



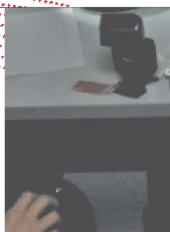
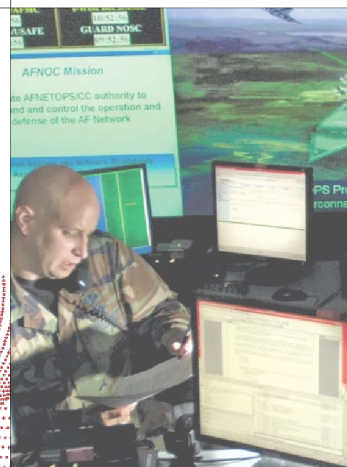
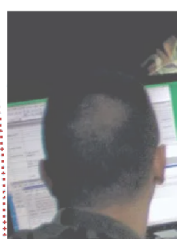
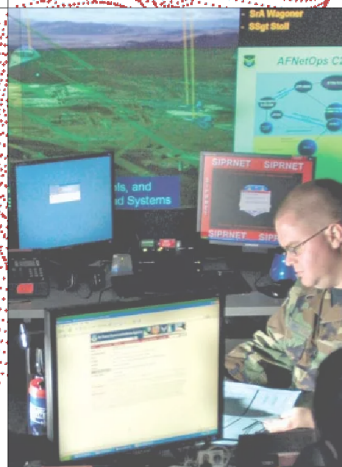
DISEC

General Assemblies

www.gtmun.gatech.edu

Topic 1
The responsibility of the
international community to
intervene in international
drug trade

Topic 2
Developing civil and social
infrastructure to protect against
cyberattacks & cyberwarfare



October 5-6, 2026

Committee
Disarmament and
International Security
Committee

Georgia Tech
Model United Nations

Bridging technology and diplomacy.



Georgia Tech
Model United Nations

Table of Contents

Letter from the Secretary General	5
Position Paper Rubric	6
Introduction to Committee	8
Disclaimer	8
Topic 1	9
Introduction	11
History	12
Current Developments	15
International Community Response	16
Case Studies	17
The Golden Triangle	17
Eastern and Southern Africa	19
The Mexican Drug War	21
Maritime routes	22
Directives / QARMAs	24
Topic 2	25
Introduction	28
History	29
Current Developments	33
Directives / QARMAs	37
Bibliography	38

#GTMUN2026



Letter from the Secretary General



Esteemed delegates,

My name is Henry Bui, your Secretary General for the 2026 edition of the Georgia Tech Model United Nations Conference, also lovingly known as GTMUN. As your Secretary General, I would like to give you all a warm welcome as you begin your journey this conference cycle.

Every year at GTMUN, we see hundreds of you delegates spend hours speaking about your ideas, deliberating with others about the efficacy of solutions, and collaborating with compatriots to draft extensive resolutions. It is always impressive to see each delegate's ability to tackle these very significant issues affecting the real world today, proposing novel solutions, creatively applying international policy, and synthesizing resolutions that solve these urgent questions comprehensively and on a global scale.

I am especially excited to see everything you all will achieve this October. With over 1,000 delegates attending, this will be the largest GTMUN to date, and with it, we are bringing you 18 diverse committees to further test your abilities. Each committee has been carefully crafted to open unique perspectives and to allow each delegate to apply their skills in possibly new, unique ways. I hope that in the midst of being lost in deep research rabbit holes and hours of debate in each session, you all are satisfactorily challenged and that you all leave with joy and excitement in the work you accomplish.

Outside of the Scheller building where you will debate for two days, you will find that many of the skills you have used will be applicable to other aspects of your professional career: your ability to speak publicly, to improvise and adapt, and to act diplomatically. As a computer science student and teaching assistant, I have found that my experience in Model UN has been some of my most valuable. It has taught me to be confident in what I say, and it has taught me how to work with people with all different kinds of backgrounds and perspectives. One of our core values at Georgia Tech is that we thrive on diversity, and that is something that shines strongly at GTMUN.

As you prepare for committee, I want you to remember the most important thing you should get out of GTMUN—even more important than demonstrating your abilities or honing your skills for your professional career—is having fun. Not every speech has to be perfect, and not every unmoderated caucus has to go your way! Take the opportunity to try eccentric things in your speeches and diplomatic approach, and take the opportunity to meet new people. Do not forget that you are surrounded by many others who have similar goals, aspirations, and interests as you do! You might find a future close friend. Though competing is quite fulfilling (and the prospect of awarding is exciting), it can also be very stressful, so it is critical to find joy in what you are doing.

Once again, we, the GTMUN Secretariat, are excited to see everything you will achieve.

Good luck & have fun,

A stylized, handwritten signature in black ink that reads "HBui". The signature is fluid and cursive, with the letters "H" and "B" being particularly prominent.

Henry Bui

Secretary General of GTMUN 2026



What is a *Position Paper*?

A position paper is a paper which describes how a country intends to address the topics of the committee, detailing tangible solutions to committee issues and connection to the country's policies. A position paper should contain details for each topic that will be addressed by the committee.

Formatting Requirements

- 12-point font, double spaces Times New Roman
- 1-2 pages per topic (excluding Works Cited page)
- A Works Cited page with citations in MLA format
- Files submitted in .pdf format with title "GTMUN26_COMMITTEE_COUNTRY.pdf"
- e.g., "GTMUN26_DISEC_Germany.pdf" or "GTMUN26_UNEP_United_States.pdf"

Start Each Topic Page With

- Committee: [Name of committee]
- Delegation: [Name of delegation]
- Topic: [Topic name/decription]

Position Paper Rubric

In order to be eligible for awards, delegates must submit a position paper and receive a score of at least 12/20 (for single-topic committees) or 24/40 (for double-topic committees). Refer to the next page for the exact scoring guidelines.

Our AI Policy

Delegates are expected to be drafting documents during the span of the conference using their own thoughts and ideas. As such, GTMUN **does not permit** plagiarism, pre-writing, or the use of generative AI during conferences.

- Plagiarism is the act of using another individual's work or writing and passing it as one's own without proper citation or credit. This includes writing from other delegates in the committee or from online sources.
- Pre-writing is the act of writing material for in-conference documents (e.g., working papers, draft resolutions, crisis directives) ahead of the conference. While doing prior research and bringing research notes is permitted (and encouraged), these notes should not contain text that is intended to be directly copied and pasted into a document. Suspicion of pre-writing is subject to the chair's discretion.
- Generative AI tools (such as ChatGPT, Claude, and Gemini) cannot be used to partially or wholly write a conference document. GTMUN recognizes the rapidly evolving landscape of artificial intelligence engines as a tool for research. Though discouraged, GTMUN accepts the use of such tools to locate resources and brainstorm starting solutions. However, generative AI must not be used to generate content for the conference, such as in-conference documents and position papers. GTMUN encourages the development of creative, unique solutions in committee and knows delegates are more than capable of producing such ideas without relying on generative AI.

Delegates that violate the writing policy will face consequences that may include disqualification from awards.

	Great (5)	Good (4)	Adequate (3)	Poor (1)
Background	- Detailed description of the topic (including dates and stakeholders) - Several facts and statistics - Discusses many relevant UN documents and resolutions	- Basic description of topic (including some dates and stakeholders) - Some facts and statistics - Discusses some relevant UN documents and resolutions	- Minimal description of topic (with no or few dates and stakeholders) - Few facts and statistics - Misses some key relevant UN documents and resolutions	- Unclear or incorrect description of topic - Incorrect or missing facts or statistics - No mention of relevant UN documents and resolutions
Policy	- Country's detailed history with issue - Detailed present position (or a strongly-defended inferred position) of country - Several references to statements from appropriate officials or documents - Several facts and statistics	- Country's basic history with issue - Present position (or reasonable inferred position) of country - Some references to statements from appropriate officials or documents - Some facts and statistics	- Sparsely describes country's history with issue - Present position (or basic inferred position) of country - Few references to statements from appropriate officials and documents - Few facts and statistics	- Incorrect or missing description of country's history with issue - Incorrect present position (or unreasonably inferred position) of country - No references to statements from appropriate officials and documents - Incorrect or missing facts and statistics
Solutions	- Detailed personal objectives - Proposes well-supported potential solutions - Identifies delegates to work with and provides strong reasoning for selections - Actionable, reasonable solutions which are within the scope of the committee	- Expresses personal objectives - Proposes reasonable potential solutions - Identifies delegates to work with and provides reasonable justification for selections - Actionable solutions within the scope of committee	- States personal objective - Proposes potential solutions - Identifies delegates to work with - Actionable solutions	- No proposed goals or plans - No potential collaborators mentioned - Implausible or missing actionable solutions
Mechanics	- No grammar, spelling, or punctuation errors - Numerous and diverse citations from appropriate sources	- Few grammar, spelling, or punctuation errors - Citations from appropriate sources	- Some grammar, spelling, or punctuation mistakes - One or two citations from inappropriate sources	- Many grammar, spelling, or punctuation mistakes - No citations from appropriate sources

Introduction to Committee

Since 1945, the General Assembly has allocated to its Disarmament and International Security Committee, or DISEC, agenda items relating to disarmament, global challenges, and threats to peace that affect the international community. As the First Committee, DISEC meets annually to make recommendations and consider the general principles of cooperation in the maintenance of international peace and security. DISEC cannot directly mandate armed interventions or sanctions, nor can it enforce state actions; however, it can draft resolutions and make diplomatic recommendations to UN member states and the Security Council. Delegates in this committee are tasked with drafting resolutions that thoughtfully balance state sovereignty while addressing emerging security challenges.

Disclaimer

Model United Nations provides an opportunity for delegates to engage diplomatically with topics of global importance and explore possibilities for conflict resolution in a meaningful way. Many of the topics at hand may involve sensitive or controversial subject matter. We ask delegates to be respectful and professional when engaging with their committee and communicating with fellow delegates and GTMUN Conference staff. The content warning below is meant to warn you of potentially controversial topics that are present in the content of this background guide, as well as content that may appear in other aspects of the committee (e.g. debate, speeches, directives), so that you can prepare yourself before reading this background guide and participating in the committee. At GTMUN, we take equity violations very seriously and require delegates to fully comply with our equity guidelines. Failure to do so will result in an immediate disqualification from awards, and you may be asked to leave the conference. Please remain respectful in committee, and avoid overgeneralizations as well as take into account individual differences and contexts during your speeches. If you have any questions regarding our equity guidelines, we encourage you to contact one of our staff members. If, because of this committee's content warning, you have any questions or concerns, please feel free to reach out to our staff via email at gtmunconference@gmail.com.



