deo
DEUTSCHE EVANGELISCHE OBERSCHULE KAIRO
seit 1873

Generalversammlung
Handbuch

Inhalt

Die Generalversammlung

Die Generalversammlung ist das höchste Gremium der Vereinten Nationen (UN) und setzt sich aus Vertretern aller 193 UN-Mitgliedsstaaten zusammen. Die Generalversammlung hat das Mandat, über internationale Fragen zu beraten und Empfehlungen zu geben, um Frieden, Sicherheit und das Wohlergehen der Menschen weltweit zu fördern.

Die Generalversammlung trifft sich einmal im Jahr zu einer ordentlichen Sitzung, die im September beginnt und im folgenden Jahr im September endet. Während dieser Sitzungen kommen die Vertreter der Mitgliedsstaaten zusammen, um über eine Vielzahl von Themen zu diskutieren, einschließlich Frieden und Sicherheit, Entwicklung, Menschenrechte, Umweltschutz und internationale Zusammenarbeit.

Zu den wichtigsten Aufgaben der Generalversammlung gehört die Verabschiedung von Resolutionen, die Empfehlungen zu verschiedenen Themenbereichen enthalten. Diese Resolutionen sind nicht rechtlich bindend, sondern haben eher den Charakter von politischen Erklärungen oder Absichtserklärungen.

Die Generalversammlung wählt auch die nicht-ständigen Mitglieder des Sicherheitsrates und die Mitglieder des Wirtschafts- und Sozialrates sowie des Internationalen Gerichtshofs. Darüber hinaus wählt die Generalversammlung den Generalsekretär der Vereinten Nationen auf Vorschlag des Sicherheitsrates.

Die Generalversammlung spielt eine wichtige Rolle bei der Förderung des Dialogs und der Zusammenarbeit zwischen den Mitgliedsstaaten und bei der Entwicklung von Politiken und Programmen zur Förderung des Friedens, der Sicherheit und des Wohlergehens der Menschen weltweit.

Cyberkrieg und Regierungshacking

Einführung

Der Krieg hat sich im Laufe der Jahrhunderte von primitiven Taktiken zu den fortschrittlichsten Technologien, die wir heute besitzen, entwickelt. Eine der gefährlichsten sowie auch bemerkenswertesten neuen Kriegsformen ist der Cyberkrieg. Unter Cyberkrieg versteht man eine Form der Kriegsführung, die im Cyberspace stattfindet, d. h. in Computern und den Netzwerken, die sie miteinander verbinden. Staaten, die diese Art von Feindseligkeit ausüben, versuchen die Infrastrukturen ihrer Gegner zu zerstören. Bei Cyberangriffen spricht man meistens auch von Regierungshacking. Dazu gehört unter anderem der Diebstahl von vertraulichen Informationen, die Manipulation von Daten, sowie auch die Sabotage von kritischen Computersystemen.
Aufgrund der zunehmenden Digitalisierung sind Staaten und Organisationen in den letzten Jahren immer verwundbarer für Cyberangriffe geworden.
Das Hauptproblem bei Cyberangriffen ist, dass jeder mit den erforderlichen Fähigkeiten und einer Internetverbindung ein potenzieller „Cyber-Terrorist" sein kann, und der Angriff könnte von überall auf dem Planeten aus erfolgen. Cyberangriffe können enorme Schäden verursachen, nicht nur für Individuen oder Gruppen, sondern auch für ganze Länder. Ein weiteres Problem ist, dass die Wirtschaft durch Cyberangriffe erleiden könnte. Es wird geschätzt, dass weltweit 445 Milliarden Dollar Schaden durch Cyberangriffe verursacht wurden, was 1 % des weltweiten Einkommens entspricht.

Abgesehen von Angriffen auf die Cyberinfrastruktur des Landes, Wirtschaft und Regierungen steigt die Gefahr von Cyberangriffen dramatisch an, wenn es um den Militär der Welt geht. Moderne militärische Geheimdienste umfassen die Integration von modernsten Computern und Elektronik, die Militärs auf der ganzen Welt anfällig für Cyberangriffe machen.
Da die Welt immer stärker vernetzt wird, sind wir immer mehr von Technologie abhängig. Dies erhöht die Gefahr von Cyberangriffen. Es ist daher von entscheidender Bedeutung, dass Organisationen und Regierungen ständig ihre Verteidigungsprogramme aktualisieren. Cyberangriffe stellen eine ernsthafte Bedrohung für die Sicherheit und Stabilität der Gesellschaft dar und erfordern eine ständige Überwachung der Verteidigungsmaßnahmen. Es liegt in der Verantwortung der Vereinten Nationen, dieses Problem anzugehen und eine sicherere Welt zu schaffen.

