlefield.

Trubowitz, Peter, and Kohei Watanabe. "The Geopolitical Threat Index: A Text-Based Computational Approach to Identifying Foreign Threats ." *International Studies Quarterly*, vol. 65, no. 3, 2021, pp. 852–865, https://doi.org/10.1093/isq/sqab029.

.