Disarmament and International Security Study Guide

DISEC

Topic A: The Reemergence of the Nuclear Threat

Topic B: Curbing the Global Threat of Cyber-Terrorism

AtidMUN 2023

CHAIRS LETTER

Dear esteemed delegates,

We hope this letter finds you in good health and high spirits as we prepare for the upcoming AtidMUN conference. As the Chairs of the DISEC Committee, we are excited and honored to welcome you to what promises to be an engaging and intellectually stimulating event.

Our committee is tasked with addressing some of the most pressing global issues facing the international community today. With your diverse backgrounds, unique perspectives, and unwavering dedication to diplomacy, I am confident we can foster meaningful discussions and craft innovative solutions to these challenges.

The success of our committee sessions will depend on your active participation, dedication to research, and commitment to the principles of diplomacy and compromise. We encourage you to thoroughly research your assigned country's or organization's positions on the agenda items and to come prepared to defend and advance those positions. Remember that constructive dialogue and cooperation are keys to achieving our goals.

Sincerely,

Nana Awadeie Phone number:0547553263 Email: nohadawadeie@gmail.com

Maayan Avraham Phone number;0535330855 Email: maayana2619@gmail.com

TABLE OF CONTENTS

TOPIC A: THE REEMERGENCE OF THE NUCLEAR THREAT

BACKGROUND TO THE COMMITTEE

Nuclear bombs, seemingly a relic of the past and a cautionary tale, may return soon. With tensions rising both in the East and West, the use of a weapon of mass destruction becomes more and more probable. Iran is predicted to be very close to its first nuclear weapon test, and Russia may be forced to use a nuclear weapon if things go south in Ukraine. The committee must agree on how to best mitigate the risk of atomic warfare for the sake of humanity.

But first, a quick overview of the history of nuclear weapons, the Cold War, and the NPT.

THE WORLD'S NUCLEAR BEGINNINGS

The origins of nuclear weapons lie in the discovery of **atomic fission** in Germany in 1938. In layperson's terms, nuclear fission is when a particle splits into two smaller particles and releases substantial energy. There is also a process called **nuclear fusion**, where two lighter atoms (usually hydrogen) combine and release energy (History, 2022).

The destructive potential of nuclear fission moved Albert Einstein to urge the US to expand their atomic research and stockpile uranium before the Germans do so (McEvoy, 2023). With the help of Lyman Briggs, the Roosevelt administration investigated the matter and concluded that a proper research force was needed. Following this development, President Roosevelt authorized the beginning of "The Manhattan Project" on December 28, 1942 – with the primary goal of nuclear research and development (History, 2022). The project occurred at more than 30 US, UK, and Canada sites. However, most breakthroughs were produced in Los Alamos, New Mexico, under the direction of theoretical physicist J. Robert Oppenheimer. Three years later, in 1945, they had two working designs for the nuclear bomb: a uranium-based weapon called "the Little Boy" and a plutonium-based weapon called "the Fat Man."

In the summer of 1945, while the German forces had already surrendered, Japan was still fighting. Instead of an assault on Japanese territory, the US sent a request through the Potsdam Declaration, which promised "prompt and utter destruction" if Japan did not surrender. Japan did not surrender, so "The Little Boy" was dropped on Hiroshima on August 6, 1945. The initial bomb killed 80,000 people instantly, and many more died from radiation poisoning. The second bomb,

"the Fat Man," was dropped on Nagasaki on August 9, 1945 – killing another 40,000 people. This devastating attack marked the war's end (History, 2023).

Tensions Rising in the Cold War

The USSR quickly caught up with the United States' nuclear prowess. Soon after the war, in August 1949, the Soviet Union acquired its atomic bomb. In response, the US expanded its nuclear weapons research and began the Cold War arms race. Over the next few years, the US and USSR could produce hydrogen bombs – weapons with 1,000 times more destructive potential than the original atomic bombs. The UK, France, and China also caught up (History, 2022).

Tensions between the two nuclear powerhouses constantly rose until the late 1960s with the signing of the Nuclear Non-Proliferation Treaty (NPT). The treaty states that nuclear-weaponized countries will not use or help countries without nuclear weapons acquire them. The treaty outlines a gradual decrease in nuclear weapon stockpiles with the eventual goal of total disarmament.

A Shaky Status Quo

Although the NPT delivered an excellent foundation for a nuclear-safe world, some countries wanted nuclear weapons for themselves and did not sign the NPT. India acquired and tested their first nuclear bomb in 1974, Pakistan has an extensive nuclear program, and Israel is widely believed to possess nuclear weapons (History, 2022).

Some countries have signed the NPT and backed out of it. Most notably – North Korea. North Korea backed out of the NPT in 2003 and has been openly testing their nuclear weapons since 2006. In 2017, North Korea claimed to have an intercontinental hydrogen bomb that could reach the US (Lester, 2019).

Iran, while still a signatory of the NPT, has not abided by it for the last few years. In 2015, Iran signed an agreement with the West, the Joint Comprehensive Plan of Action (JCPOA), to relieve them of economic sanctions. The JCPOA massively restricted Iran's nuclear weaponry research and development industries to enforce the NPT. In 2018, the US backed out of the agreement. As a result, Iran has been neglecting the restrictions set by the JCPOA and has threatened to leave the NPT (United States Institute of Peace, 2020).

Iran is no longer diplomatically and economically isolated. Their new allyship with Russia gives them the funds and resources to expand their nuclear facilities and stockpile uranium. Tensions

between Iran and Israel have also been rising. A nuclear war between Iran and Israel is becoming more likely (Bronner & Meyer, 2023).

" Enemies, particularly the Zionist regime, have received the message that any tiny action against (our) country will prompt a harsh answer from the armed forces, which will accompany the destruction of Haifa and Tel Aviv. "

- *President Ebrahim Raisi* (The Times of Israel, 2023).