Hintergrund und Fakten

Cyberkrieg ist eine Form der Kriegsführung, die sich ausschließlich auf digitale Strategien stützt. Dabei versucht ein Staat, in die Computernetzwerke eines anderen Staates einzudringen, um dort Schaden anzurichten. Die Methoden des Cyberkriegs umfassen:
- Online-Spionage und das Ausnutzen von Sicherheitslücken, um an Informationen zu gelangen (z.B. durch den Einsatz von Schadsoftware)
- Sabotageakte, bei denen das Internet genutzt wird, um die Online-Kommunikationssysteme (z.B. des Militärs) eines Landes zu stören oder zu unterbrechen
- Angriffe auf SCADA- (Supervisory Control and Data Acquisition) oder NCI- (National Critical Infrastructure) Netzwerke, die für die Steuerung von kritischen Infrastrukturen wie Energieversorgung oder Verkehr zuständig sind

CYBERKRIEG UND REGIERUNGSHACKING

Cyberkrieg ist eine neue Form der Kriegsführung, die durch die Entwicklung moderner Technologien ermöglicht wurde. Nach Land, Wasser, Luft und Weltraum wird der virtuelle Raum (Cyberspace) zur fünften Dimension, in der Kriege geführt werden können. Ein Beispiel für einen Cyberkrieg ist der russische Angriff auf die Ukraine im Jahr 2022, der nicht nur mit konventionellen Waffen, sondern auch mit digitalen Mitteln stattfand. Dabei waren sowohl staatliche Akteure als auch mehr als 40 nicht-staatliche Cyber-Gruppen und Kollektive beteiligt.
Regierungshacking bezeichnet das Eindringen in Computernetzwerke durch staatliche Akteure wie Nachrichtendienste und Militär. Dabei werden Daten ausspioniert, sabotiert oder manipuliert. Cyberkrieg unterscheidet sich von Cyberkriminalität oder Cyberterrorismus, die von nicht-staatlichen Akteuren ausgehen.
Die Länder, die am meisten von Cyberangriffen betroffen sind, variieren je nach Art des Angriffs und der Quelle der Information. Laut dem Microsoft Digital Defense Report 2021 sind die USA das am stärksten betroffene Land, gefolgt von China, Japan Deutschland und den Vereinigten Arabischen Emiraten. In Bezug auf die finanziellen Schäden durch Internetkriminalität liegt China vorn, gefolgt von Brasilien. Es ist wichtig zu beachten, dass Cyberangriffe ein globales Problem sind und jedes Land betroffen sein kann. Deshalb ist es wichtig, dass jedes Land Maßnahmen ergreift, um seine Cybersicherheit zu erhöhen und sich gegen mögliche Angriffe zu schützen.

Aktuelles

In den letzten Jahren hat die Zahl der Cyberangriffe auf Staaten und staatliche Einrichtungen stetig zugenommen.
Der Ransomware-Angriff auf die Colonial Pipeline ist vielleicht einer der letzten Angriffe, der die Komplexität, die Raffinesse und das Ausmaß der Auswirkungen von Cyberangriffen zeigt. Die Colonial Pipeline ist das größte Pipelinesystem für raffinierte Ölprodukte in den USA. Die aus drei Röhren bestehende Pipeline ist 5.500 Meilen lang und kann 3 Millionen Barrel Kraftstoff pro Tag zwischen Texas und New York befördern. Im Jahr 2021 wurden die Computersysteme, die das Abrechnungssystem der Pipeline betreiben, mit einer Ransomware infiziert, die 100 Gigabyte an Daten stahl und das Unternehmen zwang, den gesamten Betrieb einzustellen, um weitere Angriffe auf gefährdete Teile des Systems zu verhindern. Unter Aufsicht des FBI zahlte das Unternehmen ein Lösegeld von 75 Bitcoins, was damals 4,4 Millionen Dollar entsprach, und konnte den Betrieb nach zwei Wochen wieder aufnehmen.

