A pie chart with numbers and text

Description automatically generatedA graph of a number of individuals

Description automatically generated with medium confidenceDelegate Name: Lina Abdel-Hadi

Country: Ukraine

Institution: The Sultan’s School

Topic: Assessing and Mitigating the Dangers of Cyberattacks

“Cyberthreat does not recognize socioeconomic discrimination.” ― Bradley B Dalina

Since the late 20th century, cyberattacks have evolved from rare occurrences to pervasive threats. For instance, The Morris Worm, one of the earliest documented cyberattacks, infected thousands of computers in 1988. Semi-recent major attacks also include the compromise of Canadian government departments in 2011, the targeting of Ukrainian government entities in 2019, and the targeting of U.S. oil and gas companies in 2021. Conscious of the urgency, the UN GGE has focused on developing principles guiding governmental behavior in cyberspace. Additionally, the United Nations-wide framework on activities regarding Cybersecurity and Cybercrime has established principles for program development.

Moreover, Ukraine has been under frequent cyberattacks by external hackers in the wake of the recent Russia-Ukraine war in the east. These attacks, along with attacks prior to the conflict, have severely damaged the nation’s economy and infrastructure with severe financial consequences. For instance, the 2017 NotPetya attack, originating in Ukraine, is estimated by the White House to have cost over $10 billion in damages worldwide. In addition to this, a substantial proportion of these losses were borne by Ukrainian firms. In Kyiv alone, this attack hit at least four hospitals, six power companies, two airports, and over twenty-two Ukrainian banks. in 2015, hacks known as BlackEnergy caused Ukrainian power companies to experience unscheduled power outages, impacting roughly 230,000 consumers. In an attempt to proactively handle the issue of cyberattacks in the nation, Ukraine adopted a National Cybersecurity Strategy in 2016. These establishments have, in fact, positively demonstrated some effectiveness. Additionally, Ukraine has organized cybersecurity drills and collaborations with international organizations in the past. However, on a negative note, the effectiveness of these efforts is restricted due to a lack of funding.

A graph of a number of green bars

Description automatically generatedAs research showed that there were 50% more cyberattack attempts on corporate networks in 2021 than in 2020, the delegate aims to innovate fresh proposals to tackle this challenge. One of the suggested ways is the establishment of international standards in cybersecurity. This will ensure an exchange of cybersecurity defense practices among states and can minimize cyberattacks. However, resource constraints and divergent national priorities can make it difficult to achieve this proposed solution. Another suggested solution would be the formation of a cybersecurity framework that operates under the UN’s authority. This UN-backed framework would facilitate crisis management and could provide policy guidance to member states and may protect human rights in cyberspace. A consequential challenge to this proposal would be achieving consensus among all states, as each country may have varying priorities and interests. This challenge may result in delays when making decisions, along with incidental conflicts of interest, hindering the framework’s effectiveness.

References: -

Wikipedia <https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack>

CISA (.gov) <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>

Digital Watch Observatory <https://dig.watch/resource/un-gge-2021-report>

Just Security <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/>

Wired <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

The Economic Times <https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the-world/articleshow/89997076.cms?from=mdr>

Ukraine Cybersecurity Governance Assessment <https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf>

National Coordination Center for Cybersecurity <https://www.rnbo.gov.ua/en/>

Wikipedia <https://en.wikipedia.org/wiki/Cyberattack>

Cyber Operations Tracker <https://www.cfr.org/cyber-operations/>