Europe, too, may become a nuclear warzone. Since the invasion of Ukraine, tensions between Russia and NATO members have sharply risen. Early in the invasion, Russia took over one of Europe's giant nuclear power plants, lost control, and is now launching missiles at it. Damage to the nuclear power plant may cause "a nuclear disaster that would impact much of Eastern Europe and lead to hunger in many parts of the world" (Pleschberger, 2023). Not to mention, there is a possibility that NATO members and Russia would resort to nuclear warfare for other reasons.

THE RUSSIAN THREAT

A SERIES OF UNFORTUNATE NUCLEAR EVENTS

The Chernobyl Disaster

The Cold War brought a nuclear arms race with it. By the 1980s, the USSR had acquired 39,000 nuclear warheads – 16,000 more than the US had (United et al.). However, the USSR would quickly lose its nuclear prowess from then on. Near the end of the Cold War, on April 26, 1986, The USSR had its first nuclear disaster: the Chernobyl disaster.

While conducting a test on the Chornobyl four nuclear reactors, the power plant's poor design caused the reactor's cover plate to detach, causing a steam explosion followed by a second explosion that threw out graphite fragments. The extremely hot graphite and nuclear fuel that spilled out of the reactor started several fires, which released large amounts of radioactivity into the atmosphere. Two Chornobyl workers died on the impact that day, and 28 more over the following weeks due to acute radiation syndrome. Over 350,000 civilians were evacuated and relocated due to persistent nuclear fallout in the area (World Nuclear Association, 2022). The initial emergency response cost $5.32 billion, adjusted for inflation (UN, n.d.).

The Chornobyl disaster's long-term effects were devastating. The people's health declined as childhood thyroid cancer rates rose and mental illness became more common among the

surrounding population. The economy took a massive hit, too: The USSR had spent almost all its money on containment and decontamination, and 5-7% of government spending in the area is still related to Chornobyl (The Chernobyl Forum, 2010).

Budapest Memorandum

The Chernobyl disaster shaped the USSR's future in future (Patel, n.d.), and just a few years later, on December 25, 1991, the Soviet Union dissolved (U.S. Department of State, n.d.). Due to the dissolution of the Soviet Union, Ukraine inherited the third-largest stockpile of nuclear warheads (Budjeryn & Bunn, 2020).

As signatories of the NPT, the US and Russia drafted the Budapest Memorandum – an agreement between the US, Russia, Ukraine, Belarus, and Kazakhstan regarding their newly inherited nuclear force. Under the treaty's terms, Ukraine, Belarus, and Kazakhstan agreed to give up their nuclear arsenals to join the NPT as a non-nuclear state. In exchange, Ukraine initially sought guaranteed protection from the US but did not get it. It instead got "promises" that the signed countries would respect their sovereignty. The enforcement of the security of Ukraine had been left up in the air (Borda, 2022).

It would not be long before Russia utilized this fatal flaw in the memorandum. In 2014, Russia launched its invasion and eventually annexed Crimean Peninsula. The Russian annexation of Crimea was met with subpar international response. The UK even admits it: "The government has not been as active or visible on this issue as it could have been" (UK House of Lords, 2015). The US had placed sanctions on Russia and provided military support to Ukraine, but as we see today, that did not stop them from trying to take over Ukraine again.

IT ALL CHANGED WHEN THE FIRE NATION ATTACKED (RUSSIANS ARE COMING)

The Invasion, Its Progress, and the Potential Use of Tactical Nukes

On February 24, 2022, Russia launched its second invasion of Ukrainian soil. After the quick victory over the Crimean Peninsula back in 2014, it was expected that Russia would take over Ukraine in a matter of weeks. It is over a year into the war, and Russia has not gotten too far.

Ukraine is pushing back, and it is scaring the Kremlin more than ever before. In July, former Russian president and current deputy chairman of the Russian Security Council, Dimitry Medvedev, stated that in the case of a successful Ukrainian counterattack with NATO support,

they would be forced to use a nuclear weapon on Ukraine (Pennington, Stambaugh, & Lendon, 2023).

Russia has already made the first move, transporting its first batch of tactical nukes to Belarus as a "warning to the West." With support from NATO, the Ukrainian counteroffensive is making real progress on the Crimean front. If the counteroffensive is booming, Russia may use tactical nukes to protect itself from defeat.

Oops, you got your nuclear arsenal!

Ever since the beginning of the invasion, the Levada Center has conducted monthly polls that have indicated consistent public support for the invasion of over 70%. However, in the wake of the invasion, called "a Special Military Operation.", the Kremlin drafted incredibly draconian laws prohibiting any public opposition to the Russian government or the invasion of Ukraine. Although the Kremlin can currently suppress any attempts at civilian opposition, '…**what would happen if a revolutionary organization or any rogue actor succeeded and got a hold of 5,977 nuclear weapons?'** (Kristensen, 2023)?

There was one group that tried – the Wagner Group. This Russian state-funded private military company played a crucial part in the invasion of Ukraine. It aided other Russian allies in regional conflicts, such as civil wars in Syria, Libya, and Mali.

Yevgeny Prigozhin, the Wagner Group leader, was the organization's driving force; often characterized as ruthless, efficient, practical, and uncompromising, Prigozhin had a "go big or go home" mentality regarding the invasion of Ukraine. The Wagner motto: "Blood, honor, homeland, courage." Prigozhin liked the public's attention, often filming videos of the rubble that was left after his victories.