Topic 01

**The responsibility of the
international community
to intervene in international
drug trade**

Key Terms and Acronyms

Illicit	Forbidden by law, rules, or custom
Narcotic	A drug or other substance that affects mood or behavior and is consumed for nonmedical purposes
Drug Trafficking	Illicit trade of any drug legally defined as controlled substances
Cartel	A group of similar independent companies that join together to control prices and limit competition
Psychoactive Substances	Drugs that when taken in or administered into one's system, affect mental processes
Synthetic Drug	Drugs that are chemically created in a lab with the intention to mimic the effects of existing illicit drugs
Peripheral Countries	Nations that are less economically developed, typically characterized by weak infrastructure, low industrialization and a reliance on agriculture or raw material exports
Core Countries	Nations that are the most economically developed and have significant control over the global markets, high levels of infrastructure, and high levels of industrialization
Psychotropic Substances	Refers to therapeutic, psychiatric drugs (e.g., antipsychotics, antidepressants, sedatives) designed to treat mental health conditions

Introduction

From the chewing of coca leaves in the early Incan Empire to the consumption of opium, even to one's morning coffee, psychoactive substances, defined by the United Nations as chemical substances that affect the normal functioning of the body or brain, have intertwined with the biological and cultural development of humanity (1971 Convention on Psychotropic Substances, 1975). What were once crops used by small farmholders who cultivated resources like coca, opium poppies, and cannabis for medicinal, spiritual, and healing properties in their local communities have transformed into the international drug trade. Production and consumption have become widely separated, and the scale of trade, with all its impacts, stretches far beyond the communities they once began in. Over time, this transformation has resulted in the expansion of a global industry worth hundreds of billions of dollars annually (Klenowski, 2023).

In the modern era, globalization and increasingly efficient distribution networks have intensified cross-border flow, enabling substances to reach markets farther and linking the trade to organized crime groups, institutional instability, public health crises, and widespread human rights violations. As of 2024, the United Nations Office on Drugs and Crime (UNODC) estimates that there are nearly 316 million drug users globally, contributing to significant health impacts and increasing strain on healthcare systems worldwide. Furthermore, vulnerable populations such as youth are also affected, leading to long-term health consequences, higher rates of healthy years of life lost, and severe academic and socioeconomic disadvantages.

Moreover, in recent years, New Psychoactive Substances (NPS) have become a global phenomenon. Created by modifying the chemical structure of controlled substances to mimic the effects of illicit or prescription drugs, NPS contains the ability to routinely bypass legal restrictions. Their rapid appearance in the drug trafficking

networks has posed severe public health risks and challenges towards effectively monitoring the global drug trade.

As this submarket has expanded, its growth has been parallel to the increase of global inequality. With the wealth gap between the elite and working classes continuing to widen, more individuals have moved towards illegal drug trade economies as a means of survival. The illicit drug trade provides an alternative economic route for those facing poverty



Andean woman harvests coca leaves.

or limited legitimate opportunities. Trafficking networks can make substantial profits, particularly given the low production cost of synthetic opioids such as fentanyl, which can be sold for hundreds of times greater than their initial production value. However, these economic benefits have been shaded by the violence, corruption, and erosion of communities that accompany them.

Over the last few decades, world communities have gathered to combat the global drug issue, being faced with the growing debate over their role and responsibility in responding to the international drug trade. This has included the attempt to regulate the trade through multilateral policies, including the 1961 Single Convention on Narcotic Drugs, the 1971 Convention on Psychotropic Substances, and the 1988 UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. These three international drug control conventions provide legal structures for the control of the production, trafficking, and misuse of narcotics (Niaz, 2017). Member states, however, have contended that instead of reducing drug consumption or mitigating issues surrounding the industry, the conventions have enabled the creation of an increasingly disruptive and illegal narcotic market. Concerns about the treaties are often rooted in their lack of enforcement, inflexibility, and inability to reduce demand (“International Drug Control Conventions,” 2026). These existing guideline systems have struggled to keep pace with an ever-changing global reality, including the emergence of new substances, expansion of trafficking networks, and evolving social and economic conditions. These complex components have led countries to remain divided over the extent to which the international community should intervene in global trafficking routes, balancing concerns of public health, security, development, and national sovereignty.

While the Commission on Narcotic Drugs (CND) analyzes the global drug situation and oversees the implementation of these conventions, DISEC can pass non-binding resolutions, recommendations, and declarations that reflect the consensus of the international community and suggest frameworks for prospective action.

History

One of the first major national efforts to control the distribution of narcotics occurred in 19th century China. Leaders of the Qing dynasty sought to discourage opium importation and use due to its growing detrimental effects on society. However, the English East India Company, which controlled the majority of British trade in the region, was heavily engaged in the profitable export of opium from India to China. At the peak of the opium trade, tens of millions of Chinese people were addicted to the drug, with nearly a quarter of the adult male population using it annually (United Nations Office on Drugs and Crime, 2010). As tensions continued to escalate over enforcement efforts and foreign merchants brought in increasing amounts of opium, armed conflict erupted and culminated in the first and second Opium Wars (1839-



Group of people holding a sign saying "In compliance with the 18th Amendment, NO intoxication liquor allowed on the premises" surrounded by bottles of alcohol in the Prohibition era.

1860). These early conflicts helped lay the groundwork for future international efforts to regulate the trade of narcotics.

In 1909, United States President Theodore Roosevelt proposed an international investigation of the growing opium issue. That same year, a meeting of thirteen nations produced a series of recommendations that led to the establishment of the First International Opium Convention. Following the ratification of the convention, the responsibility to supervise agreements related to the trafficking of opium was given to the League of Nations.

The League of Nations' structural guidelines for international drug control were influential and informed the United Nations' own drug control system; however, they faced many limitations. There was no centralized authority mechanism, production of raw opium and coca leaves was not strictly limited, and the system relied completely on voluntary compliance by member states, allowing the illicit drug trade to continue expanding at alarming rates. After the disbandment of the League of Nations and the establishment of the United Nations, the Commission on Narcotic Drugs (CND) was created in 1946 to assist with supervising the application of international drug control treaties (United Nations, n.d.). Through the CND, the United Nations focused on two primary objectives: improving the existing treaty system and increasing the effectiveness of national drug control measures.

Soon after the implementation of the CND, the United Nations moved to formalize a comprehensive drug control regime through a series of binding multilateral treaties ("International Drug Control Conventions," 2026). The most impactful was the 1961 Single Convention on Narcotic Drugs, which aimed to combat drug abuse with collaborative international action. This legal groundwork was upheld by the Vienna consensus, an informal but commanding agreement among member states to prioritize punitive, prohibition-based drug policies (Arana, 2019). Under this regime, a unified body regulated the cultivation, production, distribution, and use of narcotic substances. In contrast with the League of Nations, the convention limited the use of coca leaves and cannabis to medical and scientific needs, paving the way for the International Narcotics Control Board.

The 1971 Convention on Psychotropic Substances later expanded this system to psychotropic substances. This convention broadened the scope of international

control by including synthetic drugs and establishing special provisions for the regulation of pharmaceuticals (1971 Convention on Psychotropic Substances, 1975). At the forefront of the 1970s, many states adopted militarized “War on Drugs” strategies, focusing on strict enforcement laws, mass incarceration, and supply reduction through prohibition tactics. With campaign costs totaling over one trillion dollars, this approach became the basis for anti-drug policies for decades and heavily influenced the drafting and adoption of the 1988 convention.

The United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988 addressed the concern over the rapid growth in international drug trafficking by providing comprehensive measures that included provisions against money laundering and the diversion of precursor chemicals (“International Drug Control Conventions,” 2026). Motivated by the need for coordinated action, the convention provided international cooperation through the extradition of drug traffickers, controlled deliveries, and transfer of proceedings (United Nations, 1988).

Despite the adoption of the 1988 Convention, illicit drug trafficking continued to expand in both scope and complexity in the decades that followed. In the following years, powerful cartels emerged, particularly in Latin America and parts of Asia, demonstrating the capability to adapt rapidly to enforcement-based strategies. In the 1990s, attempts to crack down on drug trafficking in the Caribbean failed, instead redirecting activity to Mexico, a phenomenon experts call the “balloon effect.” The weakening of major Colombian cartels opened the door for Mexican organizations to gain control over land-based routes into North America. Simultaneously, East Asia developed into major hubs for methamphetamine production, sustained by complex and highly networked criminal syndicates operating across the region. The production and trafficking of illicit drugs throughout the world have generated a multi-billion-dollar black market in which criminal and terrorist organizations have been able to thrive. These groups can challenge state authority in source and transit countries where governments are often fragile and corrupted.

Furthermore, advancements in pharmacology throughout the 19th and 20th centuries underscored the medical value of concentrating and refining compounds derived from traditional remedies, contributing to the prevention and treatment of numerous diseases. Worldwide, hundreds of thousands of patients struggle to access medication due to drug and financial shortages, instead turning to black markets and the drug trade. In some low-income producer countries, illicit crop cultivation has continued to provide subsistence-level income where alternative economic opportunities remain limited. Alongside these activities, modern drug trafficking organizations generate immense profit, often laundered through the gaps of the global financial system and, in some cases, used to finance extremist groups or armed groups. As a result, the international drug trade has been followed by a cloud

of corruption, violence, and political instability, elevating it from a criminal justice concern to a broader concern about international peace and security.

Throughout the history of drug control policies, crucial questions have been raised about the extent to which the international community should intervene in drug-producing and transit regions, particularly when such involvement may conflict with state sovereignty, economic dependence, and long-term development objectives.

Current Developments

According to the World Drug Report, in 2025, a new era of global instability has intensified challenges in addressing the world drug problem, empowering organized crime groups and pushing drug use to historically high levels. Organized drug trafficking groups have continued to adapt, exploit global crises, and target vulnerable populations. As of 2023, 316 million people used drugs compared to the estimated 246 million people worldwide in 2013, outpacing global population growth over the past decade. At the same time, the overall market has continued to expand, with cannabis remaining the most widely used drug at 244 million users, followed by opium at 61 million. However, with increased hardships, instability, and conflict around the world, these numbers are expected to continue to grow.

Compounding this growth is the rise of synthetic opioids and laboratory-produced stimulants, which has further complicated international control efforts (Historic England, 2018). Due to factors like low operational costs and reduced risks of detection, the appeal of amphetamine-type stimulants (ATS) has reached a record high as of 2023. Unlike plant-based substances such as coca or opium poppy, synthetic drugs can be made in small-scale facilities almost anywhere. This eliminates the need for large-scale cultivation and reduces the dependence on traditional growing areas. This flexibility has made manufacturing more difficult to detect and regulate.

Furthermore, this ease of production has been catalyzed by a digital evolution in distribution, with criminal organizations having adapted rapidly to technological changes such as the internet. Digital infrastructure like encrypted communications, online platforms, and dark web marketplaces has equipped traffickers to evade law enforcement more effectively and reach a larger and younger customer base. By exploiting unmonitored digital infrastructure, introducing newly modified synthetic compounds and increasingly using artificial intelligence to identify alternative precursor chemicals, trafficking networks have maintained supply despite intensified security efforts.