Die Abschaltung führte jedoch zu Treibstoffengpässen an Flughäfen, die sich auf die Flugpläne auswirkten und zu Panikkäufen an Tankstellen führten. Mehrere Bundesstaaten meldeten Engpässe, wobei die Gebiete im Südosten der USA am stärksten betroffen waren. Infolgedessen stiegen die durchschnittlichen Kraftstoffpreise auf den höchsten Stand seit 2014 und überstiegen die Marke von 3 US-Dollar pro Gallone.
Die Ursache, wie dieser Angriff möglich war, ist einfach und zeigt, wie leicht Cyberangriffe sind und wie anfällig viele Computersysteme sind, auf die wir uns stark verlassen. Ein Mitarbeiter hat das Passwort eines VPN, das für den Zugang zu den Computersystemen des Unternehmens verwendet wird, an anderer Stelle nochmal verwendet, und die Hacker, die sich DarkSide nennen, haben sich Zugang dazu verschafft.
DarkSide ist offiziell mit keinem Staat verbunden. Es wird vermutet, dass sie in Osteuropa oder Russland operieren, was viele dazu veranlasste, Russland zu beschuldigen, diesen Angriff zu sponsern, was von der russischen Botschaft in den USA sofort verneint wurde.
Dieser Vorfall zeigt, dass das Thema eine ganz neue Ebene der Komplexität erreicht hat. In einem normalen physischen Krieg ist es viel einfacher festzustellen, woher der Angriff kommt, wer ihn unterstützt, ihre Motivation, dafür vorzubereiten und den Verursacher zur Rechenschaft zu ziehen. Bei Cyberangriffen könnten die kritischen Systeme eines ganzen Landes sabotiert werden, ohne dass man jemals erfährt, wer dahinter steckt.
Ein weiteres Problem ist die leichte Zugänglichkeit. In unserem Fall könnte es sich bei DarkSide um eine Gruppe normaler Menschen handeln, die keinen Zugang zu besonderen Ressourcen haben und dennoch in der Lage waren, all dies zu tun. Im Jahr 1999 gelang es einem 15-Jährigen namens Jonathan James, Daten einer Abteilung der Nasa abzufangen.
Betrachtet man die häufigsten staatlichen Täter und Opfer von Cyberangriffen in der Welt, so werden in der Regel China, Russland und die USA genannt. Dies ist nicht unerwartet, da diese drei Staaten seit langem miteinander verfeindet sind und über ein breites Netz an Ressourcen verfügen.

Als Reaktion auf die Zunahme von Cyberangriffen und die beteiligten großen Länder hat die UN eine Reihe von Initiativen gestartet, um die staatlichen Mitglieder und privaten Organisationen besser vorzubereiten. Das UNOCT/UNCCT Cybersecurity and New Technologies programme zielt darauf ab, die Fähigkeiten der Mitgliedstaaten und privater Organisationen zur Verhinderung von Cyberangriffen auf kritische Infrastrukturen zu verbessern. Das Programm zielt auch darauf ab, die Auswirkungen von Cyberangriffen zu verringern und die betroffenen Systeme wiederherzustellen, falls es zu solchen Angriffen kommt.
Der Global Cybersecurity Index (GCI) bewertet das Engagement der Länder im Bereich Cybersicherheit auf globaler Ebene und fördert das Bewusstsein für dessen Bedeutung. Es werden fünf Säulen betrachtet: Rechtliche Maßnahmen, Technische Maßnahmen, Organisatorische Maßnahmen, Kapazitätsentwicklung und Zusammenarbeit. Diese ergeben eine Gesamtbewertung, die das Entwicklungsniveau eines Landes in Sachen Cybersicherheit widerspiegelt. Der GCI ermöglicht Vergleiche, identifiziert wichtige Bereiche und fördert die internationale Zusammenarbeit zur effektiven Bewältigung der Herausforderungen im Bereich Cybersicherheit.

Wichtige Begriffe

Cyberkrieg: eine Form der Kriegsführung, die im Cyberspace stattfindet
Spionage: Das Eindringen in fremde Computersysteme zum Zwecke der Informationsgewinnung
Defacement: Veränderungen am Inhalt einer Website, um u. a. Propaganda zu schalten
C4ISR: Command, Control, Computers, Communications, Information for intelligence, surveillance, and reconnaissance
Cyberattacken: Angriffe auf Computer, Informationen, Netzwerke und computerabhängige Systeme
Cyberterrorismus: Attacke mit terroristischen Hintergrund