Prigozhin, while a lead figure in the Russian forces, had quite a few problems with the Russian cabinet. He accused Shoigu of withholding ammunition and resources from Wagner, making their victory over Bakhmut harder than it should have been. By doing that, he had earned himself an enemy. To retaliate, Shoigu introduced a policy in mid-June, backed by Putin, requiring PMC members to sign contracts with the Russian government by July 1st, relinquishing their independence. Prigozhin, aware this would end Wagner's autonomy, vehemently opposed it. He escalated criticism of the government, declaring top military figures as incompetent. **On June 24, Prigozhin announced an armed "march for justice, "an armed resistance, with Wagner**

troops leaving Ukraine and heading towards Moscow. As rebellious Wagner forces drove north toward Moscow on June 24, a contingent of military vehicles diverted east toward a fortified Russian army base with nuclear weapons. when the group was 110 km from the facility, in a televised address, Putin denounced Prigozhin's actions, calling said actions "treason" and "a stab in the back." Prigozhin, fearing a confrontation with the Russian dictator, folded then and there. He called off the mutiny and brokered a deal with the Russian government. (Yaffa, 2023).

While the rebellion did not go anywhere, it substantially impacted Putin's image within Russia. Putin is supposed to be a ruler with an iron fist that will destroy any attempt at opposition before it even begins (Yaffa, 2023). This situation could lay the groundwork for other resistance groups to take their chance at the Russian government. What if Russia's nuclear weapons fall into the wrong hands after a successful uprising? The question may become more acute as the Russian invaders struggle with the ongoing war.

Shenanigans in Zaporizhzhia

The Zaporizhzhia nuclear power station in southeastern Ukraine is the largest nuclear power plant in Europe and among the ten most significant in the world. The plant was built near the city of Enerhodar and is operated by the Enerhoatom.

Just a month into the war, on March 3, 2022, Russian forces occupied the nuclear power station in Zaporizhzhia (Hinshaw & Parkinson, 2022). During the fight, Russian shelling damaged three radiation sensors, prompting the Ukrainians to denounce Russia for "waging nuclear terror." The IAEA demanded a thorough inspection of the nuclear power plant. On August 19, 2022, Russia agreed (Koshiw & Rankin, Attack on Ukraine nuclear plant 'suicidal,' says UN chief as he urges access to the site, 2022). The report concluded that the Russian-occupied nuclear power plant violated all seven pillars of nuclear safety, and the IAEA Board of Governors passed a resolution calling Russia to leave the power plant. Russia did not go, but the plant was deactivated on September 11 (Koshiw, Putin, and Macron trade blame over risk at Ukraine's Zaporizhzhia nuclear plant, 2022).

On October 19, 2022, Ukrainian troops were spotted attempting to cross the Dnipro River to regain control over the Zaporizhzhia nuclear power plant. Over 600 elite Ukrainian soldiers and 30 armored boats were sent across the river, though they were forced to retreat under fire (Tucker, 2023).

Shelling in the area continued and spiked on November 19 and 20 (Faulconbridge, 2022). In those two days, the Zaporizhzhia was subjected to the most intense bombing in months. Members of the IAEA warned of a nuclear accident and called for "urgent measures to help prevent a nuclear accident" (Grieshaber, 2022).

IAEA Director General Rafael Grossi asked the UNSC to support suspending warfare around Zaporizhzhia to prevent a nuclear disaster. Grossi received support from the UNSC, and while tensions are still high between Ukrainian and Russian forces in the area, the shelling seems to have ended (World Nuclear News, 2023).

The constant shelling of the Zaporizhzhia nuclear power plant is quite a worrying reality. If shelling continues, a nuclear accident will inevitably happen. A nuclear disaster in a modern power plant is much more dangerous than in the past: Even the smallest of accidents could send radioactive particles that could affect agriculture in Austria and Italy. Additionally, unlike Chornobyl, Caesium is used for nuclear reactions in Zaporizhzhia, which is much more dangerous to humans than Iodine (Pleschberger, 2023).

The Iranian Threat

The History of Iran's Nuclear Program

Nuclear Dreams and Nightmares

Iran's dream is to acquire a nuclear bomb. Is it a nightmare? Just like in Scooby Doo – those meddling Western states. Over the last 60 years, Iran has been enhancing their nuclear research facilities and military capabilities. In response, the West, led by the US, has been attempting to block Iran's progress at every turn.

Ironically, the US began nuclear development in Iran in 1957 as part of the United States Atoms for Peace Program. Over the next ten years, Iran would continue expanding the scope of their nuclear reactor research and sign the NPT.

After the 1979 revolution in Iran, relations between it and the US quickly soured. The US ceased funding Iran's nuclear facilities, forcing Iran to shut down the operation. Not all was lost, though, because Iran had found itself a new ally: Russia. In 1992, Iran and Russia signed a cooperation agreement on the civil use of nuclear energy, including constructing a power plant. This cooperation displeased the US; the Clinton administration openly opposed Iran's nuclear energy

programs. Despite that, Russia and Iran continued to expand their atomic collaboration by building a second nuclear power plant (Nikou, 2021).

After years of a constant back-and-forth between the US and Iran, both countries, accompanied by the rest of the West, drafted the Joint Comprehensive Plan of Action, the JCPOA. Through this agreement, Iran agreed to restrict its production of enriched uranium and plutonium, pursue only civilian work (including industrial and medical research), and allow the IAEA to monitor activity in its nuclear facilities. In return, the P5 would lower the sanctions they had placed on Iran (Robinson, 2023).

The JCPOA? Never heard of it.

Just two years after the JCPOA was signed, in October of 2017, the Trump administration announced that it would be backing out of the agreement, accusing Iran of violating the "spirit" of the deal (Watson, 2017). It is essential to mention that Iran had not broken any actual guidelines in the agreement (Baker, 2017). The announcement was met with backlash from the international community – specifically from Theresa May, Emanuel Macron, and Angela Merkel, who issued a joint statement supporting the JCPOA (Shugerman, 2017). Nevertheless, on May 8, 2018, the US withdrew from the JCPOA and reinstated harsher sanctions on Iran (Wagner & Rocha, 2018).

Following this development, Iran did not hesitate to ignore the JCPOA. In May 2019, Iran announced that it would suspend the implementation of some parts of the JCPOA unless it received protection from US sanctions (Murphy, Iran stays within nuclear deal's primary limits while testing another, 2019). That same month, Iran began stockpiling uranium and announced it would bolster its enrichment programs (Kottasová, 2019). In November, Iran doubled its number of advanced centrifuges – a machine capable of separating isotopes of uranium to produce nuclear fuel (Anadolu Agency, 2019).

IRAN'S NUCLEAR PROGRAM IN THE MODERN DAY

Since the JCPOA lost its prominence in 2018, Iran's nuclear program has dramatically expanded. By September 2020, Iran had accumulated ten times more enriched uranium than was permitted by the JCPOA (BBC News, 2020). By April 2021, Iran had begun improving UF6 and injecting it into advanced centrifuges (Bob, Iran using advanced uranium enrichment at previously exploded facility, 2021).

In May of the same year, Iran produced 60% enriched uranium (Murphy, Iran has enriched uranium to up to 63% purity, IAEA says, 2021). According to the head of the IAEA, Rafael Grossi, only those developing nuclear bombs need such highly enriched uranium. By reaching this level of uranium enrichment, the time required for Iran to produce a bomb has plummeted from more than a year to three weeks.

In March 2022, Iran turned part of its highly enriched uranium near-weapon-grade. This form is complex for commercial purposes (Murphy, Iran defies Western powers with work on near weapons-grade uranium, 2022). In June, Iran cut off all the IAEA's access to their nuclear plants by turning off all 27 surveillance cameras belonging to the IAEA from several of their nuclear sites (Bob & Nahmias, Fatal blow to JCPOA if Iran doesn't restore access within 3-4 weeks - IAEA, 2022). In February 2023, Iran had enriched uranium to 84%. In August, it began the production of Caesium-137 (Tasnim News Agency, 2023).

With Iran's blatant hostility towards Israel and its already tarnished reputation, not much is holding it back from using its newly acquired nuclear weapons to ensure the destruction of Israel. Government officials in Iran have gone on record saying that the Iranian government will use any means necessary to remove the "Israeli threat" (The Times of Israel, 2023). Such an act could catalyze a third world war, so preventing it is paramount.

Further Reading

- https://www.britannica.com/technology/nuclear-weapon
- https://ourworldindata.org/nuclear-weapons
- https://www.history.com/topics/world-war-ii/atomic-bomb-history
- https://www.cfr.org/timeline/us-russia-nuclear-arms-control
- https://iranprimer.usip.org/resource/timeline-irans-nuclear-activities

Questions to Consider

Familiarizing Questions

- Does my country possess nuclear weapons? Do any of my country's neighbors possess nuclear weapons?
- Is my country a signatory of the NPT?

- Who are my country's allies?

CLASH-ORIENTED QUESTIONS

- What is my country's stance on the use of nuclear weapons?
- What is my country's stance on Iran and the JCPOA?
- What is my country's stance on the invasion of Ukraine?
- How can the international community mitigate the chances of nuclear warfare?
- Is complete nuclear disarmament, in all countries, a viable solution to the conflict?

BIBLIOGRAPHY

Anadolu Agency. (2019, April 11). *Iran doubles advanced centrifuges in blow-to-nuke deal*. Retrieved from Anadolu Agency: https://www.aa.com.tr/en/middle-east/iran-doubles-advanced-centrifuges-in-blow-to-nuke-deal/1635244

Baker, P. (2017, July 17). *Trump Recertifies Iran Nuclear Deal, but Only Reluctantly*. Retrieved from New York Times: https://www.nytimes.com/2017/07/17/us/politics/trump-iran-nuclear-deal-recertify.html

BBC News. (2020, September 5). *Iran's enriched uranium stockpile '10 times limit'*. Retrieved from BBC News: https://www.bbc.com/news/world-middle-east-54033441

Bob, Y. J. (2021, March 17). *Iran is using advanced uranium enrichment at a previously exploded facility*. Retrieved from The Jerusalem Post: https://www.jpost.com/breaking-news/iran-enriching-uranium-with-new-machine-at-underground-plant-iaea-662235

Bob, Y. J., & Nahmias, O. (2022, June 9). *The fatal blow to JCPOA if Iran doesn't restore access within 3-4 weeks - IAEA*. Retrieved from The Jerusalem Post: https://www.jpost.com/breaking-news/article-708998

Borda, A. Z. (2022, March 2). *Ukraine war: What is the Budapest Memorandum, and why has Russia's invasion torn it up?* Retrieved from The Conversation: Ukraine war: What is the Budapest Memorandum, and why has Russia's invasion torn it up?

Bronner, E., & Meyer, H. (2023, June 13). *Will Israel Attack Iran? What to Know About Netanyahu's Military Posturing*. Retrieved from Time: https://time.com/6286783/israel-iran-military-preparations/

Budjeryn, M., & Bunn, M. (2020, March). *Budapest Memorandum at 25: Between Past and Future*. Retrieved from Belfer Center for Science and International Affairs: https://www.belfercenter.org/publication/budapest-memorandum-25-between-past-and-future

Faulconbridge, G. (2022, November 21). *Explainer: Ukrainian nuclear plant shelled: Here's what we know*. Retrieved from Reuters: https://www.reuters.com/world/europe/close-call-ukrainian-nuclear-plant-2022-11-21/

Grieshaber, K. (2022, November 20). *Renewed shelling in Zaporizhzhia threatens the essential Ukrainian nuclear plant again*. Retrieved from PBS News Hour: https://www.pbs.org/newshour/world/renewed-shelling-in-zaporizhzhia-threatens-key-ukrainian-nuclear-plant-again

Hinshaw, D., & Parkinson, J. (2022, July 5). *Russian Army Turns Ukraine's Largest Nuclear Plant Into a Military Base*. Retrieved from The Wall Street Journal: https://www.wsj.com/articles/russian-army-turns-ukraines-largest-nuclear-plant-into-a-military-base-11657035694

History. (2022, November 9). *Atomic Bomb History*. Retrieved from History: https://www.history.com/topics/world-war-ii/atomic-bomb-history#nuclear-bombs-and-hydrogen-bombs

History. (2023, August 9). *Japan accepted Potsdam's terms and agreed to unconditional surrender*. Retrieved from History: https://www.history.com/this-day-in-history/japan-accepts-potsdam-terms-agrees-to-unconditional-surrender

Koshiw, I. (2022, September 11). *Putin and Macron trade blame over risk at Ukraine's Zaporizhzhia nuclear plant*. Retrieved from The Guardian: https://www.theguardian.com/world/2022/sep/11/reactor-ukraine-zaporizhzhia-nuclear-plant-shut-down-operator

Koshiw, I., & Rankin, J. (2022, August 8). *Attack on Ukraine nuclear plant 'suicidal,' says UN chief as he urges access to the site*. Retrieved from The Guardian:

https://www.theguardian.com/world/2022/aug/08/ukraine-nuclear-plant-attack-suicidal-un-chief-zaporizhzhia-russia

Kottasová, I. (2019, July 7). *Iran to breach uranium enrichment limits set by landmark nuclear deal*. Retrieved from CNN: https://edition.cnn.com/2019/07/07/middleeast/iran-nuclear-agreement-intl/index.html

Kristensen, H. (2023, March 31). *Status Of World Nuclear Forces*. Retrieved from FAS | Federation of American Scientists: https://fas.org/initiative/status-world-nuclear-forces/

Lester, L. (2019, June 3). *2017 North Korean nuclear test was order of magnitude larger than previous tests*. Retrieved from UC Santa Cruz: https://news.ucsc.edu/2019/06/nuclear-test.html

McEvoy, C. (2023, July 21). *J. Robert Oppenheimer*. Retrieved from Biography: https://www.biography.com/scientists/j-robert-oppenheimer#the-manhattan-project

Murphy, F. (2019, May 31). *Iran stays within the nuclear deal's primary limits while testing another*. Retrieved from Reuters: https://www.reuters.com/article/us-iran-nuclear-iaea/iran-stays-within-nuclear-deals-main-limits-while-testing-another-idUSKCN1T11PW

Murphy, F. (2021, May 11). *Iran has enriched uranium to up to 63% purity, IAEA says*. Retrieved from Reuters: https://www.reuters.com/world/middle-east/iran-has-enriched-uranium-up-63-purity-iaea-report-says-2021-05-11/

Murphy, F. (2022, March 16). *Iran defies Western powers with work on near-weapons-grade uranium*. Retrieved from Reuters: https://www.reuters.com/world/middle-east/iran-defies-western-powers-with-work-near-weapons-grade-uranium-2022-03-16/

Nikou, S. N. (2021, August 17). *Timeline of Iran's Nuclear Activities*. Retrieved from United States Institute of Peace: https://iranprimer.usip.org/resource/timeline-irans-nuclear-activities

Patel, J. (n.d.). *THE CHALLENGE OF CHORNOBYL FOR GLASNOST, PERESTROIKA, AND THE STABILITY OF THE SOVIET UNION*. Retrieved from Keele University: https://www.keele.ac.uk/extinction/controversy/chernobylandussr/#:~:text=Chernobyl%20shattered%20the%20foundation%20upon,was%20expected%20to%20save%20it.

Pennington, J., Stambaugh, A., & Lendon, B. (2023, July 31). *Medvedev says Russia could use nuclear weapons if Ukraine's fightback succeeds in the latest threat*. Retrieved from CNN: https://edition.cnn.com/2023/07/31/europe/medvedev-russia-nuclear-weapons-intl-hnk/index.html

Pleschberger, J. (2023, August 3). *What happens if Ukraine's Zaporizhzhia nuclear power plant blows up?* Retrieved from CGTN: https://newseu.cgtn.com/news/2023-08-03/What-happens-if-Ukraine-s-Zaporizhzhia-nuclear-power-plant-blows-up--1lWSkxYjQCQ/index.html#:~:text=The%20medical%20peace%20organization%20IPPNW,many%20parts%20of%20the%20world.

Robinson, K. (2023, June 21). *What Is the Iran Nuclear Deal?* Retrieved from Council of Foreign Relations: https://www.cfr.org/backgrounder/what-iran-nuclear-deal#chapter-title-0-5

Shugerman, E. (2017, October 13). *Iran nuclear deal: EU condemns Donald Trump's decision to decertify agreement*. Retrieved from Independent: https://www.independent.co.uk/news/world/politics/iran-nuclear-deal-trump-eu-federica-mogherini-netanyahu-israel-a7999556.html

Tasnim News Agency. (2023, August 27). *Iran Unveils New Nuclear Achievement*. Retrieved from Tasnim News Agency: https://www.tasnimnews.com/en/news/2023/08/27/2947739/iran-unveils-new-nuclear-achievement

The Chernobyl Forum. (2010, February 15). *Chornobyl's Legacy: Health, Environmental and Socio-Economic Impacts*. Retrieved from Wayback Machine: https://web.archive.org/web/20100215212227/http://www.iaea.org/Publications/Booklets/Chernobyl/chernobyl.pdf

The Times of Israel. (2023, April 18). *Iran threatens to destroy Tel Aviv and Haifa as Israel marks Holocaust Memorial Day*. Retrieved from The Times of Israel: https://www.timesofisrael.com/iran-threatens-to-destroy-tel-aviv-and-haifa-as-israel-marks-holocaust-memorial-day/

Tucker, M. (2023, April 7). *Ukraine's secret attempt to retake the Zaporizhzhia nuclear plant*. Retrieved from The Times: https://archive.md/20230410184810/https://www.thetimes.co.uk/article/ukrainian-zaporizhzhia-nuclear-power-plant-russia-putin-war-2023-fx82xz3xz#selection-749.0-752.0

U.S. Department of State. (n.d.). *The Collapse of the Soviet Union*. Retrieved from U.S. Department of State: https://history.state.gov/milestones/1989-1992/collapse-soviet-union

UK House of Lords. (2015, February 20). *The EU and Russia: before and beyond the crisis in Ukraine*. Retrieved from UK House of Lords: https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/115/115.pdf

UN. (n.d.). *ASSESSMENTS OF THE RADIATION EFFECTS FROM THE CHORNOBYL NUCLEAR REACTOR ACCIDENT*. Retrieved from Scientific Committee on the Effects of Atomic Radiation: https://www.unscear.org/unscear/en/areas-of-work/chernobyl.html.

United Nations. (n.d.). *Ending Nuclear Testing*. Retrieved from United Nations: https://www.un.org/en/observances/end-nuclear-tests-day/history#:~:text=The%20world%27s%20nuclear%20arsenals%20ballooned,1980s%20(United%20States%2023%2C000%20and

United States Institute of Peace. (2020, January 22). *Iran and the NPT*. Retrieved from United States Institue of Peace: https://iranprimer.usip.org/blog/2020/jan/22/iran-and-npt

Wagner, M., & Rocha, V. (2018, May 9). *Trump withdraws US from Iran nuclear deal*. Retrieved from CNN: https://edition.cnn.com/politics/live-news/trump-iran-nuclear-deal/

Watson, K. (2017, October 13). *Trump: W.H. "cannot and will not" certify Iran's compliance*. Retrieved from CBS News: https://www.cbsnews.com/news/trump-iran-nuclear-deal-announcement-as-it-happened/

World Nuclear Association. (2022, April). *Chernobyl Accident 1986*. Retrieved from World Nuclear Association: https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx

World Nuclear News. (2023, May 31). *Grossi says Zaporizhzhia principles 'step in the right direction.'* Retrieved from World Nuclear News: https://www.world-nuclear-news.org/Articles/Grossi-calls-Zaporizhzhia-principles-step-in-right

Yaffa, J. (2023, July 2023). *Inside the Wagner Group's Armed Uprising*. Retrieved from The New Yorker: https://www.newyorker.com/magazine/2023/08/07/inside-the-wagner-uprising

TOPIC B: CURBING THE GLOBAL THREAT OF CYBER-TERRORISM

What is Cyber-Terrorism? Cyberterrorism uses computer systems, networks, and digital technologies to conduct terrorist activities or provoke fear, panic, and societal disruption. It involves the deliberate and targeted exploitation of cyberspace to cause harm or damage to individuals, organizations, or governments.

THE CRITICAL CHARACTERISTICS OF CYBER-TERRORISM

Electronic attacks Cyber terrorists use various electronic attacks, such as hacking, malware distribution, and Distributed Denial of Service (DDoS) attacks, to compromise computer systems, disrupt critical infrastructure, and steal sensitive information.

Political or Ideological Motifs Cyber-terrorism is often motivated by political or ideological reasons, and perpetrators aim to advance their agendas, provoke social or political change, or instill fear and panic in the population.

Targets Cyber-terrorism targets many entities, including government agencies, financial institutions, utility companies, transportation systems, and other critical infrastructure. Its goal is to cause widespread disruption and chaos.

Mass Dissemination of Propaganda Cyber-terrorists may use the Internet and social media platforms to spread propaganda, recruit new members, and influence public opinion to further their cause.

Coordinated and Organized? Cyberterrorism activities are not only coordinated and organized, involving individuals or external groups with varying degrees of technical expertise in hacking and computer systems, but governments can often hire them to perform cyber attacks.

The consequences of cyberterrorism can be severe, leading to economic losses, compromised national security, public panic, and potential loss of life if critical systems such as healthcare or transportation are disrupted. For example, the following losses can be caused to businesses: theft of corporate and financial information, money, disruption or loss of business or contract, and disruption of trading.

THE RISE OF CYBER-TERRORISM IN THE MODERN WORLD

Cyber-terrorism is a Growing Concern in the Contemporary World.

Increased Connectivity: The world's growing interconnectedness through the Internet and digital technologies provided cyber-terrorists with more opportunities to exploit vulnerabilities in various systems—the more devices and critical infrastructure connected to the Internet, the more potential targets for cyberattacks.

The sophistication of Cyber-Attack Techniques Cyber-terrorists have increasingly employed advanced and sophisticated techniques to breach computer networks and launch disruptive attacks. These techniques include zero-day exploits, advanced persistent threats (APTs), and social engineering tactics. "Zero-day" relates to recently discovered security vulnerabilities that hackers can use to attack systems. It refers to the fact that the vendor or developer has just learned of the flaw, having "zero days" to fix it, for hackers exploited it before developers could address it.

Anonymity and Attribution Challenges The anonymous nature of the Internet makes it challenging to attribute cyber-attacks to specific individuals or groups, thereby providing cyber-terrorists with a level of protection from immediate consequences.

Political and ideological motivations drive political and Ideological Motivations for Cyberterrorism. Extremist groups and individuals seeking to promote their causes or ideologies have turned to cyberspace to amplify their messages and carry out attacks.

Low Entry Barriers Carrying out cyber-attacks only sometimes requires advanced technical skills. Various hacking tools and malware are readily available on the Dark Web, enabling individuals with limited expertise to launch cyber-attacks.