Beyond enforcement challenges, the international drug trade poses significant public health concerns. As of recently, newer synthetic drugs like fentanyl and methamphetamine are the primary drivers of fatal drug overdose deaths worldwide. According to WHO estimates in 2019, approximately 125,000 people died of opioid

overdose (World Health Organization, 2025). These rising fatalities have also caused a strain on healthcare systems. Overall healthcare cost related to the increase in opioid overdoses has increased exponentially, stemming primarily from emergency room visits, ambulance costs, and the use of overdose-reversing treatments (Walden University, n.d.). In 2017, “costs for opioid use disorder and fatal opioid overdose were estimated to be \$1.02 trillion” (Florence et al., 2021). Additionally, while the hospitals have seen a shortage of medication, the increased availability of opioids in the drug trade industry has generated a substantial surplus of medication, much of which has been diverted for non-medical use. This issue has been particularly pronounced as distribution channels have become more efficient, driving down the prices of substances such as heroin.

To combat these issues, policy responses have begun to diverge, with some states emphasizing harm reduction and public health strategies, while others continue to prioritize punitive enforcement. These evolving approaches operate within the broader United Nations treaty framework, which remains the central pillar of international drug control despite mounting pressure to adapt to rapidly changing market conditions (International Narcotics Control Board, 2025).

International Community Response

Currently the international response to the illicit drug trade has primarily focused on addressing the synthetic drug crisis, fixing the “root” causes through public health and education initiatives, and coordinating law enforcement. There has also been a push away from traditional criminalization, which critics argue gives rise to a profitable illicit drug market that in turn sustains organized crime networks (Johnstad, 2023).

This shift was followed in 2019, when the Ministerial Declaration signaled a departure from decades of stagnant drug policy. This agreement created a ten-year blueprint designed to strengthen national, regional, and international levels to accelerate the implementation of joint commitments to address and counter the world drug problem (Directorate-General for Migration and Home Affairs, 2024). The resolution had its goals set to significantly reduce the illicit drug trade by 2029, yet in 2024 the greater emergence of synthetic substances was already rapidly outpacing these initiatives. As a result, during the 69th session of the CND, the Vienna Consensus, which had long ignored the failures of prohibition, essentially fell apart, with many voting against it



Young people in Punjab, India rally against drug usage holding signs with anti-drug slogans.

in hopes of making the CND a more active group that could tackle issues that had been previously ignored (International Drug Policy Consortium (IDPC), 2025).

On March 13, 2026, the 69th session of the CND emerged after five days of deliberation on drug trends, treaty implementation, and international cooperation. Some of their efforts included adopting a resolution that promotes integrated systems of scientific evidence-based public health responses, early warning data mechanisms, and calling for stronger supply chain integrity. With over 2,078 participants and 198 non-governmental organizations, the session highlighted the Commission's central role as the United Nations' global policymaking platform on drug-related legal guidelines (UN Office of Drugs and Crime, 2026).

Beyond these diplomatic changes, regional enforcement has also evolved, as seen in initiatives such as the European Ports Alliance. In 2025, the alliance introduced a new drug-combating strategy launched as part of the broader ProtectEU framework (Directorate-General for Migration and Home Affairs, 2025). This action plan focuses on five key pillars: enhancing preparedness, protecting public health, strengthening security, increasing harm prevention, and forging stronger partnerships. By fostering public-private cooperation, the alliance aims to secure EU ports and dismantle criminal networks that exploit maritime logistics (Directorate-General for Migration and Home Affairs, 2024).

Despite these newer advancements, international responses remain slow and fragmented, often allowing traffickers to stay ahead of enforcement initiatives. This underscores the ongoing challenge for the international community: how can coordinated and effective responses be properly implemented to combat the evolving international drug trade?

Case Studies

The Golden Triangle

In northeastern Myanmar, northern Thailand, and northern Laos stands a large mountainous region of approximately 200,000 km² known as the Golden Triangle. Since the 1950s, this region has been one of the largest opium-producing areas in the world. Today, the Thai and Laotian areas of the Golden Triangle are now popular tourist destinations, with attractions primarily dedicated to the natural scenery, rich culture, and historical significance of the opium trade. The Thai portion of the region is now urbanized with modern roads, electricity, and a strong economy due to government intervention in opium production. Vietnam and Laos have also followed in the footsteps of Thailand, with opium output much lower than in the past. However, up until 2022, Myanmar produced some 25% of the world's opium, remaining the world's largest exporter ("Golden Triangle (Southeast Asia)," 2026).

This output has largely occurred due to complexities in governmental oversight and a fluctuating domestic security environment.

During the colonial times of the 19th and early 20th centuries, the opium industry operated as a state-sanctioned monopoly for British and French empires. Opium became an international cash crop, with both colonies encouraging farmers to increase their production of opium (Payne, 2026). Heroin, a refined form of opium, began appearing in the Golden Triangle alongside traditional opium farms. The demand for heroin reached a record high as U.S. troops during the Vietnam War would use the substance to relieve their fears and traumas of war. This solidified the Golden Triangle's transformation into a highly profitable heroin economy ("Opium Production in Myanmar," 2026).

While Myanmar continues to rely on its natural riches amidst political instability and conflict, targeted government initiatives have effectively reduced opium production in Thailand, Vietnam, and Laos. In 1970, in Thailand, King Bhumibol Adulyadej envisioned the idea of growing an improved peach variety that could generate more income than opium poppy and eliminate the risk for criminal activities. Now known as the alternative development model, this concept fostered an environment of security and a sustainable livelihood for local communities. This vision led to the establishment of the Royal Project, "a private charitable organization that aimed to support alternative development in Northern Thailand" (Royal Thai Consulate-General, Fukuoka, 2021). Following its implementation, the Royal Project and the Thai Narcotics Control Board partnered with the United Nations Fund for Drug Abuse Control to establish the crop replacement programs. This uniquely successful effort not only reduced illicit crop cultivation and crime but also bolstered economic, food, and environmental security. The project has since collaborated with UN agencies to introduce similar programs in countries such as Laos, Myanmar, Colombia, and Afghanistan.



Golden Triangle landmark in Sop Ruak, Thailand

In a similar vein, Vietnam and Laos have seen dramatic declines in illicit cultivation through integrated state action. Between 1990 and 2001, Vietnamese opium production decreased by 98% following the establishment of a Drug Control Committee and a national action plan that called for a new campaign to raise awareness and prevent young people from participating in trafficking and drug abuse. The committee used

funding from the central government to implement security enforcement measures, alternative economic opportunities, education, and rehabilitation. Additionally, Laos, the world's largest producer of opiates with nearly 27,000 hectares in 1988, reduced its cultivation to a mere 1,800 hectares by 2006. Following the UNODC Strategic Programme Framework (SPF), the Laotian state enacted an approach that integrated alternative development, demand reduction, security, and civic awareness, successfully decreasing the number of opiate users by an estimated 40,000.

However, at the same time, Myanmar remains a source of global concern due to its shift away from traditional opium and heroin production towards synthetic drugs. High levels of poverty and ongoing conflict have made the cultivation of NPS an attractive livelihood for impoverished farmers in Myanmar. While the UNODC involvement in the state has included regular opium surveys to track poppy cultivation trends and assistance through the Crop Monitoring Program, international attempts to curb production have faced setbacks. These setbacks are primarily due to armed conflicts, limited state capacity, and governance issues, hindering long-term success in drug eradication. Political upheaval in Myanmar, particularly following the 2021 military coup and subsequent civil conflict, has further weakened international drug control efforts and contributed to an increase in cultivation.

This pattern is not unique to Myanmar. The Golden Triangle still attracts transnational criminal experts and traffickers. Access to both overland and maritime trafficking routes provides these networks with multiple pathways to reach markets across the Indo-Pacific region and beyond.

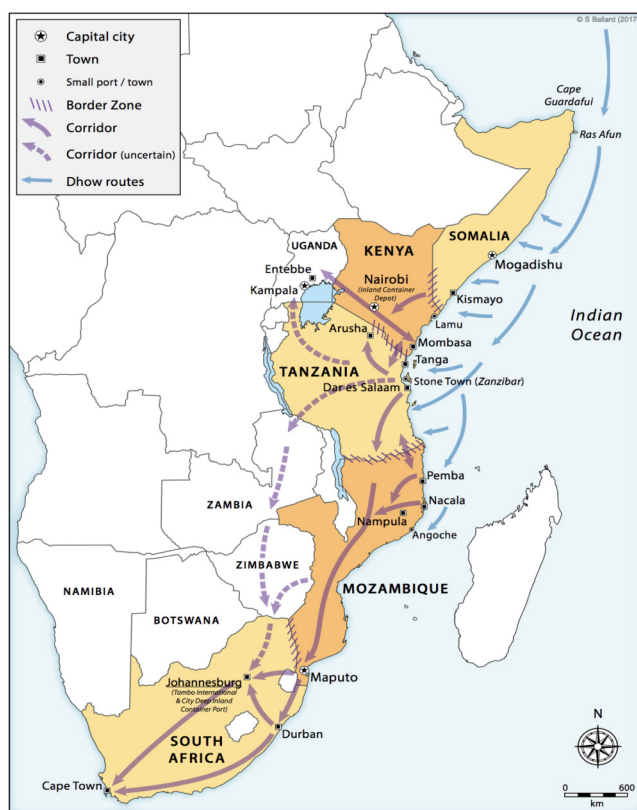
These dynamics showcase the central debate facing the international community on whether external intervention can occur and reduce illicit drug production without increasing instability, undermining sovereignty, or reinforcing economic dependency. It also showcases the responsibility nations have in solving these issues, as historically a state's dependency on another was the initial introduction to the global drug trade.

Eastern and Southern Africa

Over the past three decades, Eastern and Southern Africa (EAS) states have shifted from traditional plant-derived local drug economies into major global transit and destination hubs for illegal drugs. In countries like Kenya, Tanzania, Uganda, Somalia, and Ethiopia, drugs like heroin, marijuana, cocaine, methamphetamine, and khat are all sold and trafficked. Drug trafficking in EAS states has been sharply increasing in the past decade, correlating with corruption, terrorism, and rising cases of HIV.

Historically, trade routes through the Indian Ocean to Asia and sub-Saharan Africa have facilitated the flow of legal goods. However, due to the increased surveillance on routes to Europe and the United States, these routes have also been used to transport illicit goods to the rest of the international market. High corruption in

Indicative overview of sea- and land-based heroin routes across the eastern African coastal states



Source: Global Initiative against Transnational Organized Crime, based on interviews across the region, September 2017

Indicative overview using a map of sea and land based heroin routes across the eastern African coastal states.

smuggling hub for drugs, primarily due to being unequipped with sufficient screening equipment, staff, and sniffer dogs to interdict the shipments. This same vulnerability extends to maritime gateways; in South Africa, the port of Durban is notorious for corruption and drug trafficking, yet it handles the majority of South Africa's container traffic.