Steigende Selbstmordrate

Einführung

Selbstmord ist ein großes Gesundheitsproblem, welches jedes Jahr weltweit rund 800 000 Menschenleben fordert. Hierbei ist Selbstmord, definiert als absichtliche Selbstverursachung des eigenen Todes, die zweithäufigste Todesursache bei Jugendlichen. Sie macht 57 % aller gewaltsamen Todesfälle und etwa 1,5 % der Gesamtsterblichkeit aus - somit liegen die Rate höher als bei Malaria oder Brustkrebs (Weltgesundheitsorganisation 2019).
Die Auswirkungen auf Familien und Gemeinschaften sind weitreichend: Trauer, Stigmatisierung und der anschließende Anstieg psychiatrischer Erkrankungen und Suizidraten wirken über Generationen hinweg nach.
Die globale akademische Auseinandersetung mit der Thematik des Selbstmordes hat sich von einer individuellen Perspektive weiterentwickelt; anstatt Selbstmord ausschließlich auf die persönlichen Probleme des Individuums ruckzuschließen, untersuchen die Soziologie, Medizin, Philosophie und Psychologie unter anderen welche gesellschaftlichen und soziodemorafischen Ursachen und Muster, welche den Selbstmordraten unterliegen können. Was kann eine Person dazu bewegen, absichtlich den eigenen Tod zu verursachen?
Was die demografischen Risikofaktoren betrifft, so begehen mehr Männer als Frauen Selbstmord, während mehr Frauen als Männer einen Selbstmordversuch unternehmen. Weiterhin nimmt das Suizidrisiko mit dem Alter zu; bei Männern erreicht das Risiko im Alter von 45 Jahren und bei Frauen im Alter von 55 Jahren seinen Höhepunkt. Dennoch nehmen die Selbstmordraten unter jungen Menschen, insbesondere in der Altersgruppe der 15- bis 24-Jährigen, zu. Außerdem wirkt die Ehe als Schutzfaktor gegen Selbstmord; Selbstmordrate scheinen bei verheirateten Personen niedriger zu sein als bei etwa geschiedenen Personen.
Auch die eigene psychische Vorgeschichte spielt eine wichtige Rolle: Die Wahrscheinlichkeit, dass jemand Selbstmord begeht, steigt erheblich, wenn bei der Person eine Depression oder andere psychische Krankheiten diagnostiziert wurden. Darüber hinaus besteht ein eindeutiger Zusammenhang zwischen erhöhten Selbstmordraten und niedrigem sozialen Status, wobei Personen mit weniger finanziellen Mitteln und Ressourcen eher zum Selbstmord neigen. Hier wird die Vermeidbarkeit des Suizidproblems besonders hervorgehoben. Die Vereinigten Nationen sind somit verpflichtet das Problem anzugehen.

Hintergrund und Fakten

Laut Statistischem Bundesamt starben im Jahr 2021 in Deutschland insgesamt 9.215 Personen durch Selbstmord. Dies entspricht über 25 Personen pro Tag. Männer nahmen sich deutlich häufiger das Leben als Frauen, rund 75 % der Selbsttötungen wurden von Männernbegangen. Das durchschnittliche Alter von Männern lag zum Zeitpunkt des Selbstmords bei 59,3 Jahren. Frauen waren im Durchschnitt 61 Jahre alt.
Im Vergleich zum Vorjahr (9.206 Selbstmorde) ist ein minimaler Anstieg zu verzeichnen. Insgesamt ist die Zahl der Selbstmord jedoch in den vergangenen Jahren deutlich zurückgegangen: 1980 nahmen sich beispielsweise noch rund 50 Personen pro Tag das Leben.
Laut Schätzungen der Weltgesundheitsorganisation (WHO) begehen jährlich weltweit mehr als 700.000 Menschen Selbstmord. Die Selbstmordrate variiert jedoch von Land zu Land. Im Vergleich der G7-Staaten wiesen die USA die höchste Selbstmordrate auf (16,1), während Italien die wenigsten Selbsttötungen je 100.000 Personen aufwies (6,7). Betrachtet man die BRICS-Staaten, verzeichnete Brasilien (6,9) die niedrigste Rate.
In Deutschland ist die absichtliche Selbstvergiftung mit Medikamenten nach dem Erhängen gegenwärtig die zweithäufigste Selbstmordmethode aller tödlich endenden Selbstmordhandlungen. Die Zahl aller auf diese Weise durchgeführten Selbsdmorte liegt in den letzten Jahren kontinuierlich bei über 1000 Fällen pro Jahr.
Im Jahr 2021 haben sich deutschlandweit 9.215 Menschen das Leben genommen. Ähnlich den Vorjahren war mit rund 44 Prozent bzw. 4.035 Selbsttötungen Erhängen die mit Abstand verbreitetste Methode; gefolgt von Sturz in die Tiefe mit 897 Selbstmorden und Arzneimittel- bzw. Drogenmissbrauch mit 820 Selbstmorden.
Es gibt viele Faktoren, die zu einem Anstieg der Selbstmordraten beitragen können. Einige Experten haben auf eine erhöhte Isolation unter den Menschen hingewiesen, sowie auf wirtschaftliche Faktoren und einen Anstieg von psychischen Erkrankungen. Andere haben auf den Aufstieg der Technologie hingewiesen, die wichtige persönliche Interaktionen ersetzt hat (obwohl manche argumentieren, dass Technologie tatsächlich Einsamkeit verringert). Es ist jedoch schwierig, allgemeine Aussagen über Selbstmord zu treffen.