Global Impact Cyber-attacks can transcend borders and have a global impact. A single cyber-terrorist or small group can target entities and systems in multiple countries, magnifying the consequences of their actions.

Economic Incentives Cyberterrorism may also be driven by economic motives, such as disrupting competitors, causing stock market fluctuations, or stealing valuable intellectual property for financial gain.

State-Sponsored Cyber Terrorism: Some nations have been accused of sponsoring or supporting cyber terrorism to advance their geopolitical interests or disrupt their adversaries.

It is essential to recognize that while the risk of cyber-terrorism is a significant concern, most cyber threats continue to be attributed to cybercriminals seeking financial gain or causing disruption without explicitly aligning themselves with terrorist ideologies.

Governments, businesses, and individuals have invested in cybersecurity measures to protect against cyber-attacks and mitigate potential risks. However, the constantly evolving nature of technology and the increasing sophistication of cyber threats means that the challenge of combating cyber-terrorism remains ongoing.

Cyber Terrorism – How It Can Be A Threat

Cyberterrorism poses a significant threat to computers, networks, and lives in several ways—some examples of relevant attacks that have occurred in recent years are presented below.

Critical Infrastructure Disruption Cyber-terrorists can target critical infrastructure, such as power grids, water treatment facilities, transportation systems, and healthcare networks, causing widespread disruptions. For example, the NotPetya ransomware attack in 2017 affected numerous organizations worldwide, including critical infrastructure systems, leading to significant economic losses and disrupting essential services.

Financial System Attacks Cyber-attacks targeting financial institutions can lead to financial losses for individuals and organizations. In 2016, cybercriminals stole $81 million from Bangladesh Central Bank by exploiting vulnerabilities in their computer systems and conducting fraudulent money transfers.

Ransomware Attacks: Ransomware is malicious software that encrypts a victim's files, demanding a ransom payment to unlock them. NotPetya and WannaCry were notable ransomware attacks that caused widespread damage and affected individuals and organizations.

Internet of Things (IoT) Exploitation With the increasing adoption of IoT devices, cyber-terrorists can exploit the vulnerabilities in these devices to gain unauthorized access to networks or

carry out large-scale DDoS attacks. The 2016 Mirai botnet attack targeted IoT devices and disrupted significant websites and online services.

Social Engineering and Phishing Cyber-terrorists use social engineering techniques and phishing emails to trick individuals into revealing sensitive information or downloading malware. They can launch targeted and damaging attacks by gaining access to personal data or launching more targeted and destructive attacks.

Disinformation Campaigns Cyber-terrorists may engage in disinformation campaigns by spreading fake news and misinformation through social media and other online platforms. These campaigns aimed to manipulate public opinion and create social unrest or panic.

Attacks on Healthcare Systems Targeting healthcare systems can lead to life-threatening consequences. In 2017, the WannaCry ransomware attack affected several healthcare institutions, causing operational disruptions and delays in patient care.

Attacks on Government Institutions Governments and public institutions are also susceptible to cyberattacks. For instance, the 2014 cyberattack on Sony Pictures was attributed to North Korea, resulting in data breaches, business disruptions, and significant reputational damage.

Cyber-Physical Attacks Cyber-terrorism can be extended to physical attacks by exploiting vulnerabilities in interconnected systems. For example, an attack on an autonomous vehicle's control system can lead to life-threatening road situations.

IMPORTANCE OF DCS & SCADA SECURITY

DCS (Distributed Control System) and SCADA (Supervisory Control and Data Acquisition) systems monitor and control industrial processes. DCS systems are commonly used in manufacturing plants. They integrate with various third-party systems, support multiple communication protocols, and offer high-level programming and monitoring capabilities. DCS systems typically include features like HMI (Human-Machine Interface) and history for data storage and analysis.

Security for DCS/SCADA systems is critical due to their high connectivity, deployment in critical operational levels, and everyday use of Windows platforms, which attract attackers. Compromising

these systems offers attackers privileged access to internal processes and critical infrastructure, enabling disruptions.

Securing DCS/SCADA systems is essential because they are attractive targets for cyberattacks, with potential consequences for critical infrastructure. DCS and SCADA serve crucial roles in industrial processes but differ in their applications and capabilities.

We can predict a rise in AI-powered attacks bypassing traditional security measures. For example, AI can generate realistic phishing emails that can easily deceive users or create malware that can adapt its behavior to avoid detection by security software.

It is important to note that not all cyberattacks with significant consequences are necessarily classified as cyberterrorism, which is motivated explicitly by political or ideological reasons to induce fear, terror, or social and political change. Nevertheless, cyberattacks' potential risks and implications on computers, networks, and critical infrastructure concern governments, organizations, and individuals worldwide.

THE CURRENT SITUATION

Current cyber-terrorism and cyber threats are a significant concern. Artificial intelligence (AI) integration in various fields has increased its potential benefits and risks.

Possible Effects of AI on Cyber Threats Automated Cyber Attacks: AI can automate and enhance cyber-attacks, making them more sophisticated and efficient. It can speed up surveillance, vulnerability identification, and malware development, leading to more frequent and targeted attacks.

Advanced Phishing and Social Engineering AI-powered systems can analyze vast amounts of data to create personalized and convincing phishing emails or social engineering attempts, making it harder for individuals and organizations to detect such threats.

AI can create highly convincing deepfakes, which manipulate multimedia content (e.g., videos and audio) that can be used for disinformation campaigns, spreading propaganda, or impersonating individuals.

Enhanced Defense On the positive side, AI can also be used for cybersecurity defense. AI-driven security solutions can help detect and respond to cyber-attacks more effectively, improving incident response times and threat mitigation.