In 2025, the South African Revenue Service led an operation that resulted in the interception of a cargo ship near the port carrying 25 bricks of high-purity cocaine. Each shipment was equipped with GPS tracking devices, which transnational cartels used to monitor the packages while en route. However, if the parcel had not been intercepted, the majority of the supply would have been destined for Europe and Australia, with a significant portion siphoned off for domestic use. Local leakage from these shipments directly fuels gang violence throughout South Africa and escalates the domestic drug crisis. According to the 2025 Africa Organized Crime Index, Durban has become the primary entry point for heroin and cocaine entering from Afghanistan and South America.

Prior to the current efforts of the Eastern and Southern Africa Commission on Drugs (ESACD), mitigation endeavors were guided by the 1996 Southern African Development Community (SADC) Protocol, which established the first major

the governmental systems has enabled weak law enforcement operations that are unequipped to prevent smuggling, especially with the emergence of new illegal drugs flowing through the trade. Some political administrations in countries such as Kenya have even been funded by profits from illicit drug trade to gain greater control of power.

The illegal drug trafficking in East Africa can be traced back to the 1970s, when growth in commerce, communications technologies, and the development and integration of infrastructure into global networks provided the platform for the expansion of legal and illegal trade. One of the most significant challenges in combating the narcotics trade in EAS states is the inherent vulnerability of major transportation hubs. Bole International Airport in Ethiopia, one of Africa's busiest airports, has become a

regional framework for cooperation in combating the illicit drug supply, demand, and corruption. It prioritized eliminating the root causes of the trade by harmonizing criminal laws and creating a direct communication system to facilitate the flow of information amongst law enforcement. These initiatives were complemented by the African Union Plan of Action, which has cycled through iterations of the 1996 Action Plans to improve the health, security, and socio-economic well-being of the people of Africa (African Union Plan of Action on Drug Control and Crime Prevention (2019-2025), 2019). Yet, by 2018, the African Union (AU) indicated that the consumption and trafficking of controlled substances had escalated in all five AU regions, thereby prompting a need for greater intervention.

In response, the ESACD was established in 2023 as a regional advocacy organization prioritizing informed discussion about humane and effective drug policies, as well as engaging with policymakers to discuss new approaches to drug-related issues. These priorities carried into 2024, culminating in the third meeting of the ESACD, located in Tanzania (FIAP, 2024). Its focus was to address the impact of synthetic drugs, the growing threat that psychoactive substances present to public safety and health in the region, and the national monitoring of the drug market through accurate data. This campaign, funded by the European Union, aimed to promote the adoption of a regional approach to strengthen collective responses to the threat of the global drug trade.

The Mexican Drug War

Due to its location, Mexico has long been used as a staging and transshipment point for narcotics and contraband between Latin America and U.S. markets ("Mexican Drug War," 2026). From 1920 to 1933, the United States prohibited the production, import, transportation, and sale of alcoholic beverages, inducing Americans to cross the Mexican border to buy alcohol. This was the early arrival of the illegal drug trade. In the coming years, the United States would experience a shortage of medical morphine and work with Mexican authorities to expand regulated opium poppy cultivation in northwestern Mexico, including areas surrounding the state of Sinaloa. Although the program would end after 1945, the cultivation and smuggling of opium would persist in the Sierra Madre mountains. The Sierra Madre Occidental, Oriental, and Del Sur all make up the Sierra Madre mountain system of Mexico. It extends approximately 700 miles through northwestern and western Mexico and along the Gulf of California. Its tortuous terrain and shady valley made it the ideal area to become one of the top cultivators of opium.

From the late 1960s to the early 1970s, with the rapid surge in recreational drug use in the United States, the production of narcotics in Mexico expanded exponentially. The states of Sinaloa, Durango, and Chihuahua came to be known as the so-called "Golden Triangle" region and at one point produced up to 90% of

opium going to the United States. Due to this, Mexican officials and the United States backed several anti-narcotics initiatives, including Operation Intercept and Operation Condor (“Mexican Drug War,” 2026). The operations ultimately failed to capture any major traffickers or narcotic production; military corruption and human rights violations continued to increase.



Mexican drug lord Joaquín "El Chapo" Guzmán being escorted by Mexican navy marines after his capture in February 2014.

In 2006, the Mexican military intervened and launched the Mexican War on Drugs with the assistance of the United States. The government's main objective was to reduce drug-related violence by dismantling cartels and preventing drug trafficking. The Mexican drug war has evolved into a prolonged internal armed conflict between the state and competing trafficking syndicates. With aid from the United States, the Mexican government prioritized militarized targeting of cartel leaders, beginning with efforts such as Operation Michoacán, which deployed thousands of troops and police. While this effort weakened major cartels, it also fragmented criminal organizations into smaller, more violent factions, intensifying territorial wars and contributing to rising homicide rates nationwide. By 2012, the estimated death toll of the conflict was 60,000, raising concerns about the long-term security implications of enforcement-focused strategies implemented without parallel institutional reform (“Mexican Drug War,” 2026).

Following 2013, executive leaders have pledged to shift to de-escalation and violence reduction, but setbacks have ensued. Since the beginning of the conflict, law enforcement in Mexico has been criticized for corruption, collusion with cartels, and impunity (“Mexican Drug War,” 2026). However, critics argue that many of the issues Mexico has seen in the drug trade have been from international influence and efforts. Violent criminal organizations in Mexico are largely filled and financed by drug trafficking, with most of the supply destined for the United States (Mayar, 2025). At least 70% of firearms recovered from Mexican cartels are traced back to the United States (John, 2023). Beyond the United States, there is also a high demand for drugs from Mexico, as well as other countries in Europe, Asia-Pacific, and other parts of Latin America.

Maritime routes

Maritime cocaine smuggling involves the transportation of cocaine across international waters using boats, commercial fishing vessels, cruise ships, and other maritime means. Key points of origin remain primarily in Colombia, along with Bolivia



A homemade narco-submarine in Tumaco, Columbia.

and Peru, from which large volumes are sent to Central America, Eastern Africa, the Caribbean, and Western and Central Europe. The vulnerability of shipyards often stems from the massive volumes of containers and equipment that have to be rapidly moved during operation, opening a window for theft and smuggling of contraband to occur. Narco-submarines and semi-submersible vessels have become a common method to evade

detection. These vessels can carry tons of cocaine while remaining largely invisible to radar and aerial surveillance systems. In 2019, the U.S. Coast Guard reported 36 narco-submarine incidents, though officials acknowledged many more likely to go undetected. Advanced imaging technology has begun to be used to inspect vessels more effectively and accurately; however, this tool requires high-energy scanner infrastructure and has limitations when scanning if the illicit drug has been mixed with another substance that alters its density or physical characteristics.

The employment of maritime smuggling methods highlights the challenges facing national and international law enforcement. With the sheer scale of maritime transit, resource constraints, and jurisdictional complexity, maritime trafficking routes demonstrate the truly transnational nature of the modern drug trade and the difficulties that surround implementing policies and encouraging guidelines ("Maritime Cocaine Smuggling," 2026).

Directives / QARMAs

As delegates part of the First Committee, it is critical to take into account how international security, sovereignty, public health, and development intersect in addressing the international drug trade. Some questions to consider:

Are international communities obligated to interfere with or govern another nation's sovereignty?

How can we address technological advancements that further enable drug trade?

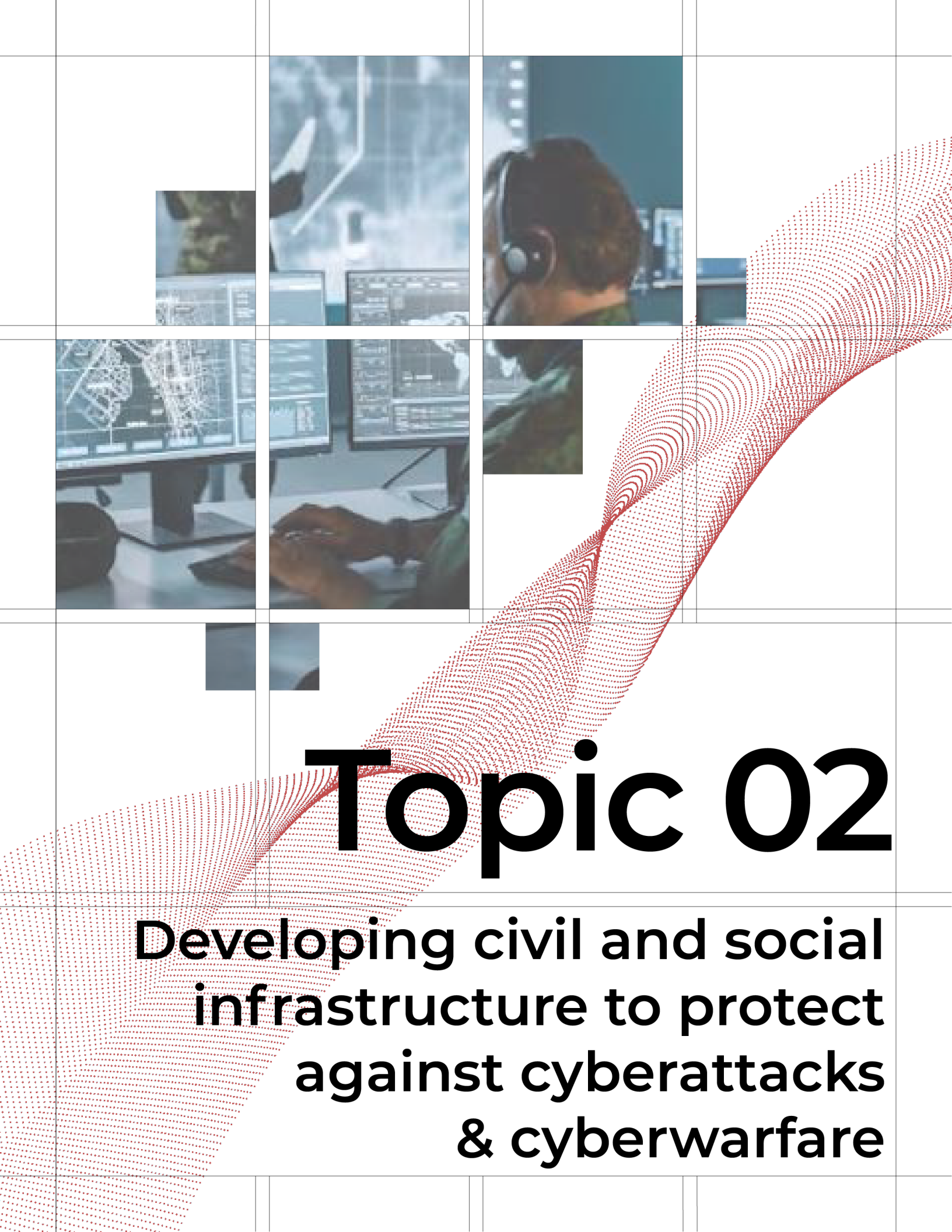
What strategies can be implemented to provide alternative economic opportunities to replace illicit crop production in low-income regions?