Aktuelles

Weltweit sterben jedes Jahr 800.000 Menschen durch Selbstmord - alle 40 Sekunden einer -, was den Selbstmord zur zweithäufigsten Todesursache bei jungen Menschen (15 bis 29 Jahre) macht.
Jedes Jahr sterben mehr Menschen durch Selbstmord als durch HIV, Malaria oder Brustkrebs oder durch Krieg und Mord, was es zu einem Problem macht, das dringend gelöst werden muss. Die SDGs wurden von der UN im September 2015 angenommen und sind auf das Jahr 2030 ausgerichtet. Ziel 3 der SDGs lautet lautet: Ein gesundes Leben zu ermöglichen und das Wohlergehen alle Menschen in jedem Alter zu fördern. Ziel 3.4 lautet: Bis 2030 die vorzeitige Sterblichkeit an nicht übertragbaren Krankheiten durch Prävention und Behandlung um ein Drittel senken und die psychische Gesundheit und das Wohlbefinden fördern. Innerhalb des Ziels 3.4 ist die Selbstmordrate ein Indikator (3.4.2).
Aufgrund der letzten Ereignisse, insbesondere der Covid-19-Pandemie, haben die mit Selbstmord verbundenen Risikofaktoren wie Arbeitsplatzverlust, Trauma oder Missbrauch, psychische Störungen und Hindernisse beim Zugang zur Gesundheitsversorgung für viele Menschen während und nach der Krise erheblich zugenommen. Im Jahr 2020 ist die Häufigkeit von Anxiety und Depressionen weltweit um 25 Prozent zugenommen.

Laut WHO ist die Welt nicht auf dem Weg, die für 2030 geplante Verringerung des Selbstmords 0zu erreichen. Aus diesem Grund hat die WHO das LIVE LIFE-Handbuch veröffentlicht, das den Ansatz der WHO zur Prävention von Selbstmord sowohl auf regionaler als auch auf individueller Ebene darstellt. Die wichtigsten Säulen sind folgende:

• Situation verstehen: Hintergrundinformationen und Daten zu Selbstmord sammeln, um Präventionsmaßnahmen zu planen.
• Gemeinsam arbeiten: Unterschiedliche Gruppen müssen zusammenarbeiten, um Selbstmordrisiken gemeinsam anzugehen.
• Aufklärung: Die Öffentlichkeit über Selbstmord als Gesundheitsproblem informieren und zum Handeln aufrufen.
• Schulung und Unterstützung: Menschen lernen, wie sie Selbstmord verhindern und Unterstützung bieten können.
• Finanzierung: Herausforderungen bei der Beschaffung von Geldern für Präventionsmaßnahmen bewältigen.
• Überwachung: Daten zu Selbstmord sammeln, um Präventionsmaßnahmen zu leiten.
• Evaluation: Überprüfen, ob Präventionsmaßnahmen wirksam sind und Verbesserungen vornehmen. Die im Leitfaden beschriebenen Maßnahmen sind:
• Begrenzung des Zugangs zu Selbstmordmitteln
• Interaktion mit den Medien, um eine verantwortungsvolle Berichterstattung über Selbstmord zuerreichen
• Förderung der sozio-emotionalen Lebenskompetenzen von Jugendlichen
• Frühzeitige Identifizierung, Bewertung, Betreuung und Nachsorge von Personen, die die von Selbstmordverhalten betroffen sind

Wichtige Begriffe

Freitod: Die Idee, das Selbsttötung ein frei gewähltes Verhalten sei.
Suizid: stammt aus dem Lateinischen suicidium. Das Wort setzt sich zusammen aus sui = sich oder selbst und dem Wort caedere = schlagen, töten.
Assistierter Suizid: Suizid mit Unterstützung durch eine andere Person