Current Threats Posed Regarding the Ukrainian war, it is essential to note that geopolitical conflicts can have cyber implications. Nation-states and state-sponsored groups may use cyber-attacks as part of their strategies to gather intelligence, disrupt an adversary's operations, or support their military campaigns. Cyber espionage, destructive attacks on critical infrastructure, and disinformation campaigns are potential threats that can be amplified during rising tensions and conflict.

Addressing Cyber-terrorism and Threats requires a multifaceted approach involving governments, international cooperation, private sector involvement, and individual awareness. The following are some broad strokes for possible solutions.

International Collaboration Cyber threats often transcend national borders, making international cooperation crucial. Nations should work together to share threat intelligence, establish norms of responsible behavior in cyberspace, and hold malicious actors accountable.

Public-Private Partnerships Collaboration between governments and private sector entities is essential to improve cyber defense capabilities. Information sharing, joint exercises, and collective efforts can help to identify and respond to threats more effectively.

Investment in Cybersecurity Governments and organizations should invest in robust cybersecurity measures, including AI-driven technologies, to detect, prevent, and mitigate cyberattacks. Regular security assessments, updates, and patches are vital for staying ahead of the evolving threats.

Awareness and Education Individuals need to be educated about cybersecurity best practices, including recognizing phishing attempts, protecting personal information, and ensuring the security of their devices and networks.

Regulation and Legislation Governments can enact and enforce cybersecurity regulations to hold organizations accountable for protecting sensitive data and critical infrastructure. Legislation can also deter cyber-criminals by imposing severe penalties for cyber-attack.

Resilience and Redundancy Critical infrastructure and systems should be designed considering resilience and redundancy. Regular backups, disaster recovery plans, and redundant systems can help mitigate the impact of cyberattacks.

Ethical AI Development As AI advances, it is essential to prioritize ethics in its development and usage. Ensuring that AI is used responsibly and not for malicious purposes can mitigate the potential risks.

It is necessary to recognize that the cyber threat landscape is constantly evolving and that no one-size-fits-all solution exists. A dynamic and adaptive approach, with ongoing research and collaboration among stakeholders, is crucial to addressing the challenges posed by cyber terrorism and threats effectively.

QUESTIONS TO CONSIDER

1. What are the most pressing global cyber threats the international community faces today, and what are their potential consequences?
2. How can international cooperation and collaboration be strengthened to effectively address and mitigate cyber threats globally?
3. What cyber-attacks occur in your country? How much does this topic affect you?
4. What cyber-defense mechanisms does your country have in place? How might they be improved via international cooperation?
5. How can member states balance the need for national security with the principles of privacy and individual freedoms when implementing cybersecurity measures?
6. What international legal frameworks and treaties exist to address cyber threats, and how can they be strengthened or expanded to address emerging challenges better?
7. How can member states promote cybersecurity capacity-building in developing countries to ensure they are not disproportionately affected by cyber threats?
8. What strategies can enhance public-private partnerships in cybersecurity and encourage the private sector to actively contribute to global cyber defense?
9. How can the international community deter state-sponsored cyber attacks and hold responsible nations accountable for their actions in cyberspace?
10. What initiatives and best practices can member states share to improve the resilience of critical infrastructure against cyber threats?

FURTHER READING

1. Ahmad et al., 2012] Ahmad, R., Yunos, Z., and Sahib, S. (2012). Understanding cyber terrorism: The grounded theory method applied. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, pages 323–328. IEEE.

2. Arora, M., Sharma, K. K., and Chouhan, S. (2014). Cybercrime Review

3. Ayres, N. and Maglaras, L. A. (2016). Cyberterrorism targets the general public through social media. Security and Communication Networks, 9(15):2864–2875.

4 Berinato, S. (2002). The truth about cyberterrorism. CIO, 15(11):66–72. Brickey, J. (2012). Defining cyberterrorism: capturing a broad range of activities in cyberspace. Combating Terrorism Centre at West Point, 5(8).

5. NATO Ponders Using Article Five for Cyber Attacks nationaldefensemagazine.org

6. https://www.ncsc.gov.uk/information/how-cyber-attacks-work

7.https://www.sciencedirect.com/science/article/pii/S2352484721007289

Ford Neil. IT Governance UK Blog.'List of Data Breaches and Cyber Attacks in 2023'. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

BIBLIOGRAPHY

1. Gable, K. A. (2010). Cyber-apocalypse now: Securing the internet against cyberterrorism and using universal jurisdiction as a deterrent. Vand. J. Transnat'l L., 43:57.

2.Gorge, M. (2007). Cyberterrorism: Hype or reality? Computer Fraud & Security, 2007(2):9–12.

3.Gross, M. L., Canetti, D., and Vashdi, D. R. (2016). Cyberterrorism affects psychological well-being, public confidence, and political attitudes. [Ince,] Ince, D. A dictionary of the internet.

4Jarvis, L. and Macdonald, S. (2015). What is cyberterrorism? findings from a survey of researchers. Terrorism and Political Violence, 27(4):657–678.

5.Keller, J. J. (2011). Cyberterrorism. J. J. Keller's Workplace Safety ez Explanations.

6. Kenney, M. (2015). Cyber-terrorism in a post-Stuxnet world. Orbis, 59(1):111–128.

7.Matusitz, J. (2008). Cyberterrorism: postmodern state of chaos. Information Security Journal: A Global Perspective, 17(4):179–187. [Mehan, 2014]

8.Mehan, J. (2014). CyberWar, CyberTerror, CyberCrime, and CyberActivism: An in-depth guide to the role of standards in the cybersecurity environment. IT Governance Publishing.

9.Recent Cyber Attacks & Data Breaches In 2023 https://purplesec.us › security insights 2023 **Cyber Attack** Newsletters · No More Ransomware Project · Maui Ransomware Attack · Conti Ransomware Attack · Kaseya Ransomware Attack · Saudi Aramco Data Breach ...Top Cyber Attacks In 2022 · Data Of More Than 200 Million...