Should public health and harm reduction policies be valued equally to militarized enforcement strategies when determining solutions?

How can cultural attitudes toward drugs and local governance structures be incorporated into effective and inclusive international policies?

How can international actors balance security concerns with the economic needs of communities reliant on illicit drug cultivation?

What are the risks of external intervention when addressing the transnational nature of drug trafficking?



Topic 02

**Developing civil and social
infrastructure to protect
against cyberattacks
& cyberwarfare**

Key Terms and Acronyms

Cyberattacks	Any attempts to gain unauthorized access to a computer network
Cyberwarfare	The utilization of cyberattacks to inflict harm or gain a military advantage against an enemy state, typically by another nation. This is different from cybercrime, whose motive is typically financial gain and is predominately done by non-state actors
Cyber security	The protection of computer systems and digital infrastructure from cyberattacks
Attack Surface	All points of entry into a computer network that a cyberattack can use to breach a secured network. This includes both digital entry points, such as websites and applications, and physical entry points, such as the physical computers and servers of the network
Social Engineering	The psychological manipulation of people with confidential information or access into giving up confidential information or gaining unauthorized access to a secured network
Digital Literacy	A person's ability to safely use digital devices and networks to find accurate information and apply that information
Cyber Awareness	The understanding and awareness of cyberattack threats and cybersecurity best practices
Insider Threat	The cybersecurity risk of a malicious actor granted legitimate access to a computer network
Encryption	The process of encoding information in a way that only authorized parties can read
Firewall	Any security system that monitors and controls network traffic going in and out of a computer network

<i>Distributed Denial of Service (DDoS)</i>	A Distributed Denial of Service attack is designed to overwhelm a system's resources and response capabilities such that it is unable to respond to legitimate service requests. This is done by supplying a system with an excess of illegitimate requests; as the site must respond to each of these, it consumes all of its response capabilities
<i>Man In the Middle (MITM)</i>	A Man In the Middle attack allows for an unauthorized observer to monitor data sent back and forth within a network. Thus effectively allowing an observer to eavesdrop on their conversation and gain access to confidential data
<i>Phishing</i>	Phishing attacks occur when a malicious actor sends an email that is disguised as being from a legitimate source in order to get sensitive information from the target or to install malware on their device. When executed, they are often combined with social engineering. Some subsets of phishing attacks include "whale phishing attacks," which are targeted at high-level individuals in an organization, and "spear phishing attacks," where an attacker targets and researches a specific individual for the attack
<i>Ransomware</i>	Ransomware attacks hold an individual's or organization's network hostage until a payment or other ransom is received
<i>Password attacks</i>	A method used to gain unauthorized access to a system by cracking a user's password. This can be done through social engineering, accessing unsecure networks, brute force attacks, and dictionary attacks
<i>SQL injection attacks</i>	SQL attacks attack websites that use a database to serve their users. It occurs when a user inserts malicious SQL code into a query and can allow the user to access sensitive information, modify data & databases, and even gain administrative access in a network
<i>Civil Infrastructure</i>	The physical systems required for society to properly function
<i>Social Infrastructure</i>	The human capital, societal norms, policies, and regulations required for a society to properly function

Introduction

In 1990, only 0.05%, or 2.6 million people, had access to the internet. By 2010, this number rose to 27%, or 1.9 billion, and by 2025, it rose to 68%, or 5.6 billion people (Conte, 2025). With the rise of internet access and the associated dependency on online technologies, there has been an increase of cyberwarfare and cyberattacks. The most common types of cyberattacks include DDoS, MITM, phishing, ransomware, password, and SQL injection attacks (Fortinet, n.d.). In 2025, Cybersecurity Ventures estimated that cyber crime cost 10.5 trillion dollars. Sentinel One reported that the average cost of a cyberattack on a company with at least 1000 employees was \$53,000, and the cost of a data breach was \$4.88 million (SentinelOne, 2024). These data breaches not only cause companies harm but also often leak personal sensitive information of their users, putting them at increased risk of follow-up crimes. A singular cyberattack can be devastating to a company's revenue, with MKS Instruments reporting a negative impact of \$200 million due to a ransomware attack. Companies have taken steps to mitigate these attacks, such as investing in security AI to prevent data breaches and cyber insurance. Investing in the aforementioned security AI has an expected cost savings of \$2.22 million when compared to not investing. However, not all organizations have the capital or technical expertise to take this preventive measure. This is further reflected in the fact that 75% of organizations with a revenue greater than 5.5 billion have cyber insurance, whilst only 25% of organizations with revenue less than 250 million have insurance policies. This disparity underlies a gap in cybersecurity infrastructure, where smaller organizations lack the access to resources, knowledge, and protections necessary to defend against increasingly sophisticated attacks.

Adding to the issue of cyberattacks is cyberwarfare. Cyber warfare is defined as the "actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks" (RAND, n.d.). The key distinction between cyber warfare and cyber attacks lies within the objectives and the resources of attackers. The tactics employed within cyberwarfare often mirror those used in traditional cyberattacks. However, the attackers often have significantly more resources, as they are backed by an international organization or nation-state, and have the objective of "undermining an adversary's digital infrastructure to advance strategic interests" (Georgia Tech Professional Education, 2025). Some strategic interests include but are not limited to acquiring sensitive information, disrupting infrastructure, and impairing military infrastructure. In addition to impacting an enemy, cyber warfare is often conducted in a manner that allows for plausible deniability for nation states, allowing them to avoid facing international repercussions. An example of this is Operation Aurora, which occurred between June and December 2009. The attacks were attributed by cybersecurity analysts to Elderwood Group, a threat actor

linked by intelligence researchers to the People's Liberation Army (PLA) of China. The attack was first disclosed by Google in 2010, and Google, Adobe Systems, Akamai Technologies, Juniper Networks, and Rackspace all confirmed they were targeted; however, others, including Yahoo, Northrop Grumman, and Morgan Stanley, were also speculated to have been targeted. One key result of the attack was the breaching of the Gmail accounts of human rights activists in China, allowing them to be spied on ("Operation Aurora," 2026). The sophistication of the attack and the international condemnation in response make it a landmark moment in international cyberwarfare.

According to the Council on Foreign Relations, 34 countries are suspected of sponsoring cyber operations since 2005, with incidents including espionage, attacks on critical infrastructure, and everything in between (Council on Foreign Relations, n.d.).

Infrastructure for cybersecurity has existed in some form since the late 1980s, when the first organizations dedicated to cybersecurity were founded: McAfee Associates, the first cybersecurity firm; the CERT Coordination Center, a joint DARPA-Carnegie Mellon University project formed as the first computer emergency response team to cyberattacks; and the Forum of Incident Response and Security Teams, the first multinational organization coordinating cyberattack incident response teams (Carnegie Mellon University, n.d.; Simonis, 2007, p. 1033). Today, a wide assortment of universities, government agencies, corporations, and NGOs provide institutional expertise, a key part of social infrastructure, in countering cyberattacks. Alongside these institutions, which provide technical expertise, is the rollout of cyber defense across all key sectors. Physical digital infrastructure has to be built or modified, such as ensuring that servers containing sensitive information are isolated from as much of the outside as possible, including restricting physical access to servers and airgapping critical networks to ensure that there is a minimal attack surface for cyberattacks to exploit (Carruthers, 2025). The social infrastructure to defend against cyberwarfare would entail measures that the average user can adopt, such as improving digital literacy to mitigate social engineering and similar attacks (LeClair, 2016).

History

Cyberwarfare was first coined in 1993 by John Arquilla and David Ronfeldt, researchers at the RAND Corporation, speculating on how terroristic non-state actors could weaponize the cyberattacks that had risen in frequency as internet adoption gradually became mainstream (Arquilla & Ronfeldt, 1993). In their seminal paper, Arquilla and Ronfeldt equated cyberwarfare as being as revolutionary as the German blitzkrieg that defined the Second World War, but the post-Cold War environment led them to primarily speculate about the use of cyberwarfare by non-state actors such as terrorist groups. However, in the 2000s, a string of highly sophisticated cyberattacks quickly demonstrated that state actors could pose even more of a threat than non-

state actors.

In 2007, one of the first widespread, state-level cyber operations against another nation occurred when Estonia was attacked for 22 days, from the 27th of April to the 18th of May, coming after high political tensions amidst the controversial relocation of the Bronze Soldier dedicated to Soviet soldiers in Tallinn, Estonia's capital (McGuinness, 2017). The statue was put up by the USSR after World War II, in place of a monument dedicated to Estonian independence. In 2007, the Estonian government controversially voted to remove it, angering many Russian nationals. The primary method of attack was botnet DDoS attacks that took down servers, crippling various government, banking, and media services, which was significant to the relatively highly networked state that Estonia was in and highlighted the vulnerability of a highly digitalized society (Ottis, 2008). This not only marked the first instance of a cyberattack with such widespread effects but also the first politically motivated and potentially the first state-led one of these attacks, as it is widely theorized that efforts were led by Russians, whether state-sponsored or not. These 2007 attacks also motivated the namesake Tallinn manual, a landmark paper within international law regarding cyberattacks.

Starting in the same year the first major cyberattack was conducted, the world's first cyberweapon was deployed. From 2007 to 2010, Stuxnet, a cyberweapon theorized to be developed by the United States and Israel, was a powerful malware that exploited a zero-day vulnerability to dismantle and physically damage Iranian nuclear weapon development ("US and Israel Were behind Stuxnet Claims Researcher," 2011). It is believed Stuxnet took out over a thousand centrifuges at the Fuel Enrichment Plant in Natanz, Iran (Albright et al., 2010). In 2009 and 2010, Iran had to replace these centrifuges due to excessive damage officially confirmed to be caused by a cyberattack. Although not explicitly confirmed to be Stuxnet, the effects of cyberattacks have long included the destruction of infrastructure and power supplies.

Over the years, cyberattacks have continued to cause data breaches and disrupt key infrastructure, whether physical or virtual (Center for Strategic and International Studies, n.d.). EternalBlue was malware that caused a memory corruption/buffer overflow flaw, which allowed the actors to execute code on a computer with full system privileges, including those they needed to spread their bug. It was silently patched by Microsoft in March



The Bronze Soldier of Tallinn, a WWII memorial.

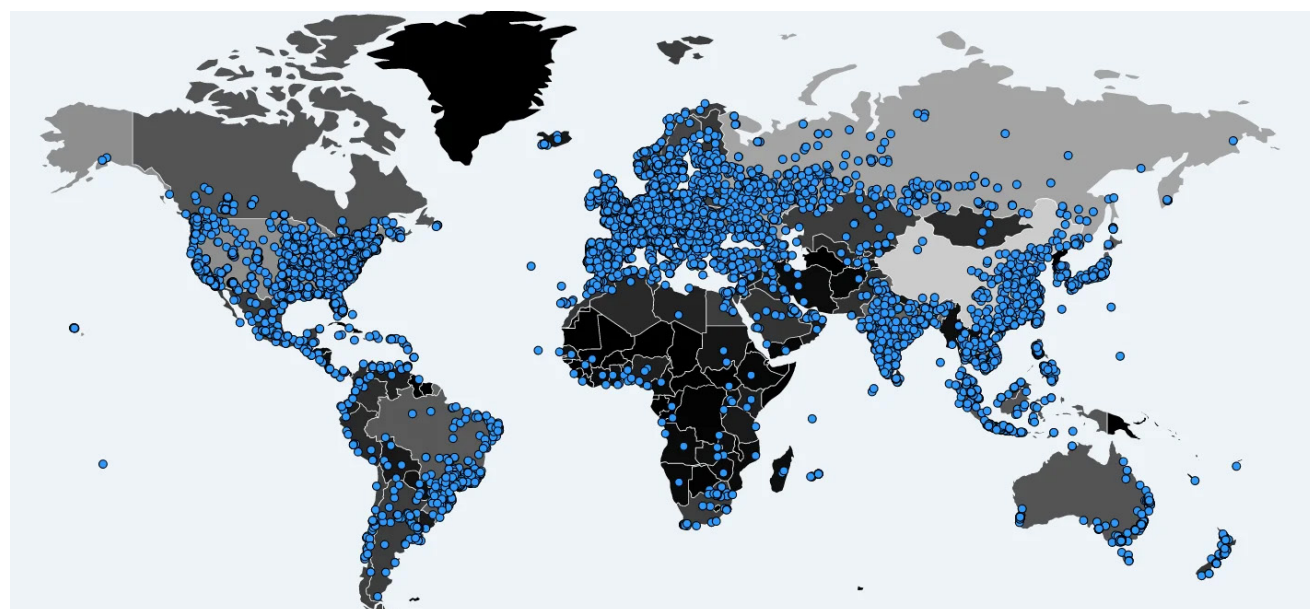


Former Iranian President Mahmoud Ahmadinejad visiting the Natanz nuclear enrichment facility on April 8, 2008

2017, but this malware developed by the NSA was discovered in the Shadow Brokers leak, which allowed it to be used against systems that were not up to date (Danielson, 2025). One of the biggest attacks was caused in 2017 by WannaCry ransomware, which hit over 300,000 computers as it took advantage of densely connected computer networks to spread like wildfire (Gregory, 2025). This culminated in an international incident, with effects ranging from

a total shutdown of one-third of all NHS hospitals to disruption of gas station payments and student submissions in China (Chappell, 2017). It took advantage of computers that were on out-of-date software, back when automatic updates were less common. Another attack that used EternalBlue was NotPetya, which combined EternalBlue with Mimikatz to get credentials for aiding access within networks. The attacks spread from the original target, Ukraine, to A.P. Møller–Maersk, where they disabled computers, critical IT systems, and heavy machinery like cranes (Steinberg et al., 2021). This shutdown of 17 of Maersk's 76 ports, and the lost revenue in addition to recovering or rebuilding affected systems, cost about \$300 million dollars, part of the estimated \$10 billion in damages the attack caused in total.

More recently, the Costa Rican government was attacked by ransomware in 2022. These attacks hit 27 different public institutions, most notably the Ministry of Finance, Ministry of Labor and Social Security, and Costa Rican Social Security Fund (CCSS). There were 2 waves by pro-Russian terrorist organizations, the Conti group and the Hive group, which demanded \$20 million to not release Ministry of Finance data and \$5 million to restore CCSS operations respectively. As a result of the attacks, "teachers were unable to get paychecks, tax and customs systems were paralyzed and health officials were unable to access medical records", causing \$125 million in losses in the first 48 hours and leading to a national emergency 3 weeks later, with the president declaring a "state of war" on May 8th, 2022 (Zerbe, 2023). This was incidentally the first such instance of a cyberattack causing a national emergency that debilitated governmental operations to this degree. Eventually, they restored operations after a few months, after getting technical support from Microsoft and the governments of the United States, Israel, and Spain. This cyberattack was a glaring example of the consequences of systems that don't have best data security practices in place. The original point of infiltration was stolen employee credentials, which could have been benign had there been more protections for sensitive data or simple user authorization (Datta & Acton, 2024). For example, many big technology

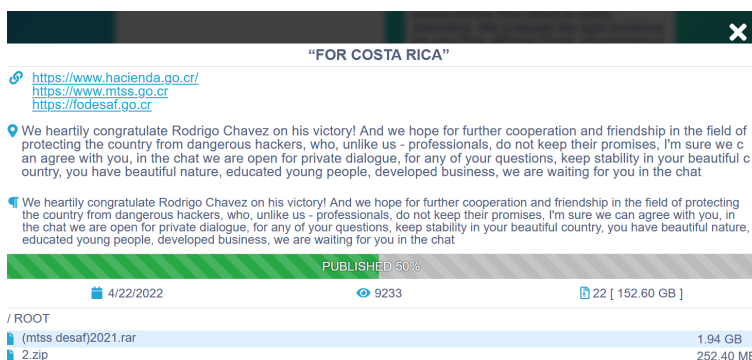


A world map of computers infected by WannaCrypt ransomware

companies implement the principle of least privilege, which may be a commonly known cybersecurity practice but requires time and effort that many newer systems do not have or aren't mandated to do.

Cybersecurity defenses become stronger after every attack, but for every time we make our technology safer we are still equally prone to the next vulnerability that can get found and attacked at any time. Even then, some of the vulnerabilities we find cannot be universally patched, as we saw in 2017, when Microsoft had already put out a patch for the vulnerability that caused the devastating WannaCry and NotPetya attacks which took advantage of out-of-date systems (Microsoft Defender Security Research Team, 2017).

Policies surrounding technology have been expanded and rewritten corresponding to the intensification and evolution of cyberattacks since 2007. The Tallinn manual was published in 2013 in response to the 2007 attacks on the namesake city in Estonia, and it serves as a foundational document attempting to create international standards for cyberattacks (Schmitt, 2017). The Tallinn manual has been endorsed by NATO to help it adapt to institutional cybercrime and cyberwarfare, but it still lacks coverage for recent attacks and does not fill the need for international collaboration that the Costa Rica incident exposed where they needed external support to regain control of their essential services (Raba, 2024).



Conti group message claiming they had leaked 50% of stolen data on April 22nd, 2022

Current Developments

Recent cybersecurity concerns have only expanded as the digitalization of our society has increased the scope of what cyberattacks can impact. This exposes gaps in legislation and policy documents that seem impossible to close before the next new issue.

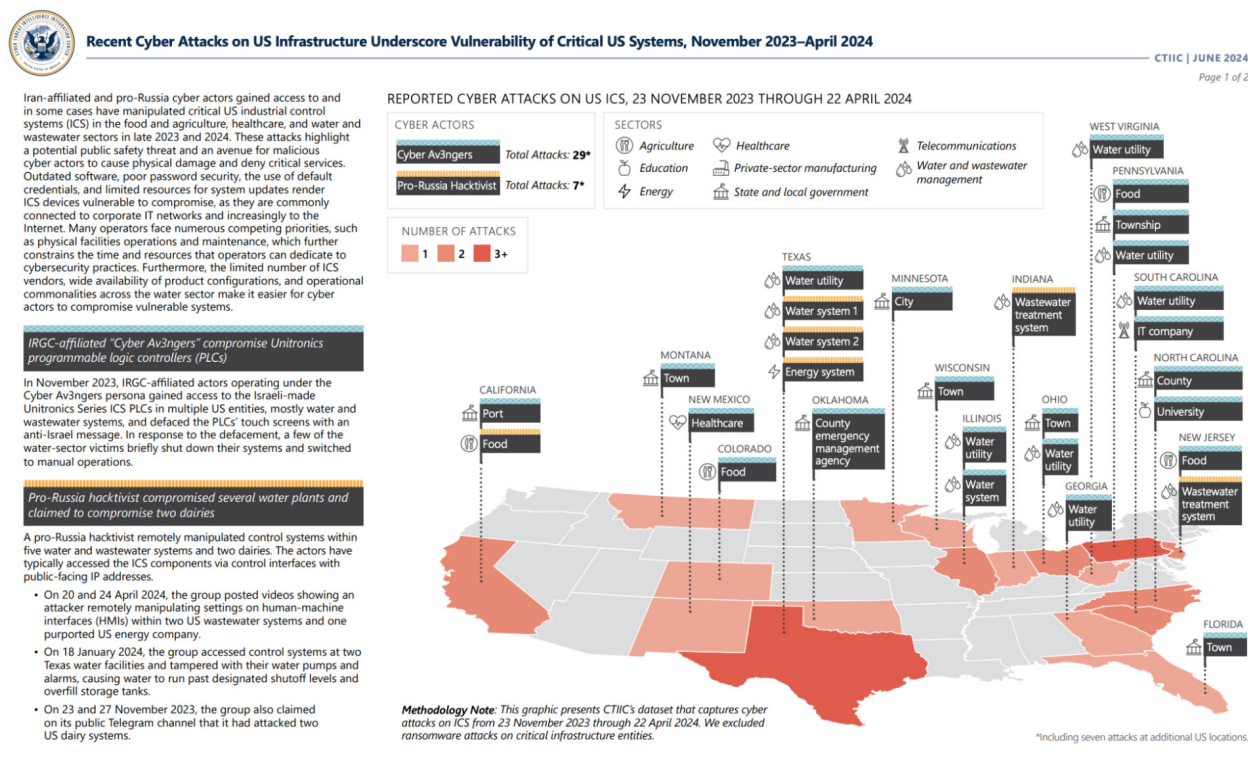
An important piece of international law is how we attribute state actors to cyber operations that they carry out, but defining attribution becomes difficult when AI agents can now initiate attacks with minimal oversight needed or can even do so rogue. Not only is it complicated to isolate an attacker, but determining if a state was truly a victim means proving that their sovereignty was infringed (JLCW Editor, 2025). This necessitates nations to adapt by defining sovereign internet zones, among other protections. For example, the digitalization of election systems led to possible tampering of the United States' 2016 presidential election by Russia. 12 Russian intelligence officers were indicted "with a computer hacking conspiracy involving gaining unauthorized access into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, stealing documents from those computers, and staging releases of the stolen documents to interfere with the 2016 U.S. presidential election" (United States Federal Bureau of Investigation, n.d.). More recently, during the 2024 US election, Cloudflare encountered significant internet traffic toward candidate campaign websites resembling DDoS attacks, and there have been many concerns over misinformation campaigns on social media by botted accounts (Tomé & Woolbright, 2024). There has also been a direct impact on American public safety in attacks on "critical US industrial control systems (ICS) in the food and agriculture, healthcare, and water and wastewater sectors" (Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024, 2024).

Two Open-Ended Working Groups (OEWG) on Information and Communications Technology (ICT) were conducted from 2019 to 2021 and 2021 to 2025, resulting in the publishing of a report by the UN Institute for Disarmament Research (UNIDIR) on how international law applies to cybersecurity threats and capacity-building within ICT (Dominioni & Paoli, 2026). A key outcome from the first OEWG was 10 principles on cyber capacity-building, which serve as standards that new ICT developments should uphold to ensure they follow international norms, including respecting state sovereignty and human rights. However, there are still critical issues with misuse, as cyber capacity-building can be used intentionally or not for surveillance or repression, among other gaps and not being legally binding. The second OEWG was meant to further examine capacity-building and emergent ICT threats, with a key result being expanding from capacity-building to universal confidence-building measures as collective action resources for member states to mitigate disasters

caused by cyberwarfare. For example, one of these measures is a points of contact (POC) network of technical and diplomatic experts for rapid response to incidents (Rupp, 2026). It also established a Global Mechanism convening for the first time in March 2026, which is a permanent body created to institutionalize further work in international cybersecurity via the “Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour in the Use of ICTs” (Rupp, 2026).

Specific nations have also taken steps to domestically address cybersecurity concerns, in various forms of creating government bodies, passing policy, or amending laws. In 2015, the US Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA 2015), which encouraged the pooling of information for cybersecurity measures and indicators between private entities and federal agencies by installing safeguards and reducing liability when such information was shared. This measure was originally in place for 10 years, getting extended twice in 2025 and 2026. In 2018, the US passed the Cybersecurity and Infrastructure Security Agency Act (CISA 2018), which turned the DHS’s National Protection and Programs Directorate into the Cybersecurity and Infrastructure Security Agency (H.R.3359 - 115th Congress (2017-2018), 2018).

Meanwhile, the EU passed their Cybersecurity Act in 2019 to strengthen the European Union Agency for Cybersecurity (ENISA) so it would have the resources



to bolster operational cooperation and crisis management across the EU (European Commission, n.d.). The Cybersecurity Act, the Cyber Resilience Act, and the NIS2 directive are all measures that ensure services and critical infrastructure used by EU citizens meet compliance standards to not be vulnerable, such as the European Cybersecurity Certification Framework (“ECCF”). In January, an expansion to these laws and more was proposed in a massive package to update the EU’s regulations surrounding ICT and cybersecurity risks, including security for 3rd party and high-risk suppliers and enhancing the process for cybersecurity certification (Bruder & Yaros, 2026).

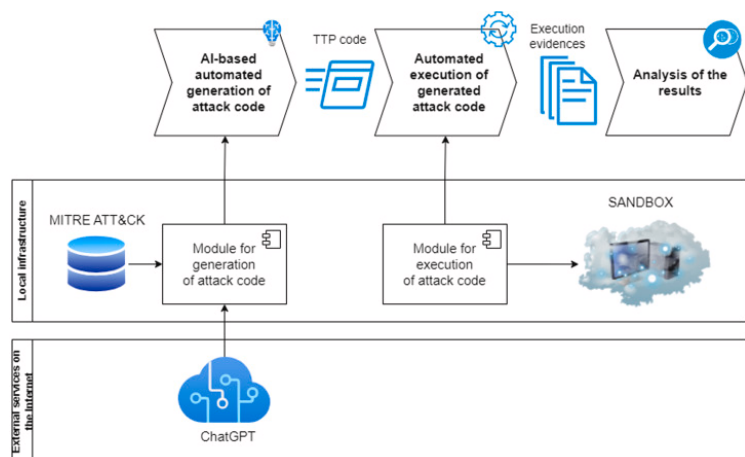
In 2026, China amended their 2017 Cybersecurity Law of China, which provided significant expansions of legal responsibilities and repercussions for cyberattacks, as well as notably including enforcement “against extra-territorial activities jeopardizing China’s cybersecurity” (Greenberg Traurig LLP, 2026). Additionally, they explicitly create goals for AI R&D and guidelines for ethics, integrating it into their cybersecurity policy.

South Africa was another pioneer of AI governance, releasing a draft national AI policy in April 2026 to help with compliance to security standards and infrastructure for development. It later got withdrawn, but they expect to publish a revision early next year (Dludla, 2026).

India established CERT-In (Indian Computer Emergency Response Team) in 2004, which was originally an advisory organization that has recently gained regulatory power to combat growing cyberattacks. In 2022, CERT-in issued guidelines that mandated applicable organizations affiliated with the government to report cybersecurity incidents within 6 hours, in addition to bolstering the support CERT-in provides for security teams and cybersecurity measures (Deloitte, n.d.).

Variants of these policies can be found across the world as every world government and organization aims to protect their digital spaces from rising threats. Brazil launched their E-Ciber proposal in 2025, which notably creates public and private cooperation in preventing and addressing cybersecurity issues and bolsters their other efforts to increase national cyber resilience (Lehmann, 2025). The Republic of Ghana’s own National Artificial Intelligence Strategy (2025–2035) focuses on concepts like data sovereignty and protections in conjunction with AI adoption (Senanu, 2026). However, beyond capability-building their strategy like many others don’t include AI mitigation or plans to respond to AI cyberattacks in their roadmap, a glaring flaw in any AI strategy that is critical to preparing a state’s cybersecurity for the future.

Thus, policies regarding cyberattacks are often reactionary, but with the exponential increase in cyberwarfare capabilities, we need a way to be proactive against advanced AI systems. Already, LLMs can generate executable code for a wide variety



Pipeline for execution of AI-generated cyberattacks

of MITRE ATT&CK techniques, reducing the effort and expertise required from attackers and potentially automating parts of the attack sequence (Iturbe et al., 2024). Recently, a rogue OpenAI bot autonomously conducted a cyberattack on Hugging Face, a large open source machine learning platform (OpenAI, 2026). This effect of AI is already being seen globally as well, as last year

INTERPOL found that AI assisted at least half of the cybercrime incidents in Africa (INTERPOL, 2026).

Consequently, we need to figure out how to adapt cybersecurity policy to mitigate AI attacks, including potentially adopting AI as part of the defense efforts. For example, the same way AI can be a powerful attack tool, it can be instrumental in red-team attacks that show us vulnerabilities before they get exploited. Red-teaming, or using the attack weapon as a defense measure, is a common cybersecurity practice that encourages states to use this new tool to attack our own systems before malicious actors use this tool against us (Anthropic, 2026). However, this invites new issues, including inequality in AI capabilities, which can quickly cause an imbalance in state power, depriving those that lack the same resources in terms of AI integration and compute power (Mansoor, 2026). States with these resources will be better equipped for cyberwarfare, whether attacking or defending critical infrastructure, so finding ways to ensure access to not just those who have frontier AI labs and the necessary semiconductors or energy.

Directives / QARMAs

What constitutes cyberwarfare and how do we need to update the definition and scope based on recent technological advances?

How can we make an Incident Response Plan (IRP) that gives states a playbook for responding to cyberattacks once they happen? Should the UN establish an international mechanism for coordinating responses to major cyberattacks?

How do we equitize access to cybersecurity resources, energy, and IT knowledge so all nations have the resources and capabilities to maintain secure systems and adequately respond to cyberwarfare? Is it the responsibility of more technologically advanced nations to contribute to such collective action efforts?

How should states assign responsibility for cyberwarfare incidents when the actor is a 3rd party? How should we address AI systems capable of autonomously conducting cyber operations?

How can the international community prevent cyberattacks from escalating into conventional military conflict?

How should we mitigate increased risks of cyberattacks from AI and bolster defenses accordingly?

Bibliography

Topic 1

- 1971 Convention on Psychotropic Substances: Resolution. (1975, December 9). United Nations. <https://digitallibrary.un.org/record/650454>
- African Union Plan of Action on Drug Control and Crime Prevention (2019-2025). (2019, July 29). African Union. <https://au.int/en/documents/20190729/african-union-plan-action-drug-control-and-crime-prevention-2019-2025>
- Arana, I. P. (2019, April 1). The Vienna Consensus is broken, and we're not going to fix it. Dejusticia. <https://www.dejusticia.org/en/column/the-vienna-consensus-is-broken-and-were-not-going-to-fix-it/>
- Directorate-General for Migration and Home Affairs. (2024, January 24). European Ports Alliance to fight drug trafficking and organised crime. European Commission. Migration and Home Affairs. https://home-affairs.ec.europa.eu/news/european-ports-alliance-fight-drug-trafficking-and-organised-crime-2024-01-24_en
- Directorate-General for Migration and Home Affairs. (2025, December 4). Commission presents new EU Drugs Strategy and Action Plan against drug trafficking. European Commission. Migration and Home Affairs. https://home-affairs.ec.europa.eu/news/commission-presents-new-eu-drugs-strategy-and-action-plan-against-drug-trafficking-2025-12-04_en
- FIAP. (2024, September 27). International experts address drug trafficking and consumption with support from EU-ACT 2. FIAP. <https://www.fiap.gob.es/en/noticias/international-experts-address-drug-trafficking-and-consumption-with-support-from-eu-act-2/>
- Florence, C., Luo, F., & Rice, K. (2021). The economic burden of opioid use disorder and fatal opioid overdose in the United States, 2017. *Drug and Alcohol Dependence*, 218, 108350. <https://doi.org/10.1016/j.drugalcdep.2020.108350>
- Golden Triangle (Southeast Asia). (2026). In Wikipedia. [https://en.wikipedia.org/w/index.php?title=Golden_Triangle_\(Southeast_Asia\)&oldid=1373283146](https://en.wikipedia.org/w/index.php?title=Golden_Triangle_(Southeast_Asia)&oldid=1373283146)
- Historic England. (2018, December 14). Home From the War: What Happened to Disabled First World War Veterans. The Historic England Blog. <https://heritagecalling.com/2018/12/14/home-from-the-war-what-happened-to-disabled-first-world-war-veterans/>
- International drug control conventions. (2026). In Wikipedia. https://en.wikipedia.org/w/index.php?title=International_drug_control_conventions&oldid=1348100845
- International Drug Policy Consortium (IDPC). (2025, August 13). Vienna after consensus: Report of the 68th session of the UN Commission on Narcotic Drugs. <https://idpc.net/publications/2025/08/vienna-after-consensus-report->

of-the-68th-session-of-the-un-cnd

- International Narcotics Control Board. (2025). Report of the International Narcotics Control Board for 2024. United Nations. https://www.incb.org/incb/uploads/documents/Publications/AnnualReports/AR2024/Annual_Report/E-INCB-2024-1-ENG.pdf
- John. (2023, June 8). Key Facts on U.S.-Sourced Guns and Violence in Mexico. Stop US Arms to Mexico. <https://stopusarmstomexico.org/key-facts-on-u-s-sourced-guns-and-violence-in-mexico/>
- Johnstad, P. G. (2023). The international regime of drug control may violate the human right to life and security. *International Journal of Drug Policy*, 113, 103960. <https://doi.org/10.1016/j.drugpo.2023.103960>
- Klenowski, P. M. (2023). Drug trafficking. EBSCO. EBSCO. <https://www.ebsco.com/research-starters/law/drug-trafficking>
- Maritime cocaine smuggling. (2026). In Wikipedia. https://en.wikipedia.org/w/index.php?title=Maritime_cocaine_smuggling&oldid=1373324329
- Mayar, A. (2025, May 13). The Challenge of Drug Trafficking to Peace in Mexico. Vision of Humanity. <https://www.visionofhumanity.org/the-challenge-of-drug-trafficking-to-peace-in-mexico/>
- Mexican drug war. (2026). In Wikipedia. https://en.wikipedia.org/w/index.php?title=Mexican_drug_war&oldid=1373672815
- Niaz, K. (2017). International drug control system and the United Nations General Assembly Special Session [UNGASS] on the world drug problem: An overview. 143–149.
- Opium production in Myanmar. (2026). In Wikipedia. https://en.wikipedia.org/w/index.php?title=Opium_production_in_Myanmar&oldid=1371812256
- Payne, L. (2026, July 31). Golden Triangle. *Encyclopedia Britannica*. <https://www.britannica.com/place/Golden-Triangle-region-Southeast-Asia>
- Royal Thai Consulate-General, Fukuoka. (2021, September 13). From Poppy to Coffee: How Thailand Became a Model for Alternative Development. <https://fukuoka.thaiembassy.org/en/content/from-poppy-to-coffee-how-thailand-became-a-model-f>
- UN Office of Drugs and Crime. (2026, March 13). 69th Commission on Narcotic Drugs: Three new substances under control, five resolutions adopted, expert panel constituted. <https://www.unodc.org/unodc/frontpage/2026/March/cnd-closing.html>
- United Nations. (n.d.). The Commission on Narcotic Drugs. Office on Drugs and Crime. Retrieved September 8, 2026, from [//www.unodc.org/unodc/en/commissions/CND/index.html](https://www.unodc.org/unodc/en/commissions/CND/index.html)

- United Nations. (1988). 1988 Convention. International Narcotics Control Board. <https://www.incb.org/incb/en/precursors/1988-convention.html>
- United Nations Office on Drugs and Crime. (2010). A Century of International Drug Control. https://www.unodc.org/documents/data-and-analysis/Studies/100_Years_of_Drug_Control.pdf
- Walden University. (n.d.). Opioid Crisis: The Strain It Places on the Healthcare System. Retrieved September 8, 2026, from <https://www.waldenu.edu/online-masters-programs/master-of-healthcare-administration/resource/opioid-crisis-the-strain-it-places-on-the-healthcare-system>
- World Health Organization. (2025, August 29). Opioid overdose. <https://www.who.int/news-room/fact-sheets/detail/opioid-overdose>

Topic 2

- Albright, D., Brannan, P., & Walrond, C. (2010). Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security. https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf
- Anthropic. (2026, January 8). AI to defend critical infrastructure. <https://www.anthropic.com/research/critical-infrastructure-defense>
- Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! RAND. <https://www.rand.org/pubs/reprints/RP223.html>
- Bruder, A. H., & Yaros, O. (2026, February 20). European Commission Proposes Major Cybersecurity Package to Strengthen EU Cyber Resilience. Mayer Brown. Mayer Brown. <https://www.mayerbrown.com/en/insights/publications/2026/02/european-commission-proposes-major-cybersecurity-package-to-strengthen-eu-cyber-resilience>
- Carnegie Mellon University. (n.d.). CERT. CMU Software Engineering Institute. Retrieved September 8, 2026, from <https://www.sei.cmu.edu/divisions/cert/>
- Carruthers, S. (2025, April 7). Physical Security in Cybersecurity. IBM. IBM. <https://www.ibm.com/think/insights/physical-cybersecurity>
- Center for Strategic and International Studies. (n.d.). Significant Cyber Incidents. Strategic Technologies Program. Retrieved September 8, 2026, from <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>
- Chappell, B. (2017, May 15). WannaCry Ransomware: What We Know Monday. NPR. <https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday>
- Conte, N. (2025, May 4). Visualized: The Growth of Global Internet Users (1990–2025).

- Visual Capitalist. <https://www.visualcapitalist.com/visualized-the-growth-of-global-internet-users-1990-2025/>
- Council on Foreign Relations. (n.d.). Cyber Operations Tracker. Council on Foreign Relations. Retrieved September 8, 2026, from <https://www.cfr.org/cyber-operations/>
- Danielson, L. (2025, December 5). CVE-2017-0143 Vulnerability: Analysis, Impact, Mitigation. Huntress. <https://www.huntress.com/threat-library/vulnerabilities/cve-2017-0143>
- Datta, P. M., & Acton, T. (2024). Ransomware and Costa Rica's national emergency: A defense framework and teaching case. *Journal of Information Technology Teaching Cases*, 14(1), 56–67. <https://doi.org/10.1177/20438869221149042>
- Deloitte. (n.d.). CERT-In Cyber Incident Reporting Guidelines Explained. Retrieved September 8, 2026, from <https://www.deloitte.com/in/en/services/consulting/services/cyber/cert-in-direction-for-reporting-cyber-incidents.html>
- Dludla, N. (2026, May 26). South Africa targets January 2027 for revised AI policy after earlier withdrawal. Reuters. <https://www.reuters.com/world/africa/south-africa-targets-january-2027-revised-ai-policy-after-earlier-withdrawal-2026-05-26/>
- Dominioni, S., & Paoli, G. P. (2026). Unpacking the United Nations Open-Ended Working Group on ICT in the Context of International Security (2021–2025). <https://doi.org/10.37559/SECTEC/26/CR/05>
- European Commission. (n.d.). EU cybersecurity policies. Shaping Europe's Digital Future. Retrieved September 8, 2026, from <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>
- Fortinet. (n.d.). Types Of Cyber Attacks: Top 20 Cyber Threats & Prevention Strategies. Fortinet. Retrieved September 8, 2026, from <https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks>
- Georgia Tech Professional Education. (2025, December 16). What Is Cyberwarfare? GTPE Communications. <https://pe.gatech.edu/blog/industry-trends/cyberwarfare>
- Greenberg Traurig LLP. (2026, February 12). China's Amended Cybersecurity Law Takes Effect. <https://www.gtlaw.com/en/insights/2026/2/chinas-amended-cybersecurity-law-takes-effect>
- Gregory, J. (2025, March 7). WannaCry: How the Widespread Ransomware Changed Cybersecurity. IBM. <https://www.ibm.com/think/x-force/wannacry-worm-ransomware-changed-cybersecurity>
- H.R.3359 - 115th Congress (2017-2018): Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. Nos. 115–278, 3359 H.R. (2018). <https://www.congress.gov/bill/115th-congress/house-bill/3359>

- INTERPOL. (2026, August 3). INTERPOL report finds AI linked to more than half of cybercrime in Africa. INTERPOL. <https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-finds-AI-linked-to-more-than-half-of-cybercrime-in-Africa>
- Iturbe, E., Llorente-Vazquez, O., Rego, A., Rios, E., & Toledo, N. (2024). Unleashing offensive artificial intelligence: Automated attack technique code generation. *Computers & Security*, 147, 104077. <https://doi.org/10.1016/j.cose.2024.104077>
- JLCW Editor. (2025). Tallinn Manual 3.0: Sovereignty and Attribution in 2025. *Journal of Law & Cyber Warfare*. <https://www.jlcw.org/articles/tallinn-manual-3-0-sovereignty-and-attribution-in-2025-cyber-warfare>
- LeClair, J. A. (2016). Cyber Literacy in the Age of Attacks. *United States Cybersecurity Magazine*. <https://www.uscybersecurity.net/csmag/cyber-literacy-in-the-age-of-attacks/>
- Lehmann, G. (2025, August 5). Brazil's new "E-Ciber" National Cybersecurity Strategy established via decree. Mattos Filho. Mattos Filho. <https://www.mattosfilho.com.br/en/unico/cybersecurity-strategy-decree/>
- Mansoor, S. (2026, July 1). Rapid spread of AI may worsen global inequality, UN warns. *The Guardian*. <https://www.theguardian.com/technology/2026/jul/01/un-report-ai-inequality>
- McGuinness, D. (2017, April 27). How a cyber attack transformed Estonia. *BBC News*. <https://www.bbc.com/news/39655415>
- Microsoft Defender Security Research Team. (2017, May 13). WannaCrypt ransomware worm targets out-of-date systems. *Microsoft Security Blog*. <https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/>
- OpenAI. (2026, May 12). The Hugging Face incident and the road ahead. OpenAI. <https://openai.com/index/hugging-face-incident-and-the-road-ahead/>
- Operation Aurora. (2026). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Operation_Aurora&oldid=1370630770
- Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. *Proceedings of the 7th European Conference on Information Warfare*, 163.
- Raba, I. (2024). Cybercrime and the outgrowing impact on developing nations. Costa Rica in the background. *Global Affairs. Global Affairs and Strategic Studies*. <https://www.unav.edu/web/global-affairs/cybercrime-and-the-outgrowing-impact-on-developing-nations.-costa-rica-in-the-background>
- RAND. (n.d.). Cyber Warfare. RAND. Retrieved September 8, 2026, from <https://www.>

rand.org/topics/cyber-warfare.html

- Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024. (2024, June). Cyber Threat Intelligence Information Center. https://archive.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf
- Rupp, C. (2026, March 6). The UN's New Global Mechanism on Cybersecurity. Interface. <https://www.interface-eu.org/publications/the-new-united-nations-mechanism-on-cybersecurity>
- Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge University Press. <https://doi.org/10.1017/9781316822524>
- Senanu, J. H. (2026). A Review of the Republic of Ghana National Artificial Intelligence Strategy (2025-2035): Cybersecurity and Policy Perspectives. SSRN. <https://doi.org/10.2139/ssrn.6682958>
- SentinelOne. (2024, September 12). Key Cyber Security Statistics for 2026. SentinelOne. <https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/>
- Simonis, D. (2007). *Inventors and Inventions*. Marshall Cavendish.
- Steinberg, S., Stepan, A., & Neary, K. (2021). NotPetya: A Columbia University Case Study. Columbia University. <https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf>
- Tomé, J., & Woolbright, J. (2024, November 6). Exploring Internet traffic shifts and cyber attacks during the 2024 US election. Cloudflare. Cloudflare Blog. <https://blog.cloudflare.com/exploring-internet-traffic-shifts-and-cyber-attacks-during-the-2024-us-election/>
- United States Federal Bureau of Investigation. (n.d.). Russian Interference In 2016 U.S. Elections [Person]. Federal Bureau of Investigation. Retrieved September 8, 2026, from <https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections>
- US and Israel were behind Stuxnet claims researcher. (2011, March 4). BBC News. <https://www.bbc.com/news/technology-12633240>
- Zerbe, Y. (2023, March 20). Costa Rica ransomware attack (2022). Cyber Law Toolkit. International Cyber Law: Interactive Toolkit. [https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_\(2022\)](https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022))

#GTMUN